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

Joaquim Borges Ayats, Cristina Fernández-Córdoba, and Roger Ten-Valls

Department of Information and Communication Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain.
{joaquim.borges,cristina.fernandez,roger.ten}@uab.cat

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 code 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 invariant the code. 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 $\mathcal{C}$.

Key words: Binary cyclic codes, Duality, Quaternary cyclic codes, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

1 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. Any non-empty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a submodule of $\mathbb{Z}_4^n$ is called a quaternary linear code.

In Delsarte's 1973 paper (see [3]), 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 [2], $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were studied.

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

* This work has been partially supported by the Spanish MICINN grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

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 quaternary linear code 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 $\kappa \leq \gamma_X \leq \kappa + \delta$.

In [2], it is shown that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with standard generator matrix of the form:

$$\mathcal{G}_S = \left(\begin{array}{cc|ccc} I_\kappa & T_b & 2T_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 2T_1 & 2I_{\gamma-\kappa} & \mathbf{0} \\ \hline \mathbf{0} & S_b & S_q & R & I_\delta \end{array}\right), \tag{1}$$

where I_k is the identity matrix of size $k \times k$; T_b, S_b are matrices over $\mathbb{Z}_2$; T_1, T_2, R are matrices over $\mathbb{Z}_4$ with all entries in $\{0, 1\} \subset \mathbb{Z}_4$; and S_q is a matrix over $\mathbb{Z}_4$.

A Gray map is defined on $\mathbb{Z}_2\mathbb{Z}_4$-additive codes 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 [2], 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 quaternary zeros and ones, respectively. The *dual code* of $\mathcal{C}$, is defined in the standard way by

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

2 Duality of non-separable codes.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is said to be separable if $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$. If $\mathcal{C}$ is separable then $\mathcal{C}^\perp = (\mathcal{C}_X)^\perp \times (\mathcal{C}_Y)^\perp$, so we will focus on non-separable codes.

Proposition 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 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 applying convenient permutations and linear combinations of rows to the generator matrix giving in [2]. 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.

The generator matrices in standard form of the related codes $\mathcal{C}_X$ and $\mathcal{C}_Y$ are very easy computable from this new generator matrix of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code.

Proposition 2. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha,\beta;\gamma,\delta;\kappa)$. Then, $\mathcal{C}_X$ has a generator matrix of the form*

$$\mathcal{G}_{\mathcal{C}_X} = \begin{pmatrix} I_{\kappa_1} & 0 & 0 & \overline{T}_{b_1} \\ 0 & I_{\kappa_2} & 0 & \overline{T}_{b_2} \\ 0 & 0 & I_{\delta_1} & \overline{S}_b \end{pmatrix},$$

and $\mathcal{C}_X$ has a parity check matrix

$$\mathcal{H}_{\mathcal{C}_\mathcal{X}} = \begin{pmatrix} \overline{T}^t_{b_1} & \overline{T}^t_{b_2} & \overline{S}^t_b & I_{\alpha-\kappa-\delta_1} \end{pmatrix}.$$

Proposition 3. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha,\beta;\gamma,\delta;\kappa)$. Then, $\mathcal{C}_Y$ has a generator matrix of the form*

$$\mathcal{G}_{\mathcal{C}_Y} = \begin{pmatrix} 2\overline{T}_2 & 2I_{\kappa_2} & 0 & 0 & 0 \\ 2\overline{T}_1 & 0 & 2I_{\gamma-\kappa} & 0 & 0 \\ S_{11} & S_{12} & R_1 & I_{\delta_1} & 0 \\ \overline{S}_{21} & \overline{S}_{22} & \overline{R}_2 & 0 & I_{\delta_2} \end{pmatrix},$$

and $\mathcal{C}_Y$ has parity check matrix

$$\mathcal{H}_{\mathcal{C}_\mathcal{Y}} = \begin{pmatrix} I_{\beta-\delta-\gamma+\kappa_1} & \overline{T}^t_2 & \overline{T}^t_1 & -S^t_{11} - S^t_{12}\overline{T}^t_2 - R^t_1\overline{T}^t_1 & -\overline{S}^t_{21} - \overline{S}^t_{22}\overline{T}^t_2 - \overline{R}^t_2\overline{T}^t_1 \\ 0 & 2I_{\kappa_2} & 0 & 2S^t_{12} & 2\overline{S}^t_{22} \\ 0 & 0 & 2I_{\gamma-\kappa} & 2R^t_1 & 2\overline{R}^t_2 \end{pmatrix}.$$

From the previous results and [2], we state the number of codewords of $\mathcal{C}$, $\mathcal{C}_X$, $\mathcal{C}_Y$ and their duals.

