IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 31, 2021, accepted April 23, 2021, date of publication April 28, 2021, date of current version May 7, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3076303

On $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-Additive Cyclic and Complementary Dual Codes

XIAOTONG HOU, XIANGRUI MENG, AND JIAN GAO
School of Mathematics and Statistics, Shandong University of Technology, Zibo 255000, China

Corresponding author: Jian Gao (dezhougaojian@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 12071264, Grant 11701336, Grant 11626144, and Grant 11671235.

ABSTRACT Aydogdu *et al.* studied the standard forms of generator and parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes, and presented generators of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes (Finite Fields Appl. 48: 241-260, 2017). In this paper, we investigate some other useful properties of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes, including asymptotically good $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes and $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive complementary dual codes. The present paper can be viewed as a necessary complementary part of Aydogdu's work.

INDEX TERMS Additive cyclic codes, asymptotically good codes, additive complementary dual codes, binary gray images.

I. INTRODUCTION

In recent years, coding scholars proposed a class of codes over additive structures, which are called additive codes [1]–[10]. Abualrub *et al.* studied the structural properties of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes [11], and Fan *et al.* proved that this class of codes are asymptotically good [12]. In fact, in 1966, Assmus *et al.* had studied the asymptotic properties of cyclic codes [13]. Afterwards, the asymptotic properties of quasi-cyclic (QC) codes, as a generalization of cyclic codes, had also received widespread attention of the asymptotic properties [14]–[18].

Aydogdu *et al.* studied $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes and $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes in [3] and [4], respectively. Yao *et al.* proved that $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes are asymptotically good [10]. Aydogdu *et al.* also introduced $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes [1], where $u^2 = 0$. In 2017, they studied some structural properties of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear codes and cyclic codes [2], where $u^3 = 0$. In 2020, Diao *et al.* studied some structural properties of $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes [5], where $v^2 = v$. In [6], we proved that $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes are asymptotically good.

Linear complementary dual (briefy LCD) codes are important linear codes due to their applications in implementations against side-channel attacks. Recently, Carlet *et al.* used LCD codes to improve the security of the information processed by sensitive devices, especially against so-called side-channel attacks and fault non-invasive attacks on embedded cryto-systems [19].

For a linear code $\mathscr{C}$, if $\mathscr{C} \cap \mathscr{C}^{\perp} = \{0\}$, then we called it an LCD code. LCD codes over finite fields were mainly studied in [**?**], [20]–[26], [28], [29]. Shi *et al.* studied LCD codes over Galois rings, and obtained some classes of asymptotically good LCD codes [30]. Dinh *et al.* studied the construction of LCD codes from $\mathbb{F}_q \times (\mathbb{F}_q + u\mathbb{F}_q) \times (\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q)$-additive cyclic codes [31], where $u^2 = 1$, $v^2 = 1$, $uv = vu$. Recently, Benbelkacem *et al.* studied some results on $\mathbb{Z}_2\mathbb{Z}_4$-additive complementary dual (brief ACD) codes [32]. It is the first paper to study ACD codes over additive structures. To be the necessary complementary part of the work [2], it is interesting to study the asymptotic properties of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes and the structural properties of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes.

The rest of this paper is organized as follows. In Section 2, we give some well known results on $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes and additive cyclic codes. In Section 3, we construct a class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes. By the probabilistic method, we prove that this class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes are asymptotically good. In Section 4, we give some sufficient conditions to show that $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes are ACD codes, and discuss the complementary duality of other subcodes. Particularly, we give a class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes, which binary Gray images are also LCD codes. In Section 5, we summarize the main results in this paper.

The associate editor coordinating the review of this manuscript and approving it for publication was Xueqin Jiang.

II. $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ADDITIVE AND ADDITIVE CYCLIC CODES

Let $\mathbb{Z}_2 = \{0, 1\}$ be the binary finite field, and $\mathbb{Z}_2[u^3] = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 = \{0, 1, u, 1+u, u^2, 1+u^2, u+u^2, 1+u+u^2\}$ be a finite chain ring, where $u^3 = 0$. For any element $d \in \mathbb{Z}_2[u^3]$, d can be written as $d = a + bu + cu^2$, where $a, b, c \in \mathbb{Z}_2$. Further, d is a unit of $\mathbb{Z}_2[u^3]$ if and only if $a \neq 0$. Let $\mathbb{Z}_2[u^3]^\times$ be the unit group of $\mathbb{Z}_2[u^3]$. Clearly, $\mathbb{Z}_2[u^3]^\times = \{1, 1+u, 1+u^2, 1+u+u^2\}$. The $I_{max} = \{0, u, u^2, u+u^2\}$ is the only maximum ideal of $\mathbb{Z}_2[u^3]$.

Let

$$\mathbb{Z}_2\mathbb{Z}_2[u^3] = \{(v|v') | v \in \mathbb{Z}_2 \text{ and } v' \in \mathbb{Z}_2[u^3]\}.$$

Define a map

$$\begin{aligned} \theta : \mathbb{Z}_2[u^3] &\to \mathbb{Z}_2 \\ d = a + bu + cu^2 &\mapsto \theta(d) = a. \end{aligned}$$

Clearly, θ is a well defined surjective ring homomorphism.

Let $\mathbb{Z}_2^\alpha$ be a α-tuple over $\mathbb{Z}_2$ and $\mathbb{Z}_2[u^3]^\beta$ be a β-tuple over $\mathbb{Z}_2[u^3]$, where α and β are positive integers. Let $v = (v|v') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$ be a vector, where $v = (v_0, v_1, \ldots, v_{\alpha-1})$ and $v' = (v'_0, v'_1, \ldots, v'_{\beta-1})$. For any $d = a + bu + cu^2 \in \mathbb{Z}_2[u^3]$, define a $\mathbb{Z}_2[u^3]$-scalar multiplication on $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$ as

$$d \cdot v = (\theta(d)v_0, \theta(d)v_1, \ldots, \theta(d)v_{\alpha-1} | dv'_0, dv'_1, \ldots, dv'_{\beta-1}).$$

The $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$ forms a $\mathbb{Z}_2[u^3]$-module under the above $\mathbb{Z}_2[u^3]$-scalar multiplication and the usual addition of vectors.

Definition 1: A non-empty subset $\mathscr{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code of length $n = \alpha + \beta$ if $\mathscr{C}$ is a $\mathbb{Z}_2[u^3]$-submodule of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$.

Definition 2: A $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code $\mathscr{C}$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic code of length $n = \alpha + \beta$ if for any codeword

$$v = (v|v') = (v_0, v_1, \ldots, v_{\alpha-1} | v'_0, v'_1, \ldots, v'_{\beta-1}) \in \mathscr{C},$$

the $(v_{\alpha-1}, v_0, \ldots, v_{\alpha-2} | v'_{\beta-1}, v'_0, \ldots, v'_{\beta-2}) \in \mathscr{C}$.

Let $R_{\alpha,\beta} = \mathbb{Z}_2[x]/\langle x^\alpha - 1\rangle \times \mathbb{Z}_2[u^3][x]/\langle x^\beta - 1\rangle$. Define a map

$$\begin{aligned} \Psi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta &\to R_{\alpha,\beta} \\ \varsigma = (c|c') &\mapsto \varsigma(x) = (c(x), c'(x)), \end{aligned}$$

where $(c|c') = (c_0, c_1, \ldots, c_{\alpha-1} | c'_0, c'_1, \ldots, c'_{\beta-1})$, $c(x) = c_0 + c_1 x + \cdots + c_{\alpha-1}x^{\alpha-1}$ and $c'(x) = c'_0 + c'_1 x + \cdots + c'_{\beta-1}x^{\beta-1}$.

For any $e(x) = e_0 + e_1 x + \cdots + e_t x^t \in \mathbb{Z}_2[u^3][x]$ and $\varsigma(x) = (c(x), c'(x)) \in R_{\alpha,\beta}$, define the $\mathbb{Z}_2[u^3][x]$-scalar multiplication

$$e(x) * \varsigma(x) = (\theta(e(x))c(x), e(x)c'(x)),$$

where $\theta(e(x)) = \theta(e_0) + \theta(e_1)x + \cdots + \theta(e_t)x^t$. Clearly, under this scalar multiplication and the usual addition of polynomials, $R_{\alpha,\beta}$ forms a $\mathbb{Z}_2[u^3][x]$-module. Therefore, we have that $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic code if and only if $\Psi(\mathscr{C})$ is a $\mathbb{Z}_2[u^3][x]$-submodule of $R_{\alpha,\beta}$. In this paper, we identify $\mathscr{C}$ with $\Psi(\mathscr{C})$.

Define a map

$$\begin{aligned} \pi : \mathbb{Z}_2[u^3] &\to \mathbb{Z}_2^3 \\ d = a + bu + cu^2 &\mapsto (a, b, c). \end{aligned}$$

Clearly, the ring $\mathbb{Z}_2[u^3]$ is isomorphic to $\mathbb{Z}_2^3$ as an additive group. If $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code, then it is additively isomorphic to a group of the form $\mathbb{Z}_2^{k_0} \times \mathbb{Z}_2^{3k_1} \times \mathbb{Z}_2^{2k_2} \times \mathbb{Z}_2^{k_3}$. Therefore, $\mathscr{C}$ is of type $(\alpha, \beta; k_0; k_1, k_2, k_3)$ and has $2^{k_0}2^{3k_1}2^{2k_2}2^{k_3}$ codewords. Let X (respectively Y) be the set of $\mathbb{Z}_2$ (respectively $\mathbb{Z}_2[u^3]$) coordinate positions. Then $|X| = \alpha$ and $|Y| = \beta$. We call $\mathscr{C}_X$ (respectively $\mathscr{C}_Y$) the punctured code of $\mathscr{C}$ by deleting the coordinates outside X (respectively Y). Note that $\mathscr{C}$ is said to be separable if $\mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$.

