Des. Codes Cryptogr. (2018) 86:463–479
https://doi.org/10.1007/s10623-017-0334-8

$\mathbb{Z}_2$-double cyclic codes

Joaquim Borges[1] · **Cristina Fernández-Córdoba**[1] · **Roger Ten-Valls**[1]

Received: 9 November 2015 / Revised: 13 January 2017 / Accepted: 19 January 2017 /
Published online: 10 February 2017

Abstract A binary linear code C is a $\mathbb{Z}_2$-double cyclic code if the set of coordinates can be partitioned into two subsets such that any cyclic shift of the coordinates of both subsets leaves invariant the code. These codes can be identified as submodules of the $\mathbb{Z}_2[x]$-module $\mathbb{Z}_2[x]/(x^r - 1) \times \mathbb{Z}_2[x]/(x^s - 1)$. We determine the structure of $\mathbb{Z}_2$-double cyclic codes giving the generator polynomials of these codes. We give the polynomial representation of $\mathbb{Z}_2$-double cyclic codes and its duals, and the relations between the generator polynomials of these codes. Finally, we study the relations between $\mathbb{Z}_2$-double cyclic and other families of cyclic codes, and show some examples of distance optimal $\mathbb{Z}_2$-double cyclic codes.

Keywords Binary linear codes · Duality · $\mathbb{Z}_2$-double cyclic codes

Mathematics Subject Classification 94B60 · 94B25

1 Introduction

Let $\mathbb{Z}_2$ be the ring of integers modulo 2. Let $\mathbb{Z}_2^n$ denote the set of all binary vectors of length n. A non-empty subset of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. In this paper we introduce a subfamily of binary linear codes, called $\mathbb{Z}_2$-*double cyclic codes*, with the property that the set of coordinates can be partitioned into two subsets, the

Communicated by J. Wolfmann.

✉ Roger Ten-Valls
rten@deic.uab.cat

Joaquim Borges
jborges@deic.uab.cat

Cristina Fernández-Córdoba
cfernandez@deic.uab.cat

[1] Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Cerdanyola del Vallès, Spain

first r coordinates and the last s coordinates, such that any cyclic shift of the coordinates of both subsets of a codeword is also a codeword.

Note that if one of these sets of coordinates is empty, for example $r = 0$, then we obtain a binary cyclic code of length s. Therefore, binary cyclic codes are a special class of $\mathbb{Z}_2$-double cyclic codes. Another special case is when $r = s$, where a $\mathbb{Z}_2$-double cyclic code is permutation equivalent to a quasi-cyclic code of index 2 and even length. Theory of binary cyclic codes and quasi-cyclic codes of index 2 can be found in [11].

Recently, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes have been studied (see [4,7]). For $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, the set of coordinates is partitioned into two subsets, the first one of binary coordinates and the second one of quaternary coordinates. The simultaneous cyclic shift of the subsets of coordinates of a codeword has been defined in [1], where the authors study $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and identify these codes as $\mathbb{Z}_4[x]$-modules of a certain ring. Furthermore $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes and $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive cyclic and constacylic codes have been studied in [2] and [3] respectively, where these codes are another special classes of mixed type codes.

Since [9], a lot of variants of linear and cyclic codes over different rings are studied. Obviously, these codes have a theoretical interest, from a mathematical point of view, since they are related to algebraic structures such as rings, ideals or modules. But the interest for such codes is not purely mathematical because some of them have binary images with better parameters than classical binary linear codes. Here, we present a new variant of cyclic codes, the $\mathbb{Z}_2$-double cyclic codes, closely related to generalized quasi-cyclic codes of index 2 [13]. We give examples of $\mathbb{Z}_2$-double cyclic codes that are optimal with respect to the minimum distance. The aim of this paper is to study the algebraic structure of $\mathbb{Z}_2$-double cyclic codes and their dual codes. The paper is organized as follows. In Sect. 2, we give the definition of $\mathbb{Z}_2$-double cyclic codes, we find the relation between some canonical projections of these codes and binary cyclic codes. Also we present the $\mathbb{Z}_2[x]$-module $\mathbb{Z}_2[x]/(x^r-1)\times\mathbb{Z}_2[x]/(x^s-1)$, denoted by $R_{r,s}$. In Sect. 3, we determine the algebraic structure of a $\mathbb{Z}_2$-double cyclic code and we state some relations between its generators. In Sect. 4, we study the concept of duality and, for a $\mathbb{Z}_2$-double cyclic code, we determine the generators of the dual code in terms of the generators of the code. In Sect. 5, we study the relations between $\mathbb{Z}_2$-double cyclic codes and other families of cyclic codes such as $\mathbb{Z}_4$-cyclic codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. Finally, in Sect. 6 we give tables with the generator polynomials of some specific $\mathbb{Z}_2$-double cyclic codes and their dual codes. In some cases, the codes are optimal with respect to the minimum distance. We also give examples of $\mathbb{Z}_2$-double cyclic codes obtained from $\mathbb{Z}_4$-cyclic and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

2 $\mathbb{Z}_2$-double cyclic codes

Let C be a binary code of length n. Let r and s be non-negative integers such that $n = r + s$. We consider a partition of the set of the n coordinates into two subsets of r and s coordinates respectively, so that C is a subset of $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$.

Definition 1 Let C be a binary linear code of length $n = r + s$. The code C is called $\mathbb{Z}_2$-*double cyclic* if

$$(u_0, u_1, \dots, u_{r-2}, u_{r-1} \mid u'_0, u'_1, \dots, u'_{s-2}, u'_{s-1}) \in C$$

implies

$$(u_{r-1}, u_0, u_1, \dots, u_{r-2} \mid u'_{s-1}, u'_0, u'_1, \dots, u'_{s-2}) \in C.$$

Let $\mathbf{u} = (u_0, u_1, \dots, u_{r-1} \mid u'_0, \dots, u'_{s-1})$ be a codeword in C and let i be an integer. We denote by

$$\mathbf{u}^{(i)} = (u_{0-i}, u_{1-i}, \dots, u_{r-1-i} \mid u'_{0-i}, \dots, u'_{s-1-i}) \tag{1}$$

the ith shift of $\mathbf{u}$, where the subscripts are read modulo r and s, respectively. Note that $\mathbf{u}^{(-1)} = \mathbf{u}^{(lcm(r,s)-1)}$ and, in fact, $\mathbf{u}^{(i)} = \mathbf{u}^{(lcm(r,s)+i)}$, for $i \in \mathbb{Z}$.

Let $C \subseteq \mathbb{Z}_2^r \times \mathbb{Z}_2^s$ be a $\mathbb{Z}_2$-double cyclic code. Let C_r be the canonical projection of C on the first r coordinates and C_s on the last s coordinates. Note that C_r and C_s are binary cyclic codes of length r and s, respectively. The code C is called *separable* if it is the direct product of C_r and C_s.

There is a bijective map between $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ and $\mathbb{Z}_2[x]/(x^r - 1) \times \mathbb{Z}_2[x]/(x^s - 1)$ given by:

$$(u_0, u_1, \dots, u_{r-1} \mid u'_0, \dots, u'_{s-1}) \mapsto (u_0 + u_1x + \cdots + u_{r-1}x^{r-1} \mid u'_0 + \cdots + u'_{s-1}x^{s-1}).$$

We denote the image of the vector $\mathbf{u}$ by $\mathbf{u}(x)$.

Definition 2 Denote the ring $\mathbb{Z}_2[x]/(x^r - 1) \times \mathbb{Z}_2[x]/(x^s - 1)$ by $R_{r,s}$. We define the operation

$$\star : \mathbb{Z}_2[x] \times R_{r,s} \to R_{r,s}$$

as

$$\lambda(x) \star (p(x) \mid q(x)) = (\lambda(x)p(x) \mid \lambda(x)q(x)),$$

where $\lambda(x) \in \mathbb{Z}_2[x]$ and $(p(x) \mid q(x)) \in R_{r,s}$.

The ring $R_{r,s}$ with the external operation $\star$ is a $\mathbb{Z}_2[x]$-module. Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ be an element of $R_{r,s}$. Note that if we operate $\mathbf{u}(x)$ by x we get

$$\begin{aligned} x \star \mathbf{u}(x) &= x \star (u(x) \mid u'(x)) \\ &= x \star (u_0 + \cdots + u_{r-2}x^{r-2} + u_{r-1}x^{r-1} \mid u'_0 + \cdots + u'_{s-2}x^{s-2} + u'_{s-1}x^{s-1}) \\ &= (u_0x + \cdots + u_{r-2}x^{r-1} + u_{r-1}x^r \mid u'_0x + \cdots + u'_{s-2}x^{s-1} + u'_{s-1}x^s) \\ &= (u_{r-1} + u_0x + \cdots + u_{r-2}x^{r-1} \mid u'_{s-1} + u'_0x + \cdots + u'_{s-2}x^{s-1}). \end{aligned}$$

Hence, $x \star \mathbf{u}(x)$ is the image of the vector $\mathbf{u}^{(1)}$. Thus, the operation of $\mathbf{u}(x)$ by x in $R_{r,s}$ corresponds to a shift of $\mathbf{u}$. In general, $x^i \star \mathbf{u}(x) = \mathbf{u}^{(i)}(x)$ for all i.

