$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes

Joaquim Borges, Cristina Fernández-Córdoba, and Roger Ten-Vallsspace

Abstract

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, such that any cyclic shift of the coordinates of both subsets leaves the code invariant. These codes can be identified as submodules of the $\mathbb{Z}_4[x]$-module $\mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$. The parameters of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code are stated in terms of the degrees of the generator polynomials of the code. The generator polynomials of the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code are determined in terms of the generator polynomials of the code $\mathcal{C}$.

Index Terms

Binary cyclic codes, Cyclic codes over $\mathbb{Z}_4$, Duality, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

I. Introduction

Denote by $\mathbb{Z}_2$ and $\mathbb{Z}_4$ the rings of integers modulo 2 and modulo 4, respectively. We denote the space of n-tuples over these rings as $\mathbb{Z}_2^n$ and $\mathbb{Z}_4^n$. A binary code is any non-empty subset C of $\mathbb{Z}_2^n$. If that subset is a vector space then we say that it is a linear code. A code over $\mathbb{Z}_4$ is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ and a submodule of $\mathbb{Z}_4^n$ is called a linear code over $\mathbb{Z}_4$.

In Delsarte's 1973 paper (see [5]), he defined additive codes as subgroups of the underlying abelian group in a translation association scheme. For the binary Hamming scheme, namely, when the underlying abelian group is of order 2^n, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$. This means that the subgroups $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in a binary Hamming scheme. In [4], $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were studied.

Manuscript received Month day, year; revised Month day, year.

J. Borges is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: joaquim.borges@uab.cat)

C. Fernández-Córdoba is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: cristina.fernandez@uab.cat).

R. Ten-Valls is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: roger.ten@uab.cat)

This work has been partially supported by the Spanish MINECO grant TIN2016-77918-P and by the Catalan AGAUR grant 2014SGR-691.

This paper was presented in part at Karatekin Mathematics Days 2014, International Mathematics Symposium, Çankırı, Turkey.

For vectors $\mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we write $\mathbf{u} = (u \mid u')$ where $u = (u_0, \dots, u_{\alpha-1}) \in \mathbb{Z}_2^\alpha$ and $u' = (u'_0, \dots, u'_{\beta-1}) \in \mathbb{Z}_4^\beta$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. 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 $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and the number of order two codewords in $\mathcal{C}$ is $2^{\gamma+\delta}$.

Let X (respectively Y) be the set of $\mathbb{Z}_2$ (respectively $\mathbb{Z}_4$) coordinate positions, so $|X| = \alpha$ and $|Y| = \beta$. Unless otherwise stated, the set X corresponds to the first α coordinates and Y corresponds to the last β coordinates. Call $\mathcal{C}_X$ (respectively $\mathcal{C}_Y$) the punctured code of $\mathcal{C}$ by deleting the coordinates outside X (respectively Y). Let $\mathcal{C}_b$ be the subcode of $\mathcal{C}$ which contains all order two codewords and let κ be the dimension of $(\mathcal{C}_b)_X$, which is a binary linear code. For the case $\alpha = 0$, we will write $\kappa = 0$.

Considering all these parameters, we will say that $\mathcal{C}$ is of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Notice that $\mathcal{C}_Y$ is a linear code over $\mathbb{Z}_4$ of type $(0, \beta; \gamma_Y, \delta; 0)$, where $0 \leq \gamma_Y \leq \gamma$, and $\mathcal{C}_X$ is a binary linear code of type $(\alpha, 0; \gamma_X, 0; \gamma_X)$, where $\kappa \leq \gamma_X \leq \kappa + \delta$. A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is said to be separable if $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$.

Let κ_1 and δ_2 be the dimensions of the subcodes $\{(u \mid 0 \dots 0) \in \mathcal{C}\}$ and $\{(0 \dots 0 \mid u') \in \mathcal{C} : \text{ the order of } u' \text{ is } 4\}$, respectively. Define $\kappa_2 = \kappa - \kappa_1$ and $\delta_1 = \delta - \delta_2$. By definition, it is clear that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is separable if and only if κ_2 and δ_1 are zero; that is, $\kappa = \kappa_1$ and $\delta = \delta_2$.

We define a Gray Map as $\phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \to \mathbb{Z}_2^{\alpha+2\beta}$ such that $\phi(\mathbf{u}) = \phi(u \mid u') = (u, \phi_4(u'))$, where ϕ_4 is the usual quaternary Gray map defined by $\phi_4(0) = (0,0), \phi_4(1) = (0,1), \phi_4(2) = (1,1), \phi_4(3) = (1,0)$.

The *standard inner product*, defined in [4], can be written as

$$\mathbf{u} \cdot \mathbf{v} = 2 \left(\sum_{i=0}^{\alpha-1} u_i v_i \right) + \sum_{j=0}^{\beta-1} u'_j v'_j \in \mathbb{Z}_4,$$

where the computations are made taking the zeros and ones in the α binary coordinates as zeros and ones in $\mathbb{Z}_4$, respectively. The *dual code* of $\mathcal{C}$, is defined in the standard way by

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \mathbf{u} \cdot \mathbf{v} = 0, \text{ for all } \mathbf{u} \in \mathcal{C}\}.$$

If $\mathcal{C}$ is separable then $\mathcal{C}^\perp = (\mathcal{C}_X)^\perp \times (\mathcal{C}_Y)^\perp$. From [4], and the previous definition of κ_1 and δ_1 we obtain the number of codewords of $\mathcal{C}$, $\mathcal{C}_X$, $\mathcal{C}_Y$ and their duals.

