Discussiones Mathematicae
General Algebra and Applications 42 (2022) 349–362
https://doi.org/10.7151/dmgaa.1395

SELF-DUAL CYCLIC CODES OVER $M_2(\mathbb{Z}_4)$

Sanjit Bhowmick

Department of Mathematics
National Institute of Technology Durgapur
West Bengal, India

e-mail: sb.17ma1108@phd.nitdgp.ac.in

Joydeb Pal

Department of Mathematics
School of Applied Sciences
Kalinga Institute of Industrial Technology (KIIT)
Deemed to be University, Odisha, India

e-mail: joydeb.palfma@kiit.ac.in

Ramakrishna Bandi

Department of Mathematics
Dr. SPM International Institute of Information Technology
Naya Raipur, India

e-mail: ramakrishna@iiitnr.edu.in

and

Satya Bagchi

Department of Mathematics
National Institute of Technology Durgapur
Burdwan, India

e-mail: satya.bagchi@maths.nitdgp.ac.in

Abstract

In this paper, we study the structure of cyclic codes over$M_2(\mathbb{Z}_4)$ (the matrix ring of matrices of order 2 over $\mathbb{Z}_4$), which is perhaps the first time that the ring is considered as a code alphabet. This ring is isomorphic to $\mathbb{Z}_4[w]+U\mathbb{Z}_4[w]$, where w is a root of the irreducible polynomial $x^2+x+1 \in \mathbb{Z}_2[x]$ and $U \cong \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. In our work, we first discuss the structure of the ring $M_2(\mathbb{Z}_4)$ and then focus on the structure of cyclic codes and self-dual cyclic codes over $M_2(\mathbb{Z}_4)$. Thereafter, we obtain the generators of the cyclic codes and their dual codes. A few non-trivial examples are given at the end of the paper.

Keywords: codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, Gray map, Lee weight, self-dual codes.

2010 Mathematics Subject Classification: Primary 94B05, Secondary 94B15.

1. Introduction

Over the past three decades, the study of codes over various finite rings has been a topic of interest [10]. However, their applications in digital communication are the most demanding problems in this ultra-modern era. Codes over rings have got the attention of researchers only after the remarkable work of Hammons *et al.* [4] in which they have shown an interesting relation between some popular non-linear codes and linear codes over residue ring of integers modulo 4, via a map called Gray map. This attracted researchers to focus on codes over rings and their applications. As a result, plenty of new ring structures have been considered as code alphabets. However, most of the study was restricted to codes over commutative rings [4, 8, 9]. In 2013, codes over a non-commutative matrix ring, the ring of 2×2 matrices over the field $\mathbb{F}_2$; i.e., $M_2(\mathbb{F}_2)$ has been taken as a code alphabet to study the space-time codes [6]. The advantage of this type of non-commutative matrix ring is that it allows to form quotient rings which are either left ideals or right ideals (cyclic codes). This is also true in the case of skew polynomial rings but polynomial factorization is a big hurdle to construct the codes over skew polynomial rings. Some notable works on cyclic codes over non-commutative finite rings can be found in [2, 3, 7, 11].

In [1], the authors have studied cyclic codes over $M_2(\mathbb{F}_2)$ and obtained some optimal codes over the same. Inspired by this work, Luo and Parampalli [5] proposed the structure of cyclic codes over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ and found some good optimal cyclic codes. Recently, the structure of cyclic codes over the ring $M_4(\mathbb{F}_2)$ has been introduced to the literature [7]. Motivated by these works, in our paper, we explore a new construction of codes over $M_2(\mathbb{Z}_4)$. The reason for choosing $\mathbb{Z}_4$ is that $\mathbb{Z}_4$ is the best-suited ring for the construction of modular lattices and also the relation established by Hammons et al. [4] between binary non-linear codes and linear codes over $\mathbb{Z}_4$. The approach which is being used to construct cyclic codes over $M_2(\mathbb{Z}_4)$ is the same as that of cyclic codes over $M_2(\mathbb{F}_2)$; however, it is not straightforward which can be realized from the later parts of our work.