Proposition 4. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha,\beta;\gamma,\delta;\kappa)$. Then,*

$$\begin{aligned} |\mathcal{C}| &= 4^{\delta}2^{\gamma}, \quad |\mathcal{C}^{\perp}| = 4^{\beta-\gamma-\delta+\kappa}2^{\alpha+\gamma-2\kappa}, \\ |\mathcal{C}_X| &= 2^{\kappa+\delta_1}, \quad |(\mathcal{C}_X)^{\perp}| = 2^{\alpha-\kappa-\delta_1}, \\ |\mathcal{C}_Y| &= 4^{\delta}2^{\gamma-\kappa_1}, \quad |(\mathcal{C}_Y)^{\perp}| = 4^{\beta-\gamma-\delta+\kappa_1}2^{\gamma-\kappa_1}, \end{aligned}$$

where $\kappa = \kappa_1 + \kappa_2$ and $\delta = \delta_1 + \delta_2$.

3 $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

3.1 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

$$\mathbf{u}^{(i)} = (u^{(i)} \mid u'^{(i)}) = (u_{0+i}, u_{1+i}, \ldots, u_{\alpha-1+i} \mid u'_{0+i}, u'_{1+i}, \ldots, u'_{\beta-1+i})$$

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 all codeword $\mathbf{u} \in \mathcal{C}$ then $\mathbf{u}^{(1)} \in \mathcal{C}$.

From [1], we know that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where β is an odd integer, then it is of the form

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

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

Since $b(x)$ divides $\frac{x^{\beta}-1}{f(x)}\ell(x) \pmod 2$, it follows that

Corollary 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 $\frac{x^{\beta}-1}{f(x)} \gcd(b(x), \ell(x)) \pmod 2$.*

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 1. *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 $\langle (b \mid 0), (\ell g \mid 2fg), (0 \mid 2fh) \rangle$. □

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

The following result shows how closely related are the parameters of the type of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code and the the degrees of the generator polynomials of the code.

Theorem 1. *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*

$$\begin{aligned}\gamma &= \alpha - \deg(b) + \deg(h),\\ \delta &= \deg(g),\\ \kappa &= \alpha - \deg(\gcd(\ell g, b)).\end{aligned}$$

Proof. The parameters γ and δ are known from [1].
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, then 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 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 4 and knowing the generators polynomials of $\mathcal{C}_X$ and $(\mathcal{C}_b)_X$. They are $\gcd(b, \ell)$ and $\gcd(b, \ell g)$, respectively.

3.2 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 binary cyclic codes and quaternary cyclic codes, reciprocal polynomials have an important role on duality (see [6], [7]).

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

Proposition 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 1. *Let $\boldsymbol{u}(x) = (u(x) \mid u'(x))$ and $\boldsymbol{v}(x) = (v(x) \mid v'(x))$ 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

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

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

$$\boldsymbol{u}(x) \circ \boldsymbol{v}(x) = 0 \mod (x^{\mathfrak{m}} - 1).$$

Proof. Let $\mathbf{v}^{(i)} = (v_{0+i}v_{1+i} \dots v_{\alpha-1+i} \mid v'_{0+i} \dots v'_{\beta-1+i})$ be the ith shift of $\mathbf{v}$. 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

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

Then, arranging the terms one obtains that

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

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

Lemma 2. *Let* $\boldsymbol{u}=(u(x)\mid u'(x))$ *and* $\boldsymbol{v}(x)=(v(x)\mid v'(x))$ *be elements in* $R_{\alpha,\beta}$ *such that* $\boldsymbol{u}(x)\circ\boldsymbol{v}(x)=0 \mod(x^{\mathfrak{m}}-1)$. *If* $u'(x)$ *or* $v'(x)$ *equal* 0, *then* $u(x)v^*(x)=0 \mod(x^{\alpha}-1)$ *over* $\mathbb{Z}_2$. *Respectively, if* $u(x)$ *or* $v(x)$ *equal* 0, *then* $u'(x)v'^*(x)=0 \mod(x^{\beta}-1)$ *over* $\mathbb{Z}_4$.