Proposition 1.1: Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Let κ_1 and δ_1 be defined as before. Then,

$$|\mathcal{C}| = 2^\gamma 4^\delta, \quad |\mathcal{C}^\perp| = 2^{\alpha+\gamma-2\kappa} 4^{\beta-\gamma-\delta+\kappa},$$

$$|\mathcal{C}_X| = 2^{\kappa+\delta_1}, \quad |(\mathcal{C}_X)^\perp| = 2^{\alpha-\kappa-\delta_1},$$

$$|\mathcal{C}_Y| = 2^{\gamma-\kappa_1} 4^\delta, \quad |(\mathcal{C}_Y)^\perp| = 2^{\gamma-\kappa_1} 4^{\beta-\gamma-\delta+\kappa_1}.$$

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Then, $\mathcal{C}$ is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with generator matrix of the form

$$\mathcal{G}_\mathcal{C} = \left(\begin{array}{cccc|ccccc} I_{\kappa_1} & T & T'_{b_1} & T_{b_1} & 0 & 0 & 0 & 0 & 0 \\ 0 & I_{\kappa_2} & T'_{b_2} & T_{b_2} & 2T_2 & 2T_{\kappa_2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2T_1 & 2T'_1 & 2I_{\gamma-\kappa} & 0 & 0 \\ \hline 0 & 0 & S_{\delta_1} & S_b & S_{11} & S_{12} & R_1 & I_{\delta_1} & 0 \\ 0 & 0 & 0 & 0 & S_{21} & S_{22} & R_2 & R_{\delta_1} & I_{\delta_2} \end{array}\right)$$

where I_r is the identity matrix of size $r \times r$; the matrices $T_{b_i}, T'_{b_i}, S_{\delta_1}, S_b$ are over $\mathbb{Z}_2$; the matrices $T_1, T_2, T_{\kappa_2}, T'_1, R_i$ are over $\mathbb{Z}_4$ with all entries in $\{0,1\} \subset \mathbb{Z}_4$; and S_{ij} are matrices over $\mathbb{Z}_4$. The matrices S_{δ_1} and T_{κ_2} are square matrices of full rank δ_1 and κ_2 respectively, $\kappa = \kappa_1 + \kappa_2$ and $\delta = \delta_1 + \delta_2$.

This new generator matrix can be obtained by applying convenient column permutations and linear combinations of rows to the generator matrix given in [4]. This new form is going to help us to relate the parameters of the code and the degrees of the generator polynomials of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code.

II. $\mathbb{Z}_2\mathbb{Z}_4$-ADDITIVE CYCLIC CODES

A. *Parameters and generators*

Let $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and i be an integer. Then we denote by

$$\begin{aligned} \mathbf{u}^{(i)} &= (u^{(i)} \mid u'^{(i)}) \\ &= (u_{0+i}, u_{1+i}, \dots, u_{\alpha-1+i} \mid u'_{0+i}, u'_{1+i}, \dots, u'_{\beta-1+i}) \end{aligned}$$

the cyclic ith shift of $\mathbf{u}$, where the subscripts are read modulo α and β, respectively.

We say that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is *cyclic* if for any codeword $\mathbf{u} \in \mathcal{C}$ we have $\mathbf{u}^{(1)} \in \mathcal{C}$.

Let $R_{\alpha,\beta} = \mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$, for $\beta \geq 0$ odd, and define the operation $\star : \mathbb{Z}_4[x] \times R_{\alpha,\beta} \to R_{\alpha,\beta}$ as $\lambda(x) \star (p(x) \mid q(x)) = (\lambda(x)p(x) \bmod (2) \mid \lambda(x)q(x))$. From [1], we know that $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes are identified as $\mathbb{Z}_4[x]$-submodules of $R_{\alpha,\beta}$. Moreover, if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then it is of the form

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle, \tag{1}$$

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 $\frac{x^\beta - 1}{f(x)}\ell(x) \pmod 2$.

Note that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle$, then the canonical projections $\mathcal{C}_X$ and $\mathcal{C}_Y$ are a cyclic code over $\mathbb{Z}_2$ and a cyclic code over $\mathbb{Z}_4$ generated by $gcd(b(x), \ell(x))$ and $(f(x)h(x) + 2f(x))$, respectively (see [6], [9]).

Since $b(x)$ divides $\frac{x^\beta - 1}{f(x)}\ell(x) \pmod 2$, we have the following result.

Corollary 2.1: Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle$. Then, $b(x)$ divides $\frac{x^\beta - 1}{f(x)} \gcd(b(x), \ell(x)) \pmod 2$ and $b(x)$ divides $h(x)\gcd(b(x), \ell(x)g(x)) \pmod 2$.

Note that if a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is separable, then $\ell(x) = 0$.

In the following, a polynomial $f(x) \in \mathbb{Z}_2[x]$ or $\mathbb{Z}_4[x]$ will be denoted simply by f and the parameter β will be an odd integer.

Lemma 2.2: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code. Then,

$$\mathcal{C}_b = \langle (b \mid 0), (\ell g \mid 2fg), (0 \mid 2fh) \rangle.$$

Proof: $\mathcal{C}_b$ is the subcode of $\mathcal{C}$ which contains all codewords of order 2. Since $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$, then all codewords of order 2 are generated by $\langle (b \mid 0), (\ell g \mid 2fg), (0 \mid 2fh) \rangle$. ■

The following results show the close relation of the parameters of the type of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code and the degrees of the generator polynomials of the code.

First, the next theorem gives the spanning sets in terms of the generator polynomials.

Theorem 2.3: [1, Theorem 13] Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fhg = x^\beta - 1$. Let

$$S_1 = \bigcup_{i=0}^{\alpha - \deg(b) - 1} \{x^i \star (b \mid 0)\},$$

$$S_2 = \bigcup_{i=0}^{\deg(g) - 1} \{x^i \star (\ell \mid fh + 2f)\}$$

and

$$S_3 = \bigcup_{i=0}^{\deg(h) - 1} \{x^i \star (\ell g \mid 2fg)\}.$$

Then, $S_1 \cup S_2 \cup S_3$ forms a minimal spanning set for $\mathcal{C}$ as a $\mathbb{Z}_4$-module. Moreover, $\mathcal{C}$ has $2^{\alpha - \deg(b)} 4^{\deg(g)} 2^{\deg(h)}$ codewords.

Note that S_2 generates all order 4 codewords and the subcode of codewords of order 2, $\mathcal{C}_b$, is generated by $\{S_1, 2S_2, S_3\}$. Hence, in the following theorem, by using these spanning sets, we can obtain the parameters $(\alpha, \beta; \gamma, \delta; \kappa)$ of the code.

