Computational and Applied Mathematics (2022) 41:172
https://doi.org/10.1007/s40314-022-01872-9

$\mathbb{Z}_2\mathbb{Z}_2[u^4]$-cyclic codes and their duals

B. Srinivasulu[1] · **Padmapani Seneviratne**[1]

Received: 20 May 2021 / Revised: 12 March 2022 / Accepted: 7 April 2022 /
Published online: 11 May 2022

Abstract
In this paper, we study the algebraic structure of a new family of linear codes over the mixed alphabet $\mathbb{Z}_2\mathrm{R}$, where $\mathrm{R} = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + u^3\mathbb{Z}_2,\ u^4 = 0$. We present generator and parity-check matrices of $\mathbb{Z}_2\mathrm{R}$-linear codes in standard form. We define a $\mathbb{Z}_2\mathrm{R}$-cyclic code of length (r, s) as a $\mathrm{R}[x]$-submodule of $\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathrm{R}[x]}{\langle x^s-1\rangle}$ and determine its generator polynomial. Also, we determine the size of a $\mathbb{Z}_2\mathrm{R}$-cyclic code by giving a minimal spanning set. Furthermore, we present the generator polynomial of dual code of a $\mathbb{Z}_2\mathrm{R}$-cyclic code of length (r, s) for odd s, while r is set arbitrary. Finally, optimal binary codes are constructed from Gray images of $\mathbb{Z}_2\mathrm{R}$-cyclic codes.

Keywords $\mathbb{Z}_2\mathbb{Z}_2[u^4]$-cyclic codes · Dual codes · Separable codes

Mathematics Subject Classification 94B05 · 94B15

1 Introduction

In 1973, (Delsarte and Levenshtein 1998) defined additive codes in terms of association schemes as subgroups of the underlying abelian group. These codes are interesting, because their coordinates are partitioned into two parts such that each part is a linear code over different alphabet. Brouwer et al. (1998) have studied mixed binary/ternary error-correcting codes and presented upper and lower bounds for their maximal size. Recently, Borges et al. (2010) have introduced $\mathbb{Z}_2\mathbb{Z}_4$-additive codes as submodules of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, where α and β are positive integers. In Borges et al. (2010), the duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are considered by defining an inner product different from the usual Euclidean inner product. Abualrub et al. (2014) have studied the cyclic structure of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes for the first time, where a minimal spanning set for these codes is presented, and generator polynomials of $\mathbb{Z}_2\mathbb{Z}_4$-

Communicated by Thomas Aaron Gulliver.

✉ B. Srinivasulu
bslu1981@gmail.com

Padmapani Seneviratne
padmapani.seneviratne@tamuc.edu

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

additive codes and their duals codes are determined. Extending the methods given in Borges et al. (2010); Aydogdu and Siap (2015) have studied $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes and presented their generator and parity-check matrices in standard form. Also, generalizing the methods in Borges et al. (2010) and Abualrub et al. (2014), Aydogdu et al. (2017a, b) have studied $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes and $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes. In another work, (Borges et al. 2018) have defined $\mathbb{Z}_2$-double cyclic codes, and obtained the form of generator polynomials of these codes and their duals codes. We note that $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes are generalization of both $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes and $\mathbb{Z}_2$-double cyclic codes. In recent times, various families of linear codes are studied over mixed alphabets and obtained good and some new optimal codes as their Gray images (Borges et al. 2012; Bilal et al. 2011; Diao et al. 2020; Dinh et al. 2020, 2021, 2020; Hou and Gao 2021; Li et al. 2020; Meng and Gao 2021; Rifà-Pous et al. 2011; Yao et al. 2020; Yao and Zhu 2020). Motivated by these studies, in this paper, we study $\mathbb{Z}_2\mathbb{Z}_2[u^4]$-cyclic codes and determine the generator polynomials of $\mathbb{Z}_2\mathbb{Z}_2[u^4]$-cyclic codes and their duals.

2 $\mathbb{Z}_2\mathbb{Z}_2[u^4]$-linear codes

Let $\mathbb{Z}_2 = \{0, 1\}$ be the binary field, and R denotes the commutative ring $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + u^3\mathbb{Z}_2 = \{a + ub + u^2c + u^3d \mid a, b, c, d \in \mathbb{Z}_2\}$, where $u^4 = 0$. R is a finite chain ring with nilpotent element u of index 4. Clearly, R contains $\mathbb{Z}_2$ as a proper subring. We use the notation $\mathbb{Z}_2\mathrm{R} := \mathbb{Z}_2 \times \mathrm{R} = \{(c_1 \mid c_2) \,|c_1 \in \mathbb{Z}_2 \text{ and } c_2 \in \mathrm{R}\}$. $\mathbb{Z}_2\mathrm{R}$ is a commutative group with respect to component wise addition. To multiply the elements of R with the elements of $\mathbb{Z}_2\mathrm{R}$, we consider the mapping $\delta : \mathrm{R} \to \mathbb{Z}_2$ defined by

$$\delta(a + ub + u^2c + u^3d) = a.$$

Clearly, δ is a ring homomorphism. Now, for any $d \in \mathrm{R}$ and $(c_1 \mid c_2) \in \mathbb{Z}_2\mathrm{R}$, define a product '$*$' as $d * (c_1 \mid c_2) = (\delta(d)c_1 \mid dc_2)$. This product is well defined and $\mathbb{Z}_2\mathrm{R}$ is an R-module with respect to the product '$*$'. Extending the product '$*$' to $\mathbb{Z}_2^r \times \mathrm{R}^s$ such that for any $d \in \mathrm{R}$ and $c = (c_{10}, c_{11}, \ldots, c_{1r-1} \mid c_{20}, c_{21}, \ldots, c_{2s-1}) \in \mathbb{Z}_2^r \times \mathrm{R}^s$, we define

$$d * c = (\delta(d)c_{10}, \delta(d)c_{11}, \ldots, \delta(d)c_{1r-1} \mid dc_{20}, dc_{21}, \ldots, dc_{2s-1}).$$

This extended multiplication is also well defined and $\mathbb{Z}_2^r \times \mathrm{R}^s$ is an R-module.

Definition 1 A non-empty subset C of $\mathbb{Z}_2^r \times \mathrm{R}^s$ is called a $\mathbb{Z}_2[u^4]$-linear code of length (r, s) if C is an R-submodule of $\mathbb{Z}_2^r \times \mathrm{R}^s$.

Recall that the Gray map $\phi : \mathrm{R} \mapsto \mathbb{Z}_2^4$ is defined as $\phi(a + bu + cu^2 + du^3) = (a + b + c + d, c + d, b + d, d)$ (Özger et al. 2014). We extend this map component wise to $\Phi : \mathbb{Z}_2^r \times \mathrm{R}^s \mapsto \mathbb{Z}_2^{r+4s}$ such that for any $c = (c_{10}, c_{11}, \ldots, c_{1r-1} \mid c_{20}, c_{21}, \ldots, c_{2s-1}) \in \mathbb{Z}_2^r \times \mathrm{R}^s$,

$$\Phi(c) = (c_{10}, c_{11}, \ldots, c_{1r-1} \mid \phi(c_{20}), \phi(c_{21}), \ldots, \phi(c_{2s-1})).$$

Clearly, Φ is a linear map. Also, if C is a $\mathbb{Z}_2\mathrm{R}$-linear code of length (r, s), then $\Phi(\mathrm{C})$ is a binary linear code of length $r + 4s$.

2.1 Generator and parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_2[u^4]$-linear codes

In this section, we present the generator matrix of a $\mathbb{Z}_2$R-linear code C of length (r, s) in standard form. Here we note that C is a binary linear code of length r when $s = 0$, and an R-linear code of length s when $r = 0$. From the definition of ϕ, we see that R is group isomorphic to $\mathbb{Z}_2^4$. Thus, as an additive group, a $\mathbb{Z}_2$R-linear code C of block length (r, s) is isomorphic to $\mathbb{Z}_2^{k_0} \times \mathbb{Z}_2^{4k_1} \times \mathbb{Z}_2^{3k_2} \times \mathbb{Z}_2^{2k_3} \times \mathbb{Z}_2^{k_4}$. In this case we say that C is of type $(r, s; k_0; k_1, k_2, k_3, k_4)$.

Theorem 1 (Aydogdu 2019) *Let* C *be a* $\mathbb{Z}_2$R*-linear code of type* $(r, s; k_0; k_1, k_2, k_3, k_4)$. *Then* C *is permutation equivalent to a* $\mathbb{Z}_2$R*-linear code with standard generator matrix of the form*

$$G_S = \left(\begin{array}{cc|ccccc} I_{k_o} & \bar{A}_{01} & 0 & 0 & 0 & 0 & u^3T_{01} \\ 0 & S_{01} & I_{k_1} & A_{01} & A_{02} & A_{03} & A_{04} \\ 0 & S_{11} & 0 & uI_{k_2} & uA_{12} & uA_{13} & uA_{14} \\ 0 & S_{21} & 0 & 0 & u^2I_{k_3} & u^2A_{23} & u^2A_{24} \\ 0 & 0 & 0 & 0 & 0 & u^3I_{k_4} & u^3A_{34} \end{array}\right),$$

where S_{01}, S_{11}, S_{21} *are binary matrices and* $A_{01}, A_{02}, A_{03}, A_{04}, A_{12}, A_{13}, A_{14}, A_{23}, A_{24}A_{34}$ *are matrices over* R. *Furthermore,* C *contains* $2^{k_0}2^{4k_1}2^{3k_2}2^{2k_3}2^{k_4}$ *codewords.*

Example 1 Let C be a $\mathbb{Z}_2$R-linear code of length $(2, 5)$ generated by the matrix

$$G = \left(\begin{array}{cc|ccccc} 1 & 1 & 0 & 0 & u^2 & u^2 & u^2 \\ 1 & 1 & 1 & 1 & 0 & 1+u & u+u^3 \\ 0 & 1 & 0 & u & 0 & u+u^2 & u+u^2 \\ 0 & 1 & 0 & u & u^2 & u & u+u^3 \\ 1 & 1 & 0 & 0 & u^2 & u^2+u^3 & u^2+u^3 \end{array}\right).$$

Then, C is permutation equivalent to a $\mathbb{Z}_2$R-linear code with generator matrix in standard form

$$G_s = \left(\begin{array}{cc|ccccc} 1 & 1 & 0 & 0 & 0 & 0 & u^3 \\ 0 & 0 & 1 & 1 & 0 & 1+u & u \\ 0 & 1 & 0 & u & 0 & u+u^2 & u+u^2 \\ 0 & 0 & 0 & 0 & u^2 & u^2 & u^2+u^3 \\ 0 & 0 & 0 & 0 & 0 & u^3 & u^3 \end{array}\right).$$

Clearly, C is of type $(2, 5; 1; 1, 1, 1, 1)$ and contains $2^1 \cdot 2^{4\cdot1} \cdot 2^{3\cdot1} \cdot 2^{2\cdot1} \cdot 2^1 = 2048$ codewords.

