Z 2 Z 4 -Additive Quasi-Cyclic codes

Minjia Shi, Shitao Li, Patrick Solé

$\mathbb{Z}_2\mathbb{Z}_4$-Additive Quasi-Cyclic codes

Minjia Shi, Shitao Li, Patrick Solé

***Abstract*—We study the codes of the title by the CRT method, that decomposes such codes into constituent codes, which are shorter codes over larger alphabets. Criteria on these constituent codes for self-duality and linear complementary duality of the decomposed codes are derived. The special class of the one-generator codes is given a polynomial representation and exactly enumerated. In particular, we present some illustrative examples of binary linear codes derived from the $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes that meet the Griesmer bound with equality.**

***Index Terms*—$\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes, Chinese Remainder Theorem, self-dual codes, ACD codes.**

I. Introduction

In this article, we consider the mixed alphabet codes with two alphabets: the first is the finite field $\mathbb{Z}_2$ and the second is the local ring $\mathbb{Z}_4$. These mixed alphabets were introduced in [7] in the additive case, and studied in the cyclic case in [1], [8]. The latter class was shown recently to be asymptotically good [12], [27]. Many other pairs of alphabets are possible [3], [4], [5], [9], [15], [24], but in the present paper, for simplicity's sake, we will focus on $\mathbb{Z}_2$ and $\mathbb{Z}_4$. A natural generalization of cyclic codes is the class of quasi-cyclic codes, which has been studied in particular by using a decomposition of the alphabet into local rings and of the codes into constituent codes [16], [17], [25], by the Chinese Remainder Theorem (CRT). These constituents codes are shorter, of length the co-index, over larger alphabets (extensions of the original alphabet of degree the index of the code). Self-dual quasi-cyclic codes and self-dual generalized quasi-cyclic codes over finite fields were proved to be asymptotically good [18], [23]. So are linear complementary dual (LCD) quasi-cyclic codes over finite fields [14].

In the present paper, we combine both trends by studying $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes. Here, it generalizes the notion of LCD codes to additive complementary dual (ACD) codes in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ [6]. The CRT decomposition allows us to give criteria bearing on the constituent codes for the quasi-cyclic codes to be self-dual, or to be ACD. Note that the family of LCD codes has known a surge of interest in recent years, due to applications in Boolean masking in embarked cryptographic computations [10]. The family of self-dual codes has been studied since the 1960's over fields [19], and since the 1990's over rings [21], and enjoys many connections with combinatorial designs and modular forms [22]. The subclass of quasi-cyclic codes called one-generator is traditionally treated by a polynomial representation akin to that of cyclic codes [11], [20]. We use this formulation over $\mathbb{Z}_2\mathbb{Z}_4$ to derive exact enumeration results.

The material is arranged as follows. The next section recalls notation and definitions needed in the other sections. Section 3 establishes the polynomial representation of $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes. Section 4 develops the CRT approach, and derives the two criterion mentioned. Section 5 studies the one-generator class. Section 6 gives some good examples of $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes. Section 7 concludes the article.

II. Preliminaries

In this section, we introduce some basic concepts, and present some auxiliary lemmas. For every vector $\mathbf{c} \in \mathbb{Z}_2^{l_2 m_2} \times \mathbb{Z}_4^{l_4 m_4}$, we write $\mathbf{c} = (\mathbf{c}_2, \mathbf{c}_4')$, where $\mathbf{c}_2 = (c_{00}, c_{01}, \ldots, c_{0,l_2-1}, c_{10}, \ldots, c_{1,l_2-1}, \ldots, c_{m_2-1,0}, \ldots, c_{m_2-1,l_2-1}) \in \mathbb{Z}_2^{l_2 m_2}$ and $\mathbf{c}_4' = (c'_{00}, c'_{01}, \ldots, c'_{0,l_4-1}, c'_{10}, \ldots,$

This research is supported by the National Natural Science Foundation of China (12071001, 61672036), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03).

Minjia Shi and Shitao Li are with the Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, 230601, China.

Patrick Solé is with I2M, CNRS, Centrale Marseille, University of Aix-Marseille, Marseille, France

$c'_{1,l_4-1},\ldots,c'_{m_4-1,0},\ldots,c'_{m_4-1,l_4-1}) \in \mathbb{Z}_4^{l_4m_4}$. We denote by T_2 (resp. T_4) the standard shift operator acting on $\mathbb{Z}_2^{l_2m_2}$ (resp. $\mathbb{Z}_4^{l_4m_4}$).

Definition II.1. A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type (l_2m_2, l_4m_4) is called a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code if for every codeword $\mathbf{c} \in \mathcal{C}$, its shift, defined as

$$T(\mathbf{c}) = (T_2^{l_2}(\mathbf{c}_2), T_4^{l_4}(\mathbf{c}'_4)) = (c_{m_2-1,0},\ldots,$$
$$c_{m_2-1,l_2-1}, c_{00}, c_{01},\ldots,c_{0,l_2-1},\ldots,c_{m_2-2,0},$$
$$\ldots, c_{m_2-2,l_2-1}, c'_{m_4-1,0},\ldots,c'_{m_4-1,l_4-1}, c'_{00},$$
$$c'_{01},\ldots,c'_{0,l_4-1},\ldots,c'_{m_4-2,0},\ldots,c'_{m_4-2,l_4-1})$$

is also a codeword of $\mathcal{C}$. Such a code $\mathcal{C}$ is said to be $\mathbb{Z}_2\mathbb{Z}_4$-*additive quasi-cyclic* of index (l_2, l_4) or (l_2, l_4)-*quasi-cyclic* over $\mathbb{Z}_2\mathbb{Z}_4$.

For any pair of vectors

$$\mathbf{u} = (\mathbf{u}_2, \mathbf{u}'_4) = (u_{00}, u_{01},\ldots,u_{0,l_2-1}, u_{10},\ldots,$$
$$u_{1,l_2-1},\ldots,u_{m_2-1,0},\ldots,u_{m_2-1,l_2-1},$$
$$u'_{00}, u'_{01},\ldots,u'_{0,l_4-1}, u'_{10},\ldots,$$
$$u'_{1,l_4-1},\ldots,u'_{m_4-1,0},\ldots,u'_{m_4-1,l_4-1})$$

and

$$\mathbf{v} = (\mathbf{v}_2, \mathbf{v}'_4) = (v_{00}, v_{01},\ldots,v_{0,l_2-1}, v_{10},\ldots,$$
$$v_{1,l_2-1},\ldots,v_{m_2-1,0},\ldots,v_{m_2-1,l_2-1},$$
$$v'_{00}, v'_{01},\ldots,v'_{0,l_4-1}, v'_{10},\ldots,v'_{1,l_4-1},\ldots,$$
$$v'_{m_4-1,0},\ldots,v'_{m_4-1,l_4-1}) \in \mathbb{Z}_2^{l_2m_2} \times \mathbb{Z}_4^{l_4m_4},$$

the *standard inner product* [7] is defined as

$$\mathbf{u}\cdot\mathbf{v} = 2\mathbf{u}_2\cdot\mathbf{v}_2 + \mathbf{u}'_4\cdot\mathbf{v}'_4$$
$$= \left[2\sum_{j=0}^{l_2-1}\sum_{i=0}^{m_2-1} u_{ij}v_{ij} + \sum_{k=0}^{l_4-1}\sum_{r=0}^{m_4-1} u'_{rk}v'_{rk}\right] \pmod 4.$$

Definition II.2. Let $\mathcal{C}$ be any $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code. The additive dual code of $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_2^{l_2m_2}\times\mathbb{Z}_4^{l_4m_4} \mid \mathbf{u}\cdot\mathbf{v} = 0, \text{ for all } \mathbf{u} \in \mathcal{C}\}$.

A natural generalization of LCD codes from linear to additive codes is as follows.

Definition II.3. [6] A $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code $\mathcal{C}$ is ACD if $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$.

Using Definition II.2 of the dual, we have the following lemma.