Theorem 2.4: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fhg = x^\beta - 1$. Then

$$\gamma = \alpha - \deg(b) + \deg(h),$$

$$\delta = \deg(g),$$

$$\kappa = \alpha - \deg(\gcd(\ell g, b)).$$

Proof: The parameters γ and δ are known from Theorem 2.3 and the parameter κ is the dimension of $(\mathcal{C}_b)_X$. By Lemma 2.2, the space $(\mathcal{C}_b)_X$ is generated by the polynomials b and ℓg. Since the ring is a polynomial ring and thus a principal ideal ring, it is generated by the greatest common divisor of the two polynomials. Then, $\kappa = \alpha - deg(gcd(\ell g, b))$. ■

In this case we have that $|\mathcal{C}| = 2^{\alpha - deg(b)} 4^{deg(g)} 2^{deg(h)}$.

Proposition 2.5: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh+2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta = \delta_1 + \delta_2; \kappa = \kappa_1 + \kappa_2)$, where $fhg = x^\beta - 1$. Then,

$$\kappa_1 = \alpha - \deg(b), \quad \kappa_2 = \deg(b) - \deg(\gcd(b, \ell g)),$$

$$\delta_1 = \deg(\gcd(b, \ell g)) - \deg(\gcd(b, \ell)) \text{ and } \delta_2 = \deg(g) - \delta_1.$$

Proof: The result follows from Proposition 1.1 and knowing the generator polynomials of $\mathcal{C}_X$ and $(\mathcal{C}_b)_X$. They are $\gcd(b, \ell)$ and $\gcd(b, \ell g)$, respectively. ■

B. Dual $\mathbb{Z}_2\mathbb{Z}_4$-Additive Cyclic Codes

In [1], it is proven that the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is also a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code. So, we will denote

$$\mathcal{C}^\perp = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \rangle,$$

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

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 cyclic codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$ (see [6], [7]), reciprocal polynomials have an important role on duality.

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

Proposition 2.6: Let $n, m \in \mathbb{N}$. Then,

$$x^{nm} - 1 = (x^n - 1)\theta_m(x^n).$$

Proof: It is well know 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 α and β.

Definition 2.7: Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $R_{\alpha,\beta}$. We define the map

$$\circ : R_{\alpha,\beta} \times R_{\alpha,\beta} \longrightarrow \mathbb{Z}_4[x]/(x^{\mathfrak{m}} - 1),$$

such that

$$\circ(\mathbf{u}(x), \mathbf{v}(x)) = 2u(x)\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) + $$
$$+ u'(x)\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)x^{\mathfrak{m}-1-\deg(v'(x))}v'^*(x) \mod (x^{\mathfrak{m}} - 1),$$

where the computations are made taking the binary zeros and ones in $u(x)$ and $v(x)$ as quaternary zeros and ones, respectively.

The map $\circ$ is linear in each of its arguments; i.e., if we fix the first entry of the map invariant, while letting the second entry vary, then the result is a linear map. Similarly, when fixing the second entry invariant. Then, the map $\circ$ is a bilinear map between $\mathbb{Z}_4[x]$-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 $\mathbb{Z}_4[x]/(x^{\mathfrak{m}} - 1)$.

Proposition 2.8: Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ with associated polynomials $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$. Then, $\mathbf{u}$ is orthogonal to $\mathbf{v}$ and all its shifts if and only if

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

Proof: The ith shift of $\mathbf{v}$ is $\mathbf{v}^{(i)} = (v_{0+i}v_{1+i} \dots v_{\alpha-1+i} \mid v'_{0+i} \dots v'_{\beta-1+i})$. Then,

$$\mathbf{u} \cdot \mathbf{v}^{(i)} = 0 \text{ if and only if } 2\sum_{j=0}^{\alpha-1} u_j v_{j+i} + \sum_{k=0}^{\beta-1} u'_k v'_{k+i} = 0.$$

Let $S_i = 2\sum_{j=0}^{\alpha-1} u_j v_{j+i} + \sum_{k=0}^{\beta-1} u'_k v'_{k+i}$. One can check that

$$\begin{aligned}\mathbf{u}(x) \circ \mathbf{v}(x) = 2\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha) &\left[\sum_{n=0}^{\alpha-1}\sum_{j=n}^{\alpha-1} u_{j-n}v_j x^{\mathfrak{m}-1-n}\right.\\ &\left.+ \sum_{n=1}^{\alpha-1}\sum_{j=n}^{\alpha-1} u_j v_{j-n} x^{\mathfrak{m}-1+n}\right]\\ &+ \theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)\left[\sum_{t=0}^{\beta-1}\sum_{k=t}^{\beta-1} u'_{k-t}v'_j x^{\mathfrak{m}-1-t}\right.\\ &\left.+ \sum_{t=1}^{\beta-1}\sum_{k=t}^{\beta-1} u'_k v'_{k-t} x^{\mathfrak{m}-1+t}\right] \mod (x^{\mathfrak{m}}-1).\end{aligned}$$

Then, arranging the terms one obtains that

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

Thus, $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$ if and only if $S_i = 0$ for $0 \le i \le \mathfrak{m}-1$. ■

Lemma 2.9: Let $\mathbf{u} = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $R_{\alpha,\beta}$ such that $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$. If $u'(x)$ or $v'(x)$ equals 0, then $u(x)v^*(x) \equiv 0 \pmod{(x^\alpha - 1)}$ over $\mathbb{Z}_2$. If $u(x)$ or $v(x)$ equals 0, then $u'(x)v'^*(x) \equiv 0 \pmod{(x^\beta - 1)}$ over $\mathbb{Z}_4$.

Proof: Let $u'(x)$ or $v'(x)$ equals 0, then

$$\begin{aligned}0 =&\mathbf{u}(x) \circ \mathbf{v}(x)\\ =&2u(x)\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) + 0 \mod (x^{\mathfrak{m}}-1).\end{aligned}$$

So,

$$2u(x)\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) = 2\mu'(x)(x^{\mathfrak{m}}-1),$$

for some $\mu'(x) \in \mathbb{Z}_4[x]$.

This is equivalent to

$$u(x)\theta_{\frac{\mathtt{m}}{\alpha}}(x^{\alpha})x^{\mathtt{m}-1-\deg(v(x))}v^{*}(x)=\mu'(x)(x^{\mathtt{m}}-1)\in\mathbb{Z}_2[x].$$

By Proposition 2.6,

$$u(x)x^{\mathtt{m}}v^{*}(x)=\mu(x)(x^{\alpha}-1),$$

$$u(x)v^{*}(x)\equiv 0 \pmod{(x^{\alpha}-1)}.$$

A similar argument can be used to prove the other case. ∎

The following proposition determines the degrees of the generator polynomials of the dual code in terms of the degrees of the generator polynomials of the code. These results will be helpful to determine the generator polynomials of the dual code.