Now, we present the standard form of generator matrix of the dual code $\mathrm{C}^\perp$ of a $\mathbb{Z}_2$R-linear code of type $(r, s; k_0; k_1, k_2, k_3, k_4)$. For this, we first define an inner product in $\mathbb{Z}_2^r \times \mathrm{R}^s$.

Definition 2 The inner product of any two elements $x = \left(x_{10}, x_{11}, \ldots, x_{1r-1} \mid x_{20}, x_{21}, \ldots, x_{2s-1}\right)$ and $y = (y_{10}, y_{11}, \ldots, y_{1r-1} \mid y_{20}, y_{21}, \ldots, y_{2s-1})$ in $\mathbb{Z}_2^r \times \mathrm{R}^s$ is defined as

$$[x \cdot y] = u^3\left[\sum_{i=0}^{r-1} x_{1i}\, y_{1i}\right] + \sum_{j=0}^{s-1} x_{2j}\, y_{2j}.$$

Definition 3 The dual code $\mathrm{C}^{\perp}$ of a $\mathbb{Z}_2$R-linear code C is defined as

$$\mathrm{C}^{\perp} = \{y \in \mathbb{Z}_2^r \times \mathrm{R}^s \mid [y \cdot c] = 0 \text{ for all } c \in \mathrm{C}\}.$$

From the definition of $\mathrm{C}^{\perp}$, it is easy to see that $\mathrm{C}^{\perp}$ is also a $\mathbb{Z}_2$R-linear code.

Theorem 2 (Aydogdu 2019) *Let* C *be a* $\mathbb{Z}_2$R*-linear code of type* $(r, s; k_0; k_1, k_2, k_3, k_4)$ *with the generator matrix as in Theorem 1. Then the generator matrix of the dual code* $\mathrm{C}^{\perp}$ *is given by*

$$H_S = \left(\begin{array}{cc|c} \bar{A}'_{01} & I_{r-k_o} & \\ T'_{01} & 0 & \\ 0 & 0 & P \\ 0 & 0 & \\ 0 & 0 & \end{array}\right.$$
$$\left.\begin{array}{ccccc} uA'_{12}S'_{21} + u^2S'_{11} & uS'_{21} & 0 & 0 \\ A'_{12}\left(A'_{23}A'_{34} + A'_{24}\right) + A'_{13}A'_{34} + A'_{14} & A'_{23}A'_{34} + A'_{24} & A'_{34} & I_{s-k_1-k_2-k_3-k_4} \\ u\left(A'_{12}A'_{23} + A'_{13}\right) & uA'_{23} & uI_{k_4} & 0 \\ u^2A'_{12} & u^2I_{k_3} & 0 & 0 \\ u^3I_{k_2} & 0 & 0 & 0 \end{array}\right),$$

where

$$P = \begin{pmatrix} u\left(A'_{01}A'_{12}S'_{21} + A'_{02}S'_{21}\right) + u^2A'_{01}S'_{11} + u^3S'_{01} \\ A'_{01}\left(A'_{12}A'_{23}A'_{34} + A'_{12}A'_{24} + A'_{13}A'_{34} + A'_{14}\right) + A'_{02}\left(A'_{23}A'_{34} + A'_{24}\right) + A'_{03}A'_{34} + A'_{04} \\ u\left(A'_{01}A'_{12}A'_{23} + A'_{01}A'_{13} + A'_{02}A'_{23} + A'_{03}\right) \\ u^2\left(A'_{01}A'_{12} + A'_{02}\right) \\ u^3A'_{01} \end{pmatrix},$$

and M' *denotes the transpose of the matrix* M.

Example 2 Let C be a $\mathbb{Z}_2$R-linear code of type (2, 5; 1; 1, 1, 1, 1) generated by the matrix in standard form

$$G = \left(\begin{array}{cc|ccccc} 1 & 1 & 0 & 0 & 0 & 0 & u^3 \\ 0 & 0 & 1 & 1 & u & 1 & u+u^3 \\ 0 & 1 & 0 & u & u+u^2 & u & u+u^2 \\ 0 & 1 & 0 & 0 & u^2 & u^2 & u^2+u^3 \\ 0 & 0 & 0 & 0 & 0 & u^3 & u^3 \end{array}\right).$$

Then the parity-check matrix of C is

$$H = \left(\begin{array}{cc|ccccc} 1 & 1 & u+u^2 & u & u & 0 & 0 \\ 1 & 0 & 1+u+u^3 & u^2 & u & 1 & 1 \\ 0 & 0 & u & u^2 & u & u & 0 \\ 0 & 0 & u^2 & u^2+u^3 & u^2 & 0 & 0 \\ 0 & 0 & u^3 & u^3 & 0 & 0 & 0 \end{array}\right)$$

and, therefore, $\mathrm{C}^{\perp}$ is of type (2, 5; 1; 1, 1, 1, 1).

3 $\mathbb{Z}_2\mathbb{Z}_2[u^4]$-cyclic codes

In this section, we generalize the Definition 3.1 given in Aydogdu et al. (2017a) and define $\mathbb{Z}_2$R-cyclic codes. A $\mathbb{Z}_2$R-linear code of length (r, s) is cyclic if the simultaneous cyclic shifts of r coordinates and s coordinates leaves the code invariant. Here, we study the structural properties of $\mathbb{Z}_2$R-cyclic codes of length (r, s) by determining their generator polynomials for odd s, while r is set to be arbitrary.

Definition 4 A $\mathbb{Z}_2$R-linear code C of length (r, s) is called a $\mathbb{Z}_2$R-cyclic code if $(c_{1\,r-1}, c_{10}, \ldots, c_{1r-2} \mid c_{2\,s-1}, c_{20}, \ldots, c_{2\,s-2}) \in$ C whenever $(c_{1\,0}, c_{1\,1}, \ldots, c_{1\,r-1} \mid c_{20}, c_{21}, \ldots, c_{2\,s-1}) \in$ C.

Let $\mathrm{R}_{4,r,s}[x] = \frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathrm{R}[x]}{\langle x^s-1\rangle}, \mathbb{Z}_{2,r}[x] = \frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle}$ and $\mathrm{R}_{4,s}[x] = \frac{\mathrm{R}[x]}{\langle x^s-1\rangle}$. Identifying each $c = (c_{1\,0}, c_{1\,1}, \ldots, c_{1\,r-1} \mid c_{20}, c_{21}, \ldots, c_{2\,s-1}) \in \mathbb{Z}_2^r \times \mathrm{R}^s$ with a pair of polynomials $(c_{1\,0} + c_{1\,1}x + \cdots + c_{1\,r-1}x^{r-1} \mid c_{20} + c_{21}x + \cdots + c_{2\,s-1}x^{s-1}) \in$ C, we have a one-one correspondence between $\mathbb{Z}_2^r \times \mathrm{R}^s$ and $\mathrm{R}_{4,r,s}[x]$. Now for any $f(x) = \sum f_i x^i \in \mathrm{R}[x]$ and $(c_1(x) \mid c_2(x)) \in \mathrm{R}_{4,r,s}[x]$, we define the product $f(x) * (c_1(x) \mid c_2(x)) = (\delta(f(x))c_1(x) \mid f(x)c_2(x))$, where $\delta(f(x)) = \sum \delta(f_i)x^i$. Following these notations, it can easily be shown that $\mathrm{R}_{4,r,s}[x]$ is an $\mathrm{R}[x]$-module with respect to the product '$*$'.

Let $c = (c_{1\,0}, c_{1\,1}, \ldots, c_{1\,r-1} \mid c_{20}, c_{21}, \ldots, c_{2\,s-1})$ be an element in $\mathbb{Z}_2^r \times \mathrm{R}^s$ and i be an integer. We denote the ith shift of c by

$$c^{(i)} = (c_{1\,0-i}, c_{1\,1-i}, \ldots, c_{1r-1-i} \mid c_{20-i}, c_{21-i}, \ldots, c_{2\,s-1-i})$$

where the subscripts are taken modulo r and s, respectively. Following these notations, it is easy to see that $x * c(x) = (c_{1\,0}x + c_{1\,1}x^2 + \cdots + c_{1\,r-1}x^r \mid c_{20}x + c_{21}x^2 + \cdots + c_{2\,s-1}x^s) = (c_{1\,r-1} + c_{1\,0}x + \cdots + c_{1\,r-2}x^{r-1} \mid c_{2\,s-1} + c_{20}x + \cdots + c_{2\,s-2}x^{s-1})$, which is the cyclic shift of c in $\mathbb{Z}_2^r \times \mathrm{R}^s$. More generally, $x^i * c(x) = c^{(i)}(x)$. The cyclic codes in the present setting are $\mathrm{R}[x]$-submodules of the residue class ring $\mathrm{R}_{4,r,s}[x]$, in fact they generalize both binary cyclic codes and cyclic codes over R.

Theorem 3 *A $\mathbb{Z}_2$R-linear code* C *of length* (r, s) *is cyclic in* $\mathbb{Z}_2^r \times \mathrm{R}^s$ *if and only if* C *is an* $\mathrm{R}[x]$*-submodule of* $\mathrm{R}_{4,r,s}[x]$.

Let C_r and C_s be the canonical projections of a $\mathbb{Z}_2$R-cyclic code C of length (r, s) on first r coordinates and last s coordinates, respectively. Then, C_r is a binary cyclic code of length r and C_s is a cyclic code of length s over R. These codes are well studied in the literature (MacWilliams and Sloane 1975; Özger et al. 2014). We now extend these known structures and obtain the generator polynomials of a $\mathbb{Z}_2$R-cyclic code by taking the back projection of C_s in $\mathrm{R}_{4,r,s}$.

Now onward s denote an odd integer and r an arbitrary integer. Also, we denote the gcd of two polynomials $f(x)$ and $g(x)$ by $(f(x), g(x))$. The following result gives the form of generator polynomials of cyclic codes of odd length over R.

Theorem 4 (Özger et al. 2014) *Let* C *be a cyclic code of length n over* R*, n odd. Then,* $\mathrm{C} = \langle g(x), ua_1(x), u^2a_2(x), u^3a_3(x)\rangle = \langle g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\rangle$*, where $g(x), a_1(x), a_2(x)$ and $a_3(x)$ are binary polynomials such that* $a_3(x)\big|a_2(x)\big|a_1(x)\big|g(x)\big|(x^n - 1)$.

The following result gives the generator polynomials for a $\mathbb{Z}_2$R-cyclic code C of length (r, s).

Theorem 5 *Let* C *be a $\mathbb{Z}_2$R-cyclic code* C *of length* (r, s)*. Then,* $\mathrm{C} = \Big\langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\Big\rangle$*, where $f(x), l(x), g(x), a_1(x), a_2(x)$ and $a_3(x)$ are binary polynomials such that* $a_3(x)\big|a_2(x)\big|a_1(x)\big|g(x)\big|(x^s - 1)$ *and* $f(x)\big|(x^r - 1)$.