Generally although $\mathscr{C}$ is not a free $\mathbb{Z}_2[u^3]$-module, there exist $\{w_i\}_{i=1}^{k_0}$ and $\{v_j\}_{j=1}^{k_1+k_2+k_3}$ such that for every codeword of $\mathscr{C}$ it can be uniquely expressed in the form $\sum_{i=1}^{k_0} \lambda_i w_i + \sum_{j=1}^{k_1+k_2+k_3} \mu_j v_i$, where $\lambda_i \in \mathbb{Z}_2$, $\mu_j \in \mathbb{Z}_2[u^3]$. Furthermore, the vectors w_i and v_j form a generator matrix G of size $(k_0 + k_1 + k_2 + k_3) \times (\alpha + \beta)$ for the code $\mathscr{C}$ and $k_0 + k_1 + k_2 + k_3$ is called the rank of $\mathscr{C}$ denoted by $k_0 + k_1 + k_2 + k_3 = rank(\mathscr{C})$. Further, G can be written as $G = (G_X|G_Y)$, where G_X is a matrix of size $(k_0+k_1+k_2+k_3)\times\alpha$ over $\mathbb{Z}_2$ and G_Y is a matrix of size $(k_0+k_1+k_2+k_3)\times\beta$ over $\mathbb{Z}_2[u^3]$. Note that G_X is the generator matrix of $\mathscr{C}_X$ and G_Y is the generator matrix of $\mathscr{C}_Y$.

Define a Gray map $\phi : \mathbb{Z}_2[u^3] \to \mathbb{Z}_2^4$ as $\phi(0) = 0000$, $\phi(1) = 0101$, $\phi(u) = 0011$, $\phi(1+u) = 0110$, $\phi(u^2) = 1111$, $\phi(1+u^2) = 1010$, $\phi(u+u^2) = 1100$ and $\phi(1+u+u^2) = 1001$. Clearly, ϕ is a $\mathbb{Z}_2$-linear map. Extend this Gray map as follows

$$\begin{aligned} \Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta &\to \mathbb{Z}_2^n \\ (v|v') &\mapsto (v_0, v_1, \ldots, v_{\alpha-1} | \phi(v'_0), \phi(v'_1), \ldots, \phi(v'_{\beta-1})), \end{aligned}$$

where $v = (v_0, \ldots, v_{\alpha-1}) \in \mathbb{Z}_2^\alpha$ and $v' = (v'_0, \ldots, v'_{\beta-1}) \in \mathbb{Z}_2[u^3]^\beta$. Then the Gray image $\Phi(\mathscr{C}) = C$ is a binary linear code of length $n = \alpha + 4\beta$.

From the Ref. [33], for $x \in \mathbb{Z}_2[u^3]$, define the homogeneous weight of x

$$wt_{hom}(x) = \begin{cases} 0, & \text{if } x = 0, \\ 4, & \text{if } x \in \langle u^2\rangle \backslash \{0\}, \\ 2, & \text{if } x \in \mathbb{Z}_2[u^3] \backslash \langle u^2\rangle. \end{cases}$$

Note that, for $x \in \mathbb{Z}_2[u^3]$, $wt_{hom}(x) = wt_H(\phi(x))$. For $w' = (w'_0, w'_1, \ldots, w'_{\beta-1}) \in \mathbb{Z}_2[u^3]^\beta$, define the homogeneous weight the of w' as $wt_{hom}(w') = \sum_{i=0}^{\beta-1} wt_{hom}(w'_i)$. For any two vectors $w', v' \in \mathbb{Z}_2[u^3]^\beta$, define the homogeneous distance $d_{hom}(w', v')$ as $d_{hom}(w', v') = wt_{hom}(w' - v')$. Clearly, we have $wt_{hom}(w') = wt_H(\Phi(w')) = \sum_{i=0}^{\beta-1} wt_H(\phi(w'_i))$ and $d_{hom}(w', v') = d_H(\Phi(w'), \Phi(v'))$.

For a vector $w = (w|w') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$, define the weight of w as $wt(w) = wt_H(w) + wt_{hom}(w') = wt_H(w) + wt_H(\Phi(w')) = wt_H(\Phi(w))$ and for two vectors $w, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$, define the distance of w and v as

$d(w, v) = wt(w - v)$. Denote $d(\mathscr{C})$ to be the minimum distance of $\mathscr{C}$. Clearly, the Gray map Φ is an isometry from $(\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta, d)$ to $(\mathbb{Z}_2^{\alpha+4\beta}, d_H)$.

Let $w = (w|w') = (w_0, w_1, \ldots, w_{\alpha-1}|w'_0, w'_1, \ldots, w'_{\beta-1})$ and $v = (v|v') = (v_0, v_1, \ldots, v_{\alpha-1}|v'_0, v'_1, \ldots, v'_{\beta-1})$, where $w, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta$. Define an inner product of w and v as $[w, v] = u^2[w, v]_2 + [w', v']_u \in \mathbb{Z}_2[u^3]$, where $[w, v]_2 = \sum_{i=0}^{\alpha-1} w_i v_i$ is the inner product of w and v over $\mathbb{Z}_2$, $[w', v']_u = \sum_{j=0}^{\beta-1} w'_j v'_j$ is the inner product of w' and v' over $\mathbb{Z}_2[u^3]$. With respect to the above inner product, we can define the dual code of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code $\mathscr{C}$ as

$$\mathscr{C}^\perp = \{v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u^3]^\beta \mid [w, v] = 0 \textit{ for all } w \in \mathscr{C}\}.$$

It is easy to prove that $\mathscr{C}^\perp$ is also a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code. Particularly, if $\mathscr{C}$ is a separable code, then $\mathscr{C}^\perp = (\mathscr{C}_X)^\perp \times (\mathscr{C}_Y)^\perp$. Further, $\mathscr{C}$ is self-orthogonal if $\mathscr{C} \subset \mathscr{C}^\perp$ and self-dual if $\mathscr{C} = \mathscr{C}^\perp$.

Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code with the generator matrix $G = (G_X|G_Y)$. Define the product

$$G \cdot G^\top = u^2 G_X G_X^\top + G_Y G_Y^\top \in M(\mathbb{Z}_2[u^3]), \tag{1}$$

where all elements in G_X are taken from $\mathbb{Z}_2$, all elements in G_Y are taken from $\mathbb{Z}_2[u^3]$, $M(\mathbb{Z}_2[u^3])$ denotes the matrix ring over $\mathbb{Z}_2[u^3]$. Note that we can use usual matrix multiplication in matrices $G_X G_X^\top$ and $G_Y G_Y^\top$, but we can not use usual matrix multiplication in matrix $G \cdot G^\top$.

III. $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ADDITIVE CYCLIC CODES ARE ASYMPTOTICALLY GOOD

In this section, we mainly study asymptotic properties of the relative minimum distance and the rate of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes. The relative minimum distance and the rate of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic code $\mathscr{C}$ are denoted by $\Delta(\mathscr{C}) = \frac{d(\mathscr{C})}{n}$ and $R(\mathscr{C}) = \frac{rank(\mathscr{C})}{n}$ respectively, where $d(\mathscr{C})$ is the minimum distance of $\mathscr{C}$ and $rank(\mathscr{C})$ is the rank of $\mathscr{C}$.

Definition 3: A class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes is called asymptotically good if there exist a sequence of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_i, \ldots$ with length $m_1, m_2, \ldots, m_i, \ldots$, when $m_i \to \infty$, both the relative minimum homogeneous distance and the rate of $\mathscr{C}_i$ are positively bounded from below.

A. A CLASS OF $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ADDITIVE CYCLIC CODES

Let $R_{km} = \mathbb{Z}_2[x]/\langle x^{km} - 1\rangle$, $R_{lm} = \mathbb{Z}_2[x]/\langle x^{lm} - 1\rangle$, $R'_{lm} = \mathbb{Z}_2[u^3][x]/\langle x^{lm} - 1\rangle$, where m, k, l are positive integers such that $gcd(m, 2) = 1$ and $2, k, l$ are pairwise prime.

Clearly, $u^2\mathbb{Z}_2[u^3] = u^2\mathbb{Z}_2 \subset \mathbb{Z}_2[u^3]$. Let

$$u^2 R'_{lm} = \left\{ b'(x) = \sum_{i=0}^{lm-1} b'_i x^i \in R'_{lm} | b'_i = u^2 b_i,\ b_i \in \mathbb{Z}_2 \right\}.$$

It is well known that $u^2 R'_{lm} \subset R'_{lm}$ is a $\mathbb{Z}_2[u^3][x]$-submodule of R'_{lm}.

For any $f(x) \in \mathbb{Z}_2[x]$ and $(a(x), b(x)) \in R_{km} \times R_{lm}$, define the following scalar multiplication

$$f(x)(a(x), b(x)) = \left(f(x)a(x) \ (mod\ x^{km} - 1), f(x)b(x) \ (mod\ x^{lm} - 1)\right).$$

For the simplify, we write the above equation as $(f(x)a(x), f(x)b(x))$. Clearly, in terms of the pairwise coordinate addition and the scalar multiplication by the elements of $R_{klm} = \mathbb{Z}_2[x]/\langle x^{klm} - 1\rangle$, the $R_{km} \times R_{lm}$ forms an R_{klm}-module.

Define a map

$$\begin{aligned} \sigma :\ R_{lm} &\to u^2 R'_{lm} \\ b(x) = \sum_{i=0}^{lm-1} b_i x^i &\mapsto b'(x) = u^2 b(x) = \sum_{i=0}^{lm-1} u^2 b_i x^i, \end{aligned}$$

where $b_i \in \mathbb{Z}_2$. Clearly, σ is a $\mathbb{Z}_2[x]$-module isomorphism. Thus, $R_{km} \times u^2 R'_{lm}$ also forms an R_{klm}-module.

For any $(a(x), b(x)) \in R_{km} \times R_{lm}$ and $f(x) \in R_{klm}$, let

$$\mathscr{C}_{a,b} = \{(f(x)a(x), u^2 f(x)b(x)) \in R_{km} \times u^2 R'_{lm}\}.$$

Then $\mathscr{C}_{a,b}$ is an R_{klm}-submodule of $R_{km} \times u^2 R'_{lm}$ generated by $(a(x), u^2 b(x))$. By the $\mathbb{Z}_2[x]$-module isomorphism σ, $\mathscr{C}_{a,b}$ can be viewed as a $\mathbb{Z}_2$-linear space.