Our proposed work is organized as follows: In Section 2, we describe the structure of $M_2(\mathbb{Z}_4)$ and show that $M_2(\mathbb{Z}_4)$ is isomorphic to $\mathbb{Z}_4[w] + U\mathbb{Z}_4[w]$, where w is a root of the polynomial x^2+x+1 and $U \equiv \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Besides, we define a Gray map from $\mathbb{Z}_4[w]+U\mathbb{Z}_4[w]$ to $\mathbb{F}_4^4$ which preserves the Lee weight in $\mathbb{Z}_4[w]+U\mathbb{Z}_4[w]$ and Hamming weight in $\mathbb{F}_4^4$. In Section 3, we discuss the structure of cyclic codes and prove some results on the dimension of cyclic codes. In Section 4, we construct the structure of dual cyclic codes and self-dual codes. We enlighten on the Hermitian self-dual cyclic codes in Section 5. Finally, we exhibit some non-trivial examples of cyclic codes and their Gray images.

2. STRUCTURE OF $M_2(\mathbb{Z}_4)$

Let us denote $\mathcal{R} = M_2(\mathbb{Z}_4)$. It is clear that $\mathcal{R}$ is a non-commutative ring of matrices of order 2 over the ring $\mathbb{Z}_4$. Now, we see that the set $\mathbb{Z}_4 + X\mathbb{Z}_4 + Y\mathbb{Z}_4 + YX\mathbb{Z}_4$ forms a non-commutative finite ring with respect to componentwise addition, and the multiplication rule defined in Table 1.

$\mathcal{R}\cdot$	1	X	Y	YX
1	1	X	0	0
X	0	0	1	X
Y	Y	YX	0	0
YX	0	0	Y	YX

Table 1. Multiplication rule of $\mathcal{R}$.

Lemma 2.1. *The ring $M_2(\mathbb{Z}_4)$ is isomorphic to the ring $\mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4$.*

Proof. We define a mapping $f : M_2(\mathbb{Z}_4) \longrightarrow \mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4$ such that $f(A) = a+Xb+Yc+YXd$, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_4)$. It is easy to verify that $f(A+B) = f(A)+f(B)$. Now, we show that $f(AB) = f(A)f(B)$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$. Then, $AB = \begin{pmatrix} aa_1+bc_1 & ab_1+bd_1 \\ ca_1+dc_1 & cb_1+dd_1 \end{pmatrix}$. Therefore, $f(AB) = (aa_1+bc_1)+X(ab_1+bd_1)+Y(ca_1+dc_1)+YX(cb_1+dd_1)$. Now,

$$\begin{aligned} f(A)f(B) &= (a+Xb+Yc+YXd)(a_1+Xb_1+Yc_1+YXd_1) \\ &= (aa_1+bc_1)+X(ab_1+bd_1)+Y(ca_1+dc_1)+YX(cb_1+dd_1) \\ &= f(AB). \end{aligned}$$

Thus, f is a ring homomorphism. One can easily verify that f is one-one and onto. Hence, $M_2(\mathbb{Z}_4) \cong \mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4$. ■

We consider a subset of $\mathbb{Z}_4 + X\mathbb{Z}_4 + Y\mathbb{Z}_4 + YX\mathbb{Z}_4$, namely $W = \{0,\ X + Y3 + YX3,\ X2 + Y2 + YX2,\ X3 + Y + YX,\ 1 + X + YX3,\ 2 + X2 + YX2,\ 3+X3+YX,\ 1+YX,\ 2+YX2,\ 3+YX3,\ 1+X2+Y2+YX3,\ 3+X2+Y2+YX,\ 1+X3+Y+YX2,\ 2+X3+Y+YX3,\ 2+X+Y3+YX,\ 3+X+Y3+YX3\}$.

Lemma 2.2. *The subset W forms a commutative ring with respect to component-wise addition and multiplication defined on* $\mathbb{Z}_4 + X\mathbb{Z}_4 + Y\mathbb{Z}_4 + YX\mathbb{Z}_4$.

Proof. For simplicity, we use the following notations:

$a_0 = 0,$	$a_1 = X + Y3 + YX3,$	$a_2 = X2 + Y2 + YX2,$	$a_3 = X3 + Y + YX,$
$a_4 = 1 + X + YX3,$	$a_5 = 2 + X2 + YX2,$	$a_6 = 3 + X3 + YX,$	$a_7 = 1 + YX,$
$a_8 = 2 + YX2,$	$a_9 = 3 + YX3,$	$a_{10} = 1 + X2 + Y2 + YX3,$	$a_{11} = 3 + X2 + Y2 + YX,$
$a_{12} = 1 + X3 + Y + YX2,$	$a_{13} = 2 + X3 + Y + YX3,$	$a_{14} = 2 + X + Y3 + YX,$	$a_{15} = 3 + X + Y3 + YX3.$