Proposition 2.10: Let $\mathcal{C}=\langle(b\mid 0),(\ell\mid fh+2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh=x^{\beta}-1$, and with dual code $\mathcal{C}^{\perp}=\langle(\bar{b}\mid 0),(\bar{\ell}\mid \bar{f}\bar{h}+2\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h}=x^{\beta}-1$. Then,

$$\begin{aligned}
\deg(\bar{b})&=\alpha-\deg(\gcd(b,\ell)),\\
\deg(\bar{f})&=\deg(g)+\deg(\gcd(b,\ell))-\deg(\gcd(b,\ell g)),\\
\deg(\bar{h})&=\deg(h)-\deg(b)-\deg(\gcd(b,\ell))+2\deg(\gcd(b,\ell g)),\\
\deg(\bar{g})&=\deg(f)+\deg(b)-\deg(\gcd(b,\ell g)).
\end{aligned}$$

Proof: Let $\mathcal{C}^{\perp}$ be a code of type $(\alpha,\beta;\bar{\gamma},\bar{\delta};\bar{\kappa})$. It is easy to prove that $(\mathcal{C}_X)^{\perp}$ is a binary cyclic code generated by $\bar{b}$, so $|(\mathcal{C}_X)^{\perp}|=2^{\alpha-\deg(\bar{b})}$. Moreover, by Proposition 1.1, $|(\mathcal{C}_X)^{\perp}|=2^{\alpha-\kappa-\delta_1}$ and by Proposition 2.5, we obtain that $\deg(\bar{b})=\alpha-\deg(\gcd(b,\ell))$. Finally, from [4] it is known that

$$\begin{aligned}
\bar{\gamma}&=\alpha+\gamma-2\kappa,\\
\bar{\delta}&=\beta-\gamma-\delta+\kappa,\\
\bar{\kappa}&=\alpha-\kappa,
\end{aligned}$$

and applying Theorem 2.4 to the parameters of $\mathcal{C}$ and $\mathcal{C}^{\perp}$, we obtain the result. ∎

We know that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is separable if and only if $\mathcal{C}^{\perp}$ is separable. Moreover, if a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is separable, then it is easy to find the generator polynomials of the dual, that are given in the following proposition.

Proposition 2.11: Let $\mathcal{C}=\langle(b\mid 0),(0\mid fh+2f)\rangle$ be a separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh=x^{\beta}-1$. Then,

$$\mathcal{C}^{\perp}=\langle(\frac{x^{\alpha}-1}{b^{*}}\mid 0),(0\mid g^{*}h^{*}+2g^{*})\rangle.$$

Proof: If $\mathcal{C}$ is separable, then $\mathcal{C}^{\perp}=(\mathcal{C}_X)^{\perp}\times(\mathcal{C}_Y)^{\perp}$, where $(\mathcal{C}_X)^{\perp}=\langle\frac{x^{\alpha}-1}{b^{*}}\rangle$ and $(\mathcal{C}_Y)^{\perp}=\langle g^{*}h^{*}+2g^{*}\rangle$. ∎

Proposition 2.12: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with dual code $\mathcal{C}^\perp = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \rangle$. Then,

$$\bar{b} = \frac{x^\alpha - 1}{(gcd(b, \ell))^*} \in \mathbb{Z}_2[x].$$

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

$$\begin{aligned} (b \mid 0) \circ (\bar{b} \mid 0) =& 0, \\ (\ell \mid fh + 2f) \circ (\bar{b} \mid 0) =& 0. \end{aligned}$$

Therefore, by Lemma 2.9,

$$\begin{aligned} b\bar{b}^* \equiv& 0 \pmod{(x^\alpha - 1)}, \\ \ell\bar{b}^* \equiv& 0 \pmod{(x^\alpha - 1)}, \end{aligned}$$

over $\mathbb{Z}_2$. So, $\gcd(b, \ell)\bar{b}^* \equiv 0 \pmod{(x^\alpha - 1)}$, and there exist $\mu \in \mathbb{Z}_2[x]$ such that $\gcd(b, \ell)\bar{b}^* = \mu(x^\alpha - 1)$. Moreover, since $\gcd(b, \ell)$ and $\bar{b}^*$ divides $(x^\alpha - 1)$ and, by Proposition 2.10, we have that $\deg(\bar{b}) = \alpha - \deg(\gcd(b, \ell))$. We conclude that

$$\bar{b}^* = \frac{x^\alpha - 1}{\gcd(b, \ell)} \in \mathbb{Z}_2[x].$$

■

Proposition 2.13: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fgh = x^\beta - 1$, and with dual code $\mathcal{C}^\perp = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \rangle$, where $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Then, $\bar{f}\bar{h}$ is the Hensel lift of the polynomial $\frac{(x^\beta - 1)\gcd(b, \ell g)^*}{f^* b^*} \in \mathbb{Z}_2[x]$.

Proof: It is known that h and g are coprime, from which we deduce easily that $p_1 fh + p_2 fg = f$, for some $p_1, p_2 \in \mathbb{Z}_4[x]$. Since $(b \mid 0)$, $(0 \mid 2fh)$ and $(\ell g \mid 2fg)$ belong to $\mathcal{C}$, then

$$(0 \mid \frac{b}{\gcd(b, \ell g)}(2p_1 fh + 2p_2 fg)) = (0 \mid \frac{b}{\gcd(b, \ell g)} 2f) \in \mathcal{C}.$$

Therefore,

$$(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (0 \mid \frac{b}{\gcd(b, \ell g)} 2f) = 0.$$

Thus, by Lemma 2.9,

$$(\bar{f}\bar{h} + 2\bar{f}) \left(\frac{b^* 2 f^*}{\gcd(b, \ell g)^*} \right) \equiv 0 \pmod{(x^\beta - 1)},$$

and

$$(2\bar{f}\bar{h}) \left(\frac{b^* f^*}{\gcd(b, \ell g)^*} \right) = 2\mu(x^\beta - 1), \tag{2}$$

for some $\mu \in \mathbb{Z}_4[x]$.