Lemma II.4. *If $\mathcal{C}$ is any $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code, then $\mathcal{C}^\perp$ is also additive quasi-cyclic.*

Proof: Let $\mathcal{C}$ be any $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code of index (l_2, l_4), and type (l_2m_2, l_4m_4). Let

$$\mathbf{v} = (\mathbf{v}_2, \mathbf{v}'_4) = (v_{00}, v_{01},\ldots,v_{0,l_2-1}, v_{10},\ldots,$$
$$v_{1,l_2-1},\ldots,v_{m_2-1,0},\ldots,v_{m_2-1,l_2-1},$$
$$v'_{00}, v'_{01},\ldots,v'_{0,l_4-1}, v'_{10},\ldots,v'_{1,l_4-1},\ldots,$$
$$v'_{m_4-1,0},\ldots,v'_{m_4-1,l_4-1}) \in \mathcal{C}^\perp,$$

It suffices to show that $T(\mathbf{v}) \in \mathcal{C}^\perp$. Since $\mathbf{v} \in \mathcal{C}^\perp$, for any codeword

$$\mathbf{u} = (\mathbf{u}_2, \mathbf{u}'_4) = (u_{00}, u_{01},\ldots,u_{0,l_2-1}, u_{10},\ldots,$$
$$u_{1,l_2-1},\ldots,u_{m_2-1,0},\ldots,u_{m_2-1,l_2-1},$$
$$u'_{00}, u'_{01},\ldots,u'_{0,l_4-1}, u'_{10},\ldots,u'_{1,l_4-1},\ldots,$$
$$u'_{m_4-1,0},\ldots,u'_{m_4-1,l_4-1}) \in \mathcal{C},$$

we have

$$\mathbf{u}\cdot\mathbf{v} = \left[2\sum_{j=0}^{l_2-1}\sum_{i=0}^{m_2-1} u_{ij}v_{ij} + \sum_{k=0}^{l_4-1}\sum_{r=0}^{m_4-1} u'_{rk}v'_{rk}\right]$$
$$= 0 \pmod 4.$$

Now we just need to prove that $\mathbf{u}\cdot T(\mathbf{v}) = 0$. Let $m = \operatorname{lcm}(m_2, m_4)$. Then $T^m(\mathbf{u}) = \mathbf{u}$ for any $\mathbf{u} \in \mathbb{Z}_2^{l_2m_2} \times \mathbb{Z}_4^{l_4m_4}$. Since $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code, $T^{m-1}(\mathbf{u}) \in \mathcal{C}$. Hence

$$0 = T^{m-1}(\mathbf{u})\cdot\mathbf{v} = \mathbf{u}\cdot T(\mathbf{v}).$$

Therefore, $T(\mathbf{v}) \in \mathcal{C}^\perp$, and hence $\mathcal{C}^\perp$ is also additive quasi-cyclic. ■

III. Additive Quasi-Cyclic Codes

In this section, we introduce a polynomial representation of a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes. Let $\mathbb{Z}_2[X]$ (resp. $\mathbb{Z}_4[X]$) denote the polynomials in the indeterminate X with coefficients in $\mathbb{Z}_2$ (resp. $\mathbb{Z}_4$). Consider now the quotient rings

$$\begin{aligned} R_2 &:= R_2(\mathbb{Z}_2, m_2) = \mathbb{Z}_2[X]/(X^{m_2}-1), \\ R_4 &:= R_4(\mathbb{Z}_4, m_4) = \mathbb{Z}_4[X]/(X^{m_4}-1). \end{aligned}$$

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code of type (l_2m_2, l_4m_4). Write an arbitrary codeword of $\mathcal{C}$ as

$$\begin{aligned} \mathbf{c} = (&c_{00}, c_{01}, \ldots, c_{0,l_2-1}, c_{10}, \ldots, \\ &c_{1,l_2-1}, \ldots, c_{m_2-1,0}, \ldots, c_{m_2-1,l_2-1}, \\ &c'_{00}, c'_{01}, \ldots, c'_{0,l_4-1}, c'_{10}, \ldots, c'_{1,l_4-1}, \ldots, \\ &c'_{m_4-1,0}, \ldots, c'_{m_4-1,l_4-1}) \in \mathcal{C}. \end{aligned}$$

Define a map $\phi : \mathbb{Z}_2^{l_2m_2} \times \mathbb{Z}_4^{l_4m_4} \longrightarrow R_2^{l_2} \times R_4^{l_4}$ by

$$\begin{aligned} \phi(\mathbf{c}) =&(\mathbf{c}_0(X), \mathbf{c}_1(X), \ldots, \mathbf{c}_{l_2-1}(X), \\ &\mathbf{c}'_0(X), \mathbf{c}'_1(X), \ldots, \mathbf{c}'_{l_4-1}(X)) \in R_2^{l_2} \times R_4^{l_4} \end{aligned}$$

where

$$\begin{aligned} \mathbf{c}_j(X) &= \sum_{i=0}^{m_2-1} c_{ij}X^i \in R_2, 0 \le j \le l_2-1, \\ \mathbf{c}'_k(X) &= \sum_{r=0}^{m_4-1} c'_{rk}X^r \in R_4, 0 \le k \le l_4-1. \end{aligned}$$

Let $\phi(\mathcal{C})$ denote the image of $\mathcal{C}$ under ϕ. For any element $\mathbf{c}(X) = (\mathbf{c}_0(X), \mathbf{c}_1(X), \ldots, \mathbf{c}_{l_2-1}(X), \mathbf{c}'_0(X), \mathbf{c}'_1(X), \ldots, \mathbf{c}'_{l_4-1}(X)) \in R_2^{l_2} \times R_4^{l_4}$, and any $\mathbf{a}(X) \in \mathbb{Z}_4[X]$, we have

$$\begin{aligned} \mathbf{a}(X)\mathbf{c}(X) = (&\overline{\mathbf{a}}(X)\mathbf{c}_0(X), \overline{\mathbf{a}}(X)\mathbf{c}_1(X), \ldots, \\ &\overline{\mathbf{a}}(X)\mathbf{c}_{l_2-1}(X), \mathbf{a}(X)\mathbf{c}'_0(X), \\ &\mathbf{a}(X)\mathbf{c}'_1(X), \ldots, \mathbf{a}(X)\mathbf{c}'_{l_4-1}(X)), \end{aligned}$$

where $\overline{\mathbf{a}}(X) = \mathbf{a}(X) \pmod 2$. We have the following lemma.

Lemma III.1. *The map ϕ induces a one-to-one correspondence between $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes of index (l_2, l_4) and $\mathbb{Z}_4[X]$-submodules of $R_2^{l_2} \times R_4^{l_4}$.*

Proof: The result follows from [16, Lemma 3.1] and [17, Lemma 3.1], so we omit it here. ■

We define a "conjugation" map $\sim$ on R_2 (resp. R_4) as one that acts as the identity on the elements of $\mathbb{Z}_2$ (resp. $\mathbb{Z}_4$) and that sends X to $X^{-1} = X^{m_2-1}$ (resp. $X^{-1} = X^{m_4-1}$). The *reciprocal polynomial* of a polynomial $f(X)$ is $X^{deg(f(X))}f(X^{-1})$ and is denoted by $f^*(X)$. Let $\theta_m(X) = \sum_{i=0}^{m-1} X^i$. Let $\mathbf{x} = (x_0, x_1, \ldots, x_{l_2-1}, x'_0, x'_1, \ldots, x'_{l_4-1}), \mathbf{y} = (y_0, y_1, \ldots, y_{l_2-1}, y'_0, y'_1, \ldots, y'_{l_4-1}) \in R_2^{l_2} \times R_4^{l_4}$, $m = \mathrm{lcm}(m_2, m_4)$. We define an extension map of [8, Definition 8]

$$\begin{aligned} \circ(\mathbf{x}, \mathbf{y}) = &\sum_{i=0}^{l_2-1} 2x_i\theta_{\frac{m}{m_2}}(X^{m_2})X^{m-1-deg(y_i)}y_i^* \\ &+ \sum_{j=0}^{l_4-1} x'_j\theta_{\frac{m}{m_4}}(X^{m_4})X^{m-1-deg(y'_j)}y'^*_j \\ &\pmod{(X^m-1)}, \end{aligned}$$

where the computations are made taking the binary zeros and ones in x_i and y_i as quaternary zeros and ones. We call it $\circ$-*inner product* and denote $\circ(\mathbf{x}, \mathbf{y})$ by $\mathbf{x} \circ \mathbf{y}$.

