Computational and Applied Mathematics (2021) 40:64
https://doi.org/10.1007/s40314-021-01428-3

Some results on $\mathbb{F}_4[v]$-double cyclic codes

Srinivasulu Bathala[1] · **Padmapani Seneviratne**[1]

Received: 9 February 2020 / Revised: 24 May 2020 / Accepted: 16 January 2021 /
Published online: 26 February 2021

Abstract
Let $\mathrm{R} = \mathbb{F}_4 + v\mathbb{F}_4$, $v^2 = v$. A linear code over R is a double cyclic code of length (r, s), if the set of its coordinates can be partitioned into two parts of sizes r and s, so that any cyclic shift of coordinates of both parts leave the code invariant. In polynomial representation, these codes can be viewed as $\mathrm{R}[x]$-submodules of $\frac{\mathrm{R}[x]}{\langle x^r-1\rangle} \times \frac{\mathrm{R}[x]}{\langle x^s-1\rangle}$. In this paper, we determine generator polynomials of R-double cyclic codes and their duals for arbitrary values of r and s. We enumerate R-double cyclic codes of length $(2^{e_1}, 2^{e_2})$ by giving a mass formula, where e_1 and e_2 are positive integers. Some structural properties of double constacyclic codes over R are also studied. These results are illustrated with some good examples.

Keywords Double cyclic codes · Dual codes · Mass formula · Double constacyclic codes

Mathematics Subject Classification 94B05 · 11T71

1 Introduction

Codes over rings were introduced in early seventies. These studies received a great attention after a breakthrough paper by Hammons et al. (1994), where certain good non-linear binary codes were obtained as images of some linear codes over $\mathbb{Z}_4$ under a map, called the Gray map. Since then, several families of codes have been studied over various finite ring structures. Most of these studies are concentrated over finite chain rings (Cao 2013; Dinh and López-permouth 2004). Recently, researchers also studied linear codes over finite non-chain rings. Unlike chain rings, the algebraic structure of non-chain rings do not possess any common pattern, and linear codes over these rings do not have any compact form. Zhu et al. (2010) constructed some binary optimal codes as Gray images of cyclic codes over the non-chain ring $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$. Generalizing these results, Bayram and Siap (2014), have studied cyclic and constacyclic codes over $\mathbb{Z}_p[v]/\langle v^p - v\rangle$. Some lower and upper bounds on the covering

Communicated by Thomas Aaron Gulliver.

✉ Srinivasulu Bathala
bslu1981@gmail.com

Padmapani Seneviratne
padmapani.seneviratne@tamuc.edu

[1] Department of Mathematics, Texas A&M University-Commerce, Commerce TX-75428, USA

radius of repetition codes, simplex codes and MacDonald codes with Chinese Euclidean distance over the finite non-chain ring $\mathbb{F}_2 + v\mathbb{F}_2$ with $v^2 = v$ are determined in Gao et al. (2018). Further, Wang and Gao (2019) have studied MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_2$ and their applications in constructing secret sharing schemes and associations schemes, where p is a prime and $v^3 = v$.

Many good quantum error correcting codes and DNA codes are constructed from cyclic codes over finite non-chain rings (Ashraf and Mohammad 2016; Dinh et al. 2019, 2018; Shi and Lu 2019).

More recently, linear codes are also studied over mixed alphabets. Borges et al. (2009) have studied $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. Wherein, the set of coordinates is partitioned into two parts such that the projections of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code on these coordinates are a binary code and a quaternary code. These additive codes were later generalized to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes (Aydogdu and Siap 2014). In Borges and Fernàndez-Còrdoba (2017), Borges et al. have studied the algebraic structure of $\mathbb{Z}_2$-double cyclic codes as $\mathbb{Z}_2[x]$-submodules of $\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}$. In this study, the authors have determined the generating polynomials of $\mathbb{Z}_2$-double cyclic codes and their duals. Similarly, the structure of $\mathbb{Z}_4$-double cyclic codes and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$-double cyclic codes have been studied in Gao et al. (2016) and Yao et al. (2015), respectively. Gao et al. (2016), determined the generator polynomials of duals of free $\mathbb{Z}_4$-double cyclic codes, and obtained some optimal or suboptimal non-linear binary codes from these family of codes. Diao et al. (2019) have studied the structure of $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes and constructed some good quantum codes as their Gray images. A double cyclic code is in fact a generalized quasi-cyclic (GQC) code of index two. Siap and Kulhan (2005) introduced GQC codes over finite fields, and the study has been extended to various finite rings (Bhaintwal and Wasan 2009; Cao 2011; Esmaeili and Yari 2009). Generalizing these concepts further, Aydin and Halilović (2017) have studied Multi-twisted codes, a generalization of quasi-twisted codes. Gao et al. (2016), have studied the structural properties skew GQC codes over finite fields by giving Chinese Reminder Theorem in the skew polynomial ring $\mathbb{F}_q[x, \sigma]$, which leads to a canonical decomposition of skew GQC codes. Similarly, by using the Chinese Remainder Theorem, structural properties and decompositions of GQC codes with arbitrary lengths over the ring $\mathbb{F}_q + u\mathbb{F}_q$, where $u^2 = 0, q = p^n$, n a positive integer and p a prime number, are investigated in Gao et al. (2014). Motivated by these studies, in this paper we introduce and study the algebraic structure of double cyclic codes over the ring $\mathrm{R} = \mathbb{F}_4 + v\mathbb{F}_4,\ v^2 = v$. We determine the generating polynomials of R-double cyclic codes and their duals. We also investigate some algebraic properties of double constacyclic codes and their duals over R.

The paper is organized as follows. In Sect. 2, we give some basic definitions and recall some structural properties of cyclic codes over R. In Sect. 3, we present the generator polynomials of $\mathbb{F}_4$-double cyclic codes, and study R-double cyclic codes as direct sum of $\mathbb{F}_4$-double cyclic codes. We determine the general form of the generator polynomials of R-double cyclic codes and their duals. We give a mass formula to enumerate R-double cyclic codes of length $(2^{e_1}, 2^{e_2})$, where e_1 and e_2 are positive integers. In Sect. 4, we determine the structural properties of R-double constacyclic codes.

2 Preliminaries

Let $\mathbb{F}_4 = \{0, 1, w, 1 + w\}$ be the finite field with four elements, where $w^2 = 1 + w$. Throughout this paper, R denote the commutative ring $\mathbb{F}_4 + v\mathbb{F}_4 = \{a + vb \mid a, b \in \mathbb{F}_4\}$ with

$v^2 = v$. R is a finite non-chain ring with sixteen elements and of characteristic two. The unit elements in R are $\{1, w, w+1, v+w, 1+v+w, 1+vw, 1+v+vw, 1+w+vw, v+w+vw\}$, while the non-units are $\{0, v, vw, 1+v, v+vw, w+vw, 1+v+w+vw\}$. Further, R is a semi-local Frobenius ring with two maximal ideals $\langle v\rangle$ and $\langle 1+v\rangle$. From the Chinese Remainder Theorem, any element $a+vb$ in R can uniquely be expressed as $a+vb = (1+v)a+v(a+b)$. More information about the ring can be found in Bayram et al. (2016).

A linear code C of length n over R is an R-submodule of R^n. The dual code $\mathrm{C}^\perp$ of C is defined as $\mathrm{C}^\perp = \{y \in \mathrm{R}^n \mid c \cdot y = 0,\ \forall c \in \mathrm{C}\}$, where $c \cdot y$ is the standard Euclidean inner product of c and y in R^n. A code C is self-orthogonal if $\mathrm{C} \subseteq \mathrm{C}^\perp$, and self-dual if $\mathrm{C} = \mathrm{C}^\perp$.

The Hamming weight $w_H(c)$ of any $c \in \mathbb{F}_4^n$ is the number of non-zero coordinates in c. The Hamming distance between any two elements c_1 and c_2 in $\mathbb{F}_4^n$ is defined as $d_H(c_1, c_2) = w_H(c_1 - c_2)$. The minimum Hamming distance of a linear code C, denoted by $d_H(\mathrm{C})$, is the minimum of the Hamming weights of non-zero codewords in C.

Now, recall the definition of the Gray map which was defined in Gursoy et al. (2014) as follows:

$$\begin{aligned}\phi &: \mathrm{R} \to \mathbb{F}_4^2\\ \phi(a+vb) &= (a+b, a),\end{aligned}$$

where $a, b \in \mathbb{F}_4$. This map can be extended naturally to the case over R^n.

The Lee weight of any $c \in \mathrm{R}^n$ is the Hamming weight of its Gray image, i.e., $w_L(c) = w_H(\phi(c))$. The Lee distance between x, y in R is defined by $d_L(x-y) = w_L(x-y)$. The minimum Lee distance between distinct pairs of codewords of a linear code C over R is called the minimum distance of C and denoted by $d_L(C)$ or shortly d_L. Further, it is easy to check that ϕ is a linear isometry from $(\mathrm{R}^n,\ d_L)$ to $(\mathbb{F}_4^{2n},\ d_H)$. Therefore, if C is a linear code of length n over R with 4^k codewords and minimum Lee distance d, then $\phi(\mathrm{C})$ is a $[2n, k, d]$-linear code over $\mathbb{F}_4$ (Gursoy et al. 2014).

Recall that, for any two sets A and B, the operations $\oplus$ and $\otimes$ are defined as $A \oplus B = \{a+b \mid a \in A,\ b \in B\}$, $A \otimes B = \{(a,b) \mid a \in A,\ b \in B\}$. Also note that, for any linear code C of length n over R the two sets $\mathrm{C}_1 = \{x \in \mathbb{F}_4^n \mid x+vy \in \mathrm{C} \text{ for some } y \in \mathbb{F}_4^n\}$ and $\mathrm{C}_2 = \{x+y \in \mathbb{F}_4^n \mid x+vy \in \mathrm{C}\}$ are linear codes of length n over $\mathbb{F}_4$.

Following these notations, the following theorem gives the structure of linear codes over R and their Gray images. The results follows directly from Gursoy et al. (2014) for $q = 2^2$.

Theorem 1 Gursoy et al. (2014) *Let* C *be a linear code of length n over the ring* R. *Then* C *can be uniquely expressed as* $\mathrm{C} = (1+v)\mathrm{C}_1 \oplus v\mathrm{C}_2$, *where* $\mathrm{C}_1 = \{x \in \mathbb{F}_4^n \mid x+vy \in \mathrm{C} \text{ for some } y \in \mathbb{F}_4^n\}$ *and* $\mathrm{C}_2 = \{x+y \in \mathbb{F}_4^n \mid x+vy \in \mathrm{C}\}$. *Further, if* C_1 *and* C_2 *are linear codes over* $\mathbb{F}_4$ *with dimensions* k_1, k_2 *and minimum Hamming distances* $d_H(\mathrm{C}_1), d_H(\mathrm{C}_2)$, *respectively, then* $\phi(\mathrm{C})$ *is a* $[2n, k_1+k_2,\ \min\{d_H(\mathrm{C}_1), d_H(\mathrm{C}_2)\}]$*-linear code over* $\mathbb{F}_4$. *Also, the dual code of* C *is* $\mathrm{C}^\perp = (1+v)\mathrm{C}_1^\perp \oplus v\mathrm{C}_2^\perp$.