3 Algebraic structure and generators

In this section, we shall study submodules of $R_{r,s}$. We describe the generators of such submodules and state some properties. From now on, $\langle S \rangle$ will denote the submodule generated by a subset S of $R_{r,s}$. Let $\pi_r : R_{r,s} \to \mathbb{Z}_2[x]/(x^r - 1)$ and $\pi_s : R_{r,s} \to \mathbb{Z}_2[x]/(x^s - 1)$ be the canonical projections, and let N be a submodule of $R_{r,s}$. If $\pi_r(N) = \{0\}$ (resp. $\pi_s(N) = \{0\}$) then we may consider that the generator polynomial of $\pi_r(N)$ (resp. $\pi_s(N)$) is $x^r - 1$ (resp. $x^s - 1$). Define $N' = \{(p(x)|q(x)) \in N \mid q(x) = 0\}$. It is easy to check that $N' \cong \pi_r(N')$ by considering the map $(p(x) \mid 0) \mapsto p(x)$.

Theorem 1 *The $\mathbb{Z}_2[x]$-module $R_{r,s}$ is a noetherian $\mathbb{Z}_2[x]$-module, and every submodule N of $R_{r,s}$ can be written as*

$$N = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle,$$

where $b(x), \ell(x) \in \mathbb{Z}_2[x]/(x^r - 1)$ with $b(x) \mid (x^r - 1)$, and $a(x) \in \mathbb{Z}_2[x]/(x^s - 1)$ with $a(x) \mid (x^s - 1)$.

Proof By using the fact that $\mathbb{Z}_2[x]/(x^r - 1)$ and $\mathbb{Z}_2[x]/(x^s - 1)$ are principal ideal rings, we have that $N_s = \pi_s(N)$ and $\pi_r(N')$ are finitely generated. Moreover, since $N' \cong \pi_r(N')$, it follows that N' is finitely generated.

The generators of $\pi_r(N')$ may not be unique. Consider $b(x)$ the generator of $\pi_r(N')$ satisfying $b(x) \mid (x^r - 1)$. Then $(b(x) \mid 0)$ is a generator of N'. Similarly, consider $a(x) \in N_s$ such that $N_s = \langle a(x) \rangle$ and $a(x) \mid (x^s - 1)$. Then there exists $\ell(x) \in \mathbb{Z}_2[x]/(x^r - 1)$ such that $(\ell(x) \mid a(x)) \in N$.

We claim that

$$N = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle.$$

Let $(p(x) \mid q(x)) \in N$. We shall prove that $(p(x) \mid q(x))$ is generated by $(b(x) \mid 0)$ and $(\ell(x) \mid a(x))$. First, since $q(x) = \pi_s(p(x) \mid q(x)) \in N_s$ and $N_s = \langle a(x) \rangle$, there exists $\lambda(x) \in \mathbb{Z}_2[x]$ such that $q(x) = \lambda(x)a(x)$. Moreover,

$$(p(x) \mid q(x)) - \lambda(x) \star (\ell(x) \mid a(x)) = (p(x) - \lambda(x)\ell(x) \mid 0) \in N',$$

that is generated by $(b(x) \mid 0)$. Then, there exists $\mu(x) \in \mathbb{Z}_2[x]$ such that $(p(x) - \lambda(x)\ell(x) \mid 0) = \mu(x) \star (b(x) \mid 0)$. Thus,

$$(p(x) \mid q(x)) = \mu(x) \star (b(x) \mid 0) + \lambda(x) \star (\ell(x) \mid a(x)).$$

Therefore, N is finitely generated by $(b(x) \mid 0)$ and $(\ell(x) \mid a(x))$, and then $R_{r,s}$ is a noetherian $\mathbb{Z}_2[x]$-module. □

From the previous result, it is clear that we can identify $\mathbb{Z}_2$-double cyclic codes in $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ as submodules of $R_{r,s}$. Hence, any submodule of $R_{r,s}$ is a $\mathbb{Z}_2$-double cyclic code. From now on, we will denote by C indistinctly both the code and the corresponding submodule.

Note that if $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ is a $\mathbb{Z}_2$-double cyclic code, then the canonical projections C_r and C_s are binary cyclic codes generated by $\gcd(b(x), \ell(x))$ and $a(x)$, respectively. Moreover, the generator polynomials of C_r, C_s and C may not be unique. In the following proposition we give some conditions to the generator polynomials of a $\mathbb{Z}_2$-double cyclic code.

Proposition 1 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code. Then, we can assume that*

1. *$C_s = \langle a(x) \rangle$, with $a(x) | (x^s - 1)$,*
2. *$\pi_r(C') = \langle b(x) \rangle$, with $b(x) | (x^r - 1)$,*
3. *$\deg(\ell(x)) < \deg(b(x))$.*

Proof The conditions for $a(x)$ and $b(x)$ follow from the proof of Theorem 1. Now, suppose that $\deg(\ell(x)) \geq \deg(b(x))$. Let $i = \deg(\ell(x)) - \deg(b(x))$ and let $C_1 = \langle (b(x) \mid 0), (\ell(x) + x^i \star b(x) \mid a(x)) \rangle$.

On the one hand, $\deg(\ell(x) + x^i \star b(x)) < \deg(\ell(x))$ and since the generators of C_1 belong to C, we have that $C_1 \subseteq C$. On the other hand,

$$(\ell(x) \mid a(x)) = (\ell(x) + x^i \star b(x) \mid a(x)) + x^i \star (b(x) \mid 0).$$

Then, $\langle(\ell(x) \mid a(x))\rangle \subseteq C_1$ and hence $C \subseteq C_1$. It follows that $C = C_1$, which implies that we may consider $\deg(\ell(x)) < \deg(b(x))$. □

Example 1 Consider the code C_1 generated by $\langle(x^2 + x + 1 \mid 0), (x + 1 \mid x^4 + x^3 + x^2 + x + 1)\rangle \subseteq R_{3,5}$. Since $(x + 1) \star (x + 1 \mid x^4 + x^3 + x^2 + x + 1) = (x^2 + 1 \mid 0)$ and $(x^2 + x + 1 \mid 0)$ belong to C_1, it is easy to see that $\pi_r(C_1) = \langle 1\rangle$. Clearly, the generators of C_1 are not as in Proposition 1 since $\langle x^2 + x + 1\rangle \neq \pi_r(C_1)$. Thus, we may consider $C_1 = \langle(1 \mid 0), (0 \mid x^4 + x^3 + x^2 + x + 1)\rangle$, and these polynomials satisfy the conditions of Proposition 1.

Proposition 2 *Let $C = \langle(b(x) \mid 0), (\ell(x) \mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, $b(x) \mid \frac{x^s-1}{a(x)}\ell(x)$.*

Proof By Proposition 1, $N' = \langle(b(x) \mid 0)\rangle$. We have that $\frac{x^s-1}{a(x)} \star (\ell(x) \mid a(x)) \in N'$ and, therefore, $\frac{x^s-1}{a(x)}\ell(x) \in \langle b(x)\rangle$ and $b(x) \mid \frac{x^s-1}{a(x)}\ell(x)$. □

Corollary 1 *Let $C = \langle(b(x) \mid 0), (\ell(x) \mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, $b(x) \mid \frac{x^s-1}{a(x)} \gcd(b(x), \ell(x))$.*

We have seen that $R_{r,s}$ is a $\mathbb{Z}_2[x]$-module, and the product by $x \in \mathbb{Z}_2[x]$ is equivalent to the double right shift on the vector space $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$. Moreover, we have that $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ is a $\mathbb{Z}_2$-module, where the operations are addition and multiplication by elements of $\mathbb{Z}_2$. Our goal now is to find a set of generators for C as a $\mathbb{Z}_2$-module.