Proof Consider the projection mapping $\pi : \mathrm{C} \to \mathrm{R}_{4,s}[x]$ such that $(c_1(x) \mid c_2(x)) \mapsto c_2(x)$. Clearly π is an $\mathrm{R}[x]$-module homomorphism with kernel $\ker(\pi) = \{(a(x) \mid 0) \in \mathrm{C} \mid a(x) \in$

$\mathbb{Z}_{2,r}[x]\}$. Since $\mathbb{Z}_{2,r}[x]$ is a principal ideal ring, the set $K = \{a(x) \in \mathbb{Z}_{2,r}[x] \mid (a(x) \mid 0) \in \mathrm{C}\}$ is a principal ideal. Therefore, there exists $f(x) \in \mathbb{Z}_{2,r}[x]$, $f(x)\big|(x^r - 1)$ such that $K = \langle f(x)\rangle$, and therefore, $\ker(\pi) = \langle (f(x) \mid 0)\rangle$. On the other hand, the homomorphic image of C under π is an ideal of $\mathrm{R}_{4,s}[x]$. From Theorem 4, we have $\pi(\mathrm{C}) = \langle g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\rangle$. This implies $(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)) \in \mathrm{C}$ for some $l(x) \in \mathbb{Z}_{2,r}[x]$. Therefore, $\langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle \subseteq \mathrm{C}$. To show $\mathrm{C} \subseteq \langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle$, let $(p_1(x) \mid p_2(x)) \in \mathrm{C}$. This implies $p_2(x) \in \mathrm{C}_s$ and $p_2(x) = \lambda(x)(g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))$ for some $\lambda(x) \in \mathrm{R}[x]$. Furthermore,

$$\begin{aligned}
&(p_1(x) \mid p_2(x)) - \lambda(x)(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)) \\
&= (p_1(x) - \lambda(x)l(x) \mid 0) \\
&= \lambda'(x)(f(x) \mid 0),
\end{aligned}$$

for some $\lambda'(x) \in \mathbb{Z}_2[x]$. This implies $(p_1(x) \mid p_2(x)) \in \langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle$, and therefore, $\mathrm{C} \subseteq \langle (f \mid 0), (l \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle$. □

Remark 1 From Theorem 5, it is obvious that $f(x)$ is a monic polynomial of least degree such that $(f(x) \mid 0) \in \mathrm{C}$. Also, for any $(a(x) \mid 0) \in \mathrm{C}$, $f(x)$ divides $a(x)$.

Theorem 6 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2\mathrm{R}$*-cyclic code of length* (r, s)*. Then,* $f(x)$ *divides* $\frac{x^s-1}{a_3(x)}l(x)$.

Proof Consider

$$\begin{aligned}
\frac{x^s - 1}{a_3(x)}\left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right) &= \left(\delta\left(\frac{x^s - 1}{a_3(x)}\right)l(x) \,\middle|\, 0\right) \\
&= \left(\frac{x^s - 1}{a_3(x)}l(x) \,\middle|\, 0\right) \in \mathrm{C}.
\end{aligned}$$

This implies that $f(x)$ divides $\frac{x^s-1}{a_3(x)}l(x)$ from Remark 1. □

Corollary 1 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2\mathrm{R}$*-cyclic code of length* (r, s)*. Then,* $f(x)$ *divides* $\frac{x^s-1}{a_3(x)}(l(x), f(x))$.

Theorem 7 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2\mathrm{R}$*-cyclic code of length* (r, s)*. Then* $deg(l(x)) < deg(f(x))$.

Proof Assume $\deg(l(x)) \geq \deg(f(x))$. Since $f(x)$ is a monic polynomial, we can apply division algorithm. To that end, there exist polynomials $q(x)$ and $r(x)$ in $\mathbb{Z}_2[x]$ such that $l(x) = f(x)q(x) + r(x)$, where $r(x) = 0$ or $0 \leq \deg(r(x)) < \deg(f(x))$. Therefore

$$\begin{aligned}
&\langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle \\
&\quad = \langle (f(x) \mid 0), (f(x)q(x) + r(x) \mid g(x) + ua_1(x) \\
&\qquad + u^2a_2(x) + u^3a_3(x))\rangle \\
&\quad = \langle (f(x) \mid 0), q(x)(f(x) \mid 0) + (r(x) \mid g(x) + ua_1(x) \\
&\qquad + u^2a_2(x) + u^3a_3(x))\rangle \\
&\quad = \langle (f(x) \mid 0), (r(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle.
\end{aligned}$$

As $\deg(r(x)) < \deg(f(x))$, we may assume that $\deg(l(x)) < \deg(f(x))$. □

The following result present a minimal spanning set for a $\mathbb{Z}_2$R-cyclic code that given in Theorem 5.

Theorem 8 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *such that* $g(x)h(x) = x^s - 1, g(x) = a_1(x)b_1(x), a_1(x) = a_2(x)b_2(x)$ *and* $a_2(x) = a_3(x)b_3(x)$*. Then,* $S = S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5$ *forms a minimal spanning set for* C *as an* $\mathrm{R}[x]$*-submodule of* $\mathrm{R}_{4,r,s}$*, where*

$$
\begin{aligned}
S_1 &= \bigcup_{i=0}^{r-deg(f)-1} x^i * (f \mid 0)\\
S_2 &= \bigcup_{i=0}^{s-deg(g)-1} x^i * \left(l \mid g + ua_1 + u^2a_2 + u^3a_3\right)\\
S_3 &= \bigcup_{i=0}^{deg(g)-deg(a_1)-1} x^i * \left(lh \mid ua_1h + u^2a_2h + u^3a_3h\right)\\
S_4 &= \bigcup_{i=0}^{deg(a_1)-deg(a_2)-1} x^i * \left(lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1\right)\\
S_5 &= \bigcup_{i=0}^{deg(a_2)-deg(a_3)-1} x^i * \left(lhb_1b_2 \mid u^3a_3hb_1b_2\right).
\end{aligned}
$$

Proof Let c be a codeword in C. Then there exist d_1 and d_2 in $\mathrm{R}[x]$ such that

$$
\begin{aligned}
c &= d_1 * (f \mid 0) + d_2 * (l \mid g + ua_1 + u^2a_2 + u^3a_3)\\
&= (\delta(d_1)f \mid 0) + d_2 * (l \mid g + ua_1 + u^2a_2 + u^3a_3). \qquad (1)
\end{aligned}
$$

We first show that $d_1 * (f \mid 0) \in \mathrm{span}(S_1)$. If $\deg(\delta(d_1)) < r - \deg(f)$, then $d_1 * (f_1 \mid 0) \in \mathrm{span}(S_1)$. Otherwise, by division algorithm, there exist $q_1, r_1 \in \mathbb{Z}_2[x]$ such that $\delta(d_1) = q_1\frac{x^r-1}{f} + r_1$ with $r_1 = 0$ or $0 \le \deg(r_1) < r - \deg(f)$. Then

$$
\begin{aligned}
(\delta(d_1)f \mid 0) &= \left(\left(q_1\frac{x^r-1}{f} + r_1\right) f \mid 0\right)\\
&= (q_1(x^r - 1) + r_1 f \mid 0)\\
&= q_1(x^r - 1 \mid 0) + r_1(f \mid 0)\\
&= r_1(f \mid 0) \in \mathrm{span}(S_1).
\end{aligned}
$$

If $\deg(d_2) < s - \deg(g)$, then $d_2 * (l \mid g + ua_1 + u^2a_2 + u^3a_3) \in \mathrm{span}(S_2)$ and $c \in \mathrm{span}(S)$. Otherwise, by division algorithm, we have $d_2 = q_2h + r_2$ with $r_2 = 0$ or $0 \le \deg(r_2) < s - \deg(g)$, $q_2, r_2 \in \mathrm{R}[x]$. Therefore

$$
\begin{aligned}
d_2 * (l \mid g + ua_1 + u^2a_2 + u^3a_3) &= (q_2h + r_2)(l \mid g + ua_1 + u^2a_2 + u^3a_3)\\
&= q_2 * (lh \mid ua_1h + u^2a_2h + u^3a_3h)\\
&\quad + r_2 * (l \mid g + ua_1 + u^2a_2 + u^3a_3).
\end{aligned}
$$

Since $\deg(r_2) < s - \deg(g)$, $r_2 * (l \mid g + ua_1 + u^2a_2 + u^3a_3) \in \mathrm{span}(S_2)$. Also, if $\deg(q_2) < \deg(g) - \deg(a_1)$, $q_2 * (lh \mid ua_1h + u^2a_2h + u^3a_3h) \in \mathrm{span}(S_3)$, and therefore, $c \in \mathrm{span}(S)$.

Otherwise, compute $q_2 = q_3b_1 + r_3$, where $r_3 = 0$ or $0 \leq \deg(r_3) < \deg(g) - \deg(a_1)$. Then

$$\begin{aligned} q_2 * (lh \mid ua_1h + u^2a_2h + u^3a_3h) &= (q_3b_1 + r_3) * (lh \mid ua_1h + u^2a_2h + u^3a_3h) \\ &= q_3 * (lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1) \\ &\quad + r_3 * (lh \mid ua_1h + u^2a_2h + u^3a_3h) \end{aligned}$$

Clearly, $r_3 * (lh \mid ua_1h + u^2a_2h + u^3a_3h) \in \text{span}(S_3)$. If $\deg(q_3) < \deg(a_1) - \deg(a_2)$, then $q_3 * (lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1) \in \text{span}(S_4)$, and therefore, $c \in \text{span}(S)$. Otherwise, compute $q_3 = q_4b_2 + r_4$ with $r_4 = 0$ or $0 \leq \deg(r_4) < \deg(a_1) - \deg(a_2)$. Then

$$\begin{aligned} q_3 * (lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1) &= (q_4b_2 + r_4) * (lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1) \\ &= q_4 * (lhb_1b_2 \mid u^3a_3hb_1b_2) \\ &\quad + r_4 * (lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1) \end{aligned}$$

Again, since $\deg(r_4) < \deg(a_1) - \deg(a_2)$, $r_4 * (lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1) \in span(S_4)$. Now, we show $q_4 * (lhb_1b_2 \mid u^3a_3hb_1b_2) \in \text{span}(S_1 \cup S_5)$. If $\deg(q_4) < \deg(a_2) - \deg(a_3)$ then we are done. Otherwise, compute $q_4 = q_5b_3 + r_5$ with $r_5 = 0$ or $0 \leq \deg(r_5) < \deg(a_2) - \deg(a_3)$. This implies that

$$\begin{aligned} q_4 * (lhb_1b_2 \mid u^3a_3hb_1b_2) &= (q_5b_3 + r_5) * (lhb_1b_2 \mid u^3a_3hb_1b_2) \\ &= q_5 * (lhb_1b_2b_3 \mid 0) + r_5 * (lhb_1b_2 \mid u^3a_3hb_1b_2). \end{aligned}$$