Proposition III.2. *Let $\boldsymbol{u}$, $\boldsymbol{v} \in \mathbb{Z}_2^{l_2m_2} \times \mathbb{Z}_4^{l_4m_4}$, $m = \mathrm{lcm}(m_2, m_4)$. Then $\boldsymbol{u} \cdot (T^n(\boldsymbol{v})) = 0$ for all $0 \le n \le m-1$ if and only if $\phi(\boldsymbol{u}) \circ \phi(\boldsymbol{v}) = 0$.*

Proof: Let

$$\begin{aligned} \mathbf{u} = (\mathbf{u}_2, \mathbf{u}'_4) = (&u_{00}, u_{01}, \ldots, u_{0,l_2-1}, u_{10}, \ldots, \\ &u_{1,l_2-1}, \ldots, u_{m_2-1,0}, \ldots, u_{m_2-1,l_2-1}, \\ &u'_{00}, u'_{01}, \ldots, u'_{0,l_4-1}, u'_{10}, \ldots, \\ &u'_{1,l_4-1}, \ldots, u'_{m_4-1,0}, \ldots, u'_{m_4-1,l_4-1}), \\ \mathbf{v} = (\mathbf{v}_2, \mathbf{v}'_4) = (&v_{00}, v_{01}, \ldots, v_{0,l_2-1}, v_{10}, \ldots, \\ &v_{1,l_2-1}, \ldots, v_{m_2-1,0}, \ldots, v_{m_2-1,l_2-1}, \\ &v'_{00}, v'_{01}, \ldots, v'_{0,l_4-1}, v'_{10}, \ldots, v'_{1,l_4-1}, \ldots, \\ &v'_{m_4-1,0}, \ldots, v'_{m_4-1,l_4-1}) \in \mathbb{Z}_2^{l_2m_2} \times \mathbb{Z}_4^{l_4m_4}, \end{aligned}$$

Then

$$\begin{aligned} \phi(\mathbf{u}) = (&\mathbf{u}_0(X), \mathbf{u}_1(X), \ldots, \mathbf{u}_{l_2-1}(X), \\ &\mathbf{u}'_0(X), \mathbf{u}'_1(X), \ldots, \mathbf{u}'_{l_4-1}(X)), \\ \phi(\mathbf{v}) = (&\mathbf{v}_0(X), \mathbf{v}_1(X), \ldots, \mathbf{v}_{l_2-1}(X), \\ &\mathbf{v}'_0(X), \mathbf{v}'_1(X), \ldots, \mathbf{v}'_{l_4-1}(X)). \end{aligned}$$

The condition $\phi(\mathbf{u}) \circ \phi(\mathbf{v}) = 0$ is equivalent to

$$\begin{aligned}
&\sum_{i=0}^{l_2-1} 2\mathbf{u}_i(X)\theta_{\frac{m}{m_2}}(X^{m_2})X^{m-1-deg(\mathbf{v}_i(X))}\mathbf{v}_i^*(X) \\
&+ \sum_{j=0}^{l_4-1} \mathbf{u}'_j(X)\theta_{\frac{m}{m_4}}(X^{m_4})X^{m-1-deg((\mathbf{v}'_j(X)))}\mathbf{v}'^*_j(X) \\
&= \theta_{\frac{m}{m_2}}(X^{m_2})\left(\sum_{r=0}^{m_2-1} 2\sum_{i=0}^{l_2-1}\sum_{k=0}^{m_2-1} u_{ki}v_{k+r,i}X^{m-1-r}\right) \\
&+ \theta_{\frac{m}{m_4}}(X^{m_4})\left(\sum_{t=0}^{m_4-1}\sum_{j=0}^{l_4-1}\sum_{s=0}^{m_4-1} u'_{sj}v'_{s+t,j}X^{m-1-t}\right) \\
&= \sum_{n=0}^{m-1}\left(2\sum_{i=0}^{l_2-1}\sum_{k=0}^{m_2-1} u_{ki}v_{k+n,i} + \right. \\
&\left. \sum_{j=0}^{l_4-1}\sum_{s=0}^{m_4-1} u'_{sj}v'_{s+n,j}\right)X^{m-1-n} \mod (X^m-1), \\
&= 0,
\end{aligned}$$

where the subscripts $k+n$ (resp. $s+n$) are taken modulo m_2 (resp. m_4). Comparing the coefficient of X^{m-1-n} on both sides, the above equation is equivalent to

$$2\sum_{i=0}^{l_2-1}\sum_{k=0}^{m_2-1} u_{ki}v_{k+n,i} + \sum_{j=0}^{l_4-1}\sum_{s=0}^{m_4-1} u'_{sj}v'_{s+n,j} = 0,$$

for all $0 \le n \le m-1$. The equation means precisely that

$$\begin{aligned}
&\mathbf{u}_2 \cdot \left(T_2^{-l_2 n}(\mathbf{v}_2)\right) + \mathbf{u}'_4 \cdot \left(T_4^{-l_4 n}(\mathbf{v}'_4)\right) \\
&= \mathbf{u} \cdot \left(T^{-n}(\mathbf{v})\right) \\
&= 0.
\end{aligned}$$

Since $T^{-n} = T^{m-n}$, $\phi(\mathbf{u}) \circ \phi(\mathbf{v}) = 0$, is equivalent to $\mathbf{u} \cdot (T^n(\mathbf{v})) = 0$ for all $0 \le n \le m-1$. ∎

By applying Proposition III.2, we can obtain the following.

Corollary III.3. *Let $\mathcal{C}$ be an additive quasi-cyclic code and $\mathcal{C} \subset \mathbb{Z}_2^{l_2 m_2} \times \mathbb{Z}_4^{l_4 m_4}$, let $\phi(\mathcal{C})$ be its image in $R_2^{l_2} \times R_4^{l_4}$ under ϕ. Then $\phi(\mathcal{C})^{\perp_\circ} = \phi(\mathcal{C}^\perp)$, where the dual in $\mathbb{Z}_2^{l_2 m_2} \times \mathbb{Z}_4^{l_4 m_4}$ is taken with respect to the standard inner product, while the dual in $R_2^{l_2} \times R_4^{l_4}$ is taken with respect to the $\circ$-inner product. In particular, a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code is self-dual with respect to the standard inner product if and only if $\phi(\mathcal{C})$ is self-dual with respect to the $\circ$-inner product.*

Example III.4. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code with generator matrix

$$G = \left(\begin{array}{cccc|cccc}
10 & 01 & 00 & & 00 & 00 & 20 \\
00 & 10 & 01 & & 20 & 00 & 00 \\
01 & 00 & 10 & & 00 & 20 & 00 \\
10 & 01 & 01 & & 10 & 01 & 02 \\
01 & 10 & 01 & & 02 & 10 & 01 \\
01 & 01 & 10 & & 01 & 02 & 10
\end{array}\right).$$

Thus $l_2 = 2, l_4 = 2$. It can be checked that $\mathcal{C}$ is self-orthogonal, and that $|\mathcal{C}| = 2^3 4^3$. Hence $|\mathcal{C}^\perp| = 2^6 4^6 / 2^3 4^3 = 2^3 4^3 = |\mathcal{C}|$. Therefore $\mathcal{C} = \mathcal{C}^\perp$ and $\mathcal{C}$ is self-dual with respect to the standard inner product. Under the mapping of ϕ,

$$R_2^2 \times R_4^2 = \left(\frac{\mathbb{Z}_2[X]}{(X^3-1)}\right)^2 \times \left(\frac{\mathbb{Z}_4[X]}{(X^3-1)}\right)^2,$$

$\phi(\mathcal{C})$ is $\mathbb{Z}_4[X]$-submodule of $R_2^2 \times R_4^2$ with generator vectors $\underline{a_1}(X) = (1, X, 2X^2, 0)$ and $\underline{a_2}(X) = (1, X + X^2, 1, X + 2X^2)$. It is easy to verify that $\phi(\mathcal{C})$ is self-dual with respect to the $\circ$-inner product. And $\underline{a_1}(X)$ and $\underline{a_2}(X)$ are generator polynomials of $\mathcal{C}$.

IV. The Rings $R_2(\mathbb{Z}_2, m)$ and $R_4(\mathbb{Z}_4, m)$

When m is an odd integer > 1, upon using the CRT for polynomials, we see that the ring $R_2 = R_2(\mathbb{Z}_2, m) = \mathbb{Z}_2[X]/(X^m - 1)$ is never a finite field, and that R_2 is a direct product of finite fields. The ring $R_4 = R_4(\mathbb{Z}_4, m) = \mathbb{Z}_4[X]/(X^m - 1)$ is not a local ring, and R_4 is a direct product of local rings. The following background material can be found in [26].