Theorem 2 Gursoy et al. (2014) *Let* $\mathrm{C} = (1+v)\mathrm{C}_1 \oplus v\mathrm{C}_2$ *be a linear code over* R, *and* G_1 *and* G_2 *be the generator matrices of* $\mathbb{F}_4$*-linear codes* C_1 *and* C_2, *respectively. Then the generator matrix of* C *is* $\begin{pmatrix}(1+v)G_1\\ vG_2\end{pmatrix}$.

Theorem 3 *Let* $\mathrm{C} = (1+v)\mathrm{C}_1 \oplus v\mathrm{C}_2$ *be a linear code of length n over* R *and* G_1, G_2 *be the generator matrices of* $\mathbb{F}_4$*-linear codes* C_1 *and* C_2, *respectively. Then, the generator matrix of* $\phi(\mathrm{C})$ *is* $\begin{pmatrix}G_1 & 0\\ 0 & G_2\end{pmatrix}$.

Proof The proof follows from the definition of the Gray map ϕ and Theorm 2. □

Let σ be the cyclic shift operator on R^n such that, $\sigma(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2})$. A linear code C of length n over R is called a cyclic code if $\sigma(\mathrm{C}) = \mathrm{C}$. Let R_n denote the quotient ring $\mathrm{R}[x]/\langle x^n - 1\rangle$. Identifying each n-tuple $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{R}^n$ with the polynomial $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathrm{R}_n$, we see that C is a cyclic code of length n over R if and only if C is an ideal of R_n. Further, C is a λ-constacyclic code if $(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathrm{C}$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{C}$, where λ is a unit in R. Also, C is a λ-constacyclic code if and only if C is an ideal of $\frac{\mathrm{R}[x]}{\langle x^n - \lambda\rangle}$ (Gao et al. 2017).

Theorem 4 Gursoy et al. (2014) *Let* $\mathrm{C} = (1 + v)\mathrm{C}_1 \oplus v\mathrm{C}_2$ *be a linear code of length n over* R. *Then* C *is a cyclic code over* R *if and only if* C_1 *and* C_2 *are cyclic codes over* $\mathbb{F}_4$. *Further, if* $\mathrm{C}_1 = \langle g_1(x)\rangle$ *and* $\mathrm{C}_2 = \langle g_2(x)\rangle$, *then* $\mathrm{C} = \langle (1 + v)g_1(x) + vg_2(x)\rangle$.

The following result characterizes the generator polynomials of a cyclic code over R:

Theorem 5 *Let* C *be a cyclic code in* R_n.

1. *If the least degree polynomial in* C *is monic, then* $\mathrm{C} = \langle g(x)\rangle$, *where* $g(x) \in \mathbb{F}_4[x]/\langle x^n - 1\rangle$ *such that* $g(x)|(x^n - 1)$.
2. *If* C *has no monic polynomial of least degree, then* $\mathrm{C} = \langle vf_1(x)\rangle$ *or* $\mathrm{C} = \langle (1 + v) f_1(x)\rangle$ *or* $\mathrm{C} = \langle vf_1(x), (1 + v) f_2(x)\rangle$, *where* $f_1(x), f_2(x) \in \mathbb{F}_4[x]/\langle x^n - 1\rangle$.
3. *If* C *contain some monic polynomials and least degree polynomials that are non-monic, then* $\mathrm{C} = \langle g(x), vf_1(x)\rangle$ *or* $\mathrm{C} = \langle g(x), (1 + v) f_2(x)\rangle$ *or* $\mathrm{C} = \langle vf_1(x), (1 + v) f_2(x)\rangle$, *where* $f_1(x), f_2(x) \in \mathbb{F}_4[x]/\langle x^n - 1\rangle$ *and* $g(x)$ *is the monic polynomial of least degree in* C.

In the examples given below, the parameters marked with '$*$' denote an optimal code according to Grassl (2020).

Example 1 Let $\mathrm{C} = \langle x + 1\rangle$ be a cyclic code of length 3 over R. Clearly, C is a free cyclic code with parameters [3, 2, 2]. Also, it is easy to see that $\mathrm{C}_1 = \langle x + 1\rangle$ and $\mathrm{C}_2 = \langle x + 1\rangle$. As C_1 and C_2 are cyclic codes over $\mathbb{F}_4$ with parameters [3, 2, 2]* and [3, 2, 2]*, respectively, we have $\phi(\mathrm{C})$ a [6, 4, 2]*-quasi-cyclic code of index two over $\mathbb{F}_4$.

Example 2 Let $n = 4$ and $\mathrm{C} = (1 + v)\mathrm{C}_1 \oplus v\mathrm{C}_2$ be a cyclic code of length n over R, where $\mathrm{C}_1 = \langle x + 1\rangle$ and $\mathrm{C}_2 = \langle x + 1\rangle$. As C_1 and C_2 are cyclic codes of length 4 over $\mathbb{F}_4$ with parameters [4, 3, 2]* and [4, 3, 2]*, respectively, $\phi(\mathrm{C})$ is a [8, 6, 2]*-linear code over $\mathbb{F}_4$.

3 Double cyclic codes over R

In this section, we study some the structural properties of R-double cyclic codes and their duals by determining their generator polynomials. Also, we give a complete classification of R-double cyclic codes of length $(2^{e_1}, 2^{e_2})$. We enumerate such codes by giving mass formula. It may be noted here that R-double cyclic codes are in fact generalized quasi-cyclic codes of index two over R. Also, it is obvious to see that an R-double cyclic code of length (r, s) is a cyclic code over R of length r or s whenever $s = 0$ or $r = 0$, respectively.

Let r and s be two non-negative integers and $n = r + s$. The n coordinates of each n-tuple in R^n can be partitioned into two sets of sizes r and s. Then, R^n can be treated as an R-submodule of $\mathrm{R}^r \times \mathrm{R}^s$, and any linear code C of length n over R is an R-submodule of $\mathrm{R}^r \times \mathrm{R}^s$.

For any element $c = (c_{10}, c_{11}, \ldots, c_{1\,r-1} \mid c_{20}, c_{21}, \ldots, c_{2\,s-1})$ in $\mathrm{R}^r \times \mathrm{R}^s$, we define the double cyclic shift of c as follows:

$$\tau(c) = (c_{1\,r-1}, c_{10}, \ldots, c_{1\,r-2} \mid c_{2\,s-1}, c_{20}, \ldots, c_{2\,s-2}).$$

Definition 1 A linear code C of length $n = r + s$ over R is called an R-double cyclic code of length (r, s) if $\tau(c) \in \mathrm{C}$ whenever $c \in \mathrm{C}$.

Now, we identify each $(c_{10}, c_{11}, \ldots, c_{1\,r-1} \mid c_{20}, c_{21}, \ldots, c_{2\,s-1}) \in \mathrm{R}^r \times \mathrm{R}^s$ with a pair of polynomials $(c_{10} + c_{11}x + \cdots + c_{1\,r-1}x^{r-1} \mid c_{20} + c_{21}x + \cdots + c_{2\,s-1}x^{s-1})$ in $\mathrm{R}_{r,s}[x] = \frac{\mathrm{R}[x]}{\langle x^r-1\rangle} \times \frac{\mathrm{R}[x]}{\langle x^s-1\rangle}$. Clearly, this correspondence is one-to-one. Further, for any $f(x) = \sum f_i x^i \in \mathrm{R}[x]$ and $(c_1(x) \mid c_2(x)) \in \mathrm{R}_{r,s}[x]$, we define the product $f(x) \cdot (c_1(x) \mid c_2(x)) = (f(x)c_1(x) \mid f(x)c_2(x))$. We can see that $\mathrm{R}_{r,s}[x]$ is an $\mathrm{R}[x]$-module with respect to this product. Also, the product $x \cdot (c_1(x) \mid c_2(x)) = (xc_1(x) \mid xc_2(x))$ represents the double cyclic shift of $(c_1(x) \mid c_2(x))$ in $\mathrm{R}_{r,s}[x]$.

Theorem 6 *A code* C *is an* R*-double cyclic of length* (r, s) *if and only if* C *is an* $\mathrm{R}[x]$*-submodule of* $\mathrm{R}_{r,s}[x]$.

Theorem 7 *Let* C *be an* R*-double cyclic codes of length* (r, s). *Then*

$$\mathrm{C} = \langle((1+v)b_1(x) + vb_2(x) \mid 0), ((1+v)l_1(x) + vl_2(x) \mid (1+v)a_1(x) + va_2(x))\rangle,$$

where $a_1(x), a_2(x), b_1(x)$ *and* $b_2(x)$ *are monic polynomials such that* $a_1(x)|(x^s - 1)$, $a_2(x)|(x^s - 1)$, $b_1(x)|(x^r - 1)$ *and* $b_2(x)|(x^r - 1)$.

Proof Consider the map $\pi : \mathrm{C} \to \mathrm{R}[x]/\langle x^s - 1\rangle$ such that $\pi(c_1(x) \mid c_2(x)) = c_2(x)$. Since $\mathrm{R}[x]/\langle x^s - 1\rangle$ and C are $\mathrm{R}[x]$ submodules $\mathrm{R}_{r,s}$, the map ϕ is an $\mathrm{R}[x]$-modular homomorphism with kernel $ker_{\mathrm{C}}(\pi) = \{(f(x) \mid 0) \in \mathrm{C} \mid f(x) \in \mathrm{R}[x]/\langle x^r - 1\rangle\}$. Define a set $K = \{f(x) \in \mathrm{R}[x] \mid (f(x) \mid 0) \in \mathrm{C}\}$. Clearly, K is an ideal of $\frac{\mathrm{R}[x]}{\langle x^r-1\rangle}$. On the other hand, the homomorphic image of C under π is an ideal of $\frac{\mathrm{R}[x]}{\langle x^s-1\rangle}$. As cyclic codes over R are principally generated (Bayram et al. 2016), we have $K = \langle(1+v)b_1(x) + vb_2(x)\rangle$ and $\pi(\mathrm{C}) = \langle(1+v)a_1(x)+va_2(x)\rangle$, where $a_i(x)$ and $b_i(x)$ are monic polynomials in $\mathbb{F}_4[x]$ such that $a_i(x)|(x^s-1)$ and $b_i(x)|(x^r-1), i = 1, 2$. Thus, $ker_{\mathrm{C}}(\pi) = \langle((1+v)b_1(x)+vb_2(x) \mid 0)\rangle$ and $\mathrm{C} = \langle((1+v)b_1(x) + vb_2(x) \mid 0), ((1+v)l_1(x) + vl_2(x) \mid (1+v)a_1(x) + va_2(x))\rangle$ for some $(1+v)l_1(x) + vl_2(x) \in \mathrm{R}[x]$. □

Let C be an R-double cyclic code of length (r, s). Define $\mathrm{C}_1 = \{x \in \mathbb{F}_4^r \times \mathbb{F}_4^s \mid x + vy \in \mathrm{C}$ for some $y \in \mathbb{F}_4^r \times \mathbb{F}_4^s\}$ and $\mathrm{C}_2 = \{x + y \in \mathbb{F}_4^r \times \mathbb{F}_4^s \mid x + vy \in \mathrm{C}\}$. Then it is easy to prove that C_1 and C_2 are $\mathbb{F}_4$-double cyclic codes of length (r, s). In Sect. 3.2, we see that an R-double cyclic code is completely determined by the constituent $\mathbb{F}_4$-double cyclic codes. Thus, we first present the structural properties of $\mathbb{F}_4$-double cyclic codes and then we use these results further to describe the structure of R-double cyclic codes.