Since $x^s - 1 = a_3b_1b_2b_3h$, and $f \left| \frac{x^s-1}{a_3} \right.$ (from Theorem 6), we have $q_5 * (lhb_1b_2b_3 \mid 0) \in span(S_1)$. Also, since $r_5 * (lhb_1b_2 \mid u^3a_3hb_1b_2) \in span(S_5)$, we finally see $c \in span(S)$. Therefore, C is spanned by S. □

Corollary 2 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code such that* $f(x)\left|(x^r - 1), a_3(x)\right|a_2(x)\left|a_1(x)\right|g(x)\left|(x^s - 1)\right.$. *Then,*

$$|\mathrm{C}| = 2^{r-deg(f)}16^{s-deg(g)}8^{deg(g)-deg(a_1)}4^{deg(a_1)-deg(a_2)}2^{deg(a_2)-deg(a_3)}.$$

Corollary 3 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code such that* $f(x)\left|(x^r - 1), a_3(x)\right|a_2(x)\left|a_1(x)\right|g(x)\left|(x^s - 1)\right.$ *and* $\mathrm{C}^\perp$ *be its dual code. Then*

$$|\mathrm{C}^\perp| = 2^{deg(f)}16^{deg(a_3)}8^{deg(a_2)-deg(a_3)}4^{deg(a_1)-deg(a_2)}2^{deg(g)-deg(a_1)}.$$

Proof The result follows as $|\mathrm{C}| = 2^{r-\deg(f)}16^{s-\deg(g)}8^{\deg(g)-\deg(a_1)}4^{\deg(a_1)-\deg(a_2)}2^{\deg(a_2)-\deg(a_3)}$ from Corollary 2 and $|\mathrm{C}||\mathrm{C}^\perp| = 2^r16^s$. □

Note that, if $\mathrm{C} = \langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle$ is a $\mathbb{Z}_2$R-cyclic code of length (r, s), then the canonical projection C_s is an R-cyclic code generated by $g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)$. Also, it can easily be seen that the spanning set of an R-cyclic codes of odd length given in Özger et al. (2014) is a special case of Theorem 8 for $r = 0$.

Theorem 9 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of type* $(r, s; k_0; k_1, k_2, k_3, k_4)$ *such that* $f(x)\left|(x^r - 1), a_3(x)\right|a_2(x)\left|a_1(x)\right|g(x)\left|(x^s - 1)\right.$. *Then,* $k_0 = r - deg(f, lhb_1b_2)$, $k_1 = s - deg(g)$, $k_2 = deg(g) - deg(a_1)$, $k_3 = deg(a_1) - deg(a_2)$ *and* $k_4 = deg(a_2) - deg(a_3) - deg(f) + deg(f, lhb_1b_2)$.

Proof From Theorems 1 and 8, we have k_0 is the dimension of the projection of the space generated by $(f \mid 0)$ and $\left(lhb_1b_2 \mid u^3a_3hb_1b_2\right)$ on first r coordinates. Clearly, the polynomials f and lhb_1b_2 generates this space. Since the projection of $\mathrm{R}_{4,r,s}$ on first r coordinates is a principal ideal in $\mathbb{Z}_{2,r}[x]$, the monic polynomial (f, lhb_1b_2) generates this projection space. Thus, $k_0 = r - \deg(f, lhb_1b_2)$. Furthermore, the parameters k_1, k_2 and k_3 are clear from Theorem 8. Finally, as $|\mathrm{C}| = 2^{r-\deg(f)}16^{s-\deg(g)}8^{\deg(g)-\deg(a_1)}4^{\deg(a_1)-\deg(a_2)}2^{\deg(a_2)-\deg(a_3)} = 2^{k_0}16^{k_1}8^{k_2}4^{k_3}2^{k_4}$, we have $k_4 = \deg(a_2) - \deg(a_3) - \deg(f) + \deg(f, lhb_1b_2)$. □

4 Duals of $\mathbb{Z}_2\mathbb{Z}_2[u^4]$-cyclic codes

In this section, we study the structure of duals of $\mathbb{Z}_2$R-cyclic codes. We determine the generator polynomials of these codes. The following result shows that the dual of a $\mathbb{Z}_2$R-cyclic code is also cyclic.

Theorem 10 *Let* C *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *and* $\mathrm{C}^\perp$ *be its dual. Then* $\mathrm{C}^\perp$ *is also a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s)*. Furthermore,* $\mathrm{C}^\perp = \left\langle \left(\hat{f}(x) \mid 0\right), \left(\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)\right)\right\rangle$*, where* $\hat{f}(x), \hat{g}(x), \hat{l}(x), \hat{a}_1(x), \hat{a}_2(x), \hat{a}_3(x) \in \mathbb{Z}_2[x]$ *with* $\hat{f}(x) \big| (x^r - 1)$ *and* $\hat{a}_3(x) \big| \hat{a}_2(x) \big| \hat{a}_1(x) \big| \hat{g}(x) \big| (x^s - 1)$.

Proof Let $v_1 = (a_{10}, a_{11}, \ldots, a_{1r-1} \mid b_{10}, b_{11}, \ldots, b_{1s-1}) \in \mathrm{C}$ and $v_2 = (a_{20}, a_{21}, \ldots, a_{2r-1} \mid b_{20}, b_{21}, \ldots, b_{2s-1}) \in \mathrm{C}^\perp$. Since $v_1 \in \mathrm{C}$ and C is cyclic, we have $(v_1)^{(m-1)} \in \mathrm{C}$, where $m = \mathrm{lcm}\{r, s\}$. Then

$$\begin{aligned}
0 &= [(v_1)^{(m-1)} \cdot v_2] \\
&= u^3(a_{11}a_{20} + \cdots + a_{1r-1}a_{2r-2} + a_{10}a_{2r-1}) \\
&\quad + (b_{11}b_{20} + \cdots + b_{1s-1}b_{2s-2} + b_{10}b_{2s-1}) \\
&= u^3(a_{10}a_{2r-1} + a_{11}a_{20} + \cdots + a_{1r-1}a_{2r-2}) \\
&\quad + (b_{10}b_{2s-1} + b_{11}b_{20} + \cdots + b_{1s-1}b_{2s-2}) \\
&= [v_1 \cdot v_2^{(1)}].
\end{aligned}$$

As v_1 is an arbitrary element of C, $v_2^{(1)} \in \mathrm{C}^\perp$. Therefore, $\mathrm{C}^\perp$ is a $\mathbb{Z}_2$R-cyclic code. □

Let $f(x) = f_0 + f_1x + \cdots + f_nx^n$, $f_n \neq 0$ be a polynomial of degree n. Then, the reciprocal polynomial $f^*(x)$ of $f(x)$ is defined as $f^*(x) = f_n + f_{n-1}x + \cdots + f_0x^n$, i.e., $f^*(x) = x^n f(1/x)$.

Theorem 11 (Srinivasulu and Bhinthwal 2017) *Let* f *and* g *be two binary polynomials such that* $\deg(f) \geq \deg(g)$*. Then*

1. $\deg(f) \geq \deg(f^*)$*, and equality holds if* $x \nmid f$*;*
2. $(fg)^* = f^*g^*$*;*
3. $(f + g)^* = f^* + x^{\deg(f)-\deg(g)}g^*$*;*
4. $g \mid f \Rightarrow g^* \mid f^*$ *and*
5. $(f, g)^* = (f^*, g^*)$.

Let $m = \mathrm{lcm}(r, s)$ and $\theta_m(x) = \sum_{i=0}^{m-1} x^i$. Then it is easy to show that $x^m - 1 = (x^r - 1)\theta_{\frac{m}{r}}(x^r) = (x^s - 1)\theta_{\frac{m}{s}}(x^s)$. Similar to (, Borges2010, Definition 4.3) now we define a bilinear map ψ and study the orthogonal properties of elements of $\mathrm{R}_{4,r,s}[x]$ under ψ.

Definition 5 Let $v_1(x) = (a_1(x) \mid b_1(x))$ and $v_2(x) = (a_2(x) \mid b_2(x))$ be any two elements in $\mathrm{R}_{4,r,s}[x]$. Let $\psi : \mathrm{R}_{4,r,s}[x] \times \mathrm{R}_{4,r,s}[x] \mapsto \frac{\mathrm{R}[x]}{\langle x^m-1\rangle}$ be a mapping, such that

$$\psi(v_1(x), v_2(x)) = u^3 a_1(x)\theta_{\frac{m}{r}}(x^r)x^{m-1-deg(a_2(x))}a_2^*(x) + b_1(x)\theta_{\frac{m}{s}}(x^s)x^{m-1-deg(b_2(x))}b_2^*(x) \ \ mod(x^m-1).$$

Lemma 1 *Let $v_1 = (a_1 \mid b_1)$ and $v_2 = (a_2 \mid b_2)$ be elements in $\mathbb{Z}_2^r \times \mathrm{R}^s$ with associated polynomials $v_1(x) = (a_1(x) \mid b_1(x))$ and $v_2(x) = (a_2(x) \mid b_2(x))$ in $\mathrm{R}_{4,r,s}[x]$. Then v_1 is orthogonal to v_2 and all its cyclic shifts if and only if $\psi(v_1(x), v_2(x)) = 0$.*

Proof Let $v_1 = (a_{10}, a_{11}, \ldots, a_{1r-1} \mid b_{10}, b_{11}, \ldots, b_{1s-1})$, $v_2 = (a_{20}, a_{21}, \ldots, a_{2r-1} \mid b_{20}, b_{21}, \ldots,$
$b_{2s-1}) \in \mathbb{Z}_2^r \times \mathrm{R}^s$, and $v_2^{(i)} = (a_{20-i}, a_{21-i}, \ldots, a_{2r-1-i} \mid b_{20-i}, b_{21-i}, \ldots, b_{2s-1-i})$ be the i-th shift of v_2. Then, $v_1 \cdot v_2^{(i)} = 0$ if and only if $u^3 \sum_{j=0}^{r-1} a_{1j}a_{2j-i} + \sum_{k=0}^{s-1} b_{1k}b_{2k-i} = 0$. Now, from the definition of ψ, we have

$$\begin{aligned}\psi(v_1(x), v_2(x)) &= u^3 \sum_{e=0}^{r-1}\left(\theta_{\frac{m}{r}}(x^r)\sum_{j=0}^{r-1} a_{1j}a_{2j-e}x^{m-1-e}\right) + \sum_{t=0}^{s-1}\left(\theta_{\frac{m}{s}}(x^s)\sum_{k=0}^{s-1} b_{1k}b_{2k-t}x^{m-1-t}\right)\\ &= \theta_{\frac{m}{r}}(x^r)\left(u^3\sum_{e=0}^{r-1}\sum_{j=0}^{r-1} a_{1j}a_{2j-e}x^{m-1-e}\right) + \theta_{\frac{m}{s}}(x^s)\left(\sum_{t=0}^{s-1}\sum_{k=0}^{s-1} b_{1k}b_{2k-t}x^{m-1-t}\right) \qquad (2)\end{aligned}$$

Rearranging the terms in (2) and denoting the summation: $u^3 \sum_{j=0}^{r-1} a_{1j}a_{2j-i} + \sum_{k=0}^{s-1} b_{1k}b_{2k-i}$ by S_i, we get

$$\psi(v_1(x), v_2(x)) = \sum_{i=0}^{m-1} S_i x^{m-1-k} \mod (x^m-1).$$

Therefore, $\psi(v_1(x), v_2(x)) = 0$ if and only if $S_i = 0$ for all $0 \le i \le m-1$. The result follows as $v_1 \cdot v_2^{(i)} = S_i, 0 \le i \le m-1$. □

The following result is a straightforward generalization of [Borges et al. (2010), Lemma 2].