Under the latter assumption, the polynomial $X^m - 1$ factors completely into distinct irreducible factors in $\mathbb{Z}_4[X]$, so by Hensel's lifting, we may write $X^m - 1 \in \mathbb{Z}_4[X]$ as

$$X^m - 1 = f_1 f_2 \dots f_r,$$

where f_j are distinct basic irreducible polynomials. This product is unique in the sense that, if $X^m - 1 = f'_1 f'_2 \dots f'_{r'}$ is another decomposition into basic irreducible polynomials, then $r = r'$ and, after suitable renumbering of the f'_j's, we have that f_j is an associate of f'_j for each $1 \le j \le r$. The two sides of the above equation are reciprocal.

$$X^m - 1 = -f_1^* f_2^* \dots f_r^*.$$

If f is a basic irreducible polynomial, so is f^*. By the uniqueness of the decomposition of a polynomial into basic irreducible factors, we can now write

$$X^m - 1 = g_1 \dots g_s h_1 h_1^* \dots h_t h_t^*, \tag{1}$$

where $g_1, \dots, g_s$ are those f_js that are associates to their own reciprocals, and $h_1, h_1^*, \dots, h_t, h_t^*$ are the remaining f_j^*s grouped in pairs. Therefore, let $\overline{f_i} = f_i \pmod 2$, then the polynomial $X^m - 1$ can be decomposed into the following form in $\mathbb{Z}_2[X]$

$$X^m - 1 = \overline{f_1}\ \overline{f_2} \dots \overline{f_r}.$$

By (1), we have

$$X^m - 1 = \overline{g_1} \dots \overline{g_s}\overline{h_1}\ \overline{h_1^*} \dots \overline{h_t}\ \overline{h_t^*},$$

where $\overline{g_1}, \dots, \overline{g_s}$ are associates to their own reciprocals, $\overline{h_j}$ and $\overline{h_j^*}$ are reciprocal. Consequently, we may now write

$$R_4 = \frac{\mathbb{Z}_4[X]}{(X^m-1)} = \left(\bigoplus_{i=1}^{s} \frac{\mathbb{Z}_4[X]}{(g_i)}\right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{\mathbb{Z}_4[X]}{(h_j)} \oplus \frac{\mathbb{Z}_4[X]}{(h_j^*)}\right)\right), \tag{2}$$

$$R_2 = \frac{\mathbb{Z}_2[X]}{(X^m-1)} = \left(\bigoplus_{i=1}^{s} \frac{\mathbb{Z}_2[X]}{(\overline{g_i})}\right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{\mathbb{Z}_2[X]}{(\overline{h_j})} \oplus \frac{\mathbb{Z}_2[X]}{(\overline{h_j^*})}\right)\right). \tag{3}$$

The direct sum on the right-hand side is endowed with the coordinate-wise addition and multiplication.

For simplicity of notation, whenever m is fixed, we denote $\mathbb{Z}_4[X]/(g_i)$ by G_i, $\mathbb{Z}_4[X]/(h_j)$ by H_j', $\mathbb{Z}_4[X]/(h_j^*)$ by H_j'', $\mathbb{Z}_2[X]/(\overline{g_i})$ by $\overline{G_i}$, $\mathbb{Z}_2[X]/(\overline{h_j})$ by $\overline{H_j'}$, and $\mathbb{Z}_2[X]/(\overline{h_j^*})$ by $\overline{H_j''}$. It follows from the above equations that

$$R_4^{l_4} = \left(\bigoplus_{i=1}^{s} G_i^{l_4}\right) \oplus \left(\bigoplus_{j=1}^{t} \left({H_j'}^{l_4} \oplus {H_j''}^{l_4}\right)\right),$$

$$R_2^{l_2} = \left(\bigoplus_{i=1}^{s} \overline{G_i}^{l_2}\right) \oplus \left(\bigoplus_{j=1}^{t} \left(\overline{H_j'}^{l_2} \oplus \overline{H_j''}^{l_2}\right)\right).$$

Then

$$R_2^{l_2} \times R_4^{l_4} = \left(\bigoplus_{i=1}^{s} \left(\overline{G_i}^{l_2} \times {G_i}^{l_4}\right)\right) \oplus \left(\bigoplus_{j=1}^{t} \left(\left(\overline{H_j'}^{l_2} \times {H_j'}^{l_4}\right) \oplus \left(\overline{H_j''}^{l_2} \times {H_j''}^{l_4}\right)\right)\right). \tag{4}$$

In particular, every R_2R_4-additive code C can be decomposed as the direct sum

$$C = \left(\bigoplus_{i=1}^{s} C_i\right) \oplus \left(\bigoplus_{j=1}^{t} \left(C_j' \oplus C_j''\right)\right), \tag{5}$$

where, for each $1 \le i \le s, C_i$ is a $\overline{G_i}G_i$-additive code, for each $1 \le j \le t, C_j'$ is a $\overline{H_j'}H_j'$-additive code and C_j'' is a $\overline{H_j''}H_j''$-additive code.

Every element of R_4 (resp. R_2) may be written as $\mathbf{u}(X)$ (resp. $\mathbf{v}(X)$) for some polynomial $\mathbf{u}(X) \in \mathbb{Z}_4[X]$ (resp. $\mathbf{v}(X) \in \mathbb{Z}_2[X]$). The decomposition of R_4 (resp. R_2) shows that $\mathbf{u}(X)$ (resp. $\mathbf{v}(X)$) may also be written as an $(s+2t)$-tuple

$$\begin{aligned}\mathbf{u}(X) &= (u_1(X), \dots, u_s(X), \\ &\qquad u_1'(X), u_1''(X), \dots, u_t'(X), u_t''(X)), \\ \mathbf{v}(X) &= (v_1(X), \dots, v_s(X), \\ &\qquad v_1'(X), v_1''(X), \dots, v_t'(X), v_t''(X)),\end{aligned}$$

where $u_i(X) \in G_i$, $v_i(X) \in \overline{G_i}$ $(1 \le i \le s)$, $u_j'(X) \in H_j'$, $v_j'(X) \in \overline{H_j'}$ and $u_j''(X) \in H_j''$, $v_j''(X) \in \overline{H_j''}$ $(1 \le j \le t)$. Of course, the u_i, u_j', u_j'' (resp. v_i, v_j', v_j'') may also be considered as polynomials in $\mathbb{Z}_4[X]$ (resp. $\mathbb{Z}_2[X]$).

For any element $\mathbf{r} \in R_4$ (resp. R_2), we have earlier defined its "conjugate" $\widetilde{\mathbf{r}}$, induced by the map $X \mapsto X^{-1}$ in R_4 (resp. R_2). Suppose that $\mathbf{r}$, expressed in terms of the decomposition (2) (resp. (3)), is given by

$$\mathbf{r} = (r_1, \dots, r_s, r_1', r_1'', \dots, r_t', r_t''),$$

where $r_i \in G_i$ (resp. $\overline{G_i}$) $(1 \le i \le s)$, $r_j' \in H_j'$ (resp. $\overline{H_j'}$) and $r_j'' \in H_j''$ (resp. $\overline{H_j''}$) $(1 \le j \le t)$. We now describe decomposition of $\widetilde{\mathbf{r}}$.