3.1 $\mathbb{F}_4$-double cyclic codes

A linear code C of length $r + s$ over $\mathbb{F}_4$ is an $\mathbb{F}_4$-double cyclic code of length (r, s) if it is closed with respect to the double cyclic shift operator τ. An $\mathbb{F}_4$-double cyclic code of length (r, s) is an $\mathbb{F}_4[x]$-submodule of $\frac{\mathbb{F}_4[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{F}_4[x]}{\langle x^s-1\rangle}$. We see that the structure of $\mathbb{F}_4$-double cyclic codes is similar to that of $\mathbb{Z}_2$-double cyclic codes, defined in Borges and Fernàndez-Còrdoba (2017). We omit the proofs of the results in the present setting as they are straightforward generalization of the study on $\mathbb{Z}_2$-double cyclic codes Borges and Fernàndez-Còrdoba (2017).

Theorem 8 *Let* C *be an* $\mathbb{F}_4$*-double cyclic code of length* (r, s)*. Then* $\mathrm{C} = \langle (b(x) \mid 0), (l(x) \mid a(x)) \rangle$*, where* $l(x) \in \mathbb{F}_4[x]$*,* $b(x)|(x^r - 1)$ *and* $a(x)|(x^s - 1)$*. Moreover,*

1. $\deg(l(x)) < \deg(b(x))$*;*
2. $b(x)$ *divides* $l(x)\frac{x^s-1}{a(x)}$*;*
3. *If* $\deg(b(x)) = t_1$ *and* $\deg(a(x)) = t_2$*, then* C *is spanned by* $S_1 \cup S_2$*, where* $S_1 = \bigcup_{i=0}^{r-t_1-1} x^i(b(x) \mid 0)$ *and* $S_2 = \bigcup_{i=0}^{s-t_2-1} x^i(l(x) \mid a(x))$*. Further,* $|\mathrm{C}| = 4^{r+s-t_1-t_2}$*.*

The following result provides the structure of dual code of an $\mathbb{F}_4$-double cyclic code. Note that $f^*(x)$ is the reciprocal polynomial of $f(x)$.

Theorem 9 *Let* C *be an* $\mathbb{F}_4$*-double cyclic code. Then the dual code of* C *is also an* $\mathbb{F}_4$*-double cyclic code.*

Theorem 10 *Let* C *be an* $\mathbb{F}_4$*-double cyclic code of length* (r, s) *and* $\mathrm{C}^\perp = \langle (\hat{b}(x) \mid 0), (\hat{l}(x) \mid \hat{a}(x)) \rangle$ *be the dual code of* C*. Then*

1. $\hat{b}(x) = \frac{x^r-1}{gcd(b(x),l(x))^*}$,
2. $\hat{a}(x) = \frac{(x^s-1)gcd(b(x),l(x))^*}{a^*(x)b^*(x)}$ *and*
3. $\hat{l}(x) = \frac{x^r-1}{b^*(x)}\lambda(x)$, *where* $\lambda(x) = \left[\frac{l^*(x)}{gcd(b(x),l(x))^*}\right]^{-1} x^{m-deg(a(x))+deg(l(x))} \left(mod \ \frac{b^*(x)}{gcd(b(x),l(x))^*}\right)$, $m = lcm\{r, s\}$.

An $\mathbb{F}_4$-double cyclic code C of length (r, s) is separable if $\mathrm{C} = \mathrm{C}_r \times \mathrm{C}_s$, where C_r and C_s are the projections of C on r coordinates and s coordinates, respectively. A separable $\mathbb{F}_4$-double cyclic code is of the form, $\mathrm{C} = \langle (b(x) \mid 0), (0 \mid a(x)) \rangle$, where $b(x)|(x^r - 1)$ and $a(x)|(x^s - 1)$. The dual code of a separable $\mathbb{F}_4$-double cyclic code C is $\mathrm{C}^\perp = \left\langle \left(\frac{x^r-1}{b''(x)} \,\middle|\, 0\right), \left(0 \,\middle|\, \frac{x^r-1}{a''(x)}\right) \right\rangle$.

Theorem 11 *An* $\mathbb{F}_4$*-double cyclic code of the form* $\mathrm{C} = \langle (1 \mid 0), (l(x) \mid a(x)) \rangle$ *is separable.*

Proof The result follows as $(0 \mid a(x)) = l(x)\dot{(}1 \mid 0) - (l(x) \mid a(x)) \in \mathrm{C}$. □

Example 3 Let $r = s = 5$ and $\mathrm{C} = \langle (b(x) \mid 0), (l(x) \mid a(x) \rangle$, where $b(x) = x^4 + x^3 + x^2 + x + 1$, $l(x) = x^2 + x$ and $a(x) = x + 1$. Then C is an $\mathbb{F}_4$-double cyclic code of length $(5, 5)$ with parameters $[10, 5, 4]^*$.

Example 4 Let $r = s = 6$ and $\mathrm{C} = \langle (b(x) \mid 0), (l(x) \mid a(x) \rangle$, where $b(x) = x^4 + x^3 + x + 1$, $l(x) = x + 1$ and $a(x) = x + 1$. Then C is an $\mathbb{F}_4$-double cyclic code of length $(6, 6)$ with parameters $[12, 7, 4]^*$.

Example 5 Let $r = 2$ and $s = 4$ and $\mathrm{C} = \langle (b(x) \mid 0), (l(x) \mid a(x) \rangle$, where $b(x) = x^2 + 1$, $l(x) = x + 1$ and $a(x) = x^2 + 1$. Then C is an $\mathbb{F}_4$-double cyclic code of length $(2, 4)$ with parameters $[6, 2, 4]^*$. Also, from Theorem 10, we have $\hat{b}(x) = \frac{x^2-1}{gcd(x^2+1,x+1)^*} = x + 1$, $\hat{a}(x) = \frac{(x^4-1)gcd(x^2+1,x+1)^*}{(x^2+1)^*(x^2+1)^*} = x + 1$ and $\hat{l}(x) = \frac{x^2-1}{(x^2+1)^*}\lambda(x) = \lambda(x)$ with $\lambda(x) = x^{4-2+1}\left(\frac{x+1}{x+1}\right)^{-1}\left(mod \ \frac{x^2+1}{(x+1)^*}\right) = 1$. Therefore, $\mathrm{C}^\perp = \langle (x + 1 \mid 0), (1 \mid x + 1) \rangle$. Further, $\mathrm{C}^\perp$ is an $\mathbb{F}_4$-double cyclic code with parameters $[6, 4, 2]^*$.

3.2 R-Double cyclic codes and their duals

In this subsection, we continue and study R-double cyclic codes and their duals as direct sum of $\mathbb{F}_4$-double cyclic codes. Let C be an R-double cyclic code and C_1, C_2 be the corresponding $\mathbb{F}_4$-linear codes as defined in Sect. 2. The following result shows that C is determined completely by the $\mathbb{F}_4$-double cyclic codes C_1 and C_2:

Theorem 12 *Let* $C = (1+v)C_1 \oplus vC_2$ *be a linear code of length* $r+s$ *over* R. *Then* C *is an* R*-double cyclic code of length* (r,s) *if and only if* C_1 *and* C_2 *are* $\mathbb{F}_4$*-double cyclic codes of length* (r,s).

Proof Let $x = (a_1, a_2, \ldots, a_r \mid b_1, b_2, \ldots, b_s) \in C_1$. Then $x + vy \in C$ for some $y = (a'_1, a'_2, \ldots, a'_r \mid b'_1, b'_2, \ldots, b'_s) \in \mathbb{F}_4^r \times \mathbb{F}_4^s$. If C is an R-double cyclic code, then $\tau(x+vy) = (a_r + va'_r, a_1 + va'_1, \ldots, a_{r-1} + va'_{r-1} \mid b_s + vb'_s, b_1 + vb'_1, \ldots, b_{s-1} + vb'_{s-1}) \in C$. This implies that $(a_r, a_1, \ldots, a_{r-1} \mid b_s, b_1, \ldots, b_{s-1}) \in C_1$ and, therefore, C_1 is an $\mathbb{F}_4$-double cyclic code. Similarly we can show that C_2 is an $\mathbb{F}_4$-double cyclic code. Conversely, assume C_1 and C_2 are $\mathbb{F}_4$-double cyclic codes. Then for any $x + vy \in C$, we have $\tau(x) \in C_1$ and $\tau(x+y) \in C_2$. This implies that $(1+v)\tau(x) + v\tau(x+y) = \tau(x+vy) \in C$, from the unique representation of C. Therefore C is an R-double cyclic code. Hence the result. □

Remark 1 For any $k(x) \in R[x]$, there exist some $r(x), r'(x) \in \mathbb{F}_4[x]$ such that $(1+v)k(x) = (1+v)r(x)$ and $vk(x) = vr'(x)$.

The following theorem gives the form of generators of an R-double cyclic code of length (r,s):

Theorem 13 *Let* $C_1 = \langle (b_1(x) \mid 0), (l_1(x) \mid a_1(x)) \rangle$ *and* $C_2 = \langle (b_2(x) \mid 0), (l_2(x) \mid a_2(x)) \rangle$ *be two* $\mathbb{F}_4$*-double cyclic codes of length* (r,s) *as defined in Theorem 8. If* $C = (1+v)C_1 \oplus vC_2$ *is an* R*-double cyclic code of length* (r,s), *then* $C = \langle ((1+v)b_1(x) \mid 0), ((1+v)l_1(x) \mid (1+v)a_1(x)), (vb_2(x) \mid 0), (vl_2(x) \mid va_2(x)) \rangle$.

Proof From the unique representation of C as $C = (1+v)C_1 \oplus vC_2$, we have $C \subseteq \langle (1+v)(b_1(x) \mid 0), (1+v)(l_1(x) \mid a_1(x)), v(b_2(x) \mid 0), v(l_2(x) \mid a_2(x)) \rangle$. Conversely, let $c(x) \in \langle ((1+v)b_1(x) \mid 0), ((1+v)l_1(x) \mid (1+v)a_1(x)), (vb_2(x) \mid 0), (vl_2(x) \mid va_2(x)) \rangle$. Then $c(x) = (1+v)k_1(x)(b_1(x) \mid 0) + (1+v)k_2(x)(l_1(x) \mid a_1(x)) + vk_3(x)(b_2(x) \mid 0) + vk_4(x)(l_2(x) \mid a_2(x))$ for some $k_1(x), k_2(x), k_3(x)$ and $k_4(x)$ in $R[x]$. But from Remark 1, there exist $r_1(x), r_2(x), r_3(x)$ and $r_4(x)$ in $\mathbb{F}_4[x]$ such that $c(x) = (1+v)[r_1(x)(b_1(x) \mid 0) + r_2(x)(l_1(x) \mid a_1(x))] + v[r_3(x)(b_2(x) \mid 0) + r_4(x)(l_2(x) \mid a_2(x))] \in c(x) \in C$. Therefore $\langle (1+v)(b_1(x) \mid 0), (1+v)(l_1(x) \mid a_1(x)), v(b_2(x) \mid 0), v(l_2(x) \mid a_2(x)) \rangle \subseteq C$. □

Theorem 14 *Let* $C_1 = \langle (b_1(x) \mid 0), (l_1(x) \mid a_1(x)) \rangle$ *and* $C_2 = \langle (b_2(x) \mid 0), (l_2(x) \mid a_2(x)) \rangle$ *be two* $\mathbb{F}_4$*-double cyclic codes of length* (r,s) *as defined in Theorem 8. If* $C = (1+v)C_1 \oplus vC_2$ *is an* R*-double cyclic code of length* (r,s), *then* $C = \langle ((1+v)b_1(x) + vb_2(x) \mid 0), ((1+v)l_1(x) + vl_2(x) \mid (1+v)a_1(x) + va_2(x)) \rangle$.