Lemma 2 *Let $v_1(x) = (a_1(x) \mid b_1(x))$ and $v_2(x) = (a_2(x) \mid b_2(x))$ be any two elements in $\mathrm{R}_{4,r,s}[x]$ such that $\psi\ (v_1(x), v_2(x)) = 0$.*

1. *If $a_1(x) = 0$ or $a_2(x) = 0$, then $b_1(x)b_2^*(x) = 0 \bmod (x^s-1)$.*
2. *If $b_1(x) = 0$ or $b_2(x) = 0$, then $a_1(x)a_2^*(x) = 0 \bmod (x^r-1)$.*

Proof Let $a_1(x) = 0$ or $a_2(x) = 0$. Then $\psi\ (v_1(x), v_2(x)) = 0 + b_1(x)\theta_{\frac{m}{s}}(x^s)x^{m-\deg(b_2(x))-1}$ $b_2^*(x) = 0 \bmod (x^m-1)$. This implies that $b_1(x)\theta_{\frac{m}{s}}(x^s)x^{m-\deg(b_2(x))-1}b_2^*(x) = (x^m-1)g(x)$ for some $g(x) \in \mathbb{Z}_2[x]$. Taking $f(x) = x^{\deg(b_2(x))+1}g(x)$, we get $b_1(x)\theta_{\frac{m}{s}}(x^s)x^m b_2^*(x) =$

$f(x)(x^m-1)$, and therefore, $b_1(x)(x^m-1)x^m b_2^*(x) = (x^m-1)(x^s-1)f(x)$. Since x and x^s-1 are relatively prime, we have $b_1(x)b_2^*(x) = 0 \bmod (x^s-1)$. Part (2) can be proved similarly. □

Theorem 12 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s)*, where* $gh = x^s - 1, g = a_1b_1, a_1 = a_2b_2$ *and* $a_2 = a_3b_3$*. Then*

1. $\frac{(f,hl)}{(f,l)}l \in \langle f, hl\rangle$;
2. $\frac{(f,hlb_1)}{(f,hl)}hl \in \langle f, hlb_1\rangle$ *and*
3. $\frac{(f,hlb_1b_2)}{(f,hlb_1)}hlb_1 \in \langle f, hlb_1b_2\rangle$.

Proof Let $hlb_1 = (f, hlb_1)\,t_1$ and $f = (f, hlb_1b_2)\,t_2$. Then, there exist $t_3 \in \mathbb{Z}_2[x]$ such that $hlb_1b_2 = (f,\ hlb_1b_2)\,t_1t_3$ with $(t_2, t_3) = 1$. This in turns gives $p_1t_2 + p_2t_3 = 1$ for some $p_1, p_2 \in \mathbb{Z}_2[x]$. Thus, $p_1\frac{f}{(f,hlb_1b_2)} + p_2\frac{hlb_1b_2}{(f,hlb_1b_2)t_1} = 1$, and therefore, $p_1ft_1 + p_2hlb_1b_2 = \frac{(f,hlb_1b_2)}{(f,hlb_1)}hlb_1$. Hence, $\frac{(f,hlb_1b_2)}{(f,hlb_1)}hlb_1 \in \langle f, hlb_1b_2\rangle$. Similarly, we can see that $\frac{(f,hl)}{(f,l)}l \in \langle f, hl\rangle$ and $\frac{(f,hlb_1)}{(f,hl)}hl \in \langle f, hlb_1\rangle$. □

Theorem 13 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *and* $\mathrm{C}^\perp = \left\langle \left(\hat{f}(x) \mid 0\right), \left(\hat{l}(x) \mid \hat{g}(x)+u\hat{a}_1(x)+u^2\hat{a}_2(x)+u^3\hat{a}_3(x)\right)\right\rangle$ *be the dual code of* C*. Then*

$$\hat{f}(x) = \frac{x^r-1}{(f(x), l(x))^*}.$$

Proof Let C_r be the projection of C on first r coordinates. Then $\mathrm{C}_r = \langle f, l\rangle$, which is cyclic in $\mathbb{Z}_2[x]/\langle x^r-1\rangle$. Since $\mathbb{Z}_2[x]/\langle x^r-1\rangle$ is a principal ideal ring, $\mathrm{C}_r = \langle (f, l)\rangle$, and therefore, $(\mathrm{C}_r)^\perp = \left\langle \frac{x^r-1}{(f,l)^*}\right\rangle$. From the definition of the dual, we have, for any $(a \mid b) \in \mathrm{C}$, $\psi((\hat{f} \mid 0), (a \mid b)) = 0 \bmod (x^m-1)$. This implies that $\hat{f}a^* = 0 \bmod (x^r-1)$. Thus $\hat{f} \in (\mathrm{C}_r)^\perp$ and $\frac{x^r-1}{(f,l)^*}$ divides $\hat{f}$. On the other hand, as $\hat{f}f^* = 0 \bmod (x^r-1)$ and $\hat{f}l^* = 0 \bmod (x^r-1)$ implies that $\hat{f}(f, l)^* = 0 \bmod (x^r-1)$. Hence $\hat{f}$ divides $\frac{x^r-1}{(f,l)^*}$, and therefore, $\hat{f} = \frac{x^r-1}{(f,l)^*}$. □

Theorem 14 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *and* $\mathrm{C}^\perp = \left\langle \left(\hat{f}(x) \mid 0\right), \left(\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)\right)\right\rangle$ *be the dual code of* C*. Then*

$$\hat{g}(x) = \frac{(x^s-1)(f(x), l(x)h(x)b_1(x)b_2(x))^*}{f^*(x)a_3^*(x)}.$$

Proof Since $(0 \mid u^3g) = (0 \mid u^3a_3b_1b_2b_3), (0 \mid u^3a_1h) = (0 \mid u^3a_3b_2b_3h) \in \mathrm{C}$ and $(b_1, h) = 1$, we have $(0 \mid u^3a_3b_2b_3) \in \mathrm{C}$. Again, as $(0 \mid u^3a_2b_1h) = (0 \mid u^3a_3b_1b_3h) \in \mathrm{C}$ and $(b_2, b_1h) = 1$, we have $(0 \mid u^3a_3b_3) \in \mathrm{C}$. Finally, as $(lhb_1b_2 \mid u^3a_3b_1b_2h) \in \mathrm{C}$ and $(b_3, b_1b_2h) = 1$, there exist $p \in Z_2[x]$ such that $(lhb_1b_2p \mid u^3a_3) \in \mathrm{C}$, and therefore, $\left(0 \mid u^3\frac{f}{(f,lhb_1b_2)}a_3\right) \in \mathrm{C}$.

Now, from definition of ψ and from Lemma 1, we have

$$\psi\left((\hat{l} \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)), \left(0 \mid u^3\frac{f}{(f,lhb_1b_2)}a_3\right)\right)$$

$$= 0 \mod (x^m - 1). \tag{3}$$

Furthermore, from Lemma 2, (3) is equivalent to

$$\hat{g}\frac{f^*}{(f, lhb_1b_2)^*}a_3^* = 0 \mod (x^s - 1).$$

Therefore

$$\hat{g} = \frac{(x^s - 1)(f, lhb_1b_2)^*}{f^*a_3^*}.$$

□

Remark 2 From Theorem 4, we have $\mathrm{C} = \langle g + ua_1 + u^2a_2 + u^3a_3\rangle = \langle g, ua_1, u^2a_2, u^3a_3\rangle$. Thus $u^ia_i = m_i(g + ua_1 + u^2a_2 + u^3a_3)$, for some $m_i \in \mathrm{R}[x],\ i = 1, 2, 3$.

Theorem 15 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *and* $\mathrm{C}^\perp = \left\langle \left(\hat{f}(x) \mid 0\right), \left(\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)\right)\right\rangle$ *be the dual code of* C*. Then,*

$$\hat{a}_1(x) = \frac{(x^s - 1)(f(x), l(x)h(x)b_1(x))^*}{a_2^*(x)(f(x), l(x)h(x)b_1(x)b_2(x))^*}.$$

Proof From Theorem 12 part (3), we have $\frac{(f,hlb_1b_2)}{(f,hlb_1)}hlb_1 = P_1f + Q_1hlb_1b_2$, for some $P_1, Q_1 \in \mathbb{Z}_2[x]$. Thus, $(f \mid 0)$, $(lhb_1 \mid u^2a_2hb_1 + u^3a_3hb_1)$, $(lhb_1b_2 \mid u^3a_3hb_1b_2) \in \mathrm{C}$ implies that $\left(0 \mid \frac{(f,lhb_1b_2)}{(f,lhb_1)}\left[u^2a_2hb_1 + u^3a_3hb_1\right] + u^3a_3hb_1b_2Q_1\right) \in \mathrm{C}$. Since $(0 \mid u^2a_1h + u^3a_2h) \in \mathrm{C}$ and $(a_1, b_1) = 1$, we have $\left(0 \mid \frac{(f,lhb_1b_2)}{(f,lhb_1)}\left[u^2a_2h\right] + u^3Q'\right) \in \mathrm{C}$, for some polynomial $Q' \in \mathrm{C}$. Again, as $(0 \mid u^2g + u^3a_1) \in \mathrm{C}$ and $(g, h) = 1$ implies that $\left(0 \mid \frac{(f,lhb_1b_2)}{(f,lhb_1)}\left[u^2a_2\right] + u^3Q\right) \in \mathrm{C}$, for some $Q \in \mathrm{C}$. Also, there exist $\hat{m}_1 \in \mathrm{R}[x]$ such that $(\delta(\hat{m}_1)l \mid \hat{m}_1(\hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3)) = (\delta(\hat{m}_1) \mid u\hat{a}_1) \in \mathrm{C}^\perp$.