Proposition 1: Let $\mathscr{C}_{a,b} = \{(f(x)a(x), u^2 f(x)b(x)) \in R_{km} \times u^2 R'_{lm} | f(x) \in R_{klm}\}$, where $a(x) \in R_{km}$, $b(x) \in R_{lm}$ are monic polynomials. Let $g_{a,b}(x) = gcd\left(a(x), \frac{x^{km}-1}{x^m-1}\right) \cdot gcd\left(b(x), \frac{x^{lm}-1}{x^m-1}\right) \cdot gcd(a(x), b(x), x^m - 1) \cdot \frac{(x^{klm}-1)\cdot(x^m-1)}{(x^{km}-1)\cdot(x^{lm}-1)}$ and $h_{a,b}(x) = \frac{x^{klm}-1}{g_{a,b}(x)}$. Then there is an R_{klm}-module isomorphism:

$$\begin{aligned} \langle g_{a,b}(x)\rangle_{R_{klm}} &\cong \mathscr{C}_{a,b} \\ c(x) &\mapsto (c(x)a(x), u^2 c(x)b(x)), \end{aligned}$$

and $rank(\mathscr{C}_{a,b}) = deg(h_{a,b}(x))$.

Proof: Define a map

$$\begin{aligned} \chi_{a,b} :\ R_{klm} &\to R_{km} \times u^2 R'_{lm} \\ f(x) &\mapsto (f(x)a(x), u^2 f(x)b(x)). \end{aligned}$$

Clearly, $\chi_{a,b}$ is a well defined R_{klm}-module homomorphism. For $f(x) \in R_{klm}, f(x) \in ker(\chi_{a,b})$ if and only if

$$\begin{cases} f(x)a(x) \equiv 0\ (mod\ x^{km} - 1) \\ f(x)b(x) \equiv 0\ (mod\ x^{lm} - 1) \end{cases}$$

if and only if

$$\begin{cases} f(x)a(x) \equiv 0\ \left(mod\ \frac{x^{km}-1}{x^m-1}\right) \\ f(x)b(x) \equiv 0\ \left(mod\ \frac{x^{lm}-1}{x^m-1}\right) \\ f(x)a(x) \equiv 0\ (mod\ x^m - 1) \\ f(x)b(x) \equiv 0\ (mod\ x^m - 1) \end{cases}$$

if and only if

$$\begin{cases} f(x) \equiv 0 \left(mod \ \frac{\frac{x^{km}-1}{x^m-1}}{gcd\left(a(x), \frac{x^{km}-1}{x^m-1}\right)} \right) \\ f(x) \equiv 0 \left(mod \ \frac{\frac{x^{lm}-1}{x^m-1}}{gcd\left(b(x), \frac{x^{lm}-1}{x^m-1}\right)} \right) \\ f(x) \equiv 0 \left(mod \ \frac{x^m-1}{gcd(a(x),b(x),x^m-1)} \right) \end{cases}$$

if and only if

$$f(x) \equiv 0 \ (mod \ Q_1(x) \cdot Q_2(x) \cdot Q_3(x)),$$

where $Q_1(x) = \frac{\frac{x^{km}-1}{x^m-1}}{gcd\left(a(x), \frac{x^{km}-1}{x^m-1}\right)}$, $Q_2(x) = \frac{\frac{x^{lm}-1}{x^m-1}}{gcd\left(b(x), \frac{x^{lm}-1}{x^m-1}\right)}$ and $Q_3(x) = \frac{x^m-1}{gcd(a(x),b(x),x^m-1)}$.

Thus, $ker(\chi_{a,b}) = \langle h_{a,b}(x)\rangle_{R_{klm}}$. Since $gcd(m, 2) = 1$ and $2, k, l$ are pairwise prime, then klm is odd. Thus, R_{klm} is semisimple and

$$R_{klm} = \langle g_{a,b}(x)\rangle_{R_{klm}} \oplus \langle h_{a,b}(x)\rangle_{R_{klm}}.$$

Clearly, the above R_{klm}-module homomorphism $\chi_{a,b}$ induces an R_{klm}-isomorphism:

$$\begin{aligned} \langle g_{a,b}(x)\rangle_{R_{klm}} &\to \mathscr{C}_{a,b} \\ c(x) &\mapsto (c(x)a(x), u^2c(x)b(x)). \end{aligned}$$

In particular,

$$\begin{aligned} rank(\mathscr{C}_{a,b}) &= rank(\langle g_{a,b}(x)\rangle_{R_{klm}}) \\ &= klm - deg(g_{a,b}(x)) = deg(h_{a,b}(x)). \end{aligned}$$

By Proposition 1, we can give a generator matrix of $\mathscr{C}_{a,b}$. Let $a(x) = \sum_{i=0}^{km-1} a_i x^i \in R_{km}$ and $b(x) = \sum_{i=0}^{lm-1} b_i x^i \in R_{lm}$. Let

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{km-1} \\ a_{km-1} & a_0 & \cdots & a_{km-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

and

$$B = \begin{pmatrix} b_0 & b_1 & \cdots & b_{lm-1} \\ b_{lm-1} & b_0 & \cdots & b_{lm-2} \\ \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \cdots & b_0 \end{pmatrix}.$$

Define the matrix G as

$$\left(\begin{array}{c|c} A & u^2B \\ A & u^2B \\ \vdots & \vdots \\ A & u^2B \end{array}\right)_{klm\times(k+l)m}.$$

If the rank of $\mathscr{C}_{a,b}$ is r, then the first r rows of G form a generator matrix of $\mathscr{C}_{a,b}$.

Example 1: Let $m = 1$, $k = 5$, $l = 7$. Let $\mathscr{C}_{a,b}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic code with generator $(a(x), u^2b(x)) \in R_5 \times u^2R_7'$, where $a(x) = x^3 + x \in R_5$, $b(x) = x^4 + x^3 + x^2 + 1 \in R_7$.

Let $g_{a,b}(x) = gcd\left(a(x), \frac{x^5-1}{x-1}\right) \cdot gcd\left(b(x), \frac{x^7-1}{x-1}\right) \cdot gcd(a(x), b(x), x-1) \cdot \frac{(x^{35}-1)\cdot(x-1)}{(x^5-1)\cdot(x^7-1)}$. Then $g_{a,b}(x) = x^{28} + x^{25} + x^{24} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{15} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^2 + x + 1$. Since $h(x) = \frac{x^{35}-1}{g_{a,b}(x)} = x^7 + x^4 + x^3 + x + 1$, then the rank of $\mathscr{C}_{a,b}$ is 7. Clearly, the following matrix

$$\left(\begin{array}{ccccc|ccc} 0&1&0&1&0 & u^2 & 0 & u^2 & u^2 & u^2 & 0 & 0 \\ 0&0&1&0&1 & 0 & u^2 & 0 & u^2 & u^2 & u^2 & 0 \\ 1&0&0&1&0 & 0 & 0 & u^2 & 0 & u^2 & u^2 & u^2 \\ 0&1&0&0&1 & u^2 & 0 & 0 & u^2 & 0 & u^2 & u^2 \\ 1&0&1&0&0 & u^2 & u^2 & 0 & 0 & u^2 & 0 & u^2 \\ 0&1&0&1&0 & u^2 & u^2 & u^2 & 0 & 0 & u^2 & 0 \\ 0&0&1&0&1 & 0 & u^2 & u^2 & u^2 & 0 & 0 & u^2 \end{array}\right)$$

forms a generator matrix of $\mathscr{C}_{a,b}$.

B. ASYMPTOTICALLY GOOD $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ADDITIVE CYCLIC CODES

By the Chinese remainder theorem,

$$\begin{aligned} R_m &= \mathbb{Z}_2[x]/\langle x^m - 1\rangle \\ &= \mathbb{Z}_2[x]/\langle x - 1\rangle \oplus \mathbb{Z}_2[x]/\langle x^{m-1} + \cdots + x + 1\rangle. \end{aligned}$$

Clearly, the rank of cyclic code generated by $x^{m-1} + \cdots + x + 1$ is 1. Thus, we only consider the cyclic code generated by $x - 1$.

Let

$$\begin{aligned} J_m &= \langle x-1\rangle_{R_m}, \\ J_{km} &= \left\langle \frac{x^{km}-1}{x^m-1}(x-1)\right\rangle_{R_{km}}, \\ J_{lm} &= \left\langle \frac{x^{lm}-1}{x^m-1}(x-1)\right\rangle_{R_{lm}}, \\ J_{klm} &= \left\langle \frac{x^{klm}-1}{x^m-1}(x-1)\right\rangle_{R_{klm}}, \\ J'_{lm} &= \left\langle \frac{x^{lm}-1}{x^m-1}(x-1)\right\rangle_{R'_{lm}}, \\ u^2J'_{lm} &= \left\langle u^2\left(\frac{x^{km}-1}{x^m-1}(x-1)\right)\right\rangle_{u^2R'_{lm}}. \end{aligned}$$

If $(a(x), b(x)) \in J_{km} \times J_{lm}$, it is easy to see that $\langle g_{a,b}(x)\rangle_{R_{klm}} \subseteq J_{klm}$ by Proposition 1, then the $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic code $\mathscr{C}_{a,b}$ can be reformulated as $\mathscr{C}_{a,b} = \{(f(x)a(x), u^2f(x)b(x)) \in R_{km} \times u^2R_{lm}\}$, where $f(x) \in J_{klm}$.

For any $f(x) \in J_m$, define

$$\mathscr{C}_{\bar{a},\bar{b}} = \{(f(x)\bar{a}(x), u^2f(x)\bar{b}(x)) \in R_m \times u^2R'_m\}, \qquad (2)$$

where $(\bar{a}(x), \bar{b}(x)) \in J_m \times J_m$ and $R'_m = \mathbb{Z}_2[u^3]/\langle x^m - 1\rangle$.

Let $u^2J'_m = \langle u^2(x-1)\rangle_{u^2R'_m}$. Define a map

$$\eta : J_m \times u^2J'_m \to J_{km} \times u^2J'_{lm}$$

$$(\bar{a}(x), u^2\bar{b}(x)) \mapsto \left(a(x), u^2b(x)\right),$$

where $a(x) = \bar{a}(x)\frac{x^{km}-1}{x^m-1}$ and $b(x) = \bar{b}(x)\frac{x^{lm}-1}{x^m-1}$. It is obvious that η is an R_{klm}-module isomorphism and $\mathscr{C}_{a,b} = \eta(\mathscr{C}_{\bar{a},\bar{b}})$.