If (2) holds over $\mathbb{Z}_4$, then it is equivalent to

$$(\bar{f}\bar{h}) \left(\frac{b^* f^*}{\gcd(b, \ell g)^*} \right) = \mu(x^\beta - 1) \in \mathbb{Z}_2[x].$$

It is known that $\overline{f}\overline{h}$ is a divisor of $x^\beta - 1$ and, by Corollary 2.1, we have that $\left(\frac{b^* f^*}{\gcd(b,\ell g)^*}\right)$ divides $(x^\beta - 1)$ over $\mathbb{Z}_2$. By Corollary 2.10, $\deg(\overline{f}\overline{h}) = \beta - \deg(f) - \deg(b) + \deg(\gcd(b, \ell g))$, so

$$\beta = \deg\left(\overline{f}\overline{h}\frac{b^* f^*}{\gcd(b,\ell g)^*}\right) = \deg(x^\beta - 1).$$

Hence, we obtain that $\mu = 1 \in \mathbb{Z}_2$ and

$$\overline{f}\overline{h} = \frac{(x^\beta - 1)\gcd(b,\ell g)^*}{f^* b^*} \in \mathbb{Z}_2[x]. \tag{3}$$

Since β is odd and by the uniqueness of the Hensel lift [9, p.73], $\overline{f}\overline{h}$ is the unique monic polynomial in $\mathbb{Z}_4[x]$ dividing $(x^\beta - 1)$ and satisfying (3). ■

Proposition 2.14: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fgh = x^\beta - 1$, and with dual code $\mathcal{C}^\perp = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Then, $\bar{f}$ is the Hensel lift of the polynomial $\frac{(x^\beta - 1)\gcd(b,\ell)^*}{f^* h^* \gcd(b,\ell g)^*} \in \mathbb{Z}_2[x]$.

Proof: One can factorize in $\mathbb{Z}_2[x]$ the polynomials $b, \ell, \ell g$ in the following way:

$$\ell = \gcd(b,\ell)\rho,$$

$$\ell g = \gcd(b,\ell g)\rho\tau_1,$$

$$b = \gcd(b,\ell g)\tau_2,$$

where τ_1 and τ_2 are coprime polynomials.

Hence, there exist $t_1, t_2 \in \mathbb{Z}_2[x]$ such that $t_1\tau_1 + t_2\tau_2 = 1$. Then,

$$\gcd(b,\ell g)\rho(t_1\tau_1 + t_2\tau_2) = \gcd(b,\ell g)\rho,$$

and

$$t_1\ell g + \rho t_2 b = \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}\ell.$$

Therefore,

$$\frac{\gcd(b,\ell g)}{\gcd(b,\ell)}\star(\ell \mid fh + 2f) + t_1 \star (\ell g \mid 2fg) + \rho t_2 \star (b \mid 0) =$$
$$\left(0 \mid \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}(fh + 2f) + t_1 2fg\right) \in \mathcal{C}.$$

Since $\bar{h}$ and $\bar{g}$ are coprime, there exist $\bar{p}_1, \bar{p}_2 \in \mathbb{Z}_4[x]$ such that $2\bar{p}_1\bar{f}\bar{h} + 2\bar{p}_2\bar{f}\bar{g} = 2\bar{f}$. So, $(2\bar{p}_1 + \bar{p}_2\bar{g}) \star (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) = (\bar{p}_2\bar{\ell}\bar{g} \mid 2\bar{f}) \in \mathcal{C}^\perp$.

Therefore,

$$(\bar{p}_2\bar{\ell}\bar{g} \mid 2\bar{f}) \circ \left(0 \mid \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}(fh + 2f) + t_1 2fg\right) = 0.$$

By Lemma 2.9, arranging properly, we obtain that

$$2\bar{f}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right) f^* h^* \equiv 0 \pmod{(x^\beta - 1)}$$

and

$$2\bar{f}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right)f^*h^* = 2\mu(x^\beta-1), \tag{4}$$

for some $\mu \in \mathbb{Z}_4[x]$.

If (4) holds over $\mathbb{Z}_4$, then it is equivalent to

$$\bar{f}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right)f^*h^* = \mu(x^\beta-1) \in \mathbb{Z}_2[x].$$

It is easy to prove that $\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right)f^*h^*$ divides $(x^\beta-1)$ in $\mathbb{Z}_2[x]$. By Corollary 2.10, $\deg(\bar{f}) = \beta - \deg(f) - \deg(h) + \deg(\gcd(b,\ell)) - \deg(\gcd(b,\ell g))$, so

$$\beta = \deg\left(\bar{f}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right)f^*h^*\right) = \deg(x^\beta-1).$$

Hence, we obtain that $\mu = 1$ and

$$\bar{f} = \frac{(x^\beta-1)\gcd(b,\ell)^*}{\gcd(b,\ell g)^* f^* h^*} \in \mathbb{Z}_2[x]. \tag{5}$$

Since β is odd and by the uniqueness of the Hensel lift [9, p.73] then $\bar{f}$ is the unique monic polynomial in $\mathbb{Z}_4[x]$ dividing $(x^\beta-1)$ and holding (5). ■

Lemma 2.15: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh+2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh = x^\beta - 1$. Then, the Hensel lift of $\frac{b}{\gcd(b,\ell g)}$ divides h.

Proof: In general, if $a \mid b \mid x^\beta - 1$ over $\mathbb{Z}_2[x]$ with β odd, then the Hensel lift of a divides the Hensel lift of b that divides $x^\beta-1$ over $\mathbb{Z}_4[x]$. Then, by Corollary 2.1, the result follows. ■

In the family of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes there is a particular class when the polynomials b and $\gcd(b,\ell g)$ are the same. Applying Lemma 2.2 to this class we obtain that $\mathcal{C}_b$ has only two generators, $\langle (b \mid 0), (0 \mid 2f)\rangle$, instead of three, $\langle (b \mid 0), (\ell g \mid 2fg), (0 \mid 2fh)\rangle$. So, we have to take care of this class of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

Proposition 2.16: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh+2f)\rangle$ be a non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh = x^\beta-1$, and with dual code $\mathcal{C}^\perp = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h}+2\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Let $\rho = \frac{\ell}{\gcd(b,\ell)}$. Then,

$$\begin{aligned}\bar{\ell} = &\frac{x^\alpha-1}{b^*}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}x^{\mathfrak{m}-\deg(f)}\mu_1\right.\\ &\left.+\frac{b^*}{\gcd(b,\ell g)^*}x^{\mathfrak{m}-\deg(fh)}\mu_2\right),\end{aligned}$$

where

$$\begin{cases} \mu_1 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell g)^*}\right), \\ \mu_2 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell)^*}\right). \end{cases}$$

Proof: In order to calculate $\bar{\ell}$, by using $\circ$, we are going to operate $(\bar{\ell} \mid \bar{f}\bar{h}+2\bar{f})$ by three different codewords of $\mathcal{C}$. The result of these operations is 0 modulo $x^{\mathfrak{m}}-1$.