Now, by Lemma 1, we have $\psi\left((\delta(\hat{m}_1) \mid u\hat{a}_1), \left(0 \mid \frac{(f,lhb_1b_2)}{(f,lhb_1)}\left[u^2a_2\right] + u^3Q\right)\right) = 0 \mod (x^m - 1)$. This is equivalent to

$$\hat{a}_1\frac{(f, lhb_1b_2)^*}{(f, lhb_1)^*}a_2^* = 0 \mod (x^s - 1).$$

Therefore

$$\hat{a}_1 = \frac{(x^s - 1)(f, lhb_1)^*}{a_2^*(f, lhb_1b_2)^*}.$$

□

Theorem 16 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *and* $\mathrm{C}^\perp = \left\langle \left(\hat{f}(x) \mid 0\right), \left(\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)\right)\right\rangle$ *be the dual code of* C*. Then,*

$$\hat{a}_2(x) = \frac{(x^s - 1)(f(x), l(x)h(x))^*}{a_1^*(x)(f(x), l(x)h(x)b_1(x))^*}.$$

Proof Again, from Theorem 12 part (2), we have $\frac{(f,lhb_1)}{(f,lh)}lh = P_2 f + Q_2 lhb_1$, for some $P_2, Q_2 \in \mathbb{Z}_2[x]$. Thus, $(f \mid o)$, $(lh \mid ua_1h+u^2a_2h+u^3a_3h)$, $(lhb_1 \mid u^2a_2hb_1+u^3a_3hb_1) \in$ C implies $\left(0 \mid \frac{(f,lhb_1)}{(f,lh)}\left[ua_1h+ u^2a_2h+u^3a_3h\right] + Q_2\left[u^2a_2hb_1+u^3a_3hb_1\right]\right) \in$ C. Since $(0 \mid ug + u^2a_1 + u^3a_2) \in$ C and $(g,h) = 1$, we get $\left(0 \mid \frac{(f,lhb_1)}{(f,lh)}[ua_1] + u^2Q''\right) \in$ C, for some Q'' in R$[x]$. Also, there exist $\hat{m}_2 \in$ R$[x]$ (from Remark 2) such that $(\delta(\hat{m}_2)l \mid \hat{m}_2(\hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3)) = (\delta(\hat{m}_2) \mid u^2\hat{a}_2) \in \mathrm{C}^{\perp}$. Therefore, from Lemma 1, we have $\psi\left((\delta(\hat{m}_2) \mid u^2\hat{a}_2), \left(0 \mid \frac{(f,lhb_1)}{(f,lh)}[ua_1] + u^2Q''\right)\right) = 0 \mod (x^m-1)$, which is further equivalent to

$$\hat{a}_2\frac{(f,lhb_1)^*}{(f,lh)^*}a_1^* = 0 \mod (x^s-1).$$

Thus,

$$\hat{a}_2 = \frac{(x^s-1)(f,lh)^*}{a_1^*(f,lhb_1)^*}.$$

□

Theorem 17 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r,s) *and* $\mathrm{C}^{\perp} = \left\langle \left(\hat{f}(x) \mid 0\right), \left(\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)\right)\right\rangle$ *be the dual code of* C. *Then*

$$\hat{a}_3(x) = \frac{(x^s-1)(f(x),l(x))^*}{g^*(x)(f(x),l(x)h(x))^*}.$$

Proof Since $(f \mid 0), (l \mid g + ua_1 + u^2a_2 + u^3a_3)$ and $(lh \mid ua_1h + u^2a_2h + u^3a_3h) \in$ C, and by Theorem 12 part (1), we have $(0 \mid \frac{(f,lh)}{(f,l)}\left[g + ua_1 + u^2a_2 + u^3a_3\right] + Q_3\left[ua_1h + u^2a_2h + u^3a_3h\right]) \in$ C, for some $Q_3 \in$ R$[x]$. As $(0 \mid u^3\hat{a}_3) \in \mathrm{C}^{\perp}$, $\psi\left((0 \mid u^3\hat{a}_3), \left(0 \mid \frac{(f,lh)}{(f,l)}\left[g + ua_1 + u^2a_2 + u^3a_3\right] + Q_3\left[ua_1h + u^2a_2h + u^3a_3h\right]\right)\right) = 0 \mod (x^m-1)$. This is equivalent to

$$\hat{a}_3\frac{(f,lh)^*}{(f,l)^*}g^* = 0 \mod (x^s-1).$$

Therefore

$$\hat{a}_3 = \frac{(x^s-1)(f,l)^*}{g^*(f,lh)^*}.$$

□

Now, we determine the explicit form of $l(x)$ in $\mathbb{Z}_{2,r}[x]$. Note that $(g + ua_1 + u^2a_2 + u^3a_3)^* = g^* + ux^{\deg(g)-\deg(a_1)}a_1^* + u^2x^{\deg(g)-\deg(a_2)}a_2^* + u^3x^{\deg(g)-\deg(a_3)}a_3^*$.

Lemma 3 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r,s) *such that* $gh = x^s - 1$, $g = a_1b_1$, $a_1 = a_2b_2$ *and* $a_2 = a_3b_3$. *Then* $f \mid lhb_1b_2b_3$.

Proof As $hb_1b_2b_3(l \mid g + ua_1 + u^2a_2 + u^3a_3) = (lhb_1b_2b_3 \mid 0) \in$ C, we have $f \mid lhb_1b_2b_3$ from Remark 1. □

Lemma 4 *Let* $\mathrm{C} = \langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)) \rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *and* $\mathrm{C}^{\perp} = \left\langle \left(\hat{f}(x) \mid 0\right), (\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)) \right\rangle$ *be the dual code of* C. *Then,* $\theta_{\frac{m}{s}}(x^s)\hat{g}a_1^*$, $\theta_{\frac{m}{s}}(x^s)\hat{g}g^*$, $\theta_{\frac{m}{s}}(x^s)\hat{g}a_2^*$, $\theta_{\frac{m}{s}}(x^s)\hat{a}_1g^*$, $\theta_{\frac{m}{s}}(x^s)\hat{a}_1a_1^*$ *and* $\theta_{\frac{m}{s}}(x^s)\hat{a}_2g^*$ *are congruent to* 0 *modulo* $(x^m - 1)$.

Proof Consider

$$\begin{aligned}\theta_{\frac{m}{s}}(x^s)\hat{g}a_1^* &= \frac{\theta_{\frac{m}{s}}(x^s)(x^s-1)(f, lhb_1b_2)^*a_1^*}{f^*a_3^*}\\ &= \frac{(x^m-1)(f, lhb_1b_2)^*a_3^*b_3^*b_2^*}{f^*a_3^*}\\ &= \frac{(x^m-1)(fb_3, lhb_1b_2b_3)^*a_3^*b_2^*}{f^*a_3^*}\\ &\equiv 0 \mod (x^m-1)\end{aligned}$$

from Lemma 3. The other part of the result can be proved with similar arguments. □

Theorem 18 *Let* $\mathrm{C} = \langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)) \rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r, s) *and* $\mathrm{C}^{\perp} = \left\langle \left(\hat{f}(x) \mid 0\right), (\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)) \right\rangle$ *be the dual code of* C. *Let* $\rho = \frac{l^*(x)}{(f(x), l(x))^*}$. *Then*

$$\hat{l}(x) = \frac{x^r-1}{f^*(x)}\lambda(x),$$

where

$$\lambda(x) = \rho^{-1}\left[\frac{(f, lhb_1b_2)^*}{(f, l)^*}x^{m-deg(a_3)+deg(l)} + \frac{(f, lhb_1)^*}{(f, lhb_1b_2)^*}\frac{f^*}{(f, l)^*}x^{m-deg(a_2)+deg(l)} + \frac{(f, lh)^*}{(f, lhb_1)^*}\frac{f^*}{(f, l)^*}x^{m-deg(a_1)+deg(l)} + \frac{f^*}{(f, lh)^*}x^{m-deg(g)+deg(l)}\right] mod\ \left(\frac{f^*}{(f, l)^*}\right)$$

Proof As $(\hat{l} \mid \hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3) \in \mathrm{C}^{\perp}$ and $(f \mid 0) \in \mathrm{C}$, we have $\psi((f \mid 0), (\hat{l} \mid \hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3)) = 0 \mod (x^m - 1)$. From Lemma 2, it follows that $\hat{l}f^* = 0 \mod (x^r - 1)$. Then $\hat{l} = \frac{x^r-1}{f^*}\lambda$ for some $\lambda \in \mathbb{Z}_2[x]$. Again, as $(\hat{l} \mid \hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3) \in \mathrm{C}^{\perp}$ and $(l \mid g + ua_1 + u^2a_2 + u^3a_3) \in \mathrm{C}$, $\psi((\hat{l} \mid \hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3), (l \mid g + ua_1 + u^2a_2 + u^3a_3)) = 0 \mod (x^m - 1)$. This implies that

$$\begin{aligned}&u^3\hat{l}l^*\theta_{\frac{m}{r}}(x^r)x^{m-\deg(l)-1} + \left(\hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3\right)\left(g + ua_1 + u^2a_2 + u^3a_3\right)^*\\ &\theta_{\frac{m}{s}}(x^s)x^{m-\deg(g)-1} = 0 \mod (x^m - 1). \qquad (4)\end{aligned}$$

Rewriting (4), we have

$$\begin{aligned}&u^3\hat{l}l^*\theta_{\frac{m}{r}}(x^r)x^{m-\deg(l)-1} + \left(\hat{g} + u\hat{a}_1 + u^2\hat{a}_2 + u^3\hat{a}_3\right)\\ &\left(g^* + ux^{\deg(g)-\deg(a_1)}a_1^* + u^2x^{\deg(g)-\deg(a_2)}a_2^*\right.\\ &\left.+u^3x^{\deg(g)-\deg(a_3)}a_3^*\right)\theta_{\frac{m}{s}}(x^s)x^{m-\deg(g)-1} = 0 \mod (x^m - 1). \qquad (5)\end{aligned}$$

Or

$$u^3\hat{l}l^*\theta_{\frac{m}{r}}(x^r)x^{m-\deg(l)-1} + \theta_{\frac{m}{s}}(x^s)$$

$$\begin{aligned}&\Big[x^{m-\deg(g)-1}\hat{g}g^* + ux^{m-\deg(a_1)-1}\hat{g}a_1^* + u^2x^{m-\deg(a)-1}\hat{g}a_2^*\\&+u^3x^{m-\deg(a_3)-1}\hat{g}a_3^* + ux^{m-\deg(g)-1}\hat{a}_1g^* + u^2x^{m-\deg(a_1)-1}\hat{a}_1a_1^* + u^3x^{m-\deg(a_2)-1}\hat{a}_1a_2^*\\&+u^2x^{m-\deg(g)-1}\hat{a}_2g^* + u^3x^{m-\deg(a_1)-1}\hat{a}_2a_1^* + u^3x^{m-\deg(g)-1}\hat{a}_3g^*\Big]\\&= 0 \bmod (x^m-1). \end{aligned} \tag{6}$$