The sets $J_{km} \times u^2J'_{lm}$ and $J_m \times u^2J'_m$ are probability space of $R_{km} \times u^2R'_{lm}$ and $R_m \times u^2R'_m$ respectively, whose samples are afforded with equal probability. Further, $\mathscr{C}_{a,b}$ is a random code over probability space $J_{km} \times u^2J'_{lm}$. Therefore $R(\mathscr{C}_{a,b})$ and $\Delta(\mathscr{C}_{a,b})$ are random variables over this probability space. Thus, by the definition of asymptotically good, the problem has been transformed into studying the probabilities of $Pr(\Delta(\mathscr{C}_{a,b}) > \delta)$ and $Pr(rank(\mathscr{C}_{a,b}) = m-1)$, where δ is a real number such that $0 < \delta < 1$.

By the map η, we have that

$$\begin{aligned} wt(a(x), u^2b(x)) &= wt_H(a(x)) + wt_{hom}(u^2b(x)) \\ &= kwt_H(\bar{a}(x)) + lwt_{hom}(u^2\bar{b}(x)) \\ &\geq wt(\bar{a}(x), u^2\bar{b}(x)). \end{aligned}$$

It means that $wt(\mathscr{C}_{a,b}) \geq wt(\mathscr{C}_{\bar{a},\bar{b}})$. Since $\Delta(\mathscr{C}_{a,b}) = \frac{d(\mathscr{C}_{a,b})}{(k+l)m} = \frac{wt(\mathscr{C}_{a,b})}{(k+l)m}$ and $\Delta(\mathscr{C}_{\bar{a},\bar{b}}) = \frac{d(\mathscr{C}_{\bar{a},\bar{b}})}{2m} = \frac{wt(\mathscr{C}_{\bar{a},\bar{b}})}{2m}$, then we have $\Delta(\mathscr{C}_{a,b}) \geq \frac{2}{k+l}\Delta(\mathscr{C}_{\bar{a},\bar{b}})$. Further, since $|\Delta(\mathscr{C}_{a,b}) > \delta| \geq |\Delta(\mathscr{C}_{\bar{a},\bar{b}}) > \frac{k+l}{2}\delta|$ and $|J_{km} \times J_{lm}| = |J_m \times J_m|$, then

$$\begin{aligned} Pr(\Delta(\mathscr{C}_{a,b}) > \delta) &= \frac{|\Delta(\mathscr{C}_{a,b}) > \delta|}{|J_{km} \times J_{lm}|} \geq \frac{|\Delta(\mathscr{C}_{\bar{a},\bar{b}}) > \frac{k+l}{2}\delta|}{|J_m \times J_m|} \\ &= Pr\left(\Delta(\mathscr{C}_{\bar{a},\bar{b}}) > \frac{k+l}{2}\delta\right). \end{aligned}$$

Thus, we can transform the problem again into studying the probabilities of $Pr\left(\Delta(\mathscr{C}_{\bar{a},\bar{b}}) > \frac{k+l}{2}\delta\right)$ and $Pr(rank(\mathscr{C}_{a,b}) = m-1)$.

Definition 4: The function $h_2(x)$ is called a 2-ary entropy if for $0 < x < 1$, $h_2(x) = -xlog_2x - (1-x)log_2(1-x)$.

Note that for a real number $0 < \delta < 1$, we have that $h_2(\delta) < \frac{1}{2}$.

Definition 5: The variable Y_f over the probability space $J_m \times u^2J'_m$ is called *Bernoulli variable* if for $f(x) \in J_m$, $(\bar{a}(x), u^2\bar{b}(x)) \in J_m \times u^2 J'_m$ satisfies

$$Y_f = \begin{cases} 1, & 1 \leq wt(f(x)\bar{a}(x), u^2f(x)\bar{b}(x)) \leq 2m\delta, \\ 0, & otherwise. \end{cases}$$

Moreover, the set $\{f(x)\bar{a}(x) \in R_m | \bar{a}(x) \in J_m\}$ is an ideal of R_m generated by $f(x)$ and $\{u^2f(x)\bar{b}(x) \in u^2\ R'_m | \bar{b}(x) \in J_m\}$ is an ideal of $u^2R'_m$ generated by $u^2f(x)$. Let $I_f = \langle f(x)\rangle_{R_m} \subseteq J_m$ and $r_f = rank(I_f)$. Let $I'_f = \langle u^2f(x)\rangle_{u^2R'_m} \subseteq u^2J'_m$. Since I'_f is also a $\mathbb{Z}_2$-linear space, then $rank(I'_f) = r_f$.

Lemma 1 [34]: Let $I_f \times I_f \subseteq R_m \times R_m$ and $(I_f \times I_f)^{\leq 2m\delta} = \{(f_1(x), f_2(x)) \in I_f \times I_f |\ wt(f_1(x), f_2(x)) \leq 2m\delta\}$. Then $\left|(I_f \times I_f)^{\leq 2m\delta}\right| \leq 4^{r_f h_2(\delta)}$.

Lemma 2: $E(Y_f) \leq 4^{-r_f + r_f h_2(\delta)}$.

Proof: Let $(I_f \times I'_f)^{\leq 2m\delta} = \{(f_1(x), u^2f_2(x)) \in I_f \times I'_f | wt(f_1(x), u^2f_2(x)) \leq 2m\delta\}$. By Definition 5, the expectation $E(Y_f) = Pr(Y_f = 1) = \frac{|(I_f \times I'_f)^{\leq 2m\delta}| - 1}{I_f \times I'_f}$. For $f_1(x), f_2(x) \in R_m$, by the definition Φ, we have

$$\begin{aligned} wt(f_1(x), u^2f_2(x)) &= wt_H(f_1(x)) + wt_{hom}(u^2f_2(x)) \\ &= wt_H(f_1(x)) + wt_H(\Phi(u^2f_2(x))) \\ &= wt_H(f_1(x)) + 4wt_H(f_2(x)) \\ &\geq wt_H(f_1(x), f_2(x)). \end{aligned}$$

Thus,

$$\left|(I_f \times I'_f)^{\leq 2m\delta}\right| \leq \left|(I_f \times I_f)^{\leq 2m\delta}\right|.$$

Moreover, we know that $rank(I'_f) = rank(I_f) = r_f$. Therefore, by Lemma 1, we have

$$\begin{aligned} E(Y_f) &= \frac{|(I_f \times I'_f)^{\leq 2m\delta}| - 1}{|I_f \times I'_f|} \leq \frac{|(I_f \times I_f)^{\leq 2m\delta}|}{|I_f \times I_f|} \\ &\leq \frac{4^{r_f h_p(\delta)}}{4^{d_f}} = 4^{-r_f + r_f h_p(\delta)}. \end{aligned}$$

Lemma 3 [12]: Let $\frac{x^m-1}{x-1} = p_1(x)p_2(x)\cdots p_s(x)$, where $p_1(x), \ldots, p_s(x)$ are irreducible polynomials in $\mathbb{Z}_2[x]$ and $p_k(x)$ be the lowest degree polynomial in $p_i(x)$, $i = 1, 2, \ldots, s$. Let $k_m = deg(p_k(x))$ and r be an integer with $k_m \leq r \leq m-1$. For any non-zero ideal I of R_m, if $I \subseteq J_m$, then $rank(I) \geq k_m$ and the number of non-zero ideals contained in J_m of rank r is at most $m^{\frac{r}{k_m}}$.

Lemma 4: $Pr(\Delta(\mathscr{C}_{\bar{a},\bar{b}}) \leq \delta) \leq \sum_{j=k_m}^{m-1} 4^{-j\left(\frac{1}{2} - h_2(\delta) - \frac{log_2 m}{2k_m}\right)}$, where $0 < \delta < 1$ is a real number such that $h_p(\delta) < \frac{1}{2}$ and k_m is defined as in Lemma 3.

Proof: Let $Y = \sum_{f(x) \in J_m} Y_f$ denote the number of $f(x) \in J_m$ such that the non-zero codeword $(f(x)\bar{a}(x), u^2f(x)\bar{b}(x))$ of $\mathscr{C}_{\bar{a},\bar{b}}$ with weight at most $2m\delta$. Since $\Delta(\mathscr{C}_{\bar{a},\bar{b}}) = \frac{d(\mathscr{C}_{\bar{a},\bar{b}})}{2m} = \frac{wt(\mathscr{C}_{\bar{a},\bar{b}})}{2m}$, then

$$\begin{aligned} Pr(\Delta(\mathscr{C}_{\bar{a},\bar{b}}) \leq \delta) &= Pr(wt(\mathscr{C}_{\bar{a},\bar{b}}) \leq 2m\delta) = Pr(Y > 0) \\ &\leq E(Y) = \sum_{f(x) \in J_m} E(Y_f). \end{aligned}$$

For any ideal $I \leq J_m$, let $I^* = \{f(x) \in I | I_f = I\}$, where $I_f = \langle f(x)\rangle_{R_m} \subseteq J_m$ and $rank(I_f) = r_f$. Then $I^* = \{f(x) \in I | r_f = rank(I)\}$. Clearly, $J_m = \bigcup_{I \leq J_m} I^*$, where I runs through the ideals contained in J_m. By Lemma 3, we have $k_m \leq rank(I) \leq m-1$ and the number of $I \leq J_m$ with $rank(I) = j$ is less than $m^{\frac{j}{k_m}}$. Therefore,

$$E(Y) = \sum_{f(x) \in J_m} E(Y_f) = \sum_{I \leq J_m} \sum_{f(x) \in I^*} E(Y_f)$$

$$= \sum_{j=k_m}^{m-1} \sum_{\substack{I \leq J_m, \\ rank(I)=j}} \sum_{f(x)\in I^*} E(Y_f)$$

$$\leq \sum_{j=k_m}^{m-1} m^{\frac{j}{k_m}} \sum_{f(x)\in I^*} E(Y_f).$$

By Lemma 2 and the fact that $|I^*| \leq |I| = 2^j$, we have

$$\sum_{f(x)\in I^*} E(Y_f) \leq \sum_{f(x)\in I^*} 4^{-j+jh_2(\delta)}$$

$$\leq 2^j 4^{-j+jh_2(\delta)} = 4^{-\frac{1}{2}j+jh_2(\delta)}.$$

Since $j \geq k_m$, then $log_2 m \leq \frac{jlog_2 m}{k_m}$. Thus, we have

$$E(Y) \leq \sum_{j=k_m}^{m-1} m^{\frac{j}{k_m}} 4^{-\frac{1}{2}j+jh_2(\delta)}$$

$$= \sum_{j=k_m}^{m-1} 2^{\frac{jlog_2 m}{k_m}} 4^{-\frac{1}{2}j+jh_2(\delta)}$$

$$= \sum_{j=k_m}^{m-1} 4^{-j\left(\frac{1}{2}-h_2(\delta)-\frac{log_2 m}{2k_m}\right)}.$$

For any $f(x) \in J_{m_i}$, let

$$\mathscr{C}^i_{\bar{a},\bar{b}} = \{(f(x)\bar{a}(x), u^2 f(x)\bar{b}(x)) \in R_{m_i} \times u^2 R'_{m_i}\} \quad (3)$$

be a random $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic code of length $2m_i$.