First, consider $(\bar{\ell} \mid \bar{f}\bar{h}+2\bar{f}) \circ (b \mid 0) = 0$. By Lemma 2.9, $\bar{\ell}b^* \equiv 0 \pmod{(x^\alpha-1)}$ and, for some $\lambda \in \mathbb{Z}_2[x]$, we have that $\bar{\ell} = \frac{x^\alpha-1}{b^*}\lambda$.

Second, consider $\tau = \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}$ and compute $(\bar{\ell} \mid \overline{fh} + 2\bar{f}) \circ (\tau\ell \mid \tau fh + 2\tau f)$. Let $t = \deg(\tau)$ and note that $(fh + 2f)^* = f^*h^* + 2x^{\deg(h)}f^*$. We obtain that

$$
\begin{aligned}
0 = (\bar{\ell} \mid \overline{fh} + 2\bar{f}) \circ (\tau\ell \mid \tau fh + 2\tau f) = \\
2\bar{\ell}\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)x^{\mathfrak{m}-\deg(\ell)-1-t}\tau^*\ell^* \\
+ \overline{fh}\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)x^{\mathfrak{m}-\deg(fh)-1-t}\tau^*f^*h^* \\
+ 2\overline{fh}\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)x^{\mathfrak{m}-\deg(f)-1-t}\tau^*f^* \\
+ 2\bar{f}\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)x^{\mathfrak{m}-\deg(fh)-1-t}\tau^*f^*h^* \mod (x^{\mathfrak{m}} - 1).
\end{aligned} \tag{6}
$$

Apply Proposition 2.6 to each addend and $\bar{\ell} = \frac{x^\alpha - 1}{b^*}\lambda$. In addend (6), by Proposition 2.13, we may replace $\overline{fh}$ by the Hensel lift of $\frac{(x^\beta-1)\gcd(b,\ell g)^*}{f^*b^*}$. The Hensel lift of $(x^\beta - 1)$ and $f^* \pmod 2$ are the same polynomials $(x^\beta - 1)$ and f^*. Moreover, by Lemma 2.15, the addend (6) is 0 modulo $(x^{\mathfrak{m}} - 1)$. Therefore, by Proposition 2.13 and Proposition 2.14, we get that

$$
\begin{aligned}
0 = (\bar{\ell} \mid \overline{fh} + 2\bar{f}) \circ (\tau\ell \mid \tau fh + 2\tau f) = \\
2\frac{(x^{\mathfrak{m}} - 1)}{b^*}\lambda x^{\mathfrak{m}-\deg(\ell)-1-t}\tau^*\ell^* \\
+ 2\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell)^*}{f^*h^*\gcd(b,\ell g)^*}x^{\mathfrak{m}-\deg(fh)-1-t}\tau^*f^*h^* \\
+ 2\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell g)^*}{f^*b^*}x^{\mathfrak{m}-\deg(f)-1-t}\tau^*f^* \mod (x^{\mathfrak{m}} - 1).
\end{aligned} \tag{7}
$$

Clearly, the addend (7) is 0 modulo $(x^{\mathfrak{m}} - 1)$. Since $\tau = \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}$, we have that $(\bar{\ell} \mid \overline{fh} + 2\bar{f}) \circ (\tau\ell \mid \tau fh + 2\tau f)$ is equal to

$$
\begin{aligned}
2\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell g)^*}{b^*}\Big(\lambda x^{\mathfrak{m}-\deg(\ell)-1-t}\rho^* \\
+x^{\mathfrak{m}-\deg(f)-1-t}\tau^*\Big) \equiv 0 \pmod{(x^{\mathfrak{m}} - 1)}.
\end{aligned} \tag{8}
$$

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

$$
\begin{aligned}
\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell g)^*}{b^*}\Big(\lambda x^{\mathfrak{m}-\deg(\ell)-1-t}\rho^* \\
+x^{\mathfrak{m}-\deg(f)-1-t}\tau^*\Big) \equiv 0 \pmod{(x^{\mathfrak{m}} - 1)}.
\end{aligned}
$$

Then,

$$
\begin{aligned}
\Big(\lambda x^{\mathfrak{m}-\deg(\ell)-1-t}\rho^* \\
+x^{\mathfrak{m}-\deg(f)-1-t}\tau^*\Big) \equiv 0 \pmod{(x^{\mathfrak{m}} - 1)},
\end{aligned} \tag{9}
$$

or

$$\Big(\lambda x^{\mathtt{m}-\deg(\ell)-1-t}\rho^* + x^{\mathtt{m}-\deg(f)-1-t}\tau^*\Big) \equiv 0 \pmod{\left(\frac{b^*}{\gcd(b,\ell g)^*}\right)}. \tag{10}$$

Since $(\frac{b^*}{\gcd(b,\ell g)^*})$ divides $(x^{\mathtt{m}}-1)$, then (9) implies (10).

The greatest common divisor between ρ and $\left(\frac{b}{\gcd(b,\ell g)}\right)$ is 1, then ρ^* is invertible modulo $\left(\frac{b^*}{\gcd(b,\ell g)^*}\right)$. Thus,

$$\lambda = \tau^* x^{\mathtt{m}-\deg(f)+\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell g)^*}\right).$$

Let $\lambda_1 = \tau^* x^{\mathtt{m}-\deg(f)+\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell g)^*}\right)$. Then $\lambda = \lambda_1 + \lambda_2$ with $\lambda_2 \equiv 0 \pmod{\left(\frac{b^*}{\gcd(b,\ell g)^*}\right)}$.