Proof From Theorem 13, we have $C = \langle (1+v)(b_1(x) \mid 0), (1+v)(l_1(x) \mid a_1(x)), v(b_2(x) \mid 0), v(l_2(x) \mid a_2(x)) \rangle$. Clearly $\langle ((1+v)b_1(x) + vb_2(x) \mid 0), ((1+v)l_1(x) + vl_2(x) \mid (1+v)a_1(x) + va_2(x)) \rangle \subseteq C$. On the other hand, let $c(x) \in \langle (1+v)(b_1(x) \mid 0), (1+v)(l_1(x) \mid a_1(x)), v(b_2(x) \mid 0), v(l_2(x) \mid a_2(x)) \rangle$. Then, there exist $r_1(x), r_2(x), r_3(x)$ and $r_4(x)$ in $R[x]$ such that

$$\begin{aligned}
c(x) &= r_1(x)[(1+v)(b_1(x) \mid 0)] + r_2(x)[(1+v)(l_1(x) \mid a_1(x))] \\
&\quad + r_3(x)[v(b_2(x) \mid 0)] + r_4(x)[v(l_2(x) \mid a_2(x))] \\
&= r_1(x)[(1+v)((1+v)b_1(x) + vb_2(x) \mid 0)] + r_2(x)[(1+v)((1+v)l_1(x) \\
&\quad + vl_2(x) \mid (1+v)a_1(x) + va_2(x))] \\
&\quad + r_3(x)[v((1+v)b_1(x) + vb_2(x) \mid 0)] + r_4(x)[v((1+v)l_1(x) \\
&\quad + vl_2(x) \mid (1+v)a_1(x) + va_2(x))] \\
&= ((1+v)b_1(x) + vb_2(x) \mid 0)[(1+v)r_1(x) + vr_3(x)] \\
&\quad + ((1+v)l_1(x) + vl_2(x) \mid (1+v)a_1(x) + va_2(x)) \\
&\quad [(1+v)r_2(x) + vr_4(x)].
\end{aligned}$$

Therefore $c(x) \in \langle (1+v)(b_1(x) \mid 0), (1+v)(l_1(x) \mid a_1(x)), v(b_2(x) \mid 0), v(l_2(x) \mid a_2(x))\rangle$. The result follows. □

Recall, the definitions of $\pi(\mathrm{C})$, $\ker_\pi(\mathrm{C})$ and K. In the following theorem we give the form of generator polynomials of an R-double cyclic code when $\pi(\mathrm{C})$ and K has no monic polynomials of least degree.

Theorem 15 *Let* C *be an* R*-double cyclic code of length* (r, s) *such that* $\pi(\mathrm{C}) = \langle va(x)\rangle$ *and* $\mathrm{Ker}(\pi)_\mathrm{C} = \langle (vb(x) \mid 0)\rangle$*, where* $a(x), b(x) \in \mathrm{R}[x]$*. Then* $\mathrm{C} = \langle (vb(x) \mid 0), (vl(x) \mid va(x))\rangle$ *for some* $l(x) \in \mathbb{F}_4[x]$*. Similarly, when* $\pi(\mathrm{C}) = \langle (1+v)a(x)\rangle$ *and* $\mathrm{Ker}(\pi)_\mathrm{C} = \langle ((1+v)b(x) \mid 0)\rangle$*, then* $\mathrm{C} = \langle ((1+v)b(x) \mid 0), ((1+v)l(x) \mid (1+v)a(x))\rangle$.

Proof Suppose C is an R-double cyclic code with $\pi(\mathrm{C}) = \langle va(x)\rangle$ and $\mathrm{Ker}(\pi)_\mathrm{C} = \langle (vb(x) \mid 0)\rangle$. Then $\mathrm{C} = \langle (vb(x) \mid 0), ((1+v)l' + vl(x) \mid va(x))\rangle$. Clearly, $(1+v)((1+v)l' + vl(x) \mid va(x)) = ((1+v)l' \mid 0) \in \mathrm{C}$ and hence $(1+v)l' \in K$. As K contains no polynomial with leading coefficient as $(1+v)$, we get $l' = 0$. Therefore $\mathrm{C} = \langle (vb(x) \mid 0), (vl(x) \mid va(x))\rangle$. Second part of the theorem can be proved similarly. □

Theorem 16 *Let* C *be an* R*-double cyclic code of length* (r, s)*. Then* C *is one of the following form:*

1. $\mathrm{C} = \langle ((1+v)b_1(x) + vb_2(x) \mid 0)\rangle$*, where* $b_1(x) | (x^r - 1)$ *and* $b_2(x) | (x^r - 1)$*;*
2. $\mathrm{C} = \langle (l(x) \mid (1+v)a_1(x) + va_2(x))\rangle$*, where* $b_1(x) | (x^r - 1)$*,* $b_2(x) | (x^r - 1)$*, and* $(x^r - 1)$ *divides* $\frac{x^s-1}{(1+v)a_1(x)+va_2(x)} l(x)$*;*
3. $\mathrm{C} = \langle ((1+v)b_1(x) + vb_2(x) \mid 0), ((1+v)l_1(x) + vl_2(x) \mid (1+v)a_1(x) + va_2(x))\rangle$*, where* $b_i(x) \big| (x^r - 1)$*,* $a_i(x) \big| (x^s - 1)$*,* $i = 1, 2$*, and* $((1+v)b_1(x) + vb_2(x))$ *divides* $\frac{x^s-1}{(1+v)a_1(x)+va_2(x)}((1+v)l_1(x) + vl_2(x))$.

Now, we give a minimal spanning set of an R-double cyclic code C of length (r, s) in $\mathrm{R}_{r,s}[x]$ as an R-module. Recall that the minimal spanning set of an $\mathbb{F}_4$-double cyclic code $\mathrm{C} = \langle (b(x) \mid 0), (l(x) \mid a(x))\rangle$ of length (r, s) is $S = S_1 \cup S_2$, where $S_1 = \cup_{i=0}^{r-\deg(b(x))-1} (b(x) \mid 0)$ and $S_2 = \cup_{j=0}^{s-\deg(a(x))-1} (l(x) \mid a(x))$ (Borges and Fernàndez-Còrdoba (2017), Proposition 3).

Theorem 17 *Let* $\mathrm{C} = \langle ((1+v)b_1(x) + vb_2(x) \mid 0), ((1+v)l_1(x) + vl_2(x) \mid (1+v)a_1(x) + va_2(x))\rangle$ *be an* R*-double cyclic code of length* (r, s)*. Let*

$$S_{11} = \bigcup_{i_1=0}^{r-\deg(b_1(x))-1} ((1+v)b_1(x) \mid 0) \quad S_{12} = \bigcup_{j_1=0}^{s-\deg(a_1(x))-1} ((1+v)l_1(x) \mid (1+v)a_1(x))$$

$$S_{21} = \bigcup_{i_2=0}^{r-\deg(b_2(x))-1} (vb_2(x) \mid 0) \qquad S_{22} = \bigcup_{j_2=0}^{s-\deg(a_2(x))-1} (vl_2(x) \mid va_2(x)).$$

Then, $S = S_{11} \cup S_{12} \cup S_{21} \cup S_{22}$ forms a minimal spanning set for C *as an* R*-module. Moreover,*

$$|\mathrm{C}| = 4^{2r+2s-\deg(a_1(x))-\deg(b_1(x))-\deg(a_2(x))-\deg(b_2(x))}.$$

Proof Clearly, $\mathrm{span}(S) \subseteq \mathrm{C}$. Let $c = ((1+v)f_1(x) + vf_2(x) \mid (1+v)g_1(x) + vg_2(x)) \in \mathrm{C}$. Then from the definitions of C_1 and C_2, we have $(f_1(x) \mid g_1(x)) \in \mathrm{C}_1$ and $(f_2(x) \mid g_2(x)) \in \mathrm{C}_2$. This implies $((1+v)f_1(x) \mid (1+v)g_1(x)) \in \mathrm{span}\,(S_{11} \cup S_{12})$ and $(vf_2(x) \mid vg_2(x)) \in \mathrm{span}\,(S_{21} \cup S_{22})$. Thus $c \in \mathrm{span}(S)$, and $\mathrm{C} \subseteq \mathrm{span}(S)$. Therefore S is a minimal spanning set of C. □

In the following result, we show that the dual of an R-double cyclic codes is also an R-double cyclic code.

Theorem 18 *If* C *is an* R*-double cyclic code of length (r, s), then the dual $\mathrm{C}^\perp$ of* C *is also an* R*-double cyclic code of length (r, s).*

Proof Let $y = (y_{1,0}, y_{1,1}, \ldots, y_{1,r-1} \mid y_{2,0}, y_{2,1}, \ldots, y_{2,s-1}) \in \mathrm{C}$ and $x = (x_{1,0}, x_{1,1}, \ldots, x_{1,r-1} \mid x_{2,0}, x_{2,1}, \ldots x_{2,s-1}) \in \mathrm{C}^\perp$. Since C is invariant under τ, we have $\tau^{m-1}(y) \in \mathrm{C}$, where $m = \mathrm{lcm}(r, s)$. Therefore

$$\begin{aligned} 0 = x \cdot \sigma^{m-1}(y) &= (x_{1,0}y_{1,1} + \cdots + x_{1,r-2}y_{1,r-1} + x_{1,r-1}y_{1,0}) + (x_{2,0}y_{2,1} + \cdots + x_{2,s-1}y_{2,0}) \\ &= (x_{1,r-1}y_{1,0} + x_{1,0}y_{1,1} + \cdots + x_{1,r-2}x_{1,r-1}) + (x_{2,s-1}y_{2,0} + \cdots + x_{2,s-2}y_{2,s-1}) \\ &= \tau(x) \cdot y. \end{aligned}$$

As y is an arbitrary element of C, the result follows. □

Now, we give the generators of the dual code of an R-double cyclic code.

Theorem 19 *Let* $\mathrm{C} = (1+v)\mathrm{C}_1 + v\mathrm{C}_2$ *be an* R*-double cyclic code of length (r, s), and $\mathrm{C}_1^\perp = \langle(\hat{b}_1(x) \mid 0), (\hat{l}_1(x) \mid \hat{a}_1(x))\rangle$ and $\mathrm{C}_2^\perp = \langle(\hat{b}_2(x) \mid 0), (\hat{l}_2(x) \mid \hat{a}_2(x))\rangle$ be the dual codes of $\mathrm{C}_1 = \langle(b_1(x) \mid 0), (l_1(x) \mid a_1(x))\rangle$ and $\mathrm{C}_2 = \langle(b_2(x) \mid 0), (l_2(x) \mid a_2(x))\rangle$, respectively. Then $\mathrm{C}^\perp = \langle((1+v)\hat{b}_1(x) + v\hat{b}_2(x) \mid 0), ((1+v)\hat{l}_1(x) + v\hat{l}_2(x) \mid (1+v)\hat{a}_1(x) + v\hat{a}_2(x))\rangle$.*

Proof The result follows directly from the fact that $\mathrm{C}^\perp = (1+v)\mathrm{C}_1^\perp + v\mathrm{C}_2^\perp$ and Theorem 14. □

Corollary 1 *An* R*-double cyclic code* $\mathrm{C} = (1+v)\mathrm{C}_1 + v\mathrm{C}_2$ *is self-dual if and only if* C_1 *and* C_2 *are self-dual double cyclic codes over* $\mathbb{F}_4$.