In fact, there exist some odd integers $m_1, m_2, m_3, \ldots$ such that when $m_i \to \infty$, $lim_{i\to\infty} \frac{log_2 m_i}{k_{m_i}} = 0$, where k_{m_i} is defined as in Lemma 3. Thus, we give the following proposition.

Proposition 2: Let $0 < \delta < 1$ be a real number and $h_p(\delta) < \frac{1}{2}$. Then

$$lim_{i\to\infty} Pr\left(\Delta\left(\mathscr{C}^i_{\bar{a},\bar{b}}\right) > \delta\right) = 1.$$

Proof: When $m_i \to \infty$, then $lim_{i\to\infty} \frac{log_2 m_i}{k_{m_i}} = 0$. Since $h_p(\delta) < \frac{1}{2}$, then there exist a positive integer N and a real number ε such that when $i > N$, $\frac{1}{2} - h_2(\delta) - \frac{log_2 m_i}{2k_{m_i}} \geq \varepsilon$. Thus, by Lemma 4,

$$lim_{i\to\infty} Pr\left(\Delta\left(\mathscr{C}^i_{\bar{a},\bar{b}}\right) \leq \delta\right)$$

$$\leq lim_{i\to\infty} \sum_{j=k_m}^{m_i-1} 4^{-j\left(\frac{1}{2}-h_2(\delta)-\frac{log_2 m_i}{2k_{m_i}}\right)}$$

$$\leq lim_{i\to\infty} \sum_{j=k_{m_i}}^{m_i-1} 4^{-j\varepsilon} \leq lim_{i\to\infty} m_i 4^{-k_{m_i}\varepsilon}$$

$$= lim_{i\to\infty} 4^{-k_{m_i}\left(\varepsilon-\frac{log_2 m_i}{2k_{m_i}}\right)}.$$

$lim_{i\to\infty} k_{m_i} \to \infty$ since $lim_{i\to\infty} \frac{log_2 m_i}{k_{m_i}} = 0$. Thus, $lim_{i\to\infty} 4^{-k_{m_i}\left(\varepsilon-\frac{log_2 m_i}{2k_{m_i}}\right)} = 0$. Therefore,

$$lim_{i\to\infty} Pr\left(\Delta\left(\mathscr{C}^i_{\bar{a},\bar{b}}\right) > \delta\right) = 1.$$

Since $Pr\left(\Delta(\mathscr{C}_{a,b}) > \delta\right) \geq Pr\left(\Delta(\mathscr{C}_{\bar{a},\bar{b}}) > \frac{k+l}{2}\delta\right)$, then if $h_2(\frac{k+l}{2}\delta) < \frac{1}{2}$, we have the following corollary.

Corollary 1: Let $0 < \delta < 1$ and $h_p(\frac{k+l}{2}\delta) < \frac{1}{2}$. Then

$$Pr\left(\Delta(\mathscr{C}^i_{a,b}\right) > \delta) = 1.$$

In the following, we study the $Pr\left(rank(\mathscr{C}^i_{a,b}) = m_i - 1\right)$. We need the following lemma.

Lemma 5 [12]: For any $(\bar{a}(x), \bar{b}(x)) \in J_m \times J_m$, let $\mathscr{C}_{\bar{a},\bar{b}}$ be given as in (2). Then $rank(\mathscr{C}_{\bar{a},\bar{b}}) \leq m-1$. Note that $rank(\mathscr{C}_{\bar{a},\bar{b}}) = m-1$ if and only if there is no irreducible factor $p(x)$ of $\frac{x^m-1}{x-1}$ in $\mathbb{Z}_2[x]$ such that $p(x)|\bar{a}(x)$ and $p(x)|\bar{b}(x)$.

Proposition 3: Let $\mathscr{C}^i_{\bar{a},\bar{b}}$ be given as in (3). Then

$$lim_{i\to\infty} Pr\left(rank(\mathscr{C}^i_{\bar{a},\bar{b}}) = m_i - 1\right) = 1.$$

Proof: Let $x^{m_i} - 1 = (x-1)p_{i1}(x)p_{i2}(x)\cdots p_{ir}(x)$, where $p_{i1}(x), \ldots, p_{ir}(x)$ are distinct irreducible polynomials in $\mathbb{Z}_2[x]$. By the Chinese remainder theorem,

$$J_{m_i} \simeq \mathbb{Z}_2[x]/\langle p_{i1}(x)\rangle \times \cdots \times \mathbb{Z}_2[x]/\langle p_{ir}(x)\rangle$$

$$f(x) \mapsto (f_{i1}(x), \ldots, f_{ir}(x)),$$

where $f_{ij}(x) = f(x)(mod\ p_{ij}(x))$, $j = 1, 2, \ldots, r$.

Let $(\bar{a}(x), u^2\bar{b}(x)) \in J_{m_i} \times u^2 J'_{m_i}$, where $\bar{a}(x), \bar{b}(x) \in J_{m_i}$. By Lemma 5, $rank(\mathscr{C}^i_{\bar{a},\bar{b}}) = m_i - 1$ if and only if $p_{ij}(x) \nmid \bar{a}(x)$ and $p_{ij}(x) \nmid \bar{b}(x)$ if and only if $(a_{ij}(x), b_{ij}(x)) \neq (0,0)$. Let $deg(p_{ij}(x)) = h_{ij}$. Then $|\mathbb{Z}_2[x]/\langle p_{ij}(x)\rangle| = 2^{h_{ij}}$ and

$$Pr\left((a_{ij}(x), b_{ij}(x)) \neq (0,0)\right) = \frac{2^{h_{ij}} \cdot 2^{h_{ij}-1}}{2^{h_{ij}} \cdot 2^{h_{ij}}} = 1 - 4^{-h_{ij}}.$$

Thus,

$$Pr\left(rank\left(\mathscr{C}^i_{\bar{a},\bar{b}}\right) = m_i - 1\right) = \prod_{j=1}^{r}(1 - 4^{-h_{ij}}).$$

For any $j = 1, 2, \ldots, r$, $h_{ij} \geq k_{m_i}$, where k_{m_i} is the degree of lowest degree polynomial in $p_{i1}(x), p_{i2}(x), \ldots, p_{ir}(x)$. Clearly, $r \leq \frac{m_i-1}{k_{m_i}} \leq \frac{m_i}{k_{m_i}}$. Thus,

$$Pr\left(rank\left(\mathscr{C}^i_{\bar{a},\bar{b}}\right) = m_i - 1\right) = \prod_{j=1}^{r}(1 - 4^{-h_{ij}})$$

$$\geq \left(1 - 4^{-k_{m_i}}\right)^{\frac{m_i}{k_{m_i}}}$$

$$= \left(1 - 4^{-k_{m_i}}\right)^{4^{k_{m_i}}\frac{m_i}{k_{m_i}4^{k_{m_i}}}}.$$

Since

$$\begin{aligned} &lim_{i\to\infty}\left(1-4^{-k_{m_i}}\right)^{4^{k_{m_i}}\frac{m_i}{k_{m_i}4^{k_{m_i}}}} \\ &= \left(lim_{i\to\infty}\left(1-4^{-k_{m_i}}\right)^{4^{k_{m_i}}}\right)^{lim_{i\to\infty}\frac{m_i}{k_{m_i}4^{k_{m_i}}}} \\ &= \left(\frac{1}{e}\right)^0 = 1, \end{aligned}$$

then $lim_{i\to\infty}Pr\left(rank\left(\mathscr{C}^i_{\bar{a},\bar{b}}\right)=m_i-1\right)=1$.

Since η is an isomorphism and $\mathscr{C}_{\bar{a},\bar{b}}=\eta(\mathscr{C}_{a,b})$, then we have the following corollary directly.

Corollary 2: $lim_{i\to\infty}Pr\left(rank(\mathscr{C}^i_{a,b})=m_i-1\right)=1$.

According to Corollaries 1 and 2, we obtain the following main theorem.

Theorem 1: Let $0<\delta<1$ be a real number such that $h_p(\frac{k+l}{2}\delta)<\frac{1}{2}$. Then there exist a sequence of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes $\mathscr{C}_1,\mathscr{C}_2,\ldots,\mathscr{C}_i,\ldots$ with block length $(km_1,lm_1),(km_2,lm_2),\ldots,(km_i,lm_i),\ldots$, when $m_i\to\infty$, the $\Delta(\mathscr{C}_i)>\delta$ and $lim_{i\to\infty}R(\mathscr{C}_i)=\frac{1}{k+l}$.

Proof: By Corollary 1, $lim_{i\to\infty}Pr(\Delta(\mathscr{C}_i)>\delta)=1$, which implies that there is a positive integer N_1 such that, when $i>N_1$, $\Delta(\mathscr{C}_i)>\delta$. Therefore, deleting the first N_1 codes and renumbering the remaining codes, we say that $\Delta(\mathscr{C}_i)>\delta$.

By Corollary 2, $lim_{i\to\infty}Pr\left(rank(\mathscr{C}^i_{a,b})=m_i-1\right)=1$, which implies that there is a positive integer N_2 such that, when $i>N_2$, $rank(\mathscr{C}^i_{a,b})=m_i-1$. Therefore,

$$\begin{aligned} lim_{i\to\infty}R(\mathscr{C}_i) &= lim_{i\to\infty}\frac{rank(\mathscr{C}_i)}{km_i+lm_i} \\ &= lim_{i\to\infty}\frac{m_i-1}{km_i+lm_i}=\frac{1}{k+l}. \end{aligned}$$

Theorem 1 indicates that $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes are asymptotically good.

IV. $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD CODES AND RELATED ACD AND LCD CODES

In this section, we study additive complementary duality (ACD) codes of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes.

A. $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD CODES

Firstly, we give the definition of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes.