Finally, we compute $(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell \mid fh + 2f)$.

$$\begin{aligned} 0 = (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell \mid fh + 2f) = \\ & 2\bar{\ell}\theta_{\frac{\mathtt{m}}{\alpha}}(x^{\alpha})x^{\mathtt{m}-\deg(\ell)-1}\ell^* \\ & + \bar{f}\bar{h}\theta_{\frac{\mathtt{m}}{\beta}}(x^{\beta})x^{\mathtt{m}-\deg(fh)-1}f^*h^* \\ & + 2\bar{f}\bar{h}\theta_{\frac{\mathtt{m}}{\beta}}(x^{\beta})x^{\mathtt{m}-\deg(f)-1}f^* \\ & + 2\bar{f}\theta_{\frac{\mathtt{m}}{\beta}}(x^{\beta})x^{\mathtt{m}-\deg(fh)-1}f^*h^* \mod (x^{\mathtt{m}}-1). \end{aligned} \tag{11}$$

Apply Proposition 2.6 to each addend. By Lemma 2.15 and replacing $\bar{f}\bar{h}$ by the Hensel lift of $\frac{(x^{\beta}-1)\gcd(b,\ell g)^*}{f^*b^*}$, then the addend (11) is $0 \mod (x^{\mathtt{m}}-1)$ and, by Proposition 2.13 and Proposition 2.14, $(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell \mid fh + 2f)$ is equal to

$$\begin{aligned} & 2\frac{(x^{\mathtt{m}}-1)}{b^*}(\lambda_1+\lambda_2)x^{\mathtt{m}-\deg(\ell)-1}\ell^* \\ & + 2\frac{(x^{\mathtt{m}}-1)\gcd(b,\ell g)^*}{b^*}x^{\mathtt{m}-\deg(f)-1} \\ & + 2\frac{(x^{\mathtt{m}}-1)\gcd(b,\ell)^*}{\gcd(b,\ell g)^*}x^{\mathtt{m}-\deg(fh)-1} \equiv 0 \pmod{(x^{\mathtt{m}}-1)}. \end{aligned}$$

Since $\lambda_1 = \tau^* x^{\mathtt{m}-\deg(f)+\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell g)^*}\right)$, we have that

$$\begin{aligned} & 2\frac{(x^{\mathtt{m}}-1)}{b^*}\lambda_1 x^{\mathtt{m}-\deg(\ell)-1}\ell^* \\ & + 2\frac{(x^{\mathtt{m}}-1)\gcd(b,\ell g)^*}{b^*}x^{\mathtt{m}-\deg(f)-1} \equiv 0 \pmod{(x^{\mathtt{m}}-1)}. \end{aligned}$$

Therefore, we obtain that

$$\begin{aligned} & 2\frac{(x^{\mathtt{m}}-1)}{b^*}\lambda_2 x^{\mathtt{m}-\deg(\ell)-1}\ell^* \\ & + 2\frac{(x^{\mathtt{m}}-1)\gcd(b,\ell)^*}{\gcd(b,\ell g)^*}x^{\mathtt{m}-\deg(fh)-1} \equiv 0 \pmod{(x^{\mathtt{m}}-1)}, \end{aligned}$$

and then

$$2\frac{(x^{\mathfrak{m}}-1)\gcd(b,\ell)^*}{b^*}\Big(\lambda_2 x^{\mathfrak{m}-\deg(\ell)-1}\rho^* + \frac{b^*}{\gcd(b,\ell g)^*}x^{\mathfrak{m}-\deg(fh)-1}\Big)\equiv 0 \pmod{(x^{\mathfrak{m}}-1)}.$$

Arguing similar to the calculation of λ in (8), we obtain that

$$\lambda_2 = \frac{b^*}{\gcd(b,\ell g)^*}x^{\mathfrak{m}-\deg(fh)+\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell)^*}\right).$$

Now, considering the values of λ_1 and λ_2 and defining properly μ_1 and μ_2 we obtain the expected result. ■

We summarize the previous results in the next theorem.

Theorem 2.17: Let $\mathcal{C}=\langle(b\mid 0),(\ell\mid fh+2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh=x^\beta-1$, and with dual code $\mathcal{C}^\perp=\langle(\bar b\mid 0),(\bar\ell\mid \bar f\bar h+2\bar f)\rangle$, where $\bar f\bar g\bar h=x^\beta-1$. Let $\rho=\frac{\ell}{\gcd(b,\ell)}$. Then,

1) $\bar b=\frac{x^\alpha-1}{(gcd(b,\ell))^*}\in\mathbb{Z}_2[x]$,
2) $\bar f\bar h$ is the Hensel lift of the polynomial $\frac{(x^\beta-1)\gcd(b,\ell g)^*}{f^*b^*}\in\mathbb{Z}_2[x]$.
3) $\bar f$ is the Hensel lift of the polynomial $\frac{(x^\beta-1)\gcd(b,\ell)^*}{f^*h^*\gcd(b,\ell g)^*}\in\mathbb{Z}_2[x]$.
4)
$$\bar\ell=\frac{x^\alpha-1}{b^*}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}x^{\mathfrak{m}-\deg(f)}\mu_1 + \frac{b^*}{\gcd(b,\ell g)^*}x^{\mathfrak{m}-\deg(fh)}\mu_2\right)\in\mathbb{Z}_2[x],$$
where
$$\begin{cases}\mu_1 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell g)^*}\right),\\ \mu_2 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell)^*}\right).\end{cases}$$

Note that from Theorem 2.17 and Theorem 2.3 one can easily compute the minimal spanning set of the dual code $\mathcal{C}^\perp$ as a $\mathbb{Z}_4$-module, and use the encoding method for $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes described in [1].

III. Examples

As a simple example, consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code $\mathcal{C}_1=\langle(x-1\mid(x^2+x+1)+2)\rangle$ of type $(3,3;2,1;2)$. We have that $b=x^3-1,\ell=(x-1),f=1$ and $h=x^2+x+1$.