The following result gives the cardinality of an R-double cyclic code and its dual code.

Theorem 20 *Let* $\mathrm{C} = (1+v)\mathrm{C}_1 \oplus v\mathrm{C}_2$ *be an* R*-double cyclic code and as defined in Theorem 14. Then* $|\mathrm{C}| = 4^{2(r+s)-\deg(a_1)-\deg(a_2)-\deg(b_1)-\deg(b_2)}$ *and* $|\mathrm{C}^\perp| = 4^{\deg(a_1)+\deg(a_2)+\deg(b_1)+\deg(b_2)}$.

Proof The proof follows as $|\mathrm{C}| = |\mathrm{C}_1| \cdot |\mathrm{C}_2|$ and $|\mathrm{C}^\perp| = |\mathrm{C}_1^\perp| \cdot |\mathrm{C}_2^\perp|$. □

The following theorem gives the structure of the Gray image of an R-double cyclic code.

Theorem 21 *Let* $\mathrm{C} = (1+v)\mathrm{C}_1 + v\mathrm{C}_2$ *be an* R*-double cyclic code of length* (r, s)*, where* C_1 *and* C_2 *are* $\mathbb{F}_4$*-double cyclic codes of length* (r, s) *as defined in Theorem 8. Then the Gray image of* C *under* ϕ *is a generalized quasi cyclic code of length* (r, s, r, s) *over* $\mathbb{F}_4$*. In particular if* $r = s$*, then* $\phi(\mathrm{C})$ *is a* 4*-quasi cyclic code of length* $4r$ *over* $\mathbb{F}_4$*.*

Proof The result follows as C_1 and C_2 are $\mathbb{F}_4$-double cyclic codes (quasi cyclic codes of index 2) and $\phi(\mathrm{C}) = \mathrm{C}_1 \times \mathrm{C}_2$. □

An R-double cyclic code is separable if $\mathrm{C} = \mathrm{C}_r \times \mathrm{C}_s$. It is easy to prove that $\mathrm{C} = (1+v)\mathrm{C}_1 + v\mathrm{C}_2$ is sparable R-double cyclic code if and only if C_1 and C_2 are separable $\mathbb{F}_4$-double cyclic codes. Further, the dual of an R-separable code is also separable.

Theorem 22 *Let* $\mathrm{C}^{\perp}$ *be the dual code of a separable* R*-double cyclic code* $\mathrm{C} = \langle((1+v)b_1(x)+vb_2(x) \mid 0), (0 \mid (1+v)a_1(x)+va_2(x))\rangle$*. Then* $\mathrm{C}^{\perp} = \left\langle \left((1+v)\frac{x^r-1}{b_1^*(x)} + v\frac{x^r-1}{b_2^*(x)} \;\middle|\; 0\right), \left(0 \;\middle|\; (1+v)\frac{x^r-1}{a_1^*(x)} + v\frac{x^r-1}{a_2^*(x)}\right)\right\rangle$.

Example 6 Let $\mathrm{C} = \langle((1+v)(x^4+x^3+x^2+1) \mid 0), (vx^4+vx^3+vx^2+x \mid vx^3+x+1)\rangle$ be an R-double cyclic code of length (7, 14). Then, $\mathrm{C}_1 = \langle(x^4+x^3+x^2+1 \mid 0), (x \mid x+1)\rangle$ and $\mathrm{C}_2 = \langle(x^4+x^3+x^2+x \mid x^3+x+1)\rangle$. The $\mathbb{F}_4$-double cyclic codes C_1 and C_2 are of length (7, 14) with parameters [21, 16, 3] and [21, 11, 6], respectively. Further, from Theorem 8, we see $\mathrm{C}_1^{\perp} = \langle(x^3+x+1 \mid x^9+x^8+x^6+x^5+x^4+x^3+1)\rangle$ and $\mathrm{C}_2^{\perp} = \langle(x^6+x^5+x^4+x^3+x^2+x+1 \mid 0), (x^4+x^3+1 \mid x^5+x^2+x+1)\rangle$. Therefore $\mathrm{C}^{\perp} = \langle(v(x^6+x^5+x^4+x^3+x^2+x+1) \mid 0), (vx^4+x^3+(1+v)x+1 \mid (1+v)x^9+(1+v)x^8+(1+v)x^6+x^5+(1+v)x^4+(1+v)x^3+vx^2+vx+1)\rangle$. As $\mathrm{C}_1^{\perp}$ and $\mathrm{C}_1^{\perp}$ are $\mathbb{F}_4$-double cyclic codes with parameters $[21, 5, 10]^*$ and $[21, 10, 7]^*$, respectively, we have $\phi(\mathrm{C}^{\perp})$ a generalized quasi-cyclic code of index four with parameters [42, 15, 7] over $\mathbb{F}_4$.

Example 7 Let $\mathrm{C}_1 = \langle(wx+1 \mid 0), (x+1 \mid 1)\rangle$ and $\mathrm{C}_2 = \langle(wx+1 \mid 0), (x+1 \mid x+1)\rangle$ be two $\mathbb{F}_4$-double cyclic codes of length (6, 6). We see C_1 and C_2 are optimal $\mathbb{F}_4$-codes with parameters $[12, 11, 2]^*$ and $[12, 10, 2]^*$, respectively. From Theorem 14, $\mathrm{C} = (1+v)\mathrm{C}_1 \oplus v\mathrm{C}_2 = \langle((1+v)(wx+1)+v(x+1) \mid 0), (x+1 \mid 1+vx)\rangle$, an R-double cyclic code of length (6, 6). The Gray image of C is a quasi-cyclic code of index 4 with parameters $[24, 21, 2]^*$ over $\mathbb{F}_4$.

Example 8 Let $\mathrm{C} = \langle(x+1 \mid 0), (0 \mid x+1)\rangle$ be a separable R-double cyclic code of length (10, 10). Then $\mathrm{C}_1 = \mathrm{C}_2 = \langle(x+1 \mid 0), (0 \mid x+1)\rangle$, a separable $\mathbb{F}_4$-double cyclic code with parameters $[20, 18, 2]_4^*$. The Gray image of C under ϕ is a quasi-cyclic code of index 4 and length 40 with parameters $[40, 36, 2]_4$. Also, $\mathrm{C}^{\perp} = \langle(x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 \mid 0), (0 \mid x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)\rangle$.

3.3 Enumeration of R-double cyclic codes

In this section, we give the complete classification of R-double cyclic codes of length $(2^{e_1}, 2^{e_2})$, where e_1 and e_2 are non-negative integers. We give a mass formula that enumerate these family of codes for given values of e_1 and e_2. For that we first recall the structure of cyclic codes over $\mathbb{F}_4$ of length $n = 2^e$.

Let R_n' denote the quotient ring $\mathbb{F}_4[x]/\langle x^n - 1\rangle$, where $n = 2^e$. As $(x+1)$ is a nilpotent element of nilpotency 2^e Dinh and López-permouth (2004), each polynomial in R_n' can be

written as $\sum_{i=0}^{2n-1} a_i(x+1)^i,\ a_i \in \mathbb{F}_4$, and such an element is a unit in R_n' if and only if $a_0 \neq 0$. From this we see that R_n is a finite chain ring and any ideal of R_n' is of the form $\langle (x+1)^i \rangle,\ 0 \leq i \leq n$ Dinh and López-permouth (2004). Therefore, if C is an $\mathbb{F}_4$-double cyclic code of length $(2^{e_1}, 2^{e_2})$, then $\mathrm{C} = \langle ((x+1)^{i_1} \mid 0), ((x+1)^t h(x) \mid (x+1)^{i_2}) \rangle$, where $h(x)$ is zero or unit in $\mathbb{F}_4[x]/\langle x^{2^{e_1}} - 1 \rangle$. Summarizing this discussion, the following theorem present the complete module structure of $\mathbb{F}_4$-double cyclic codes of length $(2^{e_1}, 2^{e_2})$. Throughout this section we let $r = 2^{e_1}$ and $s = 2^{e_2}$, where e_1, e_2 are non-negative integers.

Lemma 1 *Let* C *be an* $\mathbb{F}_4$*-double cyclic code of length* (r, s)*. Then* C *is one of the following:*

Type 1: $\mathrm{C} = \langle ((x+1)^{i_1} \mid 0) \rangle,\ 0 \leq i_1 \leq r$*;*
Type 2: $\mathrm{C} = \langle ((x+1)^t h(x) \mid (x+1)^{i_2}) \rangle$*, where* $0 \leq i_2 \leq s-1$ *and* $h(x)$ *is either zero or a unit in* $\mathbb{F}_4[x]/\langle x^r - 1 \rangle$ *such that* $t + \deg(h(x)) < r$*;*
Type 3: $\mathrm{C} = \langle ((x+1)^{i_1} \mid 0), ((x+1)^t h(x) \mid (x+1)^{i_2}) \rangle$*, where* $0 \leq i_1 \leq r-1,\ 0 \leq i_2 \leq s-1$ *and* $h(x)$ *is either zero or a unit in* $\mathbb{F}_4[x]/\langle x^r - 1 \rangle$ *such that* $t + \deg(h(x)) < i$*.*

Remark 2 The $\mathbb{F}_4$-double cyclic codes of length (r, s) of Type 2 are in fact $\mathrm{C} = \langle (x^r - 1 \mid 0), ((x+1)^t h(x) \mid (x+1)^{i_2}) \rangle, 0 \leq i_2 \leq s-1$.