Definition 6: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code of type $(\alpha,\beta;k_0;k_1,k_2,k_3)$. If $\mathscr{C}\cap\mathscr{C}^\perp=\{0\}$, then $\mathscr{C}$ is said to be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code. For the $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code $\mathscr{C}$, if $\beta=0$, then it is a binary LCD code of length α and if $\alpha=0$, then it is a $\mathbb{Z}_2[u^3]$-octonary LCD code of length β.

Proposition 4: Let $\mathscr{C}\subseteq\mathbb{Z}_2^\alpha\times\mathbb{Z}_2[u^3]^\beta$ be an ACD code. For any $v\in\mathbb{Z}_2^\alpha\times\mathbb{Z}_2[u^3]^\beta$, v can be written uniquely as $v=v_1+v_2$, where $v_1\in\mathscr{C}$ and $v_2\in\mathscr{C}^\perp$.

Proof: Since $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code, then $\mathscr{C}\cap\mathscr{C}^\perp=\{0\}$. Thus, $\mathbb{Z}_2^\alpha\times\mathbb{Z}_2[u^3]^\beta$ can be written as $\mathbb{Z}_2^\alpha\times\mathbb{Z}_2[u^3]^\beta=\mathscr{C}\oplus\mathscr{C}^\perp$. In other word, for any $v\in\mathbb{Z}_2^\alpha\times\mathbb{Z}_2[u^3]^\beta$, there exist unique $v_1\in\mathscr{C}$ and $v_2\in\mathscr{C}^\perp$ such that $v=v_1+v_2$.

Theorem 2: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code with the generator matrix G. Let nonzero vectors $v_1,v_2,\ldots,v_k$ be the rows of G such that $G=\langle v_1,v_2,\ldots,v_k\rangle$. Let $\mathbb{Z}_2[u^3]^\times=\{1,u+1,u^2+1,u^2+u+1\}$. If $[v_i,v_j]\in\{0,u^2\}$ and $[v_i,v_i]\in\mathbb{Z}_2[u^3]^\times$ for all $i,j\in\{1,2,\ldots,k\}$ such that $i\neq j$, then $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code.

Proof: Let w be any nonzero codeword of $\mathscr{C}$. If $w\notin\mathscr{C}^\perp$, then $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code. Since $w\in\mathscr{C}$, then $w=\sum_{i\in J}\lambda_i v_i$, where $J=\{1,2,\ldots,k\}$ and $\lambda_i\in\mathbb{Z}_2[u^3]$.

Firstly, assume that there exists $j\in J$ such that $\lambda_j\in\mathbb{Z}_2[u^3]^\times$. Then

$$[w,v_j]=\sum_{i\in J}\lambda_i[v_i,v_j]=\sum_{i\in J\setminus\{j\}}\lambda_i[v_i,v_j]+\lambda_j[v_j,v_j].$$

For $i\neq j$, since $[v_i,v_j]\in\{0,u^2\}$, then $\lambda_i[v_i,v_j]\in\{0,u^2\}$. Since $[v_j,v_j]\in\mathbb{Z}_2[u^3]^\times$, then $\lambda_j[v_j,v_j]\in\mathbb{Z}_2[u^3]^\times$. Thus, $[w,v_j]\neq0$ and $w\notin\mathscr{C}^\perp$.

Further, if $\lambda_i\in I_{max}$, let $j\in J$ such that $\lambda_j\in\{u,u^2,u^2+u\}$. Since $[v_i,v_j]\in\{0,u^2\}$, then $\lambda_i[v_i,v_j]=0$. Thus,

$$[w,v_j]=\sum_{i\in J\setminus\{j\}}\lambda_i[v_i,v_j]+\lambda_j[v_j,v_j]=\lambda_j[v_j,v_j].$$

Since $[v_j,v_j]\in\mathbb{Z}_2[u^3]^\times$, then $\lambda_j[v_j,v_j]\neq0$. Thus, $[w,v_j]\neq0$ and $w\notin\mathscr{C}^\perp$. Thus, $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code.

The following corollaries can be deduced from Theorem 2 directly.

Corollary 3: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code with the generator matrix G and $G\cdot G^\top=(v_{ij})_{i,j\in\{1,2,\ldots,k\}}$. For all $i,j\in\{1,2,\ldots,k\}$ such that $i\neq j$, if $v_{ij}\in\{0,u^2\}$ and $v_{ii}\in\mathbb{Z}_2[u^3]^\times$, then $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code.

Corollary 4: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code with the generator matrix G. If $G\cdot G^\top$ is nonsingular over $\mathbb{Z}_2[u^3]$, then $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code.

Note that conditions in Theorem 2, Corollaries 3 and 4 are only sufficient conditions to prove that $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code. The reverse statements are not true in general.

Example 2: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code generated by

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

By Magma Computational Algebra System [35], $\mathscr{C}\bigcap\mathscr{C}^\perp=\{0\}$. Thus, $\mathscr{C}$ is an ACD code. Let $v_1=(1,1,0\mid u,u^2+u,u+1)$, $v_2=(0,1,0\mid1,u,u)$, $v_3=(0,1,1\mid0,u^2,0)$. Clearly, $[v_3,v_3]=0\notin\mathbb{Z}_2[u^3]^\times$. So it does not satisfy the conditions of Theorem 2. Further,

$$G\cdot G^\top=\left(\begin{array}{ccc}0&u^2&0\\u^2&1&u^2\\0&u^2&0\end{array}\right)\in M(\mathbb{Z}_2[u^3]).$$

Clearly, it does not satisfy the conditions of Corollary 3. Further,

$$|G\cdot G^\top|=0,$$

which implies that it does not satisfy the conditions of Corollary 4.

Theorem 3: Let C be a binary $[\alpha, k]$ linear code with basis $\{v_1, v_2, \ldots, v_k\}$, where α is the length of C and k is the dimension of C. Let $\zeta \geq k$ and G_X be a $\zeta \times \alpha$ matrix, which non-zero row vectors are $v_1, v_2, \ldots, v_k$. Let $G = (G_X \mid \lambda I_\zeta)$, where $\lambda \in \mathbb{Z}_2[u^3]^\times$. Then the $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code $\mathscr{C}$ generated by G is an ACD code.

Proof: Let $\mathscr{C}$ be the $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code generated by $G = (G_X \mid \lambda I_\zeta)$. By (1), we have

$$\begin{aligned} G \cdot G^\top &= u^2 G_X G_X^\top + \lambda^2 I_\zeta I_\zeta^\top \\ &= u^2 G_X G_X^\top + \lambda^2 I_\zeta = (v_{ij})_{i,j\in\{1,2,\ldots,\zeta\}}, \end{aligned}$$

where all elements in G_X belong to $\{0, 1\}$. Since all elements in $u^2 G_X G_X^\top$ are in $\{0, u^2\}$, then for $i \neq j$, $v_{ij} \in \{0, u^2\}$ and $v_{ii} \in \{\lambda^2, \lambda^2 + u^2\} \subseteq \mathbb{Z}_2[u^3]^\times$. Therefore, by Corollary 3, $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code.

Example 3: Let C be a binary $[3, 3]$ linear code with the basis $v_1 = (0, 1, 0)$, $v_2 = (0, 0, 1)$, $v_3 = (1, 0, 0)$. Let $\zeta = 4$, and $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code generated by the matrix

$$G = \left(\begin{array}{ccc|cccc} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

Let w_i be the rows of G for $i = 1, 2, 3, 4$. Clearly, $[w_i, w_j] = 0$ for $i \neq j$ and $[w_i, w_i] \in \{1, 1 + u^2\} \subseteq \mathbb{Z}_2[u^3]^\times$. Thus, by Theorem 3, $\mathscr{C}$ is an ACD code.

B. COMPLEMENTARY DUALITY OF $\mathscr{C}$, $\mathscr{C}_X$ AND $\mathscr{C}_Y$

In this subsection, we discuss the complementary duality between $\mathscr{C}$ and $\mathscr{C}_X$ or $\mathscr{C}_Y$.

Case 1: $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code, $\mathscr{C}_X$ is a binary LCD code and $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code.

Theorem 4: Let $\mathscr{C}$ be a separable $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code. Then $\mathscr{C}$ is an LCD code if and only if $\mathscr{C}_X$ is a binary LCD code and $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code.

Proof: Let $\mathscr{C}$ be separable. Then $\mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$, which implies that $\mathscr{C}^\perp = (\mathscr{C}_X)^\perp \times (\mathscr{C}_Y)^\perp$. If $\mathscr{C}$ is an ACD code, then for any $v = (v|v') \in \mathscr{C} \cap \mathscr{C}^\perp$ and so $v = 0$, which implies that $v = 0$ and $v' = 0$. Therefore, $\mathscr{C}_X$ is an LCD code and $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code.

Conversely, let $\mathscr{C}_X$ be an LCD code and $\mathscr{C}_Y$ be a $\mathbb{Z}_2[u^3]$-octonary LCD code. Since $\mathscr{C}$ is separable, then for any $v = (v|v') \in \mathscr{C} \cap \mathscr{C}^\perp$, we have that $v \in \mathscr{C}_X \cap (\mathscr{C}_X)^\perp = \{0\}$ and $v' \in \mathscr{C}_Y \cap (\mathscr{C}_Y)^\perp = \{0\}$, which implies that $v = (v|v') = 0$, i.e. $\mathscr{C} \cap \mathscr{C}^\perp = \{0\}$. Thus, $\mathscr{C}$ is an ACD code.

From Theorem 4, a separable code $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code if and only if $\mathscr{C}_X$ is a binary LCD code and $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code. However, there exist non-separable $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes such that $\mathscr{C}_X$ is an LCD code and $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code. Let us look at the following example.

Example 4: Let $\mathscr{C}$ be a non-separable $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code generated by

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

By Magma Computational Algebra System [35], $\mathscr{C} \bigcap \mathscr{C}^\perp = \{0\}$. Thus, $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code. Moreover, we have $\mathscr{C}_X \bigcap \mathscr{C}_X^\perp = \{0\}$ and $\mathscr{C}_Y \bigcap \mathscr{C}_Y^\perp = \{0\}$, Thus, $\mathscr{C}_X$ is an LCD code and $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code.

Case 2: $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code, either $\mathscr{C}_X$ is a binary LCD code or $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code.

In Theorem 3, we have obtained a class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes, i.e. $\mathscr{C}_X$ is not an LCD code, but $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code since $G_Y = \lambda^2 I_\zeta$.

The following result is a special case of Theorem 3.