Proof. Let $u'(x)$ or $v'(x)$ equal 0, then

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

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

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

By Proposition 6,

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

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

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

The following two propositions determine the degrees of the generator polynomials of the dual in terms of the degrees of the generators polynomials of the code. These results are going to be very helpful later to determine the generator polynomials of the dual code.

Proposition 8. *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,*

$$\deg(\bar{b}) = \alpha - \deg(\gcd(b, \ell)).$$

Proof. 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 4, $|(\mathcal{C}_X)^\perp| = 2^{\alpha - \kappa - \delta_1}$.
And by Proposition 5, we obtain that $\deg(\bar{b}) = \alpha - \deg(\gcd(b, \ell))$. □

Proposition 9. *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,*

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

Proof. Let $\mathcal{C}^\perp$ a code of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$. From [2] 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 1 to the parameters of $\mathcal{C}$ and $\mathcal{C}^\perp$, we obtain the result. □

In general, we already said that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is separable if and only if $\mathcal{C}^\perp$ is separable. The property of be separable is very helpful in a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code to find the generator polynomials of the –dual code.

Proposition 10. *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. The codes $\mathcal{C}_X$ and $\mathcal{C}_Y$ are a binary cyclic code and a quaternary cyclic code, respectively. Since $\mathcal{C}$ is separable, it is well known that $\mathcal{C}_X^\perp = \langle \frac{x^\alpha - 1}{b^*} \rangle$ and $\mathcal{C}_Y^\perp = \langle g^*h^* + 2g^* \rangle$.
Since $\mathcal{C}$ is separable, then $\mathcal{C}^\perp$ is separable. Therefore, $\mathcal{C}^\perp = \mathcal{C}_X^\perp \times \mathcal{C}_Y^\perp$. □

Proposition 11. *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, $\langle (0 \mid g^*h^* + 2g^*) \rangle \subseteq \mathcal{C}^\perp$.*

Proof. The code $\mathcal{C}_Y$ is a quaternary cyclic code generated by $\langle (fh+2f)\rangle$. As shown in [7], $(\mathcal{C}_Y)^{\perp} = \langle (g^*h^* + 2g^*)\rangle$.

Let $\mathbf{v} = (v \mid v') \in \mathcal{C}$, then $(0 \mid g^*h^* + 2g^*) \circ \mathbf{v} = 0 \mod (x^{\mathfrak{m}} - 1)$. By Lemma 2, $(g^*h^* + 2g^*)v'^* = 0 \mod (x^{\beta} - 1)$. Thus, $\langle (0 \mid g^*h^* + 2g^*)\rangle \subseteq \mathcal{C}^{\perp}$. □

Corollary 2. *Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, where $fgh = x^{\beta} - 1$, and with dual code $\mathcal{C}^{\perp} = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f})\rangle$. Then, $(\bar{f}\bar{h} + 2\bar{f})$ divides $(g^*h^* + 2g^*)$.*

Proof. By Proposition 11, $\langle (0 \mid g^*h^* + 2g^*)\rangle \subseteq \mathcal{C}^{\perp}$. Thus, $(g^*h^* + 2g^*) \in \langle \bar{f}\bar{h} + 2\bar{f}\rangle$. □

Corollary 3. *Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, where $fgh = x^{\beta} - 1$. Let $T = \{(0 \mid p) \in \mathcal{C}^{\perp}\}$. Then, T is generated by $\langle (0 \mid g^*h^* + 2g^*)\rangle$.*

Proof. Let $T = \{(0 \mid p) \in \mathcal{C}^{\perp}\}$. By Proposition 11, we have that $\langle (0 \mid g^*h^* + 2g^*)\rangle \subseteq T$. Since $T_Y \subseteq (C_Y)^{\perp} = \langle g^*h^* + 2g^*\rangle$, for all $(0 \mid p) \in T$ we have that $p \in \langle g^*h^* + 2g^*\rangle$. Hence, there exists $\lambda \in \mathbb{Z}_4[x]$ such that $p = \lambda(g^*h^* + 2g^*)$. Therefore, for all $(0 \mid p) \in T$ we have that

$$(0 \mid p) = (0 \mid \lambda(g^*h^* + 2g^*)) = \lambda \star (0 \mid g^*h^* + 2g^*).$$