Proposition 3 *Let $C = \langle(b(x) \mid 0), (\ell(x) \mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Define the sets*

$$S_1 = \{(b(x) \mid 0), x \star (b(x) \mid 0), \dots, x^{r-\deg(b(x))-1} \star (b(x) \mid 0)\},$$
$$S_2 = \{(\ell(x) \mid a(x)), x \star (\ell(x) \mid a(x)), \dots, x^{s-\deg(a(x))-1} \star (\ell(x) \mid a(x))\}.$$

Then, $S_1 \cup S_2$ forms a minimal generating set for C as a $\mathbb{Z}_2$-module.

Proof It is easy to check that the codewords of $S_1 \cup S_2$ are linearly independent.

Let $c(x) = p_1(x) \star (b(x) \mid 0) + p_2(x) \star (\ell(x) \mid a(x)) \in C$. We have to check that $c(x) \in \langle S_1 \cup S_2\rangle$.

If $\deg(p_1(x)) \leq r - \deg(b(x)) - 1$, then $p_1(x) \star (b(x) \mid 0) \in \langle S_1\rangle$. Otherwise, using the division algorithm, we compute $p_1(x) = q_1(x)\frac{x^r-1}{b(x)} + r_1(x)$ with $\deg(r_1(x)) \leq r - \deg(b(x)) - 1$, hence

$$p_1(x) \star (b(x) \mid 0) = \left(q_1(x)\frac{x^r-1}{b(x)} + r_1(x)\right) \star (b(x) \mid 0) = r_1(x) \star (b(x) \mid 0) \in \langle S_1\rangle.$$

It follows that $c(x) \in \langle S_1 \cup S_2\rangle$ if $p_2(x) \star (\ell(x) \mid a(x)) \in \langle S_1 \cup S_2\rangle$.

If $\deg(p_2(x)) \leq s - \deg(a(x)) - 1$, then $p_2(x) \star (\ell(x) \mid a(x)) \in \langle S_2\rangle$. If not, using the division algorithm, consider $p_2(x) = q_2(x)\frac{x^s-1}{a(x)} + r_2(x)$, where $\deg(r_2(x)) \leq s - \deg(a(x)) - 1$. Then,

$$\begin{aligned}p_2(x)\star(\ell(x)\mid a(x)) &= \left(q_2(x)\frac{x^s-1}{a(x)}+r_2(x)\right)\star(\ell(x)\mid a(x))\\ &= \left(q_2(x)\frac{x^s-1}{a(x)}\right)\star(\ell(x)\mid a(x))+r_2(x)\star(\ell(x)\mid a(x))\\ &= (q_2(x)\frac{x^s-1}{a(x)}\ell(x)\mid 0)+r_2(x)\star(\ell(x)\mid a(x)).\end{aligned}$$

To prove that $p_2(x)\star(\ell(x)\mid a(x))\in\langle S_1\cup S_2\rangle$ first note that $r_2(x)\star(\ell(x)\mid a(x))\in\langle S_2\rangle$. Finally, by Proposition 2, $b(x)$ divides $\frac{x^s-1}{a(x)}\ell(x)$ and it follows that $(q_2(x)\frac{x^s-1}{a(x)}\ell(x)\mid 0)\in\langle S_1\rangle$. Thus, $c(x)\in\langle S_1\cup S_2\rangle$. □

Corollary 2 *Let $C=\langle(b(x)\mid 0),(\ell(x)\mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, C is a binary linear code of dimension $r+s-\deg(b(x))-\deg(a(x))$.*

4 Duality

Let C be a $\mathbb{Z}_2$-double cyclic code and $C^{\perp}$ be its dual code (see [10]). Taking a vector $\mathbf{v}$ of $C^{\perp}$, $\mathbf{u}\cdot\mathbf{v}=0$ for all $\mathbf{u}$ in C. Since $\mathbf{u}$ belongs to C, we know that $\mathbf{u}^{(-1)}$ is also a codeword. So, $\mathbf{u}^{(-1)}\cdot\mathbf{v}=\mathbf{u}\cdot\mathbf{v}^{(1)}=0$ for all $\mathbf{u}\in C$, therefore $\mathbf{v}^{(1)}$ is in $C^{\perp}$ and $C^{\perp}$ is also a $\mathbb{Z}_2$-double cyclic code. Consequently, we obtain the following proposition.

Proposition 4 *Let C be a $\mathbb{Z}_2$-double cyclic code. Then the dual code of C is also a $\mathbb{Z}_2$-double cyclic code.*

We denote $C^{\perp}=\langle(\bar{b}(x)\mid 0),(\bar{\ell}(x)\mid\bar{a}(x))\rangle$, where $\bar{b}(x),\bar{\ell}(x)\in\mathbb{Z}_2[x]/(x^r-1)$ with $\bar{b}(x)\mid(x^r-1)$ and $\bar{a}(x)\in\mathbb{Z}_2[x]/(x^s-1)$ with $\bar{a}(x)\mid(x^s-1)$.

The *reciprocal polynomial* of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. As in the theory of binary cyclic codes, reciprocal polynomials have an important role in duality (see [11]).

We denote the polynomial $\sum_{i=0}^{m-1}x^i$ by $\theta_m(x)$. Using this notation we have the following proposition.

Proposition 5 *Let $n,m\in\mathbb{N}$. Then, $x^{nm}-1=(x^n-1)\theta_m(x^n)$.*

Proof It is well known that $y^m-1=(y-1)\theta_m(y)$. Replacing y by x^n, the result follows. □

From now on, $\mathfrak{m}$ denotes the least common multiple of r and s.

Definition 3 Let $\mathbf{u}(x)=(u(x)\mid u'(x))$ and $\mathbf{v}(x)=(v(x)\mid v'(x))$ be elements in $R_{r,s}$. We define the map

$$\circ: R_{r,s}\times R_{r,s}\longrightarrow\mathbb{Z}_2[x]/(x^{\mathfrak{m}}-1),$$

such that

$$\begin{aligned}\circ(\mathbf{u}(x),\mathbf{v}(x)) =& u(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r)x^{\mathfrak{m}-1-\deg(v(x))}v^*(x)+\\ &+u'(x)\theta_{\frac{\mathfrak{m}}{s}}(x^s)x^{\mathfrak{m}-1-\deg(v'(x))}v'^*(x)\quad\bmod(x^{\mathfrak{m}}-1).\end{aligned}$$

The map $\circ$ is linear in each of its arguments. That is, $\circ$ is a bilinear map between $\mathbb{Z}_2[x]$-modules.

From now on, we denote $\circ(\mathbf{u}(x),\mathbf{v}(x))$ by $\mathbf{u}(x)\circ\mathbf{v}(x)$. Note that $\mathbf{u}(x)\circ\mathbf{v}(x)$ belongs to $\mathbb{Z}_2[x]/(x^{\mathfrak{m}}-1)$.

Proposition 6 *Let* $\mathbf{u}$ *and* $\mathbf{v}$ *be vectors in* $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ *with associated polynomials* $\mathbf{u}(x) = (u(x) \mid u'(x))$ *and* $\mathbf{v}(x) = (v(x) \mid v'(x))$*, respectively. Then,* $\mathbf{v}$ *is orthogonal to* $\mathbf{u}$ *and all its shifts if and only if*

$$\mathbf{u}(x) \circ \mathbf{v}(x) = 0.$$

Proof Let $\mathbf{u}^{(i)} = (u_{0-i}, u_{1-i}, \dots, u_{r-1-i} \mid u'_{0-i}, \dots, u'_{s-1-i})$ be the ith shift of $\mathbf{u}$. Then,

$$\mathbf{u}^{(i)} \cdot \mathbf{v} = 0 \text{ if and only if } \sum_{j=0}^{r-1} u_{j-i} v_j + \sum_{k=0}^{s-1} u'_{k-i} v'_k = 0.$$

Let $S_i = \sum_{j=0}^{r-1} u_{j-i} v_j + \sum_{k=0}^{s-1} u'_{k-i} v'_k$. Computing $\mathbf{u}(x) \circ \mathbf{v}(x)$ we obtain

$$\begin{aligned}\mathbf{u}(x) \circ \mathbf{v}(x) = \theta_{\frac{\mathfrak{m}}{r}}(x^r) &\left[\sum_{n=0}^{r-1} \sum_{j=n}^{r-1} u_{j-n} v_j x^{\mathfrak{m}-1-n} + \sum_{n=1}^{r-1} \sum_{j=n}^{r-1} u_j v_{j-n} x^{\mathfrak{m}-1+n} \right] \\ + \theta_{\frac{\mathfrak{m}}{s}}(x^s) &\left[\sum_{t=0}^{s-1} \sum_{k=t}^{s-1} u'_{k-t} v'_j x^{\mathfrak{m}-1-t} + \sum_{t=1}^{s-1} \sum_{k=t}^{s-1} u'_k v'_{k-t} x^{\mathfrak{m}-1+t} \right].\end{aligned}$$