Theorem 5: Let C be a binary $[\alpha, \zeta]$ self-orthogonal code generated by the matrix G_X. Let $G = (G_X \mid \lambda I_\zeta)$, where $\lambda \in \mathbb{Z}_2[u^3]^\times$. Then $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code generated by λI_ζ, and the matrix G generates a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code of type $(\alpha, \zeta; 0; \zeta, 0, 0)$.

Proof: Clearly, $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code. By (1), we have

$$G \cdot G^\top = u^2 G_X G_X^\top + \lambda^2 I_\zeta I_\zeta^\top = \lambda^2 I_\zeta = (v_{ij})_{i,j\in\{1,2,\ldots,\zeta\}},$$

since G_X generates a self-orthogonal code. Since $\lambda \in \mathbb{Z}_2[u^3]^\times$, then $\lambda^2 \in \{1, u^2 + 1\}$. Thus, for $i \neq j$, $v_{ij} = 0$ and $v_{ii} \in \{1, u^2 + 1\} \subseteq \mathbb{Z}_2[u^3]^\times$. Therefore, by Corollary 3, $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code.

Example 5: Let C be a binary $[5, 2]$ self-orthogonal code generated by G_X, where

$$G_X = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Let $G = (G_X \mid \lambda I_2)$, where $\lambda = u + 1 \in \mathbb{Z}_2[u^3]^\times$. Then the matrix

$$\left(\begin{array}{ccccc|cc} 1 & 1 & 0 & 0 & 0 & u+1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & u+1 \end{array}\right)$$

generates a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code. By Magma Computational Algebra System [35], $\mathscr{C} \cap \mathscr{C}^\perp = \{0\}$, which implies that $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code of type $(5, 2; 0; 2, 0, 0)$.

Theorem 5 proves that $\mathscr{C}_Y$ is a $\mathbb{Z}_2[u^3]$-octonary LCD code, $\mathscr{C}_X$ is not an LCD code, but $\mathscr{C}$ can be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code. In the following, we will discuss that $\mathscr{C}_X$ is an LCD code, $\mathscr{C}_Y$ is not a $\mathbb{Z}_2[u^3]$-octonary LCD code, but $\mathscr{C}$ can also be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code. Similar to the construction of Theorem 5, let $\mathscr{C}_X$ be an LCD code generated by λI_ζ and $\mathscr{C}_Y$ be a self-orthogonal (self-dual in particular) code generated by G_Y. Can $G = (\lambda I_\zeta \mid G_Y)$ generate a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code?

Let $G = (\lambda I_\zeta \mid G_Y)$. Then, by (1), $G \cdot G^\top = u^2\lambda^2 I_\zeta I_\zeta^\top + G_Y G_Y^\top = u^2 I_\zeta + G_Y G_Y^\top$. Since $\mathscr{C}_Y$ is self-orthogonal, then $G_Y G_Y^\top = 0$, i.e. $G \cdot G^\top = u^2 I_\zeta$. Thus, in general, we can not confirm that whether $\mathscr{C}$ is ACD or not. However, we can find a class of special $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes generated by

$G = (G_X \mid G_Y)$ such that $\mathscr{C}_X$ is an LCD code and $\mathscr{C}_Y$ is not a $\mathbb{Z}_2[u^3]$-octonary LCD code.

Proposition 5: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive code generated by $G = (I_\zeta \mid u^2 I_\zeta)$. Then $\mathscr{C}$ is an ACD code.

Proof: Let $w = (w|w') \in \mathscr{C} \cap \mathscr{C}^\perp$. Clearly, for all $v = (v|v') \in \mathscr{C}$, we have $0 = [w, v] = u^2[w, v]_2 + [w', v']_u$. Since $\mathscr{C}_Y$ is a self-orthogonal code generated by $u^2 I_\zeta$, then $[w', v']_u = 0$. Since $\mathscr{C}_X$ is an LCD code generated by I_ζ and $[w, v]_2 \in \mathbb{Z}_2$, then $u^2[w, v]_2 = 0$, which implies that $[w, v]_2 = 0$ and so $w = 0$. Let $v_i = (v_i|v_i')$ be the i-th row of G, where v_i denote the i-th row of I_ζ and $v_i' = u^2 v_i$. Since $w \in \mathscr{C}$, then there exist $\lambda_0, \lambda_1, \ldots, \lambda_{\zeta-1} \in \mathbb{Z}_2[u^3]$ such that

$$w = \sum_{i=0}^{\zeta-1} \lambda_i v_i = \left(\sum_{i=0}^{\zeta-1} \theta(\lambda_i) v_i | u^2 \sum_{i=0}^{\zeta-1} \lambda_i v_i \right).$$

Thus, $w = \sum_{i=0}^{\zeta-1} \theta(\lambda_i) v_i$ and $w' = u^2 \sum_{i=0}^{\zeta-1} \lambda_i v_i$. Since $v_0, v_1, \ldots, v_{\zeta-1}$ are $\mathbb{Z}_2$-linearly independent, then $w = 0$ implying that $\theta(\lambda_i) = 0$ i.e. $\lambda_i = b_i u + c_i u^2$, where $b_i, c_i \in \mathbb{Z}_2$. Therefore, $w' = u^2 \sum_{i=0}^{\zeta-1} \lambda_i v_i = 0$. It means that $w = (w|w') = 0$. Thus, $\mathscr{C}$ is ACD.

Note that in Proposition 5, $\mathscr{C}_X$ is an LCD code generated by I_ζ and $\mathscr{C}_Y$ is not a $\mathbb{Z}_2[u^3]$-octonary LCD code since $\mathscr{C}_Y$ is a self-orthogonal code generated by $u^2 I_\zeta$.

Example 6: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code generated by

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

By Magma Computational Algebra System [35], $\mathscr{C} \cap \mathscr{C}^\perp = \{0\}$, which implies that $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code.

C. BINARY LCD CODES FROM $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD CODES

Although $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear codes are ACD codes, their binary Gray images are not necessary LCD codes. Thus, in the following, we give a class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes such that their binary Gray images are LCD codes.

Theorem 6: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code generated by the matrix $G = (G_X \mid G_Y)_{m\times(\alpha+\beta)}$, where G_X generates a self-orthogonal code $\mathscr{C}_X$ and G_Y generates a linear code $\mathscr{C}_Y$. If the row vectors of G_Y are $\mathbb{Z}_2[u^3]$-linearly independent and $\Phi(\mathscr{C}_Y)$ is a binary LCD code, then the binary Gray image $\Phi(\mathscr{C})$ is an LCD code.

Proof: Let $w = (w|w') \in \mathscr{C}$ such that $\Phi(w) = (w|\Phi(w')) \in C \cap C^\perp$, where $C = \Phi(\mathscr{C})$. If we can prove that $\Phi(w) = 0$, then C is a binary LCD code.

For all $v = (v|v') \in \mathscr{C}$, $\Phi(v) = (v|\Phi(v')) \in \Phi(\mathscr{C}) = C$, since $\Phi(w) = (w|\Phi(w')) \in C \cap C^\perp$, then $\Phi(w) \in C^\perp$. Clearly,

$$0 = [\Phi(w), \Phi(v)]_2 = [w, v]_2 + [\Phi(w'), \Phi(v')]_2. \quad (4)$$

Since $w, v \in \mathscr{C}_X$ and $\mathscr{C}_X$ is a self-orthogonal code, then $[w, v]_2 = 0$. Thus, by (4), $[\Phi(w'), \Phi(v')]_2 = 0$. Since $\Phi(w'), \Phi(v') \in \Phi(\mathscr{C}_Y)$ and $\Phi(\mathscr{C}_Y)$ is a binary LCD code, then $[\Phi(w'), \Phi(v')]_2 = 0$ implying $\Phi(w') = 0$. Thus, $w' = 0$.

In the following, we will prove that for any $w = (w|w') \in \mathscr{C}$, if $w' = 0$, then $w = 0$. For $i \in \{0, 1, \ldots, m-1\}$, let $v_i = (v_i|v_i')$ be the i-th row of G, where v_i and v_i' denote the i-th row of G_X and G_Y, respectively. Since $w \in \mathscr{C}$, then there exist $\lambda_0, \lambda_1, \ldots, \lambda_{m-1} \in \mathbb{Z}_2[u^3]$ such that

$$w = \sum_{i=0}^{m-1} \lambda_i v_i = \left(\sum_{i=0}^{m-1} \theta(\lambda_i) v_i | \sum_{i=0}^{m-1} \lambda_i v_i' \right).$$

Thus, $w = \sum_{i=0}^{m-1} \theta(\lambda_i) v_i$ and $w' = \sum_{i=0}^{m-1} \lambda_i v_i'$. Since $v_0', v_1', \ldots, v_{m-1}'$ are $\mathbb{Z}_2[u^3]$-linearly independent, then $w' = 0$ implying that $\lambda_i = 0$ for all $i = 0, 1, \ldots, m-1$. Therefore, $w = \sum_{i=0}^{m-1} \theta(\lambda_i) v_i = 0$. It means that $w = 0$ and $w = (w|w') = 0$. Thus, $\Phi(w) = 0$.

Example 7: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code generated by

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

where

$$G_X = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } G_Y = \begin{pmatrix} u^2+u+1 & u \\ u^2 & u+1 \end{pmatrix}.$$

Clearly, G_X generates a self-orthogonal code $\mathscr{C}_X$ and the row vectors of G_Y are $\mathbb{Z}_2[u^3]$-linearly independent. The code $\mathscr{C}_Y$ has 64 codewords. By applying the Gray map Φ to each codeword of $\mathscr{C}_Y$, the generator matrix of $C_Y = \Phi(\mathscr{C}_Y)$ is

$$\begin{pmatrix} 1&0&0&1&0&0&1&1 \\ 0&1&0&1&1&0&0&1 \\ 0&0&1&1&1&0&1&0 \\ 0&0&0&0&0&1&1&0 \end{pmatrix}.$$

By Magma Computational Algebra System [35], $C_Y \cap C_Y^\perp = \{0\}$, which implies that C_Y is a binary LCD code.

Similarly, by applying the Gray map Φ to each codeword of $\mathscr{C}$, the generator matrix of $C = \Phi(\mathscr{C})$ is given by

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

By Magma Computational Algebra System [35], we have $C \cap C^\perp = \{0\}$. It means that the binary Gray image of $\mathscr{C}$ is an LCD code. More importantly, C is an optimal $[10, 4, 4]$ binary linear code.