We note that, for a polynomial $f \in \mathbb{Z}_4[X]$, $f \mid X^m - 1$ (resp. $\overline{f} \in \mathbb{Z}_2[X]$, $\overline{f} \mid X^m - 1$), the quotients $\mathbb{Z}_4[X]/(f)$ (resp. $\mathbb{Z}_2[X]/(\overline{f})$) and

$\mathbb{Z}_4[X]/(f^*)$ (resp. $\mathbb{Z}_2[X]/(\overline{f^*})$) are isomorphic as rings. The isomorphism is given by

$$\frac{\mathbb{Z}_4[X]}{(f)} \to \frac{\mathbb{Z}_4[X]}{(f^*)},\ \ u(X)+(f) \mapsto u(X^{-1})+(f^*),$$

$$\frac{\mathbb{Z}_2[X]}{(\overline{f})} \to \frac{\mathbb{Z}_2[X]}{(\overline{f^*})},\ \ v(X)+(\overline{f}) \mapsto v(X^{-1})+(\overline{f^*}).$$

Here, the symbol X^{-1} makes sense. In fact, it can be considered as X^{m-1}, since $f, f^*, \overline{f}, \overline{f^*}$ divide X^m-1. Therefore, the element $\widetilde{\mathbf{r}}$ can now be expressed as

$$\widetilde{\mathbf{r}} = (\widetilde{r_1}, \ldots, \widetilde{r_s}, r_1'', r_1', \ldots, r_t'', r_t').$$

When f and f^* are associates, for vectors $\mathbf{u} = (u_0, \ldots, u_{l_2-1}, u_0', \ldots, u_{l_4-1}')$, $\mathbf{v} = (v_0, \ldots, v_{l_2-1}, v_0', \ldots, v_{l_4-1}') \in (\mathbb{Z}_2[X]/(\overline{f}))^{l_2} \times (\mathbb{Z}_4[X]/(f))^{l_4}$, we define the Hermitian inner product on $(\mathbb{Z}_2[X]/(\overline{f}))^{l_2} \times (\mathbb{Z}_4[X]/(f))^{l_4}$ to be

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=0}^{l_2-1} 2u_i\widetilde{v_i} + \sum_{j=0}^{l_4-1} u_j'\widetilde{v_j'} \pmod f.$$

Proposition IV.1. *Let C be a R_2R_4-additive code and $\boldsymbol{a}, \boldsymbol{b} \in C \subset R_2^{l_2} \times R_4^{l_4}$ and write $\boldsymbol{a} = (\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{l_2-1}, \boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{l_4-1})$ and $\boldsymbol{b} = (\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{l_2-1}, \boldsymbol{d}_0, \boldsymbol{d}_1, \ldots, \boldsymbol{d}_{l_4-1})$. Decomposing each $\boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}_j, \boldsymbol{d}_j$, we write*

$$\begin{aligned}
\boldsymbol{a}_i &= (a_{i1}, \ldots, a_{is}, a_{i1}', a_{i1}'', \ldots, a_{it}', a_{it}''),\\
\boldsymbol{c}_j &= (c_{j1}, \ldots, c_{js}, c_{j1}', c_{j1}'', \ldots, c_{jt}', c_{jt}''),\\
\boldsymbol{b}_i &= (b_{i1}, \ldots, b_{is}, b_{i1}', b_{i1}'', \ldots, b_{it}', b_{it}''),\\
\boldsymbol{d}_j &= (d_{j1}, \ldots, d_{js}, d_{j1}', d_{j1}'', \ldots, d_{jt}', d_{jt}''),
\end{aligned}$$

where $a_{ik}, b_{ik} \in \overline{G_k}, a_{ik'}', b_{ik'}' \in \overline{H_{k'}'}, a_{ik''}'', b_{ik''}'' \in \overline{H_{k''}''}, c_{jr}, d_{jr} \in G_r, c_{jr'}', d_{jr'}' \in \overline{G_{r'}'}, c_{jr''}'', d_{jr''}'' \in G_{r''}''$. Let $\widetilde{\boldsymbol{b}_i(X)} = \boldsymbol{b}_i(X^{-1}), \widetilde{\boldsymbol{d}_j(X)} = \boldsymbol{d}_j(X^{-1})$. Then $\boldsymbol{a} \circ \boldsymbol{b} = 0$ if and only if

$$\sum_{i=0}^{l_2-1} 2a_{ir}\widetilde{b_{ir}} + \sum_{j=0}^{l_4-1} c_{jr}\widetilde{d_{jr}} = 0 \quad (1 \le r \le s)$$

and

$$\sum_{i=0}^{l_2-1} 2a_{ik}'b_{ik}'' + \sum_{j=0}^{l_4-1} c_{jk}'d_{jk}'' = 0,$$

$$\sum_{i=0}^{l_2-1} 2a_{ik}''b_{ik}' + \sum_{j=0}^{l_4-1} c_{jk}''d_{jk}' = 0 \ (1 \le k \le t).$$

Proof:

$$\begin{aligned}
&\boldsymbol{a} \circ \boldsymbol{b}\\
&= \sum_{i=0}^{l_2-1} 2\mathbf{a}_i X^{m-1-deg(\mathbf{b}_i)}\mathbf{b}_i^* + \sum_{j=0}^{l_4-1} \mathbf{c}_j X^{m-1-deg(\mathbf{d}_j)}\mathbf{d}_j^*\\
&= X^{m-1}\left(\sum_{i=0}^{l_2-1} 2\mathbf{a}_i\widetilde{\mathbf{b}_i}\right) + X^{m-1}\left(\sum_{j=0}^{l_4-1} \mathbf{c}_j\widetilde{\mathbf{d}_j}\right)\\
&= X^{m-1}\left(\sum_{i=0}^{l_2-1} 2a_{i1}\widetilde{b_{i1}} + \sum_{j=0}^{l_4-1} c_{j1}\widetilde{d_{j1}}, \ldots,\right.\\
&\quad \sum_{i=0}^{l_2-1} 2a_{is}\widetilde{b_{is}} + \sum_{j=0}^{l_4-1} c_{js}\widetilde{d_{js}}, \sum_{i=0}^{l_2-1} 2a_{i1}'b_{i1}'' + \sum_{j=0}^{l_4-1} c_{j1}'d_{j1}'',\\
&\quad \sum_{i=0}^{l_2-1} 2a_{i1}''b_{i1}' + \sum_{j=0}^{l_4-1} c_{j1}''d_{j1}', \ldots,\\
&\quad \left.\sum_{i=0}^{l_2-1} 2a_{it}'b_{it}'' + \sum_{j=0}^{l_4-1} c_{jt}'d_{jt}'', \sum_{i=0}^{l_2-1} 2a_{it}''b_{it}' + \sum_{j=0}^{l_4-1} c_{jt}''d_{jt}'\right).
\end{aligned}$$

The result follows. ∎

Theorem IV.2. *A R_2R_4-additive code C with $C \subset R_2^{l_2} \times R_4^{l_4}$ the CRT decomposition of which is as in (4), it is self-dual with respect to the $\circ$-inner product, or equivalently, a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code of index (l_2, l_4) is self-dual with respect to the standard inner product, if and only if*

$$C = \left(\bigoplus_{i=1}^{s} C_i\right) \oplus \left(\bigoplus_{j=1}^{t} \left(C_j' \oplus (C_j')^{\perp}\right)\right),$$

where, for $1 \le i \le s$, C_i is a self-dual $\overline{G_i}G_i$-additive code (with respect to the Hermitian inner product), for $1 \le j \le t$, C_j' is a $\overline{H_j'}H_j'$-additive code and $(C_j')^{\perp}$ is its dual with respect to the standard inner product.

Proof: By Proposition IV.1, we have that C is self-dual with respect to the $\circ$-inner product, if and only if, C_i is self-dual with respect to the Hermitian inner product and C_j'' is dual of C_j' with respect to the standard inner product. ∎

Example IV.3. Let $m = 3, l_2 = l_4 = 2$, $X^3-1 = (X-1)(X^2+X+1)$ in $\mathbb{Z}_4[X]$, according to the CRT decomposition,

$$\begin{aligned}
R_2^2 \times R_4^2 &= \left(\frac{\mathbb{Z}_2[X]}{(X^3-1)}\right)^2 \times \left(\frac{\mathbb{Z}_4[X]}{(X^3-1)}\right)^2\\
&= \left(\overline{G_1}^2 \times G_1^2\right) \oplus \left(\overline{G_2}^2 \times G_2^2\right),
\end{aligned}$$

where $\overline{G_1} = \frac{\mathbb{Z}_2[X]}{(X-1)} \cong \mathbb{Z}_2, G_1 = \frac{\mathbb{Z}_4[X]}{(X-1)} \cong \mathbb{Z}_4, \overline{G_2} = \frac{\mathbb{Z}_2[X]}{(X^2+X+1)}, G_2 = \frac{\mathbb{Z}_4[X]}{(X^2+X+1)}$.