Then, arranging the terms, we have that

$$\mathbf{u}(x) \circ \mathbf{v}(x) = \sum_{i=0}^{\mathfrak{m}-1} S_i x^{\mathfrak{m}-1-i} \mod (x^{\mathfrak{m}} - 1).$$

This implies that $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$ if and only if $S_i = 0$ for $0 \le i \le \mathfrak{m} - 1$. □

Lemma 1 *Let* $\mathbf{u}(x) = (u(x) \mid u'(x))$ *and* $\mathbf{v}(x) = (v(x) \mid v'(x))$ *be elements in* $R_{r,s}$ *such that* $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$*. If* $u'(x)$ *or* $v'(x)$ *equals* 0*, then* $u(x)v^*(x) \equiv 0 \pmod{(x^r - 1)}$*. Respectively, if* $u(x)$ *or* $v(x)$ *equals* 0*, then* $u'(x)v'^*(x) \equiv 0 \pmod{(x^s - 1)}$*.*

Proof Let $u'(x)$ or $v'(x)$ equals 0. Then

$$0 = \mathbf{u}(x) \circ \mathbf{v}(x) = u(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r) x^{\mathfrak{m}-1-\deg(v(x))} v^*(x) + 0 \mod (x^{\mathfrak{m}} - 1).$$

Therefore, $u(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r) x^{\mathfrak{m}-1-\deg(v(x))} v^*(x) = \mu'(x)(x^{\mathfrak{m}} - 1)$, for some $\mu'(x) \in \mathbb{Z}_2[x]$. Let $\mu(x) = \mu'(x) x^{\deg(v(x))+1}$. By Proposition 5, $u(x) x^{\mathfrak{m}} v^*(x) = \mu(x)(x^r - 1)$, and hence $u(x)v^*(x) \equiv 0 \pmod{(x^r - 1)}$. The same argument can be used to prove the other case. □

The following proposition shows that the dual of a separable $\mathbb{Z}_2$-double cyclic code is also separable.

Proposition 7 *Let* $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ *be a separable* $\mathbb{Z}_2$*-double cyclic code. Assume the generator polynomials of* C *satisfy the conditions in Proposition 1. Then* $\ell(x) = 0$*. Moreover,* $C^\perp$ *is a separable* $\mathbb{Z}_2$*-double cyclic code such that* $C^\perp = \langle (\frac{x^r-1}{b^*(x)} \mid 0), (0 \mid \frac{x^s-1}{a^*(x)}) \rangle$*.*

Proof If C is separable, then $C = C_r \times C_s$ and clearly $\ell(x) = 0$. Hence, it is easy to see that $C^\perp = C_r^\perp \times C_s^\perp$. By [11], we have that $C_r^\perp = \langle \frac{x^r-1}{b^*(x)} \rangle$ and $C_s^\perp = \langle \frac{x^s-1}{a^*(x)} \rangle$. Therefore, the statement follows. □

In view of Proposition 7, we shall focus on non-separable $\mathbb{Z}_2$-double cyclic codes for the rest of the section. From now on, we will denote $\gcd(b(x), l(x))$ by $g_{b,l}(x)$.

Proposition 8 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then,*

$$|C_r| = 2^{r-\deg(b(x))+\kappa}, |C_s| = 2^{s-\deg(a(x))},$$
$$|(C_r)^\perp| = 2^{\deg(b(x))-\kappa}, |(C_s)^\perp| = 2^{\deg(a(x))},$$
$$|(C^\perp)_r| = 2^{\deg(b(x))}, |(C^\perp)_s| = 2^{\deg(a(x))+\kappa},$$

where $\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$.

Proof Let C be a $\mathbb{Z}_2$-double cyclic code with $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$, and assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, by Proposition 3, C is generated by the matrix whose rows are the elements of the set $S_1 \cup S_2$. The subcode of C generated by the elements of S_1 and the subcode generated by the elements of S_2 have generator matrices of the form

$$G_1 = \left(I_{r-\deg(b(x))} \ A \middle| \ 0 \right),$$
$$G_2 = \left(B \middle| \ D \ \ I_{s-\deg(a(x))} \right),$$

respectively.

Consider the subcode C_0 of C with 0 in the first r coodinates. Clearly C_0 is generated by elements in S_2 and therefore the dimension of C_0 is $s - \deg(a(x)) - \kappa$, for some $\kappa \geq 0$. Taking into account κ and the matrices G_1 and G_2, we have that C is permutation equivalent to a binary linear code with generator matrix of the form

$$G = \left(\begin{array}{ccc|ccc} I_{r-\deg(b(x))} & A_1 & A_2 & 0 & 0 & 0 \\ 0 & B_\kappa & B_1 & D_1 & I_\kappa & 0 \\ 0 & 0 & 0 & D_2 & R & I_{s-\deg(a(x))-\kappa} \end{array} \right),$$

where B_κ is a square matrix of full rank. Note that $\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$. The cardinalities of C_r, $(C_r)^\perp$, C_s and $(C_s)^\perp$ follow easily from G. The values of $|(C^\perp)_r|$ and $|(C^\perp)_s|$ can be obtained from the projections on the first r and on the last s coordinates of the following parity check matrix of C

$$H = \left(\begin{array}{ccc|ccc} A_1^t & I_\kappa & 0 & 0 & B_\kappa^t & B_\kappa^t R^t \\ A_2^t & 0 & I_{\deg(b(x))-\kappa} & 0 & B_1^t & B_1^t R^t \\ 0 & 0 & 0 & I_{\deg(a(x))} & D_1^t & D_2^t + D_1^t R^t \end{array} \right).$$

□

Corollary 3 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

$$\deg(\bar{b}(x)) = r - \deg(g_{b,l}(x)),$$
$$\deg(\bar{a}(x)) = s - \deg(a(x)) - \deg(b(x)) + \deg(g_{b,l}(x)).$$

Proof It is easy to prove that $(C_r)^\perp$ is a cyclic code generated by $\bar{b}(x)$. Therefore, $|(C_r)^\perp| = 2^{r-\deg(\bar{b}(x))}$. Moreover, by Proposition 8, $|(C_r)^\perp| = 2^{\deg(b(x))-\kappa}$ with $\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$. Thus, $\deg(\bar{b}(x)) = r - \deg(g_{b,l}(x))$.

Since $C^\perp$ is a $\mathbb{Z}_2$-double cyclic code, $(C^\perp)_s$ is a cyclic code generated by $\bar{a}(x)$, and hence $|(C^\perp)_s| = 2^{s-\deg(\bar{a}(x))}$. By Proposition 8, we have that $|(C^\perp)_s| = 2^{\deg(a(x))+\kappa}$ with

$\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$ and consequently $\deg(\bar{a}(x)) = s - \deg(a(x)) - \deg(b(x)) + \deg(g_{b,l}(x))$. □

The previous propositions and corollaries will be helpful to determine the relations between the generator polynomials of a $\mathbb{Z}_2$-double cyclic code and the generator polynomials of its dual code.

Proposition 9 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

$$\bar{b}(x) = \frac{x^r - 1}{g^*_{b,l}(x)}.$$

Proof We have that $(\bar{b}(x) \mid 0)$ belongs to $C^\perp$. Then,

$$(b(x) \mid 0) \circ (\bar{b}(x) \mid 0) = 0,$$
$$(\ell(x) \mid a(x)) \circ (\bar{b}(x) \mid 0) = 0.$$

Applying Lemma 1 to the previous equations, we obtain

$$b(x)\bar{b}^*(x) \equiv 0 \pmod{(x^r - 1)},$$
$$\ell(x)\bar{b}^*(x) \equiv 0 \pmod{(x^r - 1)}.$$

Therefore, $g_{b,l}(x)\bar{b}^*(x) \equiv 0 \pmod{(x^r - 1)}$, and there exists $\mu(x) \in \mathbb{Z}_2[x]$ such that $g_{b,l}(x)\bar{b}^*(x) = \mu(x)(x^r - 1)$. Moreover, $g_{b,l}(x)$ and $\bar{b}^*(x)$ divide $(x^r - 1)$, and by Corollary 3 we have that $\deg(\bar{b}(x)) = r - \deg(g_{b,l}(x))$ and then $\bar{b}^*(x) = \frac{x^r - 1}{g_{b,l}(x)}$. □

Proposition 10 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

$$\bar{a}(x) = \frac{(x^s - 1)g^*_{b,l}(x)}{a^*(x)b^*(x)}.$$

Proof Consider the codeword

$$\frac{b(x)}{g_{b,l}(x)} \star (\ell(x) \mid a(x)) - \frac{\ell(x)}{g_{b,l}(x)} \star (b(x) \mid 0) = \left(0 \mid \frac{b(x)}{g_{b,l}(x)} a(x)\right).$$