From Lemma 4, the summands in (6) containing other than u^3 is 0 mod (x^m-1). This in turn gives

$$\begin{aligned}&u^3\hat{l}l^*\theta_{\frac{m}{r}}(x^r)x^{m-\deg(l)-1} + \theta_{\frac{m}{s}}(x^s)\\&\Big[u^3x^{m-\deg(a_3)-1}\hat{g}a_3^* + u^3x^{m-\deg(a_2)-1}\hat{a}_1a_2^* + u^3x^{m-\deg(a_1)-1}\hat{a}_2a_1^*\\&+u^3x^{m-\deg(g)-1}\hat{a}_3g^*\Big] = 0 \mod (x^m-1). \end{aligned} \tag{7}$$

Substituting the values $\hat{l}$, $\hat{g}$, $\hat{a}_1$, $\hat{a}_2$ and $\hat{a}_3$ in (7), we get

$$\begin{aligned}&u^3\frac{(x^r-1)}{f^*}l^*\lambda\theta_{\frac{m}{r}}(x^r)x^{m-\deg(l)-1} + \theta_{\frac{m}{s}}(x^s)\Big[u^3x^{m-\deg(a_3)-1}\frac{(x^s-1)(f,lhb_1b_2)^*}{f^*a_3^*}a_3^*\\&+u^3x^{m-\deg(a_2)-1}\frac{(x^s-1)(f,lhb_1)^*}{(f,lhb_1b_2)^*a_2^*}a_2^* + u^3x^{m-\deg(a_1)-1}\frac{(x^s-1)(f,lh)^*}{(f,lhb_1)^*a_1^*}a_1^*\\&+u^3x^{m-\deg(g)-1}\frac{(x^s-1)(f,l)^*}{(f,lh)^*a_1^*}g^*\Big] = 0 \bmod (x^m-1). \end{aligned} \tag{8}$$

Rewriting (8), we get

$$\begin{aligned}&u^3\frac{(x^m-1)(f,l)^*}{f^*}\\&\Big[\frac{l^*}{(f,l)^*}\lambda x^{m-\deg(l)-1} + \frac{(f,lhb_1b_2)^*}{(f,l)^*}x^{m-\deg(a_3)-1} + \frac{(f,lhb_1)^*}{(f,lhb_1b_2)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_2)-1}+\\&\frac{(f,lh)^*}{(f,lhb_1)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_1)-1} + \frac{f^*}{(f,lh)^*}x^{m-\deg(g)-1}\Big]\\&= 0 \bmod (x^m-1). \end{aligned} \tag{9}$$

This is equivalent, over $\mathbb{Z}_2$, to

$$\begin{aligned}&\frac{(x^m-1)(f,l)^*}{f^*}\Big[\frac{l^*}{(f,l)^*}\lambda x^{m-\deg(l)-1} + \frac{(f,lhb_1b_2)^*}{(f,l)^*}x^{m-\deg(a_3)-1}\\&+\frac{(f,lhb_1)^*}{(f,lhb_1b_2)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_2)-1}\\&+\frac{(f,lh)^*}{(f,lhb_1)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_1)-1} + \frac{f^*}{(f,lh)^*}x^{m-\deg(g)-1}\Big] = 0 \bmod (x^m-1). \end{aligned} \tag{10}$$

Since $\frac{f^*}{(f,l)^*}$ divides x^m-1, (10) is equivalent to

$$\begin{aligned}&\Big[\frac{l^*}{(f,l)^*}\lambda x^{m-\deg(l)-1} + \frac{(f,lhb_1b_2)^*}{(f,l)^*}x^{m-\deg(a_3)-1} + \frac{(f,lhb_1)^*}{(f,lhb_1b_2)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_2)-1}\\&+\frac{(f,lh)^*}{(f,lhb_1)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_1)-1} + \frac{f^*}{(f,lh)^*}x^{m-\deg(g)-1}\Big]\end{aligned}$$

$$= 0 \mod \left(\frac{f^*}{(f,l)^*}\right). \tag{11}$$

Also, since $\frac{f^*}{(f,l)^*}$ and $\frac{l^*}{(f,l)^*}$ are relatively prime, $\frac{l^*}{(f,l)^*}$ is invertible modulo $\left(\frac{f^*}{(f,l)^*}\right)$. Thus,

$$\lambda = \rho^{-1}\left[\frac{(f,lhb_1b_2)^*}{(f,l)^*}x^{m-\deg(a_3)+\deg(l)} + \frac{(f,lhb_1)^*}{(f,lhb_1b_2)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_2)+\deg(l)}\right.$$
$$\left.+\frac{(f,lh)^*}{(f,lhb_1)^*}\frac{f^*}{(f,l)^*}x^{m-\deg(a_1)+\deg(l)} + \frac{f^*}{(f,lh)^*}x^{m-\deg(g)+\deg(l)}\right] \mod \left(\frac{f^*}{(f,l)^*}\right).$$

□

Corollary 4 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code such that* $f(x)\big|l(x)$. *Then* $\hat{l}(x) = 0$ *and* $\mathrm{C}^{\perp} = \langle(\hat{f}(x) \mid 0), (0 \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x))\rangle$.

Proof If f divides l, from Theorem 18, we have

$$\lambda = \rho^{-1}\left[x^{m-\deg(a_3)+\deg(l)} + x^{m-\deg(a_2)+\deg(l)}\right.$$
$$\left.+x^{m-\deg(a_1)+\deg(l)} + x^{m-\deg(g)+\deg(l)}\right] \pmod 1$$
$$= 0.$$

Therefore, $\hat{l} = 0$. □

Corollary 5 *Let* $\mathrm{C} = \left\langle g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right\rangle$ *be an* R*-cyclic code of odd length* n, *where* $a_3(x)\big|a_2(x)\big|a_1(x)\big|g(x)\big|(x^n-1)$ *over* $\mathbb{Z}_2$. *Then,* $\mathrm{C}^{\perp} = \left\langle \frac{x^n-1}{a_3^*(x)} + u\frac{x^n-1}{a_2^*(x)} + u^2\frac{x^n-1}{a_1^*(x)} + u^3\frac{x^n-1}{g^*(x)}\right\rangle$.

Summarizing the results from Theorems 13 to 18, we have the following result.

Theorem 19 *Let* $\mathrm{C} = \left\langle (f(x) \mid 0), \left(l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)\right)\right\rangle$ *be a* $\mathbb{Z}_2$R*-cyclic code of length* (r,s) *and* $\mathrm{C}^{\perp} = \left\langle \left(\hat{f}(x) \mid 0\right), \left(\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x)\right)\right\rangle$ *be dual code of* C. *Then,*

1. $\hat{f}(x) = \frac{x^r-1}{(f(x),l(x))^*}$;
2. $\hat{g}(x) = \frac{(x^s-1)(f(x),l(x)h(x)b_1(x)b_2(x))^*}{f^*(x)a_3^*(x)}$;
3. $\hat{a}_1(x) = \frac{(x^s-1)(f(x),l(x)h(x)b_1(x))^*}{a_2^*(x)(f(x),l(x)h(x)b_1(x)b_2(x))^*}$;
4. $\hat{a}_2(x) = \frac{(x^s-1)(f(x),l(x)h(x))^*}{a_1^*(x)(f(x),l(x)h(x)b_1(x))^*}$;
5. $\hat{a}_3(x) = \frac{(x^s-1)(f(x),l(x))^*}{g^*(x)(f(x),l(x)h(x))^*}$ *and*
6. $\hat{l}(x) = \frac{x^r-1}{f^*(x)}\lambda(x)$, *where*

$$\lambda(x) = \rho^{-1}\left[\frac{(f, lhb_1b_2)^*}{(f,l)^*}x^{m-deg(a_3)+deg(l)} + \frac{(f, lhb_1)^*}{(f, lhb_1b_2)^*}\frac{f^*}{(f,l)^*}x^{m-deg(a_2)+deg(l)} + \frac{(f, lh)^*}{(f, lhb_1)^*}\frac{f^*}{(f,l)^*}x^{m-deg(a_1)+deg(l)} + \frac{f^*}{(f,lh)^*}x^{m-deg(g)+deg(l)}\right] mod \left(\frac{f^*}{(f,l)^*}\right).$$

Example 3 Let $C = \langle (x^4+x^3+x^2+x+1 \mid 0), (x+1 \mid x+1)\rangle$ be a $\mathbb{Z}_2$R-cyclic code of length $(5,5)$. Then C is of type $(5,5;1;4,0,0,0)$, and the Gray image of C under ϕ is an optimal binary code with parameters $[25,17,4]$. Let $f(x) = x^4+x^3+x^2+x+1$ and $l(x) = g(x) = a_1(x) = a_2(x) = a_3(x) = x+1$. If $C^\perp = \langle (\hat{f}(x) \mid 0), (0 \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x))\rangle$ is the dual code of C, then from Theorem 19, we have $\hat{g}(x) = \hat{a}_1(x) = \hat{a}_2(x) = x^4+x^3+x^2+x+1$, $\hat{a}_3(x) = 1$ and $\hat{f}(x) = x^5-1$. Since $\rho = \frac{l}{(f,l)} = x+1$ and $\frac{f}{(f,l)} = x^4+x^3+x^2+x+1$, we get $\rho^{-1} = x^3+x \pmod{x^4+x^3+x^2+x+1}$, $\lambda = x^3+x \pmod{x^4+x^3+x^2+x+1}$ and $\hat{l} = x^4+x^3+x^2+x$. Therefore, $C^\perp = \langle (x^5-1 \mid 0), (x^4+x^3+x^2+x \mid (1+u+u^2)(x^4+x^3+x^2+x+1)+u^3)\rangle$. The type of $C^\perp$ is $(5,5;0;1,0,0,4)$, and Gray image of $C^\perp$ under ϕ is a binary $[25,8,5]$-linear code.

5 Separable $\mathbb{Z}_2$R-cyclic codes

A $\mathbb{Z}_2$R-cyclic code of block length (r,s) is called separable if $C = C_r \times C_s$. Let $C = \langle (f(x) \mid 0), (0 \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle$ be a separable $\mathbb{Z}_2$R-cyclic code of block length (r,s), s odd. Also, let the dual code of C be $C^\perp = \langle (\hat{f}(x) \mid 0), (\hat{l}(x) \mid \hat{g}(x) + u\hat{a}_1(x) + u^2\hat{a}_2(x) + u^3\hat{a}_3(x))\rangle$. Then from Theorem 19, we have $\hat{f} = \frac{x^r-1}{f^*}$, $\hat{g} = \frac{x^s-1}{a_3^*}$, $\hat{a}_1 = \frac{x^s-1}{a_2^*}$, $\hat{a}_2 = \frac{x^s-1}{a_1^*}$ and $\hat{a}_3 = \frac{x^s-1}{g^*}$. Furthermore, as $\frac{f^*}{(f,l)^*} = 1$, we have $\lambda = 0$. This in turn gives $\hat{l} = 0$.