The generator vectors of $\phi(C)$ in Example III.4 are $\underline{a_1}(X) = (1, X, 2X^2, 0)$ and $\underline{a_2}(X) = (1, X + X^2, 1, X + 2X^2) \in R_2^2 \times R_4^2$. By (4), we have $\underline{a_1}(X) = (1, X, 2X^2, 0) = (1, 1, 2, 0, 1, X, 2 + 2X, 0)$, $\underline{a_2}(X) = (1, X + X^2, 1, X + 2X^2) = (1, 0, 1, 3, 1, 1, 1, 2+3X) \in (\overline{G_1}^2 \times G_1^2) \oplus (\overline{G_2}^2 \times G_2^2)$. By (5), let C_1 be $\mathbb{Z}_4[X]$-submodule of $\overline{G_1}^2 \times G_1^2$ with generator vectors $(1, 1, 2, 0)$ and $(1, 0, 1, 3)$, then C_1 is a self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive code with respect to the standard inner product or the Hermitian inner product. Let C_2 be $\mathbb{Z}_4[X]$-submodule of $\overline{G_2}^2 \times G_2^2$ with generator vectors $(1, X, 2 + 2X, 0)$ and $(1, 1, 1, 2 + 3X)$, then C_2 is a self-dual $\overline{G_2}G_2$-additive code with respect to the Hermitian inner product.

A similar characterization for ACD-ness is as follows.

Theorem IV.4. *A R_2R_4-additive code C with $C \subset R_2^{l_2} \times R_4^{l_4}$ the CRT decomposition of which is as in* (4)*. Then C is $\circ$-ACD if $C \cap C^{\perp_\circ} = \{0\}$, or equivalently, a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code of index (l_2, l_4) is standard ACD, if and only if C_i is Hermitian ACD, C_j' and C_j'' are standard ACD, that is, $C_i \cap C_i^{\perp_H} = \{0\}$, $C_j' \cap C_j'^{\perp} = \{0\}$, and $C_j'' \cap C_j''^{\perp} = \{0\}$, where $1 \le i \le s, 1 \le j \le t$.*

Proof: Through the previous description, the code $C^{\perp_\circ}$ is of the form

$$C^{\perp_\circ} = \left(\bigoplus_{i=1}^{s} C_i^{\perp_H}\right) \oplus \left(\bigoplus_{j=1}^{t} \left(C_j'^{\perp} \oplus C_j''^{\perp}\right)\right).$$

Then

$$C \cap C^{\perp_\circ} = \left(\bigoplus_{i=1}^{s} \left(C_i \cap C_i^{\perp_H}\right)\right) \oplus \left(\bigoplus_{j=1}^{t} \left((C_j' \cap C_j'^{\perp}) \oplus (C_j'' \cap C_j''^{\perp})\right)\right).$$

The left hand side of that equality reduces to the null space, iff each summand on the right hand side does. The result follows. ∎

V. 1-GENERATOR $\mathbb{Z}_2\mathbb{Z}_4$-ADDITIVE QUASI-CYCLIC CODES

Let m be a positive odd integer, let $ord_m(2)$ denote the order of 2 modulo m, and let l_2, l_4 be positive integers such that $gcd(l_2, ord_m(2)) = gcd(l_4, ord_m(2)) = 1$. Let $\underline{a}(X) \in R_2^{l_2} \times R_4^{l_4}$, $\underline{a}(X) = (a_0(X), \ldots, a_{l_2-1}(X), a_0'(X), \ldots, a_{l_4-1}'(X))$, then the module

$$\begin{aligned} M = R_4\underline{a}(X) = \{&\alpha(X)\underline{a}(X) = (\overline{\alpha}(X)a_0(X), \\ &\ldots, \overline{\alpha}(X)a_{l_2-1}(X), \alpha(X)a_0'(X), \\ &\ldots, \alpha(X)a_{l_4-1}'(X)) \mid \alpha(X) \in R_4\} \end{aligned}$$

is a 1-*generator* $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code with the generator $\underline{a}(X)$, where $\overline{\alpha}(X) = \alpha(X) \pmod 2$. Define

$$ann_{R_4}M = \{\alpha(X) \in R_4 | \alpha(X)\underline{a}(X) = 0\},$$

then $ann_{R_4}M$ is an ideal of R_4, and called the *annihilator* of M.

Let $I_2 = (a_0(X), a_1(X), \ldots, a_{l_2-1}(X))_{R_2}$ be the ideal generated by $a_0(X), a_1(X), \ldots, a_{l_2-1}(X)$ in R_2, and $I_4 = (a_0'(X), a_1'(X), \ldots, a_{l_4-1}'(X))_{R_4}$ be the ideal generated by $a_0'(X), a_1'(X), \ldots, a_{l_4-1}'(X)$ in R_4. Let

$$\begin{aligned} ann_{R_2}I_2 &= \{\alpha(X) \in R_2 \mid \alpha(X)a_i(X) = 0, \\ &\qquad 0 \le i \le l_2 - 1\}, \\ ann_{R_4}I_2 &= \{\alpha(X) \in R_4 \mid \overline{\alpha}(X)a_i(X) = 0, \\ &\qquad 0 \le i \le l_2 - 1\}, \\ ann_{R_4}I_4 &= \{\alpha(X) \in R_4 \mid \alpha(X)a_i'(X) = 0, \\ &\qquad 0 \le i \le l_4 - 1\}, \end{aligned}$$

then there exist monic polynomials $f_2(X), g_2(X), h_2(X), f_4(X), g_4(X), h_4(X) \in \mathbb{Z}_4[X]$ such that

$$\begin{aligned} f_2(X)g_2(X)h_2(X) &= x^m - 1, \\ f_4(X)g_4(X)h_4(X) &= x^m - 1, \end{aligned}$$

and

$$\begin{aligned} I_2 &= (\overline{h_2}(X))_{R_2}, \\ I_4 &= (g_4(X)h_4(X), 2f_4(X)h_4(X))_{R_4}, \\ ann_{R_2}I_2 &= (\overline{f_2}(X)\overline{g_2}(X))_{R_2}, \\ ann_{R_4}I_2 &= (f_2(X)g_2(X), 2f_2(X)h_2(X))_{R_4}. \end{aligned}$$

By Proposition 1 in [11], we have

$$ann_{R_4} I_4 = (f_4(X)g_4(X), 2f_4(X)h_4(X))_{R_4}.$$

Obviously, there are $f(X), g(X), h(X) \in R_4$, and $f(X)g(X)h(X) = X^m - 1$. such that

$$\begin{aligned} ann_{R_4} M &= ann_{R_4} I_2 \cap ann_{R_4} I_4 \\ &= (f(X)g(X), 2f(X)h(X)), \end{aligned}$$

Corollary V.1. *The type of the* 1*-generator* $\mathbb{Z}_2\mathbb{Z}_4$*-additive quasi-cyclic code* $M = R_4\underline{a}(X)$ *is* $4^{\deg(f(X))}2^{\deg(g(X))}$.

Proof: Since $\alpha(X) \mapsto \alpha(X)\underline{a}(X)$ (for all $\alpha(X) \in R_4$) is a surjective R_4-module homomorphism from R_4 onto $R_4\underline{a}(X)$ with kernel $annM$. According to the fundamental theorem of ring homomorphism, $R_4/annM \cong R_4\underline{a}(X)$. Since $|annM| = 4^{\deg h(X)}2^{\deg g(X)}$, $|M| = |R_4\underline{a}(X)| = |R_4/annM| = 4^{m-\deg h(X)-\deg g(X)}2^{\deg g(X)} = 4^{\deg f(X)}2^{\deg g(X)}$. ■

Lemma V.2. *Let* $\underline{a}(X) = (a_0(X), \ldots, a_{l_2-1}(X), a'_0(X), \ldots, a'_{l_4-1}(X)) \in R_2^{l_2} \times R_4^{l_4}$, *and* $M = R_4\underline{a}(X)$ *be a* 1*-generator* $\mathbb{Z}_2\mathbb{Z}_4$*-additive quasi-cyclic code. Let* I_2 *and* I_4 *be given above. Then for any* $\underline{b}(X) = (b_0(X), \ldots, b_{l_2-1}(X), b'_0(X), \ldots, b'_{l_4-1}(X)) \in R_2^{l_2} \times R_4^{l_4}, R_4\underline{a}(X) = R_4\underline{b}(X)$ *if and only if* $\underline{b}(X) = p(X)\underline{a}(X)$*, where* $p(X)$ *is a polynomial in* $\mathbb{Z}_4[X]$ *such that* $\gcd(\overline{p}(X), \overline{f_2}(X)\overline{g_2}(X)) = 1$ *and* $\gcd(\overline{p}(X), \overline{f_4}(X)\overline{g_4}(X)) = 1$.