Then, since $(\bar{\ell}(x) \mid \bar{a}(x)) \in C^\perp$, we have that $(\bar{\ell}(x) \mid \bar{a}(x)) \circ (0 \mid \frac{b(x)}{g_{b,l}(x)} a(x)) = 0$. Thus, by Lemma 1, $\bar{a}(x)\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} \equiv 0 \pmod{(x^s - 1)}$, and hence $\bar{a}(x)\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} = (x^s - 1)\mu(x)$, for some $\mu(x) \in \mathbb{Z}_2[x]$. By Corollary 1, it follows that $\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)}$ divides $(x^s - 1)$. Therefore, if $\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} \equiv 0 \pmod{(x^s - 1)}$ we may consider that $\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} = (x^s - 1)$. By Corollary 3, $\deg(\bar{a}(x)) = s - \deg(a(x)) - \deg(b(x)) + \deg(g_{b,l}(x))$, thus

$$\deg(x^s - 1) = s = \deg\left(\bar{a}(x)\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)}\right) = \deg((x^s - 1)\mu(x)).$$

Hence, we obtain that $\mu(x) = 1$ and $\bar{a}(x) = \frac{(x^s - 1)g^*_{b,l}(x)}{a^*(x)b^*(x)}$. □

Proposition 11 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a non-separable $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

$$\bar{\ell}(x) = \frac{x^r - 1}{b^*(x)} \lambda(x),$$

where $\lambda(x) = x^{\mathfrak{m} - \deg(a(x)) + \deg(\ell(x))} \left(\frac{\ell^*(x)}{g^*_{b,l}(x)} \right)^{-1} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right)$.

Proof Let $\bar{c}(x) = (\bar{b}(x) \mid 0) + (\bar{\ell}(x) \mid \bar{a}(x)) \in C^\perp$. Then

$$\begin{aligned} \bar{c}(x) \circ (b(x) \mid 0) &= (\bar{b}(x) \mid 0) \circ (b(x) \mid 0) + (\bar{\ell}(x) \mid \bar{a}(x)) \circ (b(x) \mid 0) \\ &= 0 + (\bar{\ell}(x) \mid \bar{a}(x)) \circ (b(x) \mid 0) = 0. \end{aligned}$$

By Lemma 1, we have that $\bar{\ell}(x) b^*(x) \equiv 0 \pmod{(x^r - 1)}$ and therefore

$$\bar{\ell}(x) = \frac{x^r - 1}{b^*(x)} \lambda(x).$$

Computing $(\bar{\ell}(x) \mid \bar{a}(x)) \circ (\ell(x) \mid a(x))$ and arranging properly we obtain

$$\frac{(x^{\mathfrak{m}} - 1) g^*_{b,l}(x)}{b^*(x)} \left(\lambda(x) x^{\mathfrak{m} - \deg(\ell(x)) - 1} \frac{\ell^*(x)}{g^*_{b,l}(x)} + x^{\mathfrak{m} - \deg(a(x)) - 1} \right),$$

that is congruent to $0 \pmod{(x^{\mathfrak{m}} - 1)}$. Then, either

$$\left(\lambda(x) x^{\mathfrak{m} - \deg(\ell(x)) - 1} \frac{\ell^*(x)}{g^*_{b,l}(x)} + x^{\mathfrak{m} - \deg(a(x)) - 1} \right) \equiv 0 \pmod{(x^{\mathfrak{m}} - 1)}, \tag{2}$$

or

$$\left(\lambda(x) x^{\mathfrak{m} - \deg(\ell(x)) - 1} \frac{\ell^*(x)}{g^*_{b,l}(x)} + x^{\mathfrak{m} - \deg(a(x)) - 1} \right) \equiv 0 \left(\mathrm{mod} \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right) \right). \tag{3}$$

Since $\frac{b^*(x)}{g^*_{b,l}(x)}$ divides $x^{\mathfrak{m}} - 1$, clearly (2) implies (3). Hence,

$$\lambda(x) x^{\mathfrak{m}} \frac{\ell^*(x)}{g^*_{b,l}(x)} = x^{\mathfrak{m} - \deg(a(x)) + \deg(\ell(x))} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right).$$

We have that $x^{\mathfrak{m}} \equiv 1 \left(\mathrm{mod} \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right)\right)$. Moreover, the greatest common divisor between $\frac{\ell(x)}{g_{b,l}(x)}$ and $\frac{b(x)}{g_{b,l}(x)}$ is 1, and then $\frac{\ell^*(x)}{g^*_{b,l}(x)}$ is an invertible element modulo $\left(\frac{b^*(x)}{g^*_{b,l}(x)} \right)$. Therefore,

$$\lambda(x) = x^{\mathfrak{m} - \deg(a(x)) + \deg(\ell(x))} \left(\frac{\ell^*(x)}{g^*_{b,l}(x)} \right)^{-1} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right).$$

□

We summarize the previous results in the next theorem.

Theorem 2 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

1. $\bar{b}(x) = \frac{x^r-1}{g^*_{b,l}(x)}$,
2. $\bar{a}(x) = \frac{(x^s-1)g^*_{b,l}(x)}{a^*(x)b^*(x)}$,
3. $\bar{\ell}(x) = \frac{x^r-1}{b^*(x)}\lambda(x)$, *where*

$$\lambda(x) = \begin{cases} 0, \text{ if } C \text{ is separable}, \\ x^{\mathfrak{m}-\deg(a(x))+\deg(\ell(x))} \left(\frac{\ell^*(x)}{g^*_{b,l}(x)}\right)^{-1} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)}\right), \mathit{otherwise}. \end{cases}$$

5 Relations between $\mathbb{Z}_2$-double cyclic codes and other codes

In this section, we study how $\mathbb{Z}_2$-double cyclic codes are related to other families of cyclic codes, say $\mathbb{Z}_4$-cyclic codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. Since these families of codes have part or all the coordinates over $\mathbb{Z}_4$, their generator polynomials also have coefficients over the ring $\mathbb{Z}_4$. From now on, the binary reduction of a polynomial $p(x) \in \mathbb{Z}_4[x]$ will be denoted by $\tilde{p}(x)$.

Let $p(x)$ be a divisor of $x^n - 1$ in $\mathbb{Z}_2[x]$ with n odd and let ξ be a primitive nth root of unity over $\mathbb{Z}_2$. The polynomial $(p \otimes p)(x)$ is defined as the divisor of $x^n - 1$ in $\mathbb{Z}_2[x]$ whose roots are the products $\xi^i\xi^j$ such that ξ^i and ξ^j are roots of $p(x)$.

From [12] and [10], it is known that a $\mathbb{Z}_4$-cyclic code $\mathcal{C}$ of length n is generated by a single element $f(x)h(x)+2f(x) \in \mathbb{Z}_4[x]/(x^n-1)$, where $f(x)h(x)g(x) = x^n - 1$ in $\mathbb{Z}_4[x]$, and $|\mathcal{C}| = 4^{\deg(g(x))}2^{\deg(h(x))}$.

Let $\mathbf{u} = (u_0, \ldots, u_{n-1})$ be an element of $\mathbb{Z}_4^n$ such that $u_i = \tilde{u}_i + 2u'_i$ with $\tilde{u}_i, u'_i \in \{0, 1\}$. As in [9], the *Gray map* ϕ from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ is defined by

$$\phi(\mathbf{u}) = (u'_0, \ldots, u'_{n-1} \mid \tilde{u}_0 + u'_0, \ldots, \tilde{u}_{n-1} + u'_{n-1}).$$

Let $\mathbf{u}(x) = \tilde{\mathbf{u}}(x) + 2\mathbf{u}'(x)$ be the polynomial representation of $\mathbf{u} \in \mathbb{Z}_4^n$. Then, the polynomial version of the Gray map is $\phi(\mathbf{u}(x)) = (\mathbf{u}'(x) \mid \tilde{\mathbf{u}}(x) + \mathbf{u}'(x))$. The *Nechaev permutation* is the permutation π on $\mathbb{Z}_2^{2n}$ with n odd defined by

$$\pi(v_0, v_1, \ldots, v_{2n-1}) = (v_{\tau(0)}, v_{\tau(1)}, \ldots, v_{\tau(2n-1)}),$$

where τ is the permutation on $\{0, 1, \ldots, 2n-1\}$ given by

$$(1, n+1)(3, n+3)\ldots(2i+1, n+2i+1)\ldots(n-2, 2n-2).$$

Let ψ be the map from $\mathbb{Z}_4^n$ into $\mathbb{Z}_2^{2n}$ defined by $\psi = \pi\phi$, with n odd. The map ψ is called the *Nechaev–Gray map*, [15]. Therefore we give the following theorem.