The multiplication table on W is given below:

$\cdot$	0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a_1	0	a_6	a_5	a_4	a_9	a_8	a_7	a_1	a_2	a_3	a_{13}	a_{14}	a_{10}	a_{12}	a_{15}	a_{11}
a_2	0	a_5	0	a_5	a_8	0	a_8	a_2	0	a_2	a_2	a_2	a_8	a_5	a_5	a_8
a_3	0	a_4	a_5	a_6	a_7	a_8	a_9	a_3	a_2	a_1	a_{14}	a_{13}	a_{11}	a_{15}	a_{12}	a_{10}
a_4	0	a_9	a_8	a_7	a_1	a_2	a_3	a_4	a_5	a_6	a_{15}	a_{12}	a_{14}	a_{11}	a_{10}	a_{13}
a_5	0	a_8	0	a_8	a_2	0	a_2	a_5	0	a_5	a_5	a_5	a_5	a_8	a_8	a_2
a_6	0	a_7	a_8	a_9	a_3	a_2	a_1	a_6	a_5	a_4	a_{12}	a_{15}	a_{13}	a_{10}	a_{11}	a_{14}
a_7	0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
a_8	0	a_2	0	a_2	a_5	0	a_5	a_8	0	a_8	a_8	a_8	a_5	a_2	a_2	a_5
a_9	0	a_3	a_2	a_1	a_6	a_5	a_4	a_9	a_8	a_7	a_{11}	a_{10}	a_{15}	a_{14}	a_{13}	a_{12}
a_{10}	0	a_{13}	a_2	a_{14}	a_{15}	a_5	a_{12}	a_{10}	a_8	a_{11}	a_7	a_9	a_6	a_1	a_3	a_4
a_{11}	0	a_{14}	a_2	a_{13}	a_{12}	a_5	a_{15}	a_{11}	a_8	a_{10}	a_9	a_7	a_4	a_3	a_1	a_6
a_{12}	0	a_{10}	a_8	a_{11}	a_{14}	a_5	a_{13}	a_{12}	a_5	a_{15}	a_6	a_4	a_1	a_7	a_9	a_3
a_{13}	0	a_{12}	a_5	a_{15}	a_{11}	a_8	a_{10}	a_{13}	a_2	a_{14}	a_1	a_3	a_7	a_6	a_4	a_9
a_{14}	0	a_{15}	a_5	a_{12}	a_{10}	a_8	a_{11}	a_{14}	a_2	a_{13}	a_3	a_1	a_9	a_4	a_6	a_7
a_{15}	0	a_{11}	a_8	a_{10}	a_{13}	a_2	a_{14}	a_{15}	a_5	a_{12}	a_4	a_6	a_3	a_9	a_7	a_1

Table 2. Multiplication table of W.

From the context of algebra, it can be easily proved that W is an abelian group under component-wise addition. The other criteria of the ring can be verified by using Table 2.

The ring W is commutative because

$$a_i \cdot a_j = a_j \cdot a_i \quad \text{for} \quad 0 \leq i, j \leq 15 \qquad \text{(see Table 2).}$$

Hence, W is a commutative ring. ■

We choose an element $1+X+Y+YX$ from $\mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4$ and denote it by U; i.e., $U=1+X+Y+YX$. So, $UW=\{0,\ 3+Y3,\ 2+Y2,\ 1+Y,\ X+YX,\ X2+YX2,\ X3+YX3,\ 1+X+Y+YX,\ 2+X2+Y2+YX2,\ 3+X3+Y3+YX3,\ 3+X+Y3+YX,\ 1+X3+Y+YX3,\ 2+X+Y2+YX,\ 3+X2+Y3+YX2,\ 1+X2+Y+YX2,\ 2+X3+Y2+YX3\}$. It shows that $W\cap UW=\{0\}$, which in turn implies that $W+UW=\mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4$ as $W+UW$ is a subring of $\mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4$ and $\mid W+UW\mid=256$. Therefore, $\mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4=W+UW$.