Proof: We can prove the results by considering [11, Proposition 3] and [20, Lemma 2]. ■

In the following, we enumerate 1-generator $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes. Let $f(X), g(X), h(X) \in \mathbb{Z}_4[X]$ be given as above, and let us factorize $f(X), g(X)$ in $\mathbb{Z}_4[X]$. Assume that

$$\begin{aligned} f(X) &= f_1(X)f_2(X)\ldots f_s(X), \\ g(X) &= g_1(X)g_2(x)\ldots g_t(X), \end{aligned}$$

where $f_i(X)$'s and $g_j(X)$'s are pairwise coprime basic irreducible polynomials over $\mathbb{Z}_4$, and $\deg f_i(X) = e_i, \deg g_j(X) = d_j$, respectively. Then we can factorize $\overline{f}(X), \overline{g}(X)$ in $\mathbb{Z}_2[X]$.

$$\begin{aligned} \overline{f}(X) &= \overline{f_1}(X)\overline{f_2}(X)\ldots\overline{f_s}(X), \\ \overline{g}(X) &= \overline{g_1}(X)\overline{g_2}(X)\ldots\overline{g_t}(X), \end{aligned}$$

where $\overline{f_i}(X)$'s and $\overline{g_j}(X)$'s are distinct irreducible polynomials over $\mathbb{Z}_2$, and $\deg\overline{f_i}(X) = e_i, \deg\overline{g_j}(X) = d_j$, respectively.

Theorem V.3. *The number of all distinct* 1*-generator* $\mathbb{Z}_2\mathbb{Z}_4$*-additive quasi-cyclic codes with annihilator* $(f(X)g(X), 2f(X)h(X))$ *equals*

$$\prod_{i=1}^{s} \frac{4^{l_4e_i} - 2^{l_4e_i}}{4^{e_i} - 2^{e_i}} \cdot \frac{2^{l_2e_i} - 1}{2^{e_i} - 1} \prod_{j=1}^{t} \frac{2^{l_4d_j - 1}}{2^{d_j} - 1} \cdot \frac{2^{l_2d_j} - 1}{2^{d_j} - 1}.$$

Proof: When the annihilator $(f(X)g(X), 2f(X)h(X))$ is restricted to R_2, it's a 1-generator quasi-cyclic code with parity-check polynomial $\overline{f}(X)\overline{g}(X)$, by Theorem 12 in [11],

$$\begin{aligned} L_i &= \frac{2^{l_2e_i} - 1}{2^{e_i} - 1} (1 \le i \le s), \\ L'_j &= \frac{2^{l_2d_j} - 1}{2^{d_j} - 1} (1 \le j \le t). \end{aligned}$$

Hence, there are $\prod_{i=1}^{s} L_i \prod_{j=1}^{t} L'_j$ binary 1-generator quasi-cyclic codes with parity-check polynomial $\overline{f}(X)\overline{g}(X)$. When the annihilator $(f(X)g(X), 2f(X)h(X))$ is restricted to R_4, it's a quaternary 1-generator quasi-cyclic code with the annihilator $(f(X)g(X), 2f(X)h(X))$, by Theorem 2 in [20], there are $\prod_{i=1}^{s} \frac{4^{l_4e_i} - 2^{l_4e_i}}{4^{e_i} - 2^{e_i}} \prod_{j=1}^{t} \frac{2^{l_4d_j} - 1}{2^{d_j} - 1}$ quaternary 1-generator quasi-cyclic codes with the annihilator $(f(X)g(X), 2f(X)h(X))$. Because the direct sum of two quasi-cyclic codes is also a quasi-cyclic code, this completes the proof. ■

Example V.4. Let $m = 7, l_2 = 2, l_4 = 4$, then $X^7 - 1$ can be factored into a product of basic irreducible polynomials as

$$\begin{aligned} X^7 - 1 = (X - 1)(X^3 + 2X^2 + X - 1) \\ (X^3 - X^2 + 2X - 1) \end{aligned}$$

in $\mathbb{Z}_4[X]$. Let $f(X) = X - 1, g(X) = X^3 + 2X^2 + X - 1, h(X) = X^3 - X^2 + 2X - 1$. Now we consider 1-generator $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes with annihilator $(f(X)g(X), 2f(X)h(X))_{R_4}$, so in the language of Theorem V.3, we have

$$s = t = 1,\ e_1 = 1,\ d_1 = 3.$$

According to Theorem V.3, there are

$$\frac{4^4 - 2^4}{4 - 2} \times \frac{2^2 - 1}{2 - 1} \times \frac{2^{12} - 1}{2^3 - 1} \times \frac{2^6 - 1}{2^3 - 1} = 1895400$$

1-generator $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes with annihilator $(f(X)g(X), 2f(X)h(X))$.

VI. Examples of $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes

We define a Gray map $\varphi : \mathbb{Z}_2^r \times \mathbb{Z}_4^s \to \mathbb{Z}_2^{r+2s}$ such that $\varphi(\mathbf{u}) = \varphi(u|u') = (u|\varphi_4(u'))$, where φ_4 is the usual quaternary Gray map defined by $\varphi_4(0) = (0,0), \varphi_4(1) = (0,1), \varphi_4(2) = (1,1), \varphi_4(3) = (1,0)$. Next, we give some codes whose Gray images are optimal.

Lemma VI.1. [13] *The Gray image $\mathcal{C}' = \varphi(\mathcal{C})$ of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is linear if and only if*

$$\text{for all } \boldsymbol{u} = (u|u'), \boldsymbol{v} = (v|v') \in \mathcal{C} \Rightarrow (0, 2u' * v') \in \mathcal{C}.$$

Example VI.2. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code with the generator matrix

$$G = \left(\begin{array}{cccc|cccc} 10 & 01 & 11 & 10 & 01 & 11 \\ 11 & 10 & 01 & 11 & 10 & 01 \\ 11 & 10 & 00 & 02 & 00 & 20 \\ 00 & 11 & 10 & 20 & 02 & 00 \\ 10 & 00 & 11 & 00 & 20 & 02 \end{array}\right),$$

By Lemma VI.1, $\varphi(\mathcal{C})$ is a nonlinear binary code with parameters $(18, 2^7, 7)$. $\varphi(\mathcal{C})$ is best-known, by [28].

Example VI.3. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code with generator matrix

$$G = \left(\begin{array}{ccc|ccc} 10 & 01 & 11 & 2\cdots2 & 2\cdots2 & 0\cdots0 \\ 11 & 10 & 01 & \underbrace{0\cdots0}_{l} & \underbrace{2\cdots2}_{l} & \underbrace{2\cdots2}_{l} \end{array}\right).$$

Thus $l_2 = 2, l_4 = l$, and the generator vector of $\mathcal{C}$ is $\underline{a}(X) = (1 + X^2, X + X^2, \underbrace{2 + 2X, \cdots, 2 + 2X}_{l})$. By Lemma VI.1, $\varphi(\mathcal{C})$ is a linear binary code with parameters $[6l + 6, 2, 4l + 4]$, it can be checked that it meets the Griesmer bound [19, chap.17, section 5].

Example VI.4. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic code with generator matrix G is of the form

$$\left(\begin{array}{cccc|cccccccc} 11 & 10 & 00 & 00 & 3 & 1 & 3 & 3 & 1 & 1 & 1 \\ 00 & 11 & 10 & 00 & 1 & 3 & 1 & 3 & 3 & 1 & 1 \\ 00 & 00 & 11 & 10 & 1 & 1 & 3 & 1 & 3 & 3 & 1 \\ 10 & 00 & 00 & 11 & 1 & 1 & 1 & 3 & 1 & 3 & 3 \end{array}\right).$$

Thus $l_2 = 2, l_4 = 1$, and the generator vector of $\mathcal{C}$ is $a(X) = (1 + X, 1, 3 + X + 3X^2 + 3X^3 + X^4 + X^5 + X^6)$. By Lemma VI.1, $\varphi(\mathcal{C})$ is a linear binary code with parameters $[22, 5, 10]$, it can be checked that it is optimal with respect to the Griesmer bound [19, chap.17, section 5].

Example VI.5. In the following Tables 1, 2 and 3, we collect examples of $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes with linear Gray images that is optimal with respect to the Griesmer bound for lengths $n = 10, 14, 18$, where "Parameters" denotes "parameters of Gray images", "Griesmer Bound" denotes "upper bound with respect to the Griesmer bound" [19, chap.17, section 5].

Table 1: Optimal binary codes derived from $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes with length 10.