Theorem 3 ([15, Theorem 20]) *Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$ be a $\mathbb{Z}_4$-cyclic code of odd length n and where $f(x)h(x)g(x) = x^n - 1$. Let ϕ be the Gray map and let ψ be the Nechaev–Gray map. The following properties are equivalent.*

1. $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$ *in* $\mathbb{Z}_2[x]$*;*
2. $\phi(\mathcal{C})$ *is a binary linear code of length* $2n$*;*
3. $\psi(\mathcal{C})$ *is a binary linear cyclic code of length* $2n$ *generated by* $\tilde{f}(x)^2\tilde{h}(x)$.

Using the last theorem, we can relate $\mathbb{Z}_2$-double cyclic codes to $\mathbb{Z}_4$-cyclic codes.

5.1 $\mathbb{Z}_2$-double cyclic codes versus $\mathbb{Z}_4$-cyclic codes

Let $\mathcal{C}$ be a $\mathbb{Z}_4$-cyclic code of length n, and $\mathbf{w} \in \phi(\mathcal{C})$. The codeword $\mathbf{w}$ can be written as $(u'_0, \ldots, u'_{n-1} \mid \tilde{u}_0 + u'_0, \ldots, \tilde{u}_{n-1} + u'_{n-1})$, for $(u_0, \ldots, u_{n-1}) = \mathbf{u} = \phi^{-1}(\mathbf{w}) \in \mathcal{C}$. By definition of the Gray map, we have that $\mathbf{w}^{(1)}$ is $(u'_{n-1}, u'_0, \ldots, u'_{n-2} \mid \tilde{u}_{n-1} + u'_{n-1}, \tilde{u}_0 + u'_0, \ldots, \tilde{u}_{n-2} + u'_{n-2}) = \phi(u_{n-1}, u_0, \ldots, u_{n-2})$. Therefore, since $\mathcal{C}$ is $\mathbb{Z}_4$-cyclic, we have that $\mathbf{w}^{(i)} \in \phi(\mathcal{C})$.

In general, the Gray image of a linear code over $\mathbb{Z}_4$ is not linear. Hence, we shall consider $\mathbb{Z}_2$-double cyclic codes as images of $\mathbb{Z}_4$-cyclic codes, $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$, in the case that such a code $\mathcal{C}$ has linear image under the Gray map; that is, when $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$ in $\mathbb{Z}_2[x]$, by Theorem 3. Consequently, we obtain the following proposition.

Proposition 12 *Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$ be a $\mathbb{Z}_4$-cyclic code of odd length n, where $f(x)h(x)g(x) = x^n - 1$, and $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$. Then, $\phi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$.*

Our goal is to establish a relation between the generator polynomial of the $\mathbb{Z}_4$-cyclic code $\mathcal{C}$ and its $\mathbb{Z}_2$-double cyclic image, $\phi(\mathcal{C})$.

Let $i \in \{2, 4\}$. If $\mathcal{C}$ is a $\mathbb{Z}_i[x]$-module and $g_1, \ldots, g_t \in \mathcal{C}$. Then $\langle g_1, \ldots, g_t\rangle_i$ will denote the $\mathbb{Z}_i[x]$-submodule of $\mathcal{C}$ generated by $g_1, \ldots, g_t$.

The following theorem is proved in [14, Theorem 8].

Theorem 4 *Let n be odd and let $f(x), h(x), g(x)$ be in $\mathbb{Z}_4[x]$ such that $f(x)h(x)g(x) = x^n - 1$. Then $\langle f(x)h(x) + 2f(x)\rangle_4 = \langle \tilde{f}(x)\tilde{h}(x)\rangle_2 + 2\langle \tilde{f}(x)\rangle_2$ if and only if $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$ in $\mathbb{Z}_2[x]$.*

Lemma 2 *Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_4$ of type $2^\gamma 4^\delta$ such that $\phi(\mathcal{C})$ is a linear code. Let $\{\mathbf{u}_i\}_{i=1}^{\gamma}$ be codewords of order two and $\{\mathbf{v}_j\}_{j=1}^{\delta}$ codewords of order four such that $\mathcal{C} = \langle \{\mathbf{u}_i\}_{i=1}^{\gamma}, \{\mathbf{v}_j\}_{j=1}^{\delta}\rangle_4$. Then,*

$$\phi(\mathcal{C}) = \langle \{\phi(\mathbf{u}_i)\}_{i=1}^{\gamma}, \{\phi(\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j)\}_{j=1}^{\delta}\rangle_2.$$

Proof From [6, Lemma 3], it is known that if $\mathcal{C}$ is a linear code over $\mathbb{Z}_4$ of type $2^\gamma 4^\delta$ such that $\mathcal{C} = \langle \{\mathbf{u}_i\}_{i=1}^{\gamma}, \{\mathbf{v}_j\}_{j=1}^{\delta}\rangle_4$, then

$$\langle \phi(\mathcal{C})\rangle_2 = \langle \{\phi(\mathbf{u}_i)\}_{i=1}^{\gamma}, \{\phi(\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j * \mathbf{v}_t)\}_{1\le j<t\le\delta}\rangle_2,$$

where $\mathbf{u} * \mathbf{v}$ denote the component-wise product for any $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^n$. We know that $\phi(\mathcal{C})$ is linear if and only if $2\mathbf{u} * \mathbf{v} \in \mathcal{C}$ for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, [9]. Since $\phi(\mathcal{C})$ is a binary linear code, then $\{2\mathbf{v}_j * \mathbf{v}_t\}_{1\le j<t\le\delta} \in \mathcal{C}$. Therefore, $\langle \{\phi(2\mathbf{v}_j * \mathbf{v}_t)\}_{1\le j<t\le\delta}\rangle_2 \subseteq \langle \{\phi(\mathbf{u}_i)\}_{i=1}^{\gamma}, \{\phi(\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j)\}_{j=1}^{\delta}\rangle_2$. □

Theorem 5 *Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle_4$ be a $\mathbb{Z}_4$-cyclic code of odd length n, where $f(x)h(x)g(x) = x^n - 1$ and $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$. Then,*

$$\phi(\mathcal{C}) = \langle (\tilde{f}(x)\tilde{h}(x) \mid 0), (\tilde{f}(x) \mid \tilde{f}(x))\rangle_2.$$

Proof By Theorem 4, the generators of $\mathcal{C}$ are $\langle \tilde{f}(x)\tilde{h}(x)\rangle_2$ and $2\langle \tilde{f}(x)\rangle_2$. By Proposition 12, we have that $\phi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code. Then, by Lemma 2, it is easy to see that the generator polynomials of $\phi(\mathcal{C})$ are $\phi(\tilde{f}(x)\tilde{h}(x))$ and $\phi(2\tilde{f}(x))$. The corresponding images of the Gray map are $\phi(\tilde{f}(x)\tilde{h}(x)) = (0 \mid \tilde{f}(x)\tilde{h}(x))$ and $\phi(2\tilde{f}(x)) = (\tilde{f}(x) \mid \tilde{f}(x))$, hence $\phi(\mathcal{C}) = \langle (0 \mid \tilde{f}(x)\tilde{h}(x)), (\tilde{f}(x) \mid \tilde{f}(x))\rangle_2$. Therefore,

$$\phi(\mathcal{C}) = \langle (\tilde{f}(x)\tilde{h}(x) \mid 0), (\tilde{f}(x) \mid \tilde{f}(x))\rangle_2.$$

□

5.2 $\mathbb{Z}_2$-double cyclic codes versus $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ (see [4]). Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to a commutative structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ and it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called cyclic if the set of coordinates can be partitioned into two subsets, the set of $\mathbb{Z}_2$ and the set of $\mathbb{Z}_4$ coordinates, denoted by X and Y, such that any cyclic shift of the coordinates of both subsets leaves invariant the code. As it was done in (1), for $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we also denote by $(\mathbf{u}, \mathbf{v})^{(1)}$ such shift. These codes can be identified as submodules of the $\mathbb{Z}_4[x]$-module $\mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$. From [1] and [5], we know that if $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, where β is an odd integer, then it is of the form

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle_4,$$

where $f(x)h(x)g(x) = x^\beta - 1$ in $\mathbb{Z}_4[x]$, $b(x), \ell(x) \in \mathbb{Z}_2[x]/(x^\alpha - 1)$ with $b(x)|(x^\alpha - 1)$, $deg(\ell(x)) < deg(b(x))$, and $b(x)$ divides $\frac{x^\beta - 1}{f(x)}\ell(x) \pmod 2$.