Example 8: Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD code generated by

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

where

$$G_X = \begin{pmatrix} 1&1&1&1 \\ 1&0&1&0 \end{pmatrix} \text{ and } G_Y = \begin{pmatrix} u^2+1 & u \\ u^2 & u+1 \end{pmatrix}.$$

Clearly, G_X generates a self-orthogonal code $\mathscr{C}_X$ and the row vectors of G_Y are $\mathbb{Z}_2[u^3]$-linearly independent. The code $\mathscr{C}_Y$

has 64 codewords. By applying the Gray map Φ to each codeword of $\mathscr{C}_Y$, the generator matrix of $C_Y = \Phi(\mathscr{C}_Y)$ is

$$\begin{pmatrix} 1&0&0&1&0&0&0&0\\ 0&1&0&1&0&1&0&1\\ 0&0&1&1&0&0&0&0\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix}.$$

By Magma Computational Algebra System [35], $C_Y \cap C_Y^{\perp} = \{0\}$, which implies that C_Y is a binary LCD code.

Similarly, by applying the Gray map Φ to each codeword of $\mathscr{C}$, the generator matrix of $C = \Phi(\mathscr{C})$ is given by

$$\left(\begin{array}{cccc|cccccccc} 1&0&1&0&0&0&0&0&0&1&1\\ 0&1&0&1&0&0&0&0&1&1&1\\ 0&0&0&0&1&0&0&1&1&1&0&0\\ 0&0&0&0&0&1&0&1&1&0&1&0\\ 0&0&0&0&0&0&1&1&1&0&0&1 \end{array}\right).$$

By Magma Computational Algebra System [35], we have $C \cap C^{\perp} = \{0\}$. It means that the binary Gray image of $\mathscr{C}$ is an LCD code. More importantly, C is an optimal [12, 5, 4] binary linear code.

V. CONCLUSION

In this paper, we mainly studied $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes and $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes. We constructed a class of asymptotically good $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes, and gave some sufficient conditions to show that $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes are ACD codes. Moreover, we gave a class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes, which binary Gray images are LCD codes. An computational example showed that this class of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-ACD codes can produce optimal binary LCD codes. As an open problem, it is interesting to study ACD codes over some other additive structures.

REFERENCES

[1] I. Aydogdu, T. Abualrub, and I. Siap, "On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes," *Int. J. Comput. Math.*, vol. 92, pp. 1806–1814, Sep. 2015.

[2] I. Aydogdu, I. Siap, and R. Ten-Valls, "On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes," *Finite Fields Their Appl.*, vol. 48, pp. 241–260, Nov. 2017.

[3] I. Aydogdu and I. Siap, "The structure of $\mathbb{Z}_2\mathbb{Z}_2^s$-additive codes: Bounds on the minimum distance," *Appl. Math. Inf. Sci.*, vol. 7, pp. 2271–2278, Nov. 2013.

[4] I. Aydogdu and I. Siap, "On $\mathbb{Z}_p^r\mathbb{Z}_p^s$-additive codes," *Linear Multilinear Algebra*, vol. 63, pp. 2089–2102, Oct. 2015.

[5] L. Diao, J. Gao, and J. Lu, "Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes," *Adv. Math. Commun.*, vol. 14, pp. 555–572, Nov. 2020.

[6] X. Hou and J. Gao, "$\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes are asymptotically good," *J. Appl. Math. Computing.*, Nov. 2020, doi: 10.1007/s12190-020-01466-w.

[7] M. Shi, R. Wu, and D. S. Krotov, "On $\mathbb{Z}_p\mathbb{Z}_p^k$-additive codes and their duality," *IEEE Trans. Inf. Theory*, vol. 65, pp. 3841–3847, Jun. 2019.

[8] M. Shi, D. Huang, and D. S. Krotov, "Additive perfect codes in doob graphs," *Designs, Codes Cryptogr.*, vol. 87, no. 8, pp. 1857–1869, Aug. 2019.

[9] M. Shi, C. Wang, R. Wu, Y. Hu, and Y. Chang, "One-weight and two-weight $\mathbb{Z}_2\mathbb{Z}_2[u, v]$-additive codes," *Cryptogr. Commun.*, vol. 12, pp. 443–454, May 2020.

[10] T. Yao, S. Zhu, and X. Kai, "Asymptotically good $\mathbb{Z}_p^r\mathbb{Z}_p^s$-additive cyclic codes," *Finite Fields Their Appl.*, vol. 63, Mar. 2020, Art. no. 101633.

[11] T. Abualrub, I. Siap, and N. Aydin, "$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes," *IEEE Trans. Inf. Theory*, vol. 60, pp. 1508–1514, Mar. 2014.

[12] Y. Fan and L. Lin, "$\mathbb{Z}_2\mathbb{Z}_4$-Additive cyclic codes are asymptotically good," 2019, *arXiv:1911.09350*. [Online]. Available: https://arxiv.org/abs/1911.09350

[13] E. Assmus, H. Mattson, and R. Turyn, "Cyclic Codes," in *Proc. AF Cambridge Res. Labs, Bedford*, 1966, pp. 348–366.

[14] L. M. J. Bazzi and S. K. Mitter, "Some randomized code constructions from group actions," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3210–3219, Jul. 2006.

[15] C. MartÍnez-Pérez and W. Willems, "Self-dual doubly even 2-quasi cyclic transitive codes are asymptotically good," *IEEE Trans. Inf. Theory*, vol. 53, pp. 4302–4308, Nov. 2007.

[16] Y. Fan and L. Lin, "Qyasi-cyclic codes of index $1\frac{1}{3}$," *IEEE Trans. Inf. Theory*, vol. 62, pp. 6342–6347, Nov. 2016.

[17] J. Mi and X. Cao, "Asymptotically good quasi-cyclic codes of fractional index," *Discrete Math.*, vol. 341, no. 2, pp. 308–314, Feb. 2018.

[18] J. Gao and X. Hou, "$\mathbb{Z}_4$-double cyclic codes are asymptotically good," *IEEE Commun. Lett.*, vol. 24, no. 8, pp. 1593–1597, Aug. 2020.

[19] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," *Adv. Math. Commun.*, vol. 10, no. 1, pp. 131–150, Mar. 2016.

[20] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, "Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$," *IEEE Trans. Inf. Theory*, vol. 64, pp. 3010–3017, Apr. 2018.

[21] C. Carlet, C. Güneri, F. Özbudak, and P. Solé, "A new concatenated type construction for LCD codes and isometry codes," *Discrete Math.*, vol. 341, pp. 830–835, Mar. 2018.

[22] L. Sok, M. Shi, and P. Solé, "Constructions of optimal LCD codes over large finite fields," *Finite Fields Their Appl.*, vol. 50, pp. 138–153, Mar. 2018.

[23] L. Sok, "On hermitian LCD codes and their gray image," *Finite Fields Their Appl.*, vol. 62, Feb. 2020, Art. no. 101623.

[24] C. Li, "Hermitian LCD codes from cyclic codes," *Designs, Codes Cryptogr.*, vol. 86, no. 10, pp. 2261–2278, Oct. 2018.

[25] M. Shi and D. Huang, "On LCD MRD codes," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E101.A, no. 9, pp. 1599–1602, Sep. 2018.

[26] M. Harada and K. Saito, "Binary linear complementary dual codes," *Cryptogr. Commun.*, vol. 11, no. 4, pp. 677–696, Jul. 2019.

[27] C. Gáneri, B. Özkaya, and P. Solé, "Quasi-cyclic complementary dual codes," *Finite Fields Their Appl.*, vol. 42, pp. 67–80, Nov. 2016.

[28] A. Saleh and M. Esmaeili, "On complementary dual quasi-twisted codes," *J. Appl. Math. Comput.*, vol. 56, nos. 1–2, pp. 115–129, Feb. 2018.

[29] A. Sharma, V. Chauhan, and H. Singh, "Multi-twisted codes over finite fields and their dual codes," *Finite Fields Their Appl.*, vol. 51, pp. 270–297, May 2018.

[30] M. Shi, D. Huang, L. Sok, and P. Solé, "Double circulant self-dual and LCD codes over galois rings," *Adv. Math. Commun.*, vol. 13, no. 1, pp. 171–183, 2019.

[31] H. Q. Dinh, T. Bag, A. K. Upadhyay, R. Bandi, and W. Chinnakum, "On the structure of cyclic codes over $\mathbb{F}_qRS$ and applications in Quantum and LCD Codes Constructions," *IEEE Access*, vol. 8, pp. 18902–18914, Jan. 2020.

[32] N. Benbelkacem, J. Borges, S. T. Dougherty, and C. Fernández-Córdoba, "On $\mathbb{Z}_2\mathbb{Z}_4$-additive complementary dual codes and related LCD codes," *Finite Fields Their Appl.*, vol. 62, Feb. 2020, Art. no. 101622.

[33] M. Shi, S. Zhu, and S. Yang, "A class of optimal P-ary codes from one-weight codes over $\mathbb{F}_p[u]/\langle u^m \rangle$," *J. Franklin Inst.*, vol. 350, no. 5, pp. 929–937, Jun. 2013.

[34] Y. Fan and L. Lin, "Thresholds of random quasi-abelian codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 82–90, Jan. 2015.

[35] W. Bosma, J. Cannon, and C. Playoust, "The MAGMA algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, 1997.

XIAOTONG HOU received the B.E. degree from the Shandong University of Technology, in 2019, where she is currently pursuing the master's degree with the School of Mathematics and Statistics. Her research interests include coding theory and cryptography.

XIANGRUI MENG received the B.E. degree from the Shandong University of Technology, in 2019, where she is currently pursuing the master's degree with the School of Mathematics and Statistics. Her research interests include coding theory and cryptography.

JIAN GAO received the Ph.D. degree from the Chern Institute of Mathematics, Nankai University, in 2015. He is currently working as an Associate Professor with the Shandong University of Technology, China. He has been published more than 60 articles in important international journals, including IEEE TRANSACTIONS ON INFORMATION THEORY, *Finite Fields and Their Applications*, *Designs, Codes and Cryptography*, IEEE COMMUNICATIONS LETTERS, *Applicable Algebra in Engineering, Communications and Computing*, *Cryptography and Communications*, *Advances in Mathematics of Communications*, *Quantum Information Processing*. His research interest includes coding theory and their applications.