Generator	Parameters	Griesmer Bound
(11|3333)	$[10, 2, 6]$	6
(1 0|33 31)	$[10, 3, 5]$	5
(11|33 22)	$[10, 4, 4]$	4
(00|03 12) (11|33 11)	$[10, 5, 4]$	4
(0 0|01 32) (1 0|33 31)	$[10, 6, 3]$	3
(0 0|00 21) (1 0|33 33)	$[10, 7, 2]$	2
(00|00 11) (11|33 32)	$[10, 8, 2]$	2

Table 2: Optimal binary codes derived from $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes with length 14.

Generator	Parameters	Griesmer Bound
(1 0|222 200)	$[14, 2, 9]$	9
(11|332 310)	$[14, 3, 8]$	8
(11|22 20 00)	$[14, 3, 8]$	8
(0 0|001 112) (1 0|313 311)	$[14, 6, 5]$	5
(0 0|000 112) (1 0|210 111)	$[14, 7, 4]$	4

Table 3: Optimal binary codes derived from $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes with length 18.

Generator	Parameters	Griesmer Bound
(00 11 11|00 22 22)	$[18, 2, 12]$	12
(01 01 11|00 02 22)	$[18, 3, 10]$	10
(11|00 33 22 33)	$[18, 4, 8]$	8
(11|01 23 23 23)	$[18, 5, 8]$	8
(11|01 22 32 33)	$[18, 6, 8]$	8

VII. Conclusion

In this article, we have considered quasi-cyclic codes over a specific mixed alphabet. We have established a structure theory for these codes, by using the CRT, and derived from that theory criteria for self-duality and LCDness. A polynomial formulation has been given for the one-generator subclass, yielding exact enumeration results.

Many generalizations are possible, by considering as alphabet pair a ring and one of its extensions; for instance $\mathbb{Z}_4$ and $\mathbb{Z}_4[u]$ with $u^2 = 0$, [15], or other pairs of rings [3], [4], [5], [9]. In another direction, the concept of quasi-cyclic codes could be extended to so-called generalized quasi-cyclic codes or quasi-abelian codes, or quasi-polycyclic codes [2].

Define a $\mathbb{Z}_2\mathbb{Z}_4$-code to be nondegenerate if it is neither a binary code, nor a $\mathbb{Z}_4$-code. An interesting open problem is to know if nondegenerate $\mathbb{Z}_2\mathbb{Z}_4$-additive quasi-cyclic codes are asymptotically good.

Acknowledgment

The authors thank R. Wu for helpful discussions.

References

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

[2] A. Alahmadi, C. Gueneri, H. Shohaib, P. Solé. Long quasi-polycyclic t-CIS codes. Adv. Math. Commun., 2018, **12**(1): 189–198.

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

[4] I. Aydogdu, F. Gursoy. On $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-cyclic codes. Journal of Applied Mathematics and Computing. 2019, **60**: 327–341.

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

[6] N. Benbelkacem, J. Borges, S. T. Dougherty, C. Fernández-Córdoba. On $\mathbb{Z}_2\mathbb{Z}_4$-additive complementary dual codes and related LCD codes. Finite Fields Appl., 2020, **62**: 101622.

[7] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4-$linear codes: generator matrices and duality. Des. Codes. Cryptogr., 2007, **54**(2): 167–179.

[8] J. Borges, C. Fernández-Córdoba, R. Ten-Valls. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials, and dual codes. IEEE Trans. Information Theory, 2016, **62**(11): 6348–6354.

[9] J. Borges, C. Fernández-Córdoba, R. Ten-Valls. On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. Adv. Math. Commun., 2018, **12**(1): 169–179.

[10] C. Carlet, S. Guilley. Complementary Dual Codes for Counter-Measures to Side-Channel Attacks. Adv. Math. Commun., 2016, **10**(1): 131–150.

[11] J. Cui, P. Junying. Quaternary 1-generator quasi-cyclic codes. Des. Codes Cryptogr., 2011, **58**(1): 23–33.

[12] Y. Fan, H. Liu. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes are asymptotically good. 2019, arXiv: 1911.09350.

[13] C. Fernandez-Cordoba, J. Pujol, M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel. Des. Codes Cryptogr.. 2009, **1**(1): 43-59.

[14] C. Gueneri, B. Ozkaya, P. Solé. Quasi-cyclic complementary dual codes. Finite Fields Appl., 2016, **42**(11): 67–80.

[15] H. Islam, O. Prakash, P. Solé. $\mathbb{Z}_4\mathbb{Z}_4[u]$-additive cyclic and constacyclic codes. Adv. Math. Commun., (2020), doi: 10.3934/amc.2020094.

[16] S. Ling, P. Solé. On the algebraic structure of quasi-cyclic codes I: finite fields. IEEE Trans. Information Theory, 2001, **47**(7): 2751–2760.

[17] S. Ling, P. Solé. On the algebraic structure of quasi-cyclic codes II: chain rings. Designs, Codes, Cryptogr., 2003, **30**(1): 113–130.

[18] S. Ling, P. Solé. Good self-dual quasi-cyclic codes exist. IEEE Trans. Information Theory, 2003, **49**(4): 1052-1053.

[19] F. J. MacWilliams, N. J. A. Sloane. *The theory of Error Correcting Codes*. Amsterdam. The Netherlands: North-Holland. 1977.

[20] G. E. Séguin. A class of 1-generator quasi-cyclic codes. IEEE Trans. Information Theory, 2004, **50**(8): 1745–1753.

[21] M. Shi, A. Alahmadi, P. Solé. *Codes and Rings: Theory and Practice*. Academic Press. (2017).

[22] M. Shi, Y-J. Choie, A. Sharma, P. Solé. *Codes and Modular Forms: A dictionary*. World Scientific (2020), Singapore.

[23] M. Shi, L. Qian, Y. Liu, P. Solé. Good self-dual generalized quasi-cyclic codes exist. Information Processing Letters, 2017, **118**(2): 21-24.

[24] M. Shi, R. Wu, D. Krotov. On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality. IEEE Trans. Information Theory, 2018, **65**(6): 3842-3847.

[25] M. Shi, Y. Zhang. Quasi-twisted codes with constacyclic constituent codes. Finite Fields Appl., 2016, **39**(5): 159-178.

[26] Z. Wan. *Quaternary Codes*. Singapore: World Scientific, 1997.

[27] T. Yao, S. Zhu. $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic codes are asymptotically good. Crypto and Comm., 2020, **12**(2): 253–264.

[28] K. Zeger. Table of bounds on $A(n, d)$, `https://codes.se/bounds/unr.html`.

Minjia Shi received the Ph.D. degree from the Institute of Computer Network Systems, Hefei University of Technology, China, in 2010. From August 2012 to August 2013, he was a Visiting Researcher with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. From July 2016 to August 2016, he was a Visiting Researcher with Telecom Paris Tech, Paris, France. Later, he visited the Sobolev Institute of Mathematics in 2020. He has been a Professor of School of Mathematical Sciences at Anhui University since 2017. He is the author of over 100 journal articles and two books. His research interests include algebraic coding theory and cryptography.

Shitao Li received the B.S. degree in Mathematics from Anhui University, Hefei, China, in 2020; He is currenty a M.S. student at the School of Mathematical Sciences, Anhui University, Hefei, China. His research interests include cryptography and coding theory.

Patrick Solé received the Ingénieur and Docteur-Ingénieur degrees from the Ecole Nationale Supérieure des Télécommunications, Paris, France, in 1984 and 1987, respectively, and the Habilitation à Diriger Des Recherches from the Université de Nice-Sophia Antipolis, Sophia Antipolis, France, in 1993. He has held visiting positions at Syracuse University, Syracuse, NY, USA, from 1987 to 1989, Macquarie University, Sydney, NSW, Australia, from 1994 to 1996, and Lille University, Lille, France, from 1999 to 2000. Since 1989, he has been a Permanent Member of the CNRS and became a Directeur de Recherche, in 1996. He is currently a member of the CNRS lab I2M, Marseilles, France. He is the author of more than 200 journal articles and five books. His research interests include coding theory (codes over rings, quasi-cyclic codes), interconnection networks (graph spectra, expanders), vector quantization (lattices), and cryptography (Boolean functions, pseudo random sequences). He was a co-recipient of the Best Paper Award for Information Theory, in 1995, given by the Information Theory Chapter of the IEEE. He was an Associate Editor of the Transactions from 1996 to 1999.