The *extended Gray map* Φ and the *extended Nechaev–Gray map* Ψ are the maps from $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ into $\mathbb{Z}_2^{\alpha+2\beta}$ given by

$$\Phi(\mathbf{u}, \mathbf{v}) = (\mathbf{u}, \phi(\mathbf{v})), \quad \Psi(\mathbf{u}, \mathbf{v}) = (\mathbf{u}, \psi(\mathbf{v})),$$

where $\mathbf{u} \in \mathbb{Z}_2^\alpha$, $\mathbf{v} \in \mathbb{Z}_4^\beta$, ϕ is the Gray map and ψ is the Nechaev–Gray map.

Table 1 Optimal $\mathbb{Z}_2$-double cyclic codes

Code	Generators	[r, s]	Parameters
C_1	$b(x) = x^2 + x + 1, \ell(x) = x, a(x) = x + 1$	[3,3]	$[\,6, 3, 3\,]^*$
C_2	$b(x) = x^2 + 1, \ell(x) = 1, a(x) = x^2 + x + 1$	[2,6]	$[\,8, 4, 4\,]^*_s$
C_3	$b(x) = x^3 + x^2 + x + 1, \ell(x) = x^2 + x, a(x) = x + 1$	[4,4]	$[\,8, 4, 4\,]^*_s$
C_4	$b(x) = x^4+x^3+x+1, \ell(x) = x^2+x+1, a(x) = x^2+x+1$	[6,6]	$[\,12, 6, 4\,]^*_s$
C_5	$b(x) = x^7+1, \ell(x) = x^4+x^2+x+1, a(x) = x^4+x^2+x+1$	[7,7]	$[\,14, 3, 8\,]^*$
C_6	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x^2 + 1, a(x) = x^4 + x^2 + x + 1$	[7,7]	$[\,14, 4, 7\,]^*$
C_7	$b(x) = x^4 + x^3 + x^2 + 1, \ell(x) = x^3 + x + 1, a(x) = x^3 + x^2 + 1$	[7,7]	$[\,14, 7, 4\,]^*_s$
C_8	$b(x) = x^7 + 1, \ell(x) = x^3 + x + 1, a(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$	[7,14]	$[\,21, 5, 10\,]^*$
C_9	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^4 + x^3 + 1, a(x) = x^5 + x^2 + x + 1$	[7,14]	$[\,21, 10, 7\,]^*$
C_{10}	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x)$ $s = x + 1, a(x) = x^3 + x^2 + 1$	[7,14]	$[\,21, 12, 5\,]^*$
C_{11}	$b(x) = x^3 + x^2 + 1, \ell(x) = 1, a(x) = x^2 + 1$	[7,14]	$[\,21, 16, 3\,]^*$
C_{12}	$b(x) = x^2 + 1, \ell(x) = x + 1, a(x) = x^{16} + x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x + 1$	[2,30]	$[\,32, 14, 8\,]$
C_{13}	$b(x) = x^{20} + x^{19} + x^{18} + x^{17} + x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^3 + x^2 + x + 1, \ell(x) = x^{15} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^5 + 1, a(x) = x^6 + x^4 + x^3 + 1$	[31,31]	$[\,62, 36, 10\,]$

Call $\mathcal{C}_X$ (respectively $\mathcal{C}_Y$) the punctured code of $\mathcal{C}$ by deleting the coordinates outside X (respectively Y). Notice that if $\phi(\mathcal{C}_Y)$ and $\psi(\mathcal{C}_Y)$ are binary linear codes, then $\Phi(\mathcal{C})$ and $\Psi(\mathcal{C})$ are not necessary binary linear codes.

Example 2 Let $\mathcal{C} = \langle (x-1 \mid x+1)\rangle_4 \subset \mathbb{Z}_2^2 \times \mathbb{Z}_4^3$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $b(x) = 0$, $\ell(x) = x-1$, $f(x) = 1$, $h(x) = x-1$ and $g(x) = x^2+x+1$. Since $f(x) = 1$, by Theorem 3, we have that $\phi(\mathcal{C}_Y)$ is linear. By [5], a generator matrix for $\mathcal{C}$ is

$$\left(\begin{array}{cc|ccc} 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 \end{array}\right).$$

We know that $\Phi(\mathcal{C})$ is linear if and only if $2(\mathbf{u},\mathbf{v}) * (\mathbf{w},\mathbf{z}) \in \mathcal{C}$ for all $(\mathbf{u},\mathbf{v}), (\mathbf{w},\mathbf{z}) \in \mathcal{C}$, [7]. Clearly, $2(0,0,3,1,0) * (0,0,3,0,1) = (0,0,2,0,0) \notin \mathcal{C}$. Therefore, $\Phi(\mathcal{C})$ is not a binary linear code.

Theorem 6 *Let $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x))\rangle_4 \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, where β is an odd integer and $f(x)h(x)g(x) = x^\beta - 1$. Let Ψ be the extended Nechaev–Gray map. If $\Psi(\mathcal{C})$ is a binary linear code, then $\Psi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code of length $\alpha + 2\beta$ and dimension $\alpha - \deg(b(x)) + \deg(h(x)) + 2\deg(g(x))$.*

Proof By the definition of Ψ, the length of $\Psi(\mathcal{C})$ is $\alpha+2\beta$ and, since $\Psi(\mathcal{C})$ is a linear code, we need to prove that $\Psi((\mathbf{u},\mathbf{v}))^{(1)} \in \Psi(\mathcal{C})$ for all $(\mathbf{u},\mathbf{v}) \in \mathcal{C}$. By [15], we can easily deduce that $\Psi((\mathbf{u},\mathbf{v}))^{(1)} = \Psi((\mathbf{u},-\mathbf{v})^{(1)})$. We have that $(\mathbf{u},-\mathbf{v})^{(1)} \in \mathcal{C}$ and consequently $\Psi((\mathbf{u},\mathbf{v}))^{(1)}$ belongs to $\Psi(\mathcal{C})$. Hence, $\Psi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code. Finally, since $|\Psi(\mathcal{C})| = |\mathcal{C}|$, we have that $|\mathcal{C}| = 2^{\alpha - \deg(b(x)) + \deg(h(x))} 4^{\deg(g(x))}$ by [1]. □

Table 2 Dual $\mathbb{Z}_2$-double cyclic codes

Code	Generators of the dual codes	[r, s]	Parameters
C_1	$\bar{b}(x) = x^3+1, \bar{\ell}(x) = x+1, \bar{a}(x) = 1$	[3,3]	$[\,6, 3, 3\,]$
C_2	$\bar{b}(x) = x^2+1, \bar{\ell}(x) = 1, \bar{a}(x) = x^2+x+1$	[2,6]	$[\,8, 4, 4\,]^s$
C_3	$\bar{b}(x) = x^3+x^2+x+1, \bar{\ell}(x) = x^2+x, \bar{a}(x) = x+1$	[4,4]	$[\,8, 4, 4\,]^s$
C_4	$\bar{b}(x) = x^4+x^3+x+1, \bar{\ell}(x) = x^2+x+1, \bar{a}(x) = x^2+x+1$	[6,6]	$[\,12, 6, 4\,]^s$
C_5	$\bar{b}(x) = x^3+x^2+1, \bar{\ell}(x) = 1, \bar{a}(x) = 1$	[7,7]	$[\,14, 11, 2\,]$
C_6	$\bar{b}(x) = x^4+x^2+x+1, \bar{\ell}(x) = x^3+x, \bar{a}(x) = 1$	[7,7]	$[\,14, 10, 3\,]$
C_7	$\bar{b}(x) = x^4+x^3+x^2+1, \bar{\ell}(x) = x^3+x+1, \bar{a}(x) = x^3+x^2+1$	[7,7]	$[\,14, 7, 4\,]^s$
C_8	$\bar{b}(x) = x^4+x^3+x^2+1, \bar{\ell}(x) = x, \bar{a}(x) = x+1$	[7,14]	$[\,21, 16, 3\,]$
C_9	$\bar{b}(x) = x^7+1, \bar{\ell}(x) = x^4+x^3+x^2+x, \bar{a}(x) = x^3+x+1$	[7,14]	$[\,21, 11, 6\,]$
C_{10}	$\bar{b}(x) = x^7+1, \bar{\ell}(x) = x^6+x^4+x^3+x^2+x+1, \bar{a}(x) = x^5+x^4+x^3+1$	[7,14]	$[\,21, 9, 6\,]$
C_{11}	$\bar{b}(x) = x^7+1, \bar{\ell}(x) = x^6+x^5+x^2+1, \bar{a}(x) = x^9+x^6+x^5+x^4+x^3+x+1$	[7,14]	$[\,21, 5, 7\,]$
C_{12}	$\bar{b}(x) = x+1, \bar{\ell}(x) = 1, \bar{a}(x) = x^{13}+x^{11}+x^9+x^8+x^7+x^2+x+1$	[2,30]	$[\,32, 18, 2\,]$
C_{13}	$\bar{b}(x) = x^{26}+x^{23}+x^{21}+x^{20}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^9+x^8+x^6+x^5+x^4+x^2+1, \bar{\ell}(x) = x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{13}+x^{11}+x^{10}+x^8+x^5+x^3+x, \bar{a}(x) = x^{10}+x^9+x^3+x+1$	[31,31]	$[\,62, 26, 15\,]$