Lemma 2 *Let* $r = 2^{e_1}$ *and* $s = 2^{e_2}$*,* $e_1 > 0,\ e_2 > 0$*. Then, the number of* $\mathbb{F}_4$*-double cyclic codes of length* (r, s) *is*

$$\mathcal{N} = \begin{cases} r4^s - s4^s + \frac{5}{3}4^s - \frac{1}{2}s^2 + rs + \frac{3}{2}s - \frac{5}{3} & \text{if } r \geq s \\ s4^r - r4^r + \frac{5}{3}4^s - \frac{1}{2}r^2 + rs + \frac{3}{2}r - \frac{5}{3} & \text{if } r < s. \end{cases}$$

Proof We enumerate $\mathbb{F}_4$-double cyclic codes separately in each case as given in Lemma1. Let $\mathcal{N}_i$ be the number of $\mathbb{F}_4$-double cyclic codes of Type i.
$Type\ 1$: The number of $\mathbb{F}_4$-double cyclic codes of Type $\langle ((x+1)^{i_1} \mid 0) \rangle,\ 0 \leq i_1 \leq r$ is $\mathcal{N}_1 = r + 1$.
$Type\ 2$: We enumerate the number of $\mathbb{F}_4$-double cyclic codes of Type 2 in two cases. When $h(x)$ is zero, there are $\mathcal{N}_{21} = s$ number of cyclic codes of Type $\langle (0 \mid (x+1)^{i_2}) \rangle,\ 0 \leq i_2 \leq s-1$. When, $h(x) \neq 0$, the number of $\mathbb{F}_4$-double cyclic codes of type $\langle ((x+1)^t h(x) \mid (x+1)^{i_2}) \rangle,\ 0 \leq i_2 \leq s-1$ is as follows:

$$\begin{aligned} \mathcal{N}_{22} &= \begin{cases} \sum_{t=0}^{s-1} 3 \cdot 4^t & \text{if } r \geq s \\ (s-r+1)\left[3 \cdot 4^{r-1}\right] + \sum_{t=1}^{r-1} 3 \cdot 4^{r-t-1} & \text{if } r < s. \end{cases} \\ &= \begin{cases} 4^s - 1 & \text{if } r \geq s \\ 4^r + 3s4^{r-1} - 3r4^{r-1} - 1 & \text{if } r < s. \end{cases} \end{aligned}$$

$Type\ 3$: Again, we enumerate the number of $\mathbb{F}_4$-double cyclic codes of Type 3 in two cases. When $h(x) = 0$, the $\mathbb{F}_4$-double cyclic codes are of the form $\mathrm{C} = \langle ((x+1)^{i_1} \mid 0), (0 \mid (x+1)^{i_2}) \rangle$, where $0 \leq i_1 \leq r-1,\ 0 \leq i_2 \leq s-1$. Clearly, these are separable $\mathbb{F}_4$-double cyclic codes. Thus, the number of separable $\mathbb{F}_4$-double cyclic codes of length (r,s) is $\mathcal{N}_{31} = r \cdot s$.

Let $h(x) \neq 0$ and $\mathrm{C} = \langle ((x+1)^{i_1} \mid 0), ((x+1)^t h(x) \mid (x+1)^{i_2}) \rangle$. Then it is easy to see that $(x+1)^{i_1}$ divides $(x+1)^{s-i_2}\left((x+1)^t h(x)\right)$ (see Lemma 8). As $h(x)$ a unit element in $\mathbb{F}_4[x]/\langle x^r - 1 \rangle$, we thus have $s - i_2 + t \geq i_1$. So the number of $\mathbb{F}_4$-double cyclic codes of

the form $\mathrm{C} = \langle((x+1)^{i_1} \mid 0), ((x+1)^t h(x) \mid (x+1)^{i_2})\rangle,\ 0 \le i_1 \le r-1,\ 0 \le i_2 \le s-1$ is

$$\mathcal{N}_{32} = \begin{cases} (r-s)\sum_{t=0}^{s-1} 3\cdot 4^t + \sum_{i=1}^{s-1}\left[(s-i)3\cdot 4^{i-1} + \sum_{t=0}^{i-1} 3\cdot 4^t\right] & \text{if } r \ge s \\ \sum_{i=1}^{r-1}\left[(s-i)3\cdot 4^{i-1} + \sum_{t=0}^{i-1} 3\cdot 4^t\right] & \text{if } r < s. \end{cases}$$

$$= \begin{cases} r4^s - s4^s + \frac{2}{3}4^s - \frac{1}{2}s^2 - r + \frac{1}{2}s - \frac{5}{3} & \text{if } r \ge s \\ s4^{r-1} - r4^{r-1} + \frac{2}{3}4^r - s + \frac{1}{2}r - \frac{1}{2}r^2 - \frac{5}{3} & \text{if } r < s. \end{cases}$$

Therefore, the total number of $\mathbb{F}_4$-double cyclic codes length (r, s) is

$$\mathcal{N} = \begin{cases} r4^s - s4^s + \frac{5}{3}4^s - \frac{1}{2}s^2 + rs + \frac{3}{2}s - \frac{5}{3} & \text{if } r \ge s \\ s4^r - r4^r + \frac{5}{3}4^s - \frac{1}{2}r^2 + rs + \frac{3}{2}r - \frac{5}{3} & \text{if } r < s. \end{cases}$$

□

Theorem 23 *The number of* R*-double cyclic codes of length* (r, s)*, where* $r = 2^{e_1},\ s = 2^{e_2}$*, is*

$$\mathcal{N} = \begin{cases} \left(r4^s - s4^s + \frac{5}{3}4^s - \frac{1}{2}s^2 + rs + \frac{3}{2}s - \frac{5}{3}\right)^2 & \text{if } r \ge s \\ \left(s4^r - r4^r + \frac{5}{3}4^s - \frac{1}{2}r^2 + rs + \frac{3}{2}r - \frac{5}{3}\right)^2 & \text{if } r < s. \end{cases}$$

Proof The proof follows from Lemma 2, and the fact that the size of an R-double cyclic code $\mathrm{C} = (1+v)\mathrm{C}_1 \oplus v\mathrm{C}_2$ of length (r, s) is $|\mathrm{C}| = |\mathrm{C}_1| \times |\mathrm{C}_2|$, where C_1 and C_2 are $\mathbb{F}_4$-double cyclic codes of length (r, s). □

Example 9 Let $r = s = 2$ and $\mathcal{N}_i$ be the number of $\mathbb{F}_4$-double cyclic codes of *Type i*. Then the $\mathbb{F}_4$-double cyclic codes of length (2, 2) as follows:

Type	codes	$\mathcal{N}_i$
Type 1	$\langle(1 \mid 0)\rangle,\ \langle(x+1 \mid 0)\rangle$ and $\langle(0 \mid 0)\rangle$	$\mathcal{N}_1 = 3$
Type 2 when $h(x) = 0$	$\langle(0 \mid x+1)\rangle$ and $\langle(0 \mid 1)\rangle$	$\mathcal{N}_{21} = 2$
Type 2 when $h(x) \ne 0$	$\langle(x+1 \mid x+1)\rangle,\ \langle(wx+w \mid x+1)\rangle,\ \langle(w^2x+w^2 \mid x+1)\rangle,\ \langle(x+1 \mid 1)\rangle,$ $\langle(x+w \mid 1)\rangle,\ \langle(x+w^2 \mid 1)\rangle,\ \langle(wx+1 \mid 1)\rangle,\ \langle(wx+w \mid 1)\rangle,\ \langle(wx+w^2 \mid 1)\rangle,$ $\langle(w^2x+1 \mid 1)\rangle,\ \langle(w^2x+w \mid 1)\rangle,\ \langle(w^2x+w^2 \mid 1)\rangle,\ \langle(1 \mid 1)\rangle,\ \langle(w \mid 1)\rangle$and$\langle(w^2 \mid 1)\rangle$	$\mathcal{N}_{22} = 15$
Type 3 when $h(x) = 0$	$\langle(1 \mid 0), (0 \mid 1)\rangle,\ \langle(x+1 \mid 0), (0 \mid 1)\rangle,$ $\langle(1 \mid 0), (0 \mid x+1)\rangle,\ \langle(x+1 \mid 0), (0 \mid x+1)\rangle$	$\mathcal{N}_{31} = 4$
Type 3 when $h(x) \ne 0$	$\langle(x+1 \mid 0), (1 \mid 1)\rangle,\ \langle(x+1 \mid 0), (w \mid 1)\rangle,\ \langle(x+1 \mid 0), (w^2 \mid 1)\rangle$ $\langle(x+1 \mid 0), (1 \mid x+1)\rangle,\ \langle(x+1 \mid 0), (w \mid x+1)\rangle,\ \langle(x+1 \mid 0), (w^2 \mid x+1)\rangle$	$\mathcal{N}_{32} = 6$

Therefore, the total number of $\mathbb{F}_4$-double cyclic codes of length (2, 2) is 3+2+15+4+6 = 30. Further, from Theorem 20, the total number of R-double cyclic codes of length (2, 2) is 900.

Theorem 24 *Let* $\mathrm{C} = \langle((x+1)^{i_1} \mid 0), ((x+1)^t h(x) \mid (x+1)^{i_2})\rangle$ *be an* R*-double cyclic code of length* (r, s)*, where* $r = 2^{e_1}, s = 2^{e_2}$ *and* $h(x)$ *is either zero or a unit over* $\mathbb{F}_4$*. Then* $\mathrm{C}^{\perp} = \langle((x+1)^{r-t} \mid 0), ((x+1)^{r-i_1}\delta \mid (x+1)^{s+t-i_1-i_2})\rangle$*, where* $\delta = [h]^{-1}x^{m-i_2+t+\deg(h)} \pmod{(x+1)^{i_1-t}}$.

Table 1 Some good $\mathbb{F}_4$-double constacyclic codes

Generators	$[r, s]$	Parameters
$\langle (x^3 + wx^2 + w^2x + 1 \mid 0), (w^2x + w \mid w^2)\rangle$	[4, 4]	[8, 5, 3]*
$\langle (x^3 + wx^2 + w^2x + 1 \mid 0), (w^2x + w \mid wx + w^2)\rangle$	[4, 4]	[8, 4, 4]*
$\langle (x^2 + w^2 \mid 0), (w^2x + w \mid 1)\rangle$	[4, 4]	[8, 6, 2]*
$\langle (wx^2 + 1 \mid 0), (w \mid w^2)\rangle$	[4, 6]	[10, 8, 2]*
$\langle (x + w \mid 0), (w \mid 1)\rangle$	[4, 6]	[10, 9, 2]*
$\langle (wx^3 + w^2x^2 + x + w \mid 0), (x + w^2 \mid x^2 + w)\rangle$	[4, 8]	[12, 7, 4]*
$\langle (wx^5 + x^4 + x + w^2 \mid 0), (x^3 + w^2x^2 + wx \mid w^2)\rangle$	[8, 8]	[16, 11, 4]*
$\langle (wx^5 + x^4 + x + w^2 \mid 0), (w^2x^3 + x + w \mid x + w^2)\rangle$	[8, 14]	[22, 16, 4]*
$\langle (wx^3 + x^2 + w^2x + w \mid 0), (wx^2 + wx \mid 1)\rangle$	[8, 18]	[26, 23, 2]*
$\langle (x^5 + wx^4 + w^2x^3 + wx^2 + wx + w \mid 0), (w^2x + w \mid w^2x + w)\rangle$	[20, 20]	[40, 34, 4]*

Example 10 Let $r = 4, s = 8$, and $\mathrm{C} = \langle ((x+1)^4 \mid 0), (x^2 + x \mid (x+1)^5)\rangle$ be an R-double cyclic code of length $(4, 8)$. Following the notations in Theorem 24, we have $i_1 = 4, i_2 = 5, t = 1$ and $h(x) = x = (x + 1) + 1$. Clearly, $\delta = x^2 + x + 1$, and the dual code $\mathrm{C}^\perp$ of C is $\mathrm{C}^\perp = \langle ((x+1)^3 \mid 0), (x^2 + x + 1 \mid 1\rangle$.

4 R-Double constacyclic codes

Constacyclic codes constitutes an important generalization of cyclic codes. These codes are important because of simplified algebraic structure and practical usage. In this section, we define an R-double constacyclic code of length (r, s). We characterize these codes with their Gray images. These codes are multi-twisted cyclic codes (generalization of quasi-twisted cyclic codes) of index two over R. Recently, Aydin and Halilović (2017) introduced these family of codes over finite fields and presented few construction methods. Recall, an (α, β)-double constacyclic code of length (r, s) over $\mathbb{F}_q$ is an $\mathbb{F}_4[x]$-submodule of $\frac{\mathbb{F}_4[x]}{\langle x^r - \alpha\rangle} \times \frac{\mathbb{F}_4[x]}{\langle x^s - \beta\rangle}$, where α, β are units in $\mathbb{F}_4$ Aydin and Halilović (2017).