The generator matrix ([4]) is

$$G=\left(\begin{array}{c|c}101 & 200\\ 011 & 220\\ \hline 000 & 111\end{array}\right).$$

Then, applying the formulas of Theorem 2.17 we have $\bar b=x^2+x+1,\bar\ell=x,\bar f\bar h=x-1$, and $\bar f=x-1$. Therefore, $\mathcal{C}_1^\perp=\langle(x^2+x+1\mid 0),(x\mid(x-1)+2(x-1))\rangle$, is of type $(3,3;1,2;1)$ and has generator matrix

$$H=\left(\begin{array}{c|c}111 & 000\\ \hline 100 & 310\\ 001 & 301\end{array}\right).$$

In order to determine some cyclic codes with good parameters, we will consider some optimal codes with respect to the minimum distance. Applying the classical Singleton bound [8] to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and minimum distance d, the following bound is obtained:

$$\frac{d-1}{2} \leq \frac{\alpha}{2} + \beta - \frac{\gamma}{2} - \delta. \tag{12}$$

According to [2], a code meeting the bound (12) is called maximum distance separable with respect to the Singleton bound, briefly MDSS.

By [1, Theorem 19] it is known that $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ with $b = x - 1$, $\ell = 1$ and $f = h = 1$ is an MDSS code of type $(\alpha, \beta; \alpha - 1, \beta; \alpha - 1)$. Applying Theorem 2.17 to compute the dual code of $\mathcal{C}$ one obtain that $\mathcal{C}^\perp = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \rangle$ with $\bar{b} = x^\alpha - 1$, $\bar{\ell} = \theta_\alpha(x)$, $\bar{f} = \theta_\beta(x)$ and $\bar{h} = x - 1$, which is also an MDSS code. In fact, the binary image of $\mathcal{C}$ is the set of all even weight vectors and the binary image of $\mathcal{C}^\perp$ is the repetition code. Moreover, these are the only MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with more than one codeword and minimum distance $d > 1$, as can be seen in [2].

Finally, we are going to see a pair of examples of self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, giving the generators and type of these codes.

Generators	Type
$b = x^{10} + x^8 + x^7 + x^3 + x + 1, \ell = x^6 + x^4 + x + 1, fh = y^4 + 2y^3 + 3y^2 + y + 1, f = 1$	(14, 7; 8, 3; 7)
$b = x^5+1, \ell = 0, fh = y^5-1, f = 1$	(10, 5; 10, 0; 5)

The second code in the table belongs to an infinite family of self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes that was given in [3, Theorem 4].

Proposition 3.1: Let α be even and β odd. Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $b = x^{\frac{\alpha}{2}} - 1$, $\ell = 0$, $h = x^\beta - 1$ and $f = 1$. Then $\mathcal{C}$ is a self-dual code of type $(\alpha, \beta; \beta + \frac{\alpha}{2}, 0; \frac{\alpha}{2})$.

Proof: By Theorem 2.17, one obtains that $\bar{b} = x^{\frac{\alpha}{2}} - 1$, $\bar{\ell} = 0$, $\bar{h} = x^\beta - 1$ and $\bar{f} = 1$. Hence $\mathcal{C}$ is self-dual and, by Theorem 2.4, it is of type $(\alpha, \beta; \beta + \frac{\alpha}{2}, 0; \frac{\alpha}{2})$. ■

References

[1] T. Abualrub, I. Siap, N. Aydin. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. *IEEE Trans. Info. Theory*, vol. 60, No. 3, pp. 1508–1514, Mar. 2014.

[2] M. Bilal, J. Borges, S.T. Dougherty, C. Fernández-Córdoba. Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. *Designs, Codes and Cryptography*, vol. 61, No. 3, pp. 31–40, Oct. 2011.

[3] J. Borges, S.T. Dougherty, C. Fernández-Córdoba. Characterization and constructions of self-dual codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$. *Advances in Mathematics of Communications*, vol. 6, No. 3, pp. 287–303, Aug. 2012.

[4] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. *Designs, Codes and Cryptography*, vol. 54, No. 2, pp. 167–179, Feb. 2010.

[5] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, vol. 10, pp. 1–97, Jan. 1973.

[6] F.J. MacWilliams, N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland Publishing Company, Amsterdam, New York, Oxford, 1975.

[7] V.S. Pless and Z. Qian. Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *IEEE Trans. Info. Theory*, vol. 42, No. 5, pp. 1594–1600, Sep. 1996.

[8] R.C. Singleton R.C. Maximum distance q-nary codes. *IEEE Trans. Inform. Theory*, vol. 10, No.2, pp. 116–118, Apr. 1964.

[9] Z. Wan. *Quaternary Codes.* World Scientific, Series on applied mathematics v. 8, 1997.

Joaquim Borges was born in Lleida, Catalonia, Spain, in October 1965. He received the graduate degree in Sciences (Computer Science Section) in 1988 from the Universitat Autònoma de Barcelona, Spain, and the Ph.D. degree in Computer Science Engineering in 1998 from the same university.

Since 1988, he has been with the Computer Science Department first, and from 2005 with the Information and Communications Engineering Department, at the Universitat Autònoma de Barcelona, where he is currently Associate Professor. His research interests include subjects related to Combinatorics, Coding Theory and Graph Theory.

Cristina Fernández-Córdoba was born in Sabadell, Catalonia (Spain) in December 1977. She received her Bachelor's degree in Mathematics in 2000 from the Universitat Autònoma de Barcelona and the Ph.D. degree in Science (Computer Science Section) in 2005 from the same university. In 2000 she joined the Department of Computer Science at the Universitat Autònoma de Barcelona, and in 2005 the Department of Information and Communications Engineering at the same university. In 2008, she joined the Fundación Española para la Ciencia y la Tecnología and she did a one year research stay at Auburn University under a Fulbright grant. From 2009, she is within the Department of Information and Communications Engineering at the Universitat Autònoma de Barcelona where currently is an Associate Professor. Her research interests include subjects related to combinatorics, coding theory and graph theory.

Roger Ten-Valls was born in Barcelona, Catalonia (Spain) in June 1987. He received the B.Sc. degree in mathematics in 2011 from the Universitat Autònoma de Barcelona and the M.Sc. in mathematics in 2013 from Universitat Politècnica de Catalunya. He is curenty working toward the Ph.D. at the Department of Information and Communications Engineering at the Universitat Autònoma de Barcelona. His research interests include coding theory, combinatorics and abstract algebra.