Table 3 $\mathbb{Z}_2$-double cyclic codes from $\mathbb{Z}_4$-cyclic codes

n	$\mathbb{Z}_4$-cyclic generators	$\mathbb{Z}_2$-double cyclic generators	Binary parameters
3	$f(x)h(x) = x^3 + 3,\ f(x) = x + 3$	$b(x) = x^3 + 1, \ell(x) = x + 1, a(x) = x + 1$	[6, 2, 4]
7	$f(x)h(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\ f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x^2 + 1, a(x) = x^3 + x^2 + 1$	[14, 5, 6]
7	$f(x)h(x) = x^4 + 2x^3 + 3x^2 + x + 1,\ f(x) = x + 3$	$b(x) = x^4 + x^2 + x + 1, \ell(x) = x + 1, a(x) = x + 1$	[14, 9, 4]
9	$f(x)h(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\ f(x) = x^2 + x + 1$	$b(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^2 + x + 1, a(x) = x^2 + x + 1$	[18, 8, 4]
9	$f(x)h(x) = x^7 + 3x^6 + x^4 + 3x^3 + x + 3,\ f(x) = x^6 + x^3 + 1$	$b(x) = x^7 + x^6 + x^4 + x^3 + x + 1, \ell(x) = x^6 + x^3 + 1, a(x) = x^6 + x^3 + 1$	[18, 5, 6]
15	$f(x)h(x) = x^{11} + 3x^{10} + x^6 + 3x^5 + x + 3,\ f(x) = x^4 + 3x^3 + 2x^2 + 1$	$b(x) = x^{11} + x^{10} + x^6 + x^5 + x + 1, \ell(x) = x^4 + x^3 + 1, a(x) = x^4 + x^3 + 1$	[30, 15, 6]
15	$f(x)h(x) = x^{13} + 3x^{12} + x^{10} + 3x^9 + x^7 + 3x^6 + x^4 + 3x^3 + x + 3,\ f(x) = x^4 + 3x^3 + 2x^2 + 1$	$b(x) = x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1, \ell(x) = x^4 + x^3 + 1, a(x) = x^4 + x^3 + 1$	[30, 13, 6]

Table 4 $\mathbb{Z}_2$-double cyclic codes from $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes

$[\alpha, \beta]$	$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic generators	$\mathbb{Z}_2$-double cyclic generators	Binary parameters
[2,3]	$b(x) = x^2 + 1, \ell(x) = x + 1, f(x)h(x) = x^3 + 3, f(x) = 1$	$b(x) = x^2 + 1, \ell(x) = x + 1, a(x) = x^3 + 1$	[8, 3, 4]
[3,3]	$b(x) = x^2 + x + 1, \ell(x) = x, f(x)h(x) = x^2 + x + 1, f(x) = 1$	$b(x) = x^2 + x + 1, \ell(x) = x + 1, a(x) = x^2 + x + 1$	[9, 5, 3]
[9,3]	$b(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^6 + x^3 + 1, f(x)h(x) = x^3 + 3, f(x) = x + 3$	$b(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^6 + x^3 + 1, a(x) = x^4 + x^3 + x + 1$	[15, 3, 7]
[4,7]	$b(x) = x^3 + x^2 + x + 1, \ell(x) = x^2 + 1, f(x)h(x) = x^4 + 2x^3 + 3x^2 + x + 1, f(x) = 1$	$b(x) = x^3 + x^2 + x + 1, \ell(x) = x^2 + 1, a(x) = x^4 + x^2 + x + 1$	[18, 11, 4]
[4,7]	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, f(x)h(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, a(x) = x^9 + x^6 + x^5 + x^4 + x^3 + x + 1$	[18, 5, 6]
[4,7]	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, f(x)h(x) = x^7 + 3, f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, a(x) = x^{10} + x^9 + x^7 + x^3 + x^2 + 1$	[18, 4, 8]
[7,7]	$b(x) = x^7 + 1, \ell(x) = x^6 + x^5 + x^3, f(x)h(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^7 + 1, \ell(x) = x^3 + x^2 + 1, a(x) = x^9 + x^6 + x^5 + x^4 + x^3 + x + 1$	[21, 5, 10]
[7,7]	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x + 1, f(x)h(x) = x^7 + 1, f(x) = x + 3$	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x + 1, a(x) = x^8 + x^7 + x + 1$	[21, 7, 7]
[7,7]	$b(x) = x^3 + x + 1, \ell(x) = x, f(x)h(x) = x^4 + 2x^3 + 3x^2 + x + 1, f(x) = x + 3$	$b(x) = x^3 + x + 1, \ell(x) = x^2 + x, a(x) = x^5 + x^4 + x^3 + 1$	[21, 13, 3]

6 Examples

Table 1 gives some examples of $\mathbb{Z}_2$-double cyclic codes which have the best known minimum distance. In the table, the parameters are $[n, k, d]$, where $n = r + s$ is the length, k is the dimension, and d is the minimum distance of the code. It is denoted by $[.]^*$ when the code is optimal according to [8]. It is denoted by $[.]_s$ when the code is self-dual. Table 2 shows the generators and the parameters of the dual codes of the codes in Table 1.

In Sect. 5, we have studied how $\mathbb{Z}_2$-double cyclic codes are related to other families of cyclic codes. By Theorem 5, we know how to construct the generators of $\mathbb{Z}_2$-double cyclic codes starting from the generators of $\mathbb{Z}_4$-cyclic codes. Also, by Theorem 6 we know that the image of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code under the Nechaev–Gray map, whenever it is linear, is also a $\mathbb{Z}_2$-double cyclic code. In Tables 3, 4, we present some examples of $\mathbb{Z}_2$-double cyclic codes obtained from $\mathbb{Z}_4$-cyclic codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

Acknowledgements This work has been partially supported by the Spanish MINECO Grants TIN2016-77918-P and MTM2015-69138-REDT, and by the Catalan AGAUR Grant 2014SGR-691.

References

1. Abualrub T., Siap I., Aydin N.: $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. IEEE Trans. Inf. Theory **60**, 1508–1514 (2014).
2. Aydogdu I., Abualrub T., Siap I.: On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. Int. J. Comput. Math. **92**(9), 1806–1814 (2015).
3. Aydogdu I., Abualrub T., Siap I.: $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes. IEEE Trans. Inf. Theory. doi:10.1109/TIT.2016.2632163.
4. Borges J., Fernández-Córdoba C., Pujol J., Rifà J., Villanueva M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. Des. Codes Cryptogr. **54**, 167–179 (2010).
5. Borges J., Fernández-Córdoba C., Ten-Valls R.: $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes. IEEE Trans. Inf. Theory **62**, 6348–6354 (2016).
6. Fernández-Córdoba C., Pujol J., Villanueva M.: On Rank and Kernel of $\mathbb{Z}_4$-Linear Codes. Lecture Notes in Computer Science, vol. 5228, pp. 46–55. Springer, Berlin (2008).
7. Fernández-Córdoba C., Pujol J., Villanueva M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel. Des. Codes Cryptogr. **56**, 43–59 (2010).
8. Grassl M.: Table of bounds on linear codes. [Online]. Available: http://www.codestable.de (1995).
9. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.: The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes. IEEE Trans. Inf. Theory **40**, 301–319 (1994).
10. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
11. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, New York (1977).
12. Pless V.S., Qian Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory **42**, 1594–1600 (1996).
13. Siap I., Kulhan N.: The structure of generalized quasi cyclic codes. Appl. Math. E-Notes **5**, 24–30 (2005).
14. Vega G., Wolfmann J.: Some families of $\mathbb{Z}_4$-cyclic codes. Finite Fields Appl. **10**, 530–539 (2004).
15. Wolfmann J.: Binary images of cyclic codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory **47**, 1773–1779 (2001).