So, $T \subseteq \langle (0 \mid g^*h^* + 2g^*)\rangle$. □

Lemma 3. *Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, where $fgh = x^{\beta} - 1$. Then, $\frac{\gcd(b,\ell g)}{\gcd(b,\ell)}\ell$ is linear combination of b and ℓg.*

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

$$\begin{aligned} \ell &= \gcd(b,\ell)\rho, \\ \ell g &= \gcd(b,\ell g)\rho\tau_1, \\ b &= \gcd(b,\ell g)\tau_2, \end{aligned}$$

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

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

□

The previous propositions, lemmas and corollaries will be helpful to determine the relations between the generator polynomials of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code and the generator polynomials of its dual code.

Proposition 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,

$$\begin{aligned} (b \mid 0) \circ (\bar{b} \mid 0) &= 0 \mod (x^{\mathfrak{m}} - 1), \\ (\ell \mid fh + 2f) \circ (\bar{b} \mid 0) &= 0 \mod (x^{\mathfrak{m}} - 1). \end{aligned}$$

Therefore, by Lemma 2,

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

over $\mathbb{Z}_2$. So, $\gcd(b, \ell)\bar{b}^* = 0 \mod (x^\alpha - 1)$, 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 8, 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 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,

$$(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (0 \mid \frac{b}{\gcd(b, \ell g)} 2f) = 0 \mod (x^{\mathfrak{m}} - 1).$$

Thus, by Lemma 2,

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

and

$$(2\bar{f}\bar{h}) \left(\frac{b^* f^*}{\gcd(b, \ell g)^*} \right) = 2\mu(x^\beta - 1), \tag{3}$$

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

If (3) 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 $\bar{f}\bar{h}$ is a divisor of $x^\beta - 1$ and, by Corollary 1, we have that $\left(\frac{b^* f^*}{\gcd(b, \ell g)^*} \right)$ divides $(x^\beta - 1)$ over $\mathbb{Z}_2$. By Corollary 9, $\deg(\bar{f}\bar{h}) = \beta - \deg(f) - \deg(b) + \deg(\gcd(b, \ell g))$, so

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

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

$$\bar{f}\bar{h} = \frac{(x^\beta - 1) \gcd(b, \ell g)^*}{f^* b^*} \in \mathbb{Z}_2[x]. \tag{4}$$

Since β is odd and by the uniqueness of the Hensel Lift [8, p.73] then $\bar{f}\bar{h}$ is the unique monic polynomial in $\mathbb{Z}_4[x]$ dividing $(x^\beta - 1)$ and satisfying (4). □

Proposition 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. Consider τ_1, τ_2 and ρ as in the proof of Lemma 3, there exist $t_1, t_2 \in \mathbb{Z}_4[x]$ such that

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

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, $(2\bar{p}_2 \bar{\ell}\bar{g} \mid 2\bar{f}) \in \mathcal{C}^\perp$.

Therefore,

$$(2\bar{p}_2 \bar{\ell}\bar{g} \mid 2\bar{f}) \circ \left(0 \mid \frac{\gcd(b, \ell g)}{\gcd(b, \ell)} (fh + 2f) + t_1 2fg \right) = 0 \mod (x^{\mathfrak{m}} - 1).$$

By Lemma 2 and, arranging properly, we obtain that

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

and

$$2\bar{f}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right) f^*h^* = 2\mu(x^\beta - 1), \tag{5}$$

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

If (5) 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 9, $\deg(\bar{f}) = \beta - \deg(f) - \deg(h) + \deg(\gcd(b,\ell)) - \deg(\gcd(b,\ell g))$, 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

$$\bar{f} = \frac{(x^\beta - 1)\gcd(b,\ell)^*}{\gcd(b,\ell g)^* f^*h^*} \in \mathbb{Z}_2[x]. \tag{6}$$

Since β is odd and by the uniqueness of the Hensel Lift [8, p.73] then $\bar{f}$ is the unique monic polynomial in $\mathbb{Z}_4[x]$ dividing $(x^\beta - 1)$ and holding (6). □

Proposition 15. *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 $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Then,*

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

for some $\lambda \in \mathbb{Z}_2[x]$.