The generator matrix of C is permutation equivalent to a matrix of the form

$$G_S = \left(\begin{array}{cc|ccccc} I_{k_o} & \bar{A}_{01} & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & I_{k_1} & A_{01} & A_{02} & A_{03} & A_{04} \\ 0 & 0 & 0 & uI_{k_2} & uA_{12} & uA_{13} & uA_{14} \\ 0 & 0 & 0 & 0 & u^2I_{k_3} & u^2A_{23} & u^2A_{24} \\ 0 & 0 & 0 & 0 & 0 & u^3I_{k_4} & u^3A_{34} \end{array}\right), \tag{12}$$

The following theorem gives generator polynomials of a separable $\mathbb{Z}_2$R-cyclic code and its dual.

Theorem 20 *Let* $C = \langle (f(x) \mid 0), (0 \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle$ *be a separable* $\mathbb{Z}_2$R*-cyclic code of length* (r,s) *and* $C^\perp$ *be the dual code of* C*. Then,*

1. $C^\perp$ *is also a separable* $\mathbb{Z}_2$R*-cyclic code of block length* (r,s)*;*
2. $C^\perp = \left\langle \left(\frac{x^r-1}{f^*(x)} \mid 0\right), \left(0 \mid \frac{x^s-1}{a_3^*(x)} + u\frac{x^s-1}{a_2^*(x)} + u^2\frac{x^s-1}{a_1^*(x)} + u^3\frac{x^s-1}{g^*(x)}\right)\right\rangle$ *and*
3. $d(C) = \min\{d_H(C_r), d_H(C_s)\}$.

Remark 3 Let $C = \langle (f(x) \mid 0), (l(x) \mid g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x))\rangle$ be a $\mathbb{Z}_2$R-cyclic code. If $f(x) \mid l(x)$, then C is separable.

Remark 4 If C is a non-separable $\mathbb{Z}_2$R-cyclic code of block length (r,s), then $d_{min}(C) \geq \min\{d_H(C_r), d_H(C_s)\}$.

Table 1 Gray images of $\mathbb{Z}_2$R-cyclic codes

Generators	[r,s]	Binary image
$f = x+1,\ l = 1,\ g = x+1,\ a_1 = x+1,\ a_2 = 1,\ a_3 = 1$	[1, 1]	[5, 2, 3]*
$f = x^2+1, l = x+1, g = x+1, a_1 = x+1, a_2 = 1, a_3 = 1$	[2, 1]	[6, 2, 4]*
$f = x^3+1, l = x+1, g = x+1, a_1 = x+1, a_2 = 1, a_3 = 1$	[3, 1]	[7, 2, 4]*
$f = x+1, l = 1, g = x^2+1, a_1 = x+1, a_2 = x+1, a_3 = 1$	[1, 2]	[9, 3, 4]*
$f = x^2+1, l = x+1, g = x+1, a_1 = x+1, a_2 = x+1, a_3 = 1$	[2, 2]	[10, 4, 4]*
$f = x^4+x^3+x^2+1, l = x^2+x, g = x+1, a_1 = x+1, a_2 = 1, a_3 = 1$	[7, 1]	[11, 5, 4]*
$f = x^5+1, l = x^4+x^3+x^2+x, g = x^2+1, a_1 = x^2+1, a_2 = x+1, a_3 = x+1$	[5, 2]	[13, 2, 8]*
$f = x^3+1, l = x+1, g = x+1, a_1 = x+1, a_2 = x+1, a_3 = 1$	[3, 3]	[15, 8, 4]*
$f = x^4+1, l = x^3+x^2+x+1, g = x^3+1, a_1 = x^3+1, a_2 = x^2+x+1, a_3 = x^2+x+1$	[4, 3]	[16, 2, 10]*
$f = x^5+1, l = x^4+x^3+x^2+x+1, g = x^3+1, a_1 = x^3+1, a_2 = x^2+x+1, a_3 = x^2+x+1$	[5, 3]	[17, 2, 11]*
$f = x^7+1, l = x^6+x^5+x^4+x^3+x^2+x, g = x^3+1, a_1 = x^3+1, a_2 = x^2+x+1, a_3 = x^2+x+1$	[7, 3]	[19, 2, 12]*
$f = x^7+1, l = x^6+x^5+x^4+x^3+x^2+x+1, g = x^4+1, a_1 = x^4+1, a_2 = x^3+x^2+x+1, a_3 = x^3+x^2+x+1$	[7, 4]	[23, 2, 15]*
$f = x^4+x^3+x^2+x+1, l = x^2+x, g = x+1, a_1 = x+1, a_2 = x+1, a_3 = 1$	[5, 5]	[25, 17, 4]*
$f = x^4+x^3+x^2+1, l = x^3+x^2, g = x+1, a_1 = x+1, a_2 = x+1, a_3 = 1$	[7, 5]	[27, 19, 4]*
$f = x^4+x^3+x^2+1, l = x^3+x^2, g = x+1, a_1 = x+1, a_2 = x+1, a_3 = 1$	[7, 7]	[35, 27, 4]*
$f = x^4+x^3+x^2+x+1, l = x^3+x^2+1, g = x^3+1, a_1 = x+1, a_2 = x+1, a_3 = x+1$	[5, 15]	[65, 55, 4]*

Example 4 Let $C = \langle (x+1 \mid 0), (0 \mid x^2+x+1) \rangle$ be a separable $\mathbb{Z}_2$R-cyclic code of block length $(3, 3)$. Then, from Theorem 20, the dual code of C is $C^{\perp} = \langle (x^2+x+1 \mid 0), (0 \mid x+1) \rangle$. Clearly, C and $C^{\perp}$ are of the types $(3, 3; 2; 1, 0, 0, 0)$ and $(3, 3; 1; 2, 0, 0, 0)$, respectively. Also, the Gray image of $C^{\perp}$ under ϕ is a binary linear code with parameters $[15, 9, 2]$.

Table 1 presents some good binary codes obtained as Gray images of $\mathbb{Z}_2$R-cyclic codes. Note that the parameters marked with '$*$' denotes the optimal binary codes according to the online database (Grassl 2022).

6 Conclusions

This paper is devoted to study $\mathbb{Z}_2$R-cyclic codes of length (r, s), where $R = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + u^3\mathbb{Z}_2$ with $u^4 = 0$. We first determined generator polynomials of $\mathbb{Z}_2$R-cyclic codes, and presented a minimal spanning set. Furthermore, we gave the relationship between $\mathbb{Z}_2$R-cyclic codes and their duals for odd integral values of s. Binary optimal codes obtained as Gray images of $\mathbb{Z}_2$R-cyclic codes are listed. Generalizing these results and determining the structure of dual codes of $\mathbb{Z}_2\mathbb{Z}_2[u^k]$-cyclic codes is a future interesting problem.

Acknowledgements The authors would like to thank the anonymous referees for their valuable comments and suggestions that improved the quality of this paper.

References

Abualrub T, Siap I, Aydin N (2014) $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. IEEE Trans Inform Theory 60(3):1508–1514

Aydogdu I (2019) 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(1):39–51

Aydogdu I, Siap I, Ten-Valls R (2017) On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes. Finite Fields Appl 48:241–260

Aydogdu I, Abualrub T, Siap I (2017) $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes. IEEE Trans Inform Theory 63(8):4883–4893

Aydogdu I, Siap I (2015) On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. Linear Multilinear Algebra 63(10):2089–2102

Borges J, Fernández-Córdoba C, Pujol J, Rifà J, Villanueva M (2010) $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. Des Codes Cryptogr 54(2):167–179

Borges J, Fernández-Córdoba C, Ten-Valls R (2018) $\mathbb{Z}_2$-double cyclic codes. Des Codes Cryptogr 86:463–479

Borges J, Dougherty ST, Fernández-Córdoba C (2012) Characterization and constructions of self-dual codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$. Adv Math Commun 6(3):287–303

Bilal M, Borges J, Dougherty ST, Fernández-Córdoba C (2011) Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. Des Codes Cryptogr 61:31–40. https://doi.org/10.1007/s10623-010-9437-1

Brouwer AE, Hamalainen HO, Ostergard PRJ, Sloane NJA (1998) Bounds on mixed binary/ternary codes. IEEE Trans Inform Theory 44(1):140–161

Delsarte P, Levenshtein VI (1998) Association schemes and coding theory. IEEE Trans Inform Theory 44(6):2477–2504

Diao L, Gao J, Lu J (2020) Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes. Adv Math Commun 14(4):555–572

Dinh HQ, Bag T, Upadhyay AK, Bandi R, Chinnakum W (2020) On the structure of cyclic codes over $\mathbb{F}_q$ and applications in quantum and LCD codes constructions. IEEE Access 8:18902–18914

Dinh HQ, Pathak S, Bag T, Upadhyay AK, Bandi R, Yamaka W (2021) On $\mathbb{F}_2$RS-cyclic codes and their applications in constructing optimal codes. Discrete Math. 344(5):112310

Dinh HQ, Pathak S, Bag T, Upadhyay AK, Chinnakum W (2020) A study of $\mathbb{F}_q$R-cyclic codes and their applications in constructing quantum codes. IEEE Access 8:190049–190063

Grassl M (2022) Online linear code bounds. http://www.codetables.de. Accessed 9 April

Hou X, Gao J (2021) $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes are asymptotically good. J Appl Math Comput 66:871–884. https://doi.org/10.1007/s12190-020-01466-w

Li J, Gao J, Fu FW et al (2020) $\mathbb{F}_q$R-linear skew constacyclic codes and their application of constructing quantum codes. Quantum Inf Process 19:193. https://doi.org/10.1007/s11128-020-02700-x

MacWilliams FJ, Sloane NJA (1975) The theory of error correcting codes. North-Holland Publishing Company, Amsterdam

Meng X, Gao J (2021) Complete weight enumerator of torsion codes. Adv Math Commun 1:10. https://doi.org/10.3934/amc.2020124

Özger Z, Kara Ü, Yildiz B (2014) Linear, cyclic and constacyclic over $S_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$. Filomat 28(5):897–906

Qian JF, Zhang LN, Zhu SX (2005) Cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$. IEICE Trans Fundam E88:795–797

Rifà-Pous H, Rifà J, Ronquillo L (2011) $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in steganography. Adv Math Commun 5(3):425–433

Srinivasulu B, Bhinthwal M (2017) $\mathbb{Z}_2$-Triple cyclic codes and their duals. Eur J Pure Appl Math 10(2):392–409

Yao T, Zhu S, Kai X (2020) Asymptotically good $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. Finite Fields Appl 63:101633

Yao T, Zhu S (2020) $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic codes are asymptotically good. Cryptogr Commun 12:253–264