Let x^2+x+1 be a basic irreducible polynomial over $\mathbb{Z}_4$. Then $\frac{\mathbb{Z}_4[x]}{\langle x^2+x+1\rangle}$ is called the Galois extension ring of $\mathbb{Z}_4$ and is denoted by GR(4,2). If w is a root of x^2+x+1, then $\frac{\mathbb{Z}_4[x]}{\langle x^2+x+1\rangle}\cong GR(4,2)\cong\mathbb{Z}_4[w]$.

Lemma 2.3. *The ring W is isomorphic to the ring $\mathbb{Z}_4[w]$.*

Proof. We consider an explicit form of a mapping from W to $\mathbb{Z}_4[w]$ as follows: $0\longmapsto 0$, $X+Y3+YX3\longmapsto w$, $X2+Y2+YX2\longmapsto 2w$, $X3+Y+YX\longmapsto 3w$, $1+X+Y3\longmapsto 3w^2$, $2+X2+Y2\longmapsto 2w^2$, $3+X3+Y\longmapsto w^2$, $1+YX\longmapsto 1$, $2+YX2\longmapsto 2$, $3+YX3\longmapsto 3$, $1+X2+Y2+YX3\longmapsto 2w+1$, $3+X2+Y2+YX\longmapsto 2w+3$, $1+X3+Y+YX2\longmapsto 3w+1$, $2+X3+Y+YX3\longmapsto 3w+2$, $2+X+Y3+YX\longmapsto w+2$, $3+X+Y3+YX2\longmapsto w+3$. It is clear from Table 2 that the mapping is a ring isomorphism. Therefore, $W\cong\mathbb{Z}_4[w]$. ■

Theorem 2.1. *The ring $M_2(\mathbb{Z}_4)$ is isomorphic to the ring $\mathbb{Z}_4[w]+U\mathbb{Z}_4[w]$.*

Proof. We have,

$$\begin{aligned} M_2(\mathbb{Z}_4) &\cong \mathbb{Z}_4+X\mathbb{Z}_4+Y\mathbb{Z}_4+YX\mathbb{Z}_4 \text{ from Lemma 2.1}\\ &\cong W+UW\\ &\cong \mathbb{Z}_4[w]+U\mathbb{Z}_4[w] \text{ from Lemma 2.3.}\end{aligned}$$

Therefore, $M_2(\mathbb{Z}_4)\cong\mathbb{Z}_4[w]+U\mathbb{Z}_4[w]$. ■

We get that the rings W and $\mathbb{Z}_4[w]$ are commutative; however, their extensions $W+UW$ and $\mathbb{Z}_4[w]+U\mathbb{Z}_4[w]$ are non-commutative. Summarizing the above discussion, we have $\mathcal{R}\cong\mathbb{Z}_4[w]+U\mathbb{Z}_4[w]$, where $U^2=2U$, $U^3=0$, $2U=U2$ and $2U^2=0$.

We know that each element of $\mathbb{Z}_4$ has 2-adic representation $a+2b$, where $a,\ b\in\mathbb{Z}_2$, so is $\mathbb{Z}_4[w]$. Now, we define the Gray map on $\mathcal{R}$. To accomplish it, first, we define a mapping $\mathcal{R}$ to $\mathbb{Z}_4^2[w]$, and then define a mapping $\mathbb{Z}_4^2[w]$ to $\mathbb{F}_4^4$ so that the Gray map is

$$\begin{aligned}\Phi:\quad & \mathcal{R} \longrightarrow \mathbb{F}_4^4\\ & a+2b+Uc+U2d \longmapsto (d,\ c+d,\ b+d,\ a+b+c+d),\end{aligned}$$

where $a, b, c, d \in \mathbb{F}_4$. This map can easily be extended to $\mathcal{R}^n$ component-wise. The Hamming weight w_H of $x \in \mathbb{F}_4^n$ is defined as the number of non-zero coordinates of x. For $x = a + 2b + Uc + U2d \in \mathcal{R}^n$, we define the Lee weight of x, denoted by $w_L(x)$, as

$$w_L(x) = w_H(d) + w_H(d + c) + w_H(d + b) + w_H(a + b + c + d).$$

For any x, $y \in \mathcal{R}^n$, the Lee distance $d_L(x, y)$ between x and y is the Lee weight of $x - y$, i.e., $d_L(x, y) = w_L(x - y)$. A linear code C of length n over $\mathcal{R}$ is an $\mathcal{R}$-submodule of $\mathcal{R}^n$. C is said to be a *free code* if C has a $\mathcal{R}$-basis. We define the *rank* of a code C as the cardinality of minimal generating set of C. The Lee distance of C is denoted by $d_L(C)$ and is defined by $d_L(C) = \min\{w_L(c) = \sum_{i=0}^{n-1} w_L(c_i) | c = (c_0, c_1, \ldots, c_{n-1}) \in C\}$. From the above discussion and definitions, we have the following result.