Proof. Consider

$$(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (b \mid 0) = 0 \mod (x^{\mathfrak{m}} - 1).$$

By Lemma 2,

$$\bar{\ell}b^* = 0 \mod (x^\alpha - 1)$$

and, for some $\lambda \in \mathbb{Z}_2[x]$,

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

□

Corollary 4. *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. Then,* $\deg(\lambda) < \deg(b) - \deg(\gcd(b, \ell))$.

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. For example, applying Lemma 1 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 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 $\tau = \rho\tau_1 = \frac{\ell g}{\gcd(b, \ell g)}$. If $b \neq \gcd(b, \ell g)$, then*

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

If $b = \gcd(b, \ell g)$, then

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

Proof. Let $\frac{b^*}{\gcd(b, \ell g)^*} \neq 1$. We are going to compute $(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell g \mid 2fg)$. By Proposition 13 and Proposition 15, we obtain that $(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell g \mid 2fg)$ is equal to

$$2\frac{(x^{\mathfrak{m}} - 1)}{b^*} \lambda x^{\mathfrak{m} - \deg(\ell g) - 1} (\ell g)^* + 2\frac{(x^{\mathfrak{m}} - 1) \gcd(b, \ell g)^*}{f^* b^*} x^{\mathfrak{m} - \deg(fg) - 1} f^* g^*.$$

Since they are orthogonal codewords, we have that

$$2\frac{(x^{\mathfrak{m}} - 1) \gcd(b, \ell g)^*}{b^*} (\lambda x^{\mathfrak{m} - \deg(\ell g) - 1} \tau^* + x^{\mathfrak{m} - \deg(fg) - 1} g^*) = 0 \mod (x^{\mathfrak{m}} - 1).$$

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

$$\frac{(x^{\mathfrak{m}} - 1) \gcd(b, \ell g)^*}{b^*} (\lambda x^{\mathfrak{m} - \deg(\ell g) - 1} \tau^* + x^{\mathfrak{m} - \deg(fg) - 1} g^*) = 0 \mod (x^{\mathfrak{m}} - 1).$$

Then,

$$(\lambda x^{\mathfrak{m} - \deg(\ell g) - 1} \tau^* + x^{\mathfrak{m} - \deg(fg) - 1} g^*) = 0 \mod (x^{\mathfrak{m}} - 1), \tag{7}$$

or

$$(\lambda x^{\mathfrak{m} - \deg(\ell g) - 1} \tau^* + x^{\mathfrak{m} - \deg(fg) - 1} g^*) = 0 \mod \left(\frac{b^*}{\gcd(b, \ell g)^*} \right). \tag{8}$$

Since $\left(\frac{b^*}{\gcd(b, \ell g)^*} \right)$ divides $(x^{\mathfrak{m}} - 1)$, then (7) implies (8).

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

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

For $\frac{b^*}{\gcd(b,\ell g)^*} = 1$, then one have to compute $(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell \mid fh + 2f)$. And using a similar argument, then one obtains that

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

□

We summarize the previous results in the next theorem.

Theorem 2. *Let* $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x)+2f(x)) \rangle$ *be a* $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic code of type* $(\alpha, \beta; \gamma, \delta; \kappa)$ *, where* $f(x)g(x)h(x) = x^\beta - 1$*, and with dual code* $\mathcal{C}^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{f}(x)\bar{h}(x)+2\bar{f}(x)) \rangle$*, where* $\bar{f}(x)\bar{g}(x)\bar{h}(x) = x^\beta - 1$*. Let* $\rho(x) = \frac{\ell(x)}{\gcd(b(x),\ell(x))}$ *and* $\tau(x) = \rho(x)\tau_1(x) = \frac{\ell(x)g(x)}{\gcd(b(x),\ell(x)g(x))}$*. 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. $\bar{\ell} = \frac{x^\alpha - 1}{b^*}\lambda \in \mathbb{Z}_2[x]$,

where

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

if $b \neq \gcd(b, \ell g)$ *or*

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

if $b = \gcd(b, \ell g)$.

References

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

[2] 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, 2010.

[3] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, vol. 10, 1973.

[4] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes. *IEEE Trans. Info. Theory*, vol. 40, pp. 301-319, 1994.

[5] W.C. Huffman, V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, Cambridge, 2003.

[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, 1996.

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