The following Table1 gives some examples of $\mathbb{F}_4$-double constacyclic codes, which have the best known minimum distance.

Now, we extend the definition of double constacyclic codes over finite fields given in Aydin and Halilović (2017) and define an R-double constacyclic codes.

Definition 2 Let λ_1 and λ_2 be two unit elements in R and $c = (c_0, c_1, \ldots, c_{r-1} \mid c'_0, c'_1, \ldots, c'_{s-1}) \in \mathrm{R}^r \times \mathrm{R}^s$. Then the double constacyclic shift $\sigma_{\lambda_1\lambda_2}$ of c is defined by

$$\sigma_{\lambda_1\lambda_2}(c) = (\lambda_1 c_{r-1}, c_0, \ldots, c_{r-2} \mid \lambda_2 c'_{s-1}, c'_0, \ldots, c'_{s-2}).$$

A linear code C of length $r + s$ over R is called a (λ_1, λ_2)-double constacyclic code of length (r, s) if it is invariant under the double constacyclic shift operator $\sigma_{\lambda_1\lambda_2}$. Under polynomial representation, we can easily see that C is a (λ_1, λ_2)-double constacyclic code of length (r, s) over R if and only if C is an $\mathrm{R}[x]$-submodule of $\frac{\mathrm{R}[x]}{\langle x^r - \lambda_1\rangle} \times \frac{\mathrm{R}[x]}{\langle x^s - \lambda_2\rangle}$. As a special case, if we take $\lambda_1 = \lambda_2 = 1$, then C an R-double cyclic code. Note that, when $\lambda_1 = \lambda_2 = \lambda$, we call C a λ-double constacyclic code over R.

Let $\pi_i : \mathbb{F}_4 \times \mathbb{F}_4 \to \mathbb{F}_4$ be a projection map such that $\pi_i(a_1 \mid a_2) = a_i, i = 1, 2$. Also let

$L_n = \left[\frac{\mathbb{F}_4[x]}{\langle x^r-\pi_1(\phi(\lambda_1))\rangle} \times \frac{\mathbb{F}_4[x]}{\langle x^s-\pi_1(\phi(\lambda_2))\rangle}\right] \times \left[\frac{\mathbb{F}_4[x]}{\langle x^r-\pi_2(\phi(\lambda_1))\rangle} \times \frac{\mathbb{F}_4[x]}{\langle x^s-\pi_2(\phi(\lambda_2))\rangle}\right]$, where $\phi(\lambda_1)$ and $\phi(\lambda_2)$ are Gray images of λ_1 and λ_2. Now, we extend the Gray map ϕ to Φ as follows:

$$\Phi : \frac{\mathrm{R}[x]}{\langle x^r-\lambda_1\rangle} \times \frac{\mathrm{R}[x]}{\langle x^s-\lambda_2\rangle} \to L_n$$

such that

$$\phi\left(\sum_{i=0}^{r} a_i x^i \;\middle|\; \sum_{j=0}^{s} b_i x^j\right) \mapsto \left(\sum_{i=0}^{r} \pi_1(\phi(a_i))x^i,\ \sum_{i=0}^{r} \pi_2(\phi(a_i))x^i,\ \sum_{j=0}^{s} \pi_1(\phi(b_j))x^j,\ \sum_{j=0}^{s} \pi_2(\phi(b_j))x^j\right).$$

Clearly, ϕ is a modular isomorphism, and, therefore, $\frac{\mathrm{R}[x]}{\langle x^r-\lambda_1\rangle} \times \frac{\mathrm{R}[x]}{\langle x^s-\lambda_2\rangle} \cong \left[\frac{\mathbb{F}_4[x]}{\langle x^r-\pi_1(\phi(\lambda_1))\rangle} \times \frac{\mathbb{F}_4[x]}{\langle x^s-\pi_1(\phi(\lambda_2))\rangle}\right] \times \left[\frac{\mathbb{F}_4[x]}{\langle x^r-\pi_2(\phi(\lambda_1))\rangle} \times \frac{\mathbb{F}_4[x]}{\langle x^s-\pi_2(\phi(\lambda_2))\rangle}\right]$. With this we have the following result:

Theorem 25 *Let* $\mathrm{C} = (1+v)\mathrm{C}_1 + v\mathrm{C}_2$ *be a linear code of length* $r+s$ *over* R*, and* λ_1, λ_2 *be two unit elements in* R*. Then* C *is a* (λ_1, λ_2)*-constacyclic code of length* (r, s) *over* R *if and only if* C_1 *is a* $(\pi_2(\phi(\lambda_1)), \pi_2(\phi(\lambda_2)))$*-double constacyclic code and* C_2 *is a* $(\pi_1(\phi(\lambda_1)), \pi_1(\phi(\lambda_2)))$*-double constacyclic code of length* (r, s) *over* $\mathbb{F}_4$*.*

Proof Let $\lambda_1 = \lambda_{11} + v\lambda_{12}$ and $\lambda_2 = \lambda_{21} + v\lambda_{22}$ be two unit elements in R. Let $c = (c_0, c_1, \ldots, c_{r-1} \mid c'_0, c'_1, \ldots, c'_{s-1}) \in \mathrm{C}$, where $c_i = (1+v)x_i + vy_i$, $c'_j = (1+v)x'_j + vy'_j$ for $0 \le i \le r-1$ and $0 \le j \le s-1$. Then we have

$$\begin{aligned}
\sigma_{\lambda_1\lambda_2}(c) &= \left(\lambda_1 c_{r-1}, c_0, \ldots, c_{r-2} \;\middle|\; \lambda_2 c'_{s-1}, c'_0, \ldots, c'_{s-2}\right)\\
&= ([\lambda_{11} + v\lambda_{12}][(1+v)x_{r-1} + vy_{r-1}], (1+v)x_0 + vy_0, \ldots,\\
&\quad (1+v)x_{r-2} + vy_{r-2} \;\big|\; [\lambda_{21} + v\lambda_{22}][(1+v)x'_{s-1} + vy'_{s-1}],\\
&\quad (1+v)x'_0 + vy'_0, \ldots, (1+v)x'_{s-2} + vy'_{s-2})\\
&= \Big([(1+v)\lambda_{11} + v(\lambda_{11}+\lambda_{12})][(1+v)x_{r-1} + vy_{r-1}], (1+v)x_0 + vy_0, \ldots, (1+v)x_{r-2} + vy_{r-2} \;\Big|\\
&\quad [(1+v)\lambda_{21} + v(\lambda_{21}+\lambda_{22})][(1+v)x'_{s-1} + vy'_{s-1}], (1+v)x'_0 + vy'_0, \ldots, (1+v)x'_{s-2} + vy'_{s-2}\Big)\\
&= (1+v)\left(\lambda_{11}x_{r-1}, x_0, \ldots, x_{r-2} \;\middle|\; \lambda_{21}x'_{s-1}, x'_0, \ldots, x'_{s-2}\right)\\
&\quad + v\left((\lambda_{21}+\lambda_{22})y_{r-1}, y_0, \ldots, y_{r-2} \;\middle|\; \lambda_{22}y'_{s-1}, y'_0, \ldots, y'_{s-2}\right)\\
&= (1+v)\left(\pi_2(\phi(\lambda_1))x_{r-1}, x_0, \ldots, x_{r-2} \;\middle|\; \pi_2(\phi(\lambda_2))x'_{s-1}, x'_0, \ldots, x'_{s-2}\right) +\\
&\quad v\left(\pi_1(\phi(\lambda_1))y_{r-1}, y_0, \ldots, y_{r-2} \;\middle|\; \pi_1(\phi(\lambda_2))y'_{s-1}, y'_0, \ldots, y'_{s-2}\right).
\end{aligned}$$

Suppose C_1 is a $(\pi_2(\phi(\lambda_1)), \pi_2(\phi(\lambda_2)))$-double constacyclic code and C_2 is a $(\pi_1(\phi(\lambda_1)), \pi_1(\phi(\lambda_2)))$-double constacyclic code of length (r, s) over $\mathbb{F}_4$. Then for any $c = (c_0, c_1, \ldots, c_{r-1} \mid c'_0, c'_1, \ldots, c'_{s-1}) \in \mathrm{C}$, where $c_i = (1+v)x_i + vy_i$, $c'_j = x'_j + vy'_j$ for $0 \le r-1$ and $0 \le j \le s-1$, we have $x = (x_0, x_1, \ldots, x_{r-1} \mid x'_0, x'_1, \ldots, x'_{s-1}) \in \mathrm{C}_1$ and $y = (y_0, y_1, \cdots, y_{r-1} \mid y'_0, y'_1, \ldots, y'_{s-1}) \in \mathrm{C}_2$. This implies $\sigma_{\pi_2(\phi(\lambda_1)),\pi_2(\phi(\lambda_2))}(x) \in \mathrm{C}_1$ and $\sigma_{\pi_1(\phi(\lambda_1)),\pi_1(\phi(\lambda_2))}(y) \in \mathrm{C}_2$. This further implies that $(1+v)\sigma_{\pi_2(\phi(\lambda_1)),\pi_2(\phi(\lambda_2))}(x) + v\sigma_{\pi_1(\phi(\lambda_1)),\pi_1(\phi(\lambda_2))}(y) = \sigma_{\lambda_1\lambda_2}(c) \in \mathrm{C}$. As x and y are arbitrary elements in C_1 and C_2, respectively, C is a (λ_1, λ_2)-constacyclic code of length (r, s) over R. Similarly we can prove the sufficient part of the theorem. □

Table 2 The relation between a (λ_1, λ_2)- double constacyclic code C and the codes C_1 and C_2

R-Double constacyclic code C	C_1	C_2
$(\alpha + v, \alpha)$-double constacyclic	(α, α)-double constacyclic	(α^2, α)-double constacyclic
$(1 + \alpha v, \alpha + \alpha^2 v)$-double constacyclic	$(1, \alpha)$-double constacyclic	$(\alpha^2, 1)$-double constacyclic
R-Double cyclic	$\mathbb{F}_4$-Double cyclic	$\mathbb{F}_4$-Double cyclic
(α, α^2)-double constacyclic	(α, α^2)-double constacyclic	(α, α^2)-double constacyclic
$(1 + \alpha v, 1 + \alpha v)$-double constacyclic	$\mathbb{F}_4$-Double cyclic	(α, α^2)-double constacyclic
$(\alpha^2 + v, \alpha^2)$-double constacyclic	(α^2, α^2)-double constacyclic	(α, α^2)-double constacyclic
$(\alpha^2 + \alpha v, \alpha^2 + \alpha v)$-double constacyclic	(α^2, α^2)-double constacyclic	$\mathbb{F}_4$-Double cyclic
$(\alpha + \alpha^2 v, \alpha^2 + \alpha v)$-double constacyclic	(α, α^2)-double constacyclic	$\mathbb{F}_4$-Double cyclic

The Table 2 below lists the relation between a (λ_1, λ_2)- double constacyclic code C over R and the $\mathbb{F}_4$-double constacyclic codes C_1 and C_2.

The following result characterizes the dual of a double constacyclic code over $\mathbb{F}_4$:

Lemma 3 *Let α, β be two unit elements in $\mathbb{F}_4$ and* C *be an (α, β)-double constacyclic code of length (r, s) over $\mathbb{F}_4$. Then* $C^\perp$ *is an $(\alpha^{-1}, \beta^{-1})$-double constacyclic code of length (r, s) over $\mathbb{F}_4$.*

Proof Let $m = \text{lcm}\{r, s\}$. We note that for any $a = (a_{11}, a_{12}, \ldots, a_{1\,r} \mid a_{21}, a_{22}, \ldots, a_{2\,s})$, we have $\sigma_{\alpha,\beta}^{m-1}(a) = (\alpha^{\frac{m}{s}} a_{12}, \ldots, \alpha^{\frac{m}{s}} a_{1\,r}, \alpha^{\frac{m}{s}-1} a_{11} \mid \beta^{\frac{m}{r}} a_{22}, \ldots, \beta^{\frac{m}{r}} a_{2\,s}, \beta^{\frac{m}{r}-1} a_{21})$. Also, as multiplicative order of each non-zero element in $\mathbb{F}_4$ is 3, we have $\sigma_{\alpha,\beta}^{3m}(a) = a$. Let $a = (a_{11}, a_{12}, \ldots, a_{1\,r} \mid a_{21}, a_{22}, \ldots, a_{2\,s}) \in$ C and $b = (b_{11}, b_{12}, \ldots, b_{1\,r} \mid b_{21}, b_{22}, \ldots, b_{2\,s}) \in C^\perp$. Then

$$
\begin{aligned}
\sigma_{\alpha,\beta}^{3m-1}(a) \cdot b &= \left(a_{12}b_{11} + \cdots + a_{1\,r}b_{1\,r-1} + \alpha^{3\frac{m}{s}-1} a_{11} b_{1\,r}\right) \\
&\quad + \left(a_{22}b_{21} + \cdots + a_{2\,s}b_{2\,s-1} + \beta^{3\frac{m}{r}-1} a_{21} b_{2\,s-1}\right) \\
&= \left(a_{12}b_{11} + \cdots + a_{1\,r}b_{1\,r-1} + \alpha^{3\frac{m}{s}-1}[\alpha.\alpha^{-1}] a_{11} b_{1\,r}\right) \\
&\quad + \left(a_{22}b_{21} + \cdots + a_{2\,s}b_{2\,s-1} + \beta^{3\frac{m}{r}-1}[\beta.\beta^{-1}] a_{21} b_{2\,s-1}\right) \\
&= \left(a_{12}b_{11} + \cdots + a_{1\,r}b_{1\,r-1} + [\alpha^{-1}] a_{11} b_{1\,r}\right) \\
&\quad + \left(a_{22}b_{21} + \cdots + a_{2\,s}b_{2\,s-1} + [\beta^{-1}] a_{21} b_{2\,s-1}\right) \\
&= \left(a_{11}[\alpha^{-1}b_{1\,r}] + a_{12}b_{11} + \cdots + a_{1\,r}b_{1\,r-1} + a_{21}[\beta^{-1}b_{2\,s-1}]\right) \\
&\quad + \left(a_{22}b_{21} + \cdots + a_{2\,s}b_{2\,s-1}\right) \\
&= a \cdot \sigma_{\alpha^{-1},\beta^{-1}}(b).
\end{aligned}
$$

Since $\sigma_{\alpha,\beta}^{3m-1}(a) \in$ C, $\sigma_{\alpha,\beta}^{m-1}(a) \cdot b = 0$. This implies that $a \cdot \sigma_{\alpha^{-1},\beta^{-1}}(b) = 0$. Therefore, $\sigma_{\alpha^{-1},\beta^{-1}}(b) \in C^\perp$. As b is an arbitrary element in $C^\perp$, we have $C^\perp$ an $(\alpha^{-1}, \beta^{-1})$-double constacyclic code over $\mathbb{F}_4$. □

Theorem 26 *Let $\lambda_1 = (1 + v)\lambda_{11} + v\lambda_{12}$, $\lambda_2 = (1 + v)\lambda_{21} + v\lambda_{22}$ be two unit elements in* R *and* $C = (1 + v)C_1 \oplus vC_2$ *be a (λ_1, λ_2)-double constacyclic code of length (r, s) over* R. *Then* $C^\perp$ *is a $((1 + v)\lambda_{11}^{-1} + v\lambda_{12}^{-1}, (1 + v)\lambda_{21}^{-1} + v\lambda_{22}^{-1})$-double constacyclic code of length (r, s) over* R.

Table 3 Some good R-double constacyclic codes

Constacyclic code C	$[r, s]$	Parameters of $\phi(C)$
$\langle (wx^2 + w^2x + 1 \mid 0), (wx + 1 \mid 1) \rangle$	[3, 1]	[8, 4, 3]
$\langle (wx^3 + w^2x^2 + x + w \mid 0), (w^2x^2 + x \mid x + w) \rangle$	[4, 4]	[16, 8, 4]
$\langle (w^2x^2 + w^2x + 1 \mid 0), (x \mid wx + 1) \rangle$	[5, 5]	[20, 14, 3]
$\langle (x^3 + wx^2 + 1 \mid 0), (wx^2 \mid w^2x + 1) \rangle$	[7, 7]	[28, 20, 3]
$\langle (x^5 + w^2x^4 + w^2x + w \mid 0), (x^3 + w^2x^2 + wx \mid w) \rangle$	[8, 8]	[32, 22, 4]
$\langle (x^5 + w^2x^4 + w^2x + w \mid 0), (w^2x^3 + w^2x^2 + w \mid x + w^2) \rangle$	[8, 14]	[44, 32, 4]
$\langle (1 \mid x^{14} + wx^{11} + x^{10} + wx^9 + x^8 + x^7 + wx^6 + x^5 + x^4 + w^2x^3 + w) \rangle$	[18, 18]	[72, 36, 12]

Proof The result follows from Lemma 3 and Theorem 25. □

It is easy to see that the Gray image of an R-double constacyclic code of length (r, s) is a generalized quasi-twisted code of length (r, s, r, s) over $\mathbb{F}_4$. The following Table3 gives some examples of R-double constacyclic codes whose Gray images are optimal $\mathbb{F}_4$-codes:

5 Conclusion

In this paper, we have studied generalized quasi-cyclic codes over R of index 2 as R-double cyclic codes of length (r, s). We determined the generators of R-double cyclic codes and their duals for arbitrary values of r and s. A mass formula to enumerate R-double cyclic codes of length $(2^{e_1}, 2^{e_2}), e_1, e_2 > 0$ is presented. Some structural properties of R-double constacyclic codes, and R-skew double cyclic codes are also studied. Finding generator polynomials of double constacycilc codes, skew double constacyclic codes, and their dual codes over R are a future interesting problems.

References

Abualrub T, Aydin N, Seneviratne P (2012) On θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Aust J Comb 54:115–126
Aydin N, Halilović A (2017) A generalization of quasi-twisted codes: Multi-twisted codes. Finite Fields Appl 45:96–106
Aydogdu I, Siap I (2014) $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. Linear Multilinear Algebra 63(10):2089–2102
Ashraf M, Mohammad G (2016) Quantum codes from cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. Quant Inf Process 15(10):4089–4098
Bayram A, Oztas ES, Siap I (2016) Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications. Des Codes Cryptogr 80(2):379–393
Bayram A, Siap I (2013) Structure of Codes over the Ring $\mathbb{Z}_3[v]/\langle v^3 - v \rangle$. Appl Algebra Eng Commun Comput 24(5):369–386
Bayram A, Siap I (2014) Cyclic and constacyclic codes over a non-chain ring. J Algebra Comb Disc Appl 1(1):1–14
Bhaintwal M, Wasan S (2009) On quasi-cyclic codes over $\mathbb{Z}_q$. Appl Algebra Eng Commun Comput 20:459–480
Boucher D, Sole P, Ulmer F (2008) Skew constacyclic codes over galois rings. Adv Math Commun 2:273–292
Borges J, Fernàndez-Còrdoba C, Pujol J, Rifà J, Villanueva M (2009) $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. Des Codes Cryptogr 54(2):167–179
Borges J, Fernàndez-Còrdoba C (2017) and Roger Ten-Valls, $\mathbb{Z}_2$-double cyclic codes. Des Codes Cryptogr. https://doi.org/10.1007/s10623-017-0334-8

Cao Y (2011) Generalized quasi-cyclic codes over Galois rings: structural properties and enumeration'. Appl Algebra Eng Commun Comput 22:219–233
Cao Y (2013) On constacyclic codes over finite chain rings. Finite Fields Appl 24:124–135
Diao L, Gao J, Lu J (2019) Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes. Math Commun. https://doi.org/10.3934/amc.2020029
Dinh H, López-permouth S (2004) Cyclic and negacyclic codes over finite chain rings. IEEE Trans Inf Theory 50:1728–1743
Dinh HQ, Bag T, Upadhyay AK, Ashraf M, Mohammad G, Chinnakum W (2019) Quantum codes from a class of constacyclic codes over finite commutative rings. J Algebra Appl. https://doi.org/10.1142/S0219498821500031
Dinh HQ, Singh AK, Pattanayak S et al (2018) Des Codes Cryptogr 86:1451. https://doi.org/10.1007/s10623-017-0405-x
Esmaeili M, Yari S (2009) Generalized quasi-cyclic codes: structural properties and codes construction. Appl Algebra Eng Commun Comput 20:159–173
Gao J, Shi M, Wu T, Fu F (2016) On double cyclic codes over $\mathbb{Z}_4$. Finite Fields Appl 39:233–250
Gao J, Shen L, Fu F (2016) A Chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields. Cryptogr Commun 8:51–66. https://doi.org/10.1007/s12095-015-0140-y
Gao J, Ma F, Fu F (2017) Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$. Appl Comput Math 6(3):286–295
Gao J, Wang Y, Li J (2018) Bounds on covering radius of linear codes with Chinese Euclidean distance over thefinite non chain ring $\mathbb{F}_2 + v\mathbb{F}_2$. Inform Process Lett 138:22–26
Gao J, Fu F-W, Shen L, Ren W (2014) Some results on generalized quasi-cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$. IEICE Trans Fundamentals 97(4):1005–1011
Grassl M (2020) Online Linear Code Bounds, Available Online at http://www.codetables.de, accessed on
Gursoy F, Siap I, Yildiz B (2014) Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$. Adv Math Commun 8(3):313–322
Hammons A, Kumar P, Calderbank AR, Sloane NJA, Solè P (1994) The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans Inf Theory 40:301–319
Wang Y, Gao J (2019) MacDonald codes over the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$. Comp Appl Math 38:169. https://doi.org/10.1007/s40314-019-0937-y
Yao T, Shi M, Solé Patrick (2015) Double cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. Int J Inf Coding Theory 3(2):145–157
Zhu S, Wang Y, Shi M (2010) Some result on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. IEEE Trans Inf Theory 56:1680–1684
Zhu S, Wang Y (2011) A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and their Gray image. Discret Math Theory 311:2677–2682
Siap I, Kulhan N (2005) The structure of generalized quasi-cyclic codes. Appl Math E-Notes 5:24–30
Shi M, Lu Y (2019) Cyclic DNA codes over $\mathbb{F}_2[u, v]/\langle u^3, v^2 - v, vu - uv\rangle$. Adv Math Commun 13(1):157–164