Theorem 2.2. *If C is a linear code over $\mathcal{R}$ of length n and size M with Lee distance d_L, then $\Phi(C)$ is a code of length $4n$ over $\mathbb{F}_4$ with size M.*

3. Cyclic codes over $M_2(\mathbb{Z}_4)$

Let τ be the standard cyclic shift operator on $\mathcal{R}^n$. A linear code C of length n over $\mathcal{R}$ is cyclic if $\tau(c) \in C$ whenever $c \in C$, i.e., if $(c_0, c_1, \ldots, c_{n-1}) \in C$, then $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. As usual, in the polynomial representation, a cyclic code of length n over $\mathcal{R}$ is an ideal of the quotient ring $\frac{\mathcal{R}[x]}{\langle x^n - 1\rangle}$.

Theorem 3.1. *A linear code $C = C_1 + UC_2$ of length n over $\mathcal{R}$ is cyclic if and only if C_1, C_2 are cyclic codes of length n over $\mathbb{Z}_4[w]$.*

Proof. Let $c_1 + Uc_2 \in C$, where $c_1 \in C_1$ and $c_2 \in C_2$. Then $\tau(c_1 + Uc_2) = \tau(c_1) + U\tau(c_2) \in C$, since C is cyclic and τ is a linear map. So, $\tau(c_1) \in C_1$ and $\tau(c_2) \in C_2$. Therefore, C_1, C_2 are cyclic codes.

Conversely, if C_1, C_2 are cyclic codes, then for any $c_1 + Uc_2 \in C$, where $c_1 \in C_1$ and $c_2 \in C_2$, we have $\tau(c_1) \in C_1$ and $\tau(c_2) \in C_2$, and so, $\tau(c_1 + Uc_2) = \tau(c_1) + U\tau(c_2) \in C$. Hence C is cyclic. ■

We assume that n is odd for the rest of this paper. Let $\mathcal{R}[x]$ be the ring of polynomials over the ring $\mathcal{R}$. We define a mapping

$$\begin{array}{rccc} \mu : & \mathcal{R}[x] & \longrightarrow & \mathbb{F}_4[x] \\ & \displaystyle\sum_{i=0}^{n} a_i x^i & \longmapsto & \displaystyle\sum_{i=0}^{n} \mu(a_i) x^i, \end{array}$$

where $\mu(a_i)$ denote reduction modulo 2 and U.

A polynomial $f \in \mathcal{R}[x]$ is called a basic irreducible polynomial if $\mu(f)$ is irreducible over $\mathbb{F}_4$. Two polynomials $f(x), g(x) \in \mathcal{R}[x]$ are said to be *coprime* if there exist $a(x), b(x) \in \mathcal{R}[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1.$$

The polynomial $x^n - 1$ can be factorized uniquely into pairwise coprime irreducible polynomials over $\mathbb{F}_4$. Let $x^n - 1 = f_1 f_2 f_3 \cdots f_m$, where f_i's are irreducible polynomials over $\mathbb{F}_4$.

Lemma 3.1. *Let f_i be a basic irreducible polynomial over $\mathcal{R}$ for $1 \leq i \leq m$. Then $\frac{\mathcal{R}[x]}{\langle f_i \rangle}$ is not a ring but a right module over $\mathcal{R}$.*

Proof. Since $\langle f_i \rangle$ is not two sided ideal of $\mathcal{R}[x]$, so $\frac{\mathcal{R}[x]}{\langle f_i \rangle}$ is not a ring for $1 \leq i \leq m$. Then each $\frac{\mathcal{R}[x]}{\langle f_i \rangle}$ is a right $\mathcal{R}$-module. ■

To prove our next results, we need a non-commutative analogue of the Chinese Remainder Theorem for modules.

Lemma 3.2. *Let n be an odd integer. Then*

$$\frac{\mathcal{R}[x]}{\langle x^n - 1 \rangle} = \bigoplus_{1}^{m} \frac{\mathcal{R}[x]}{\langle f_i \rangle}.$$

Proof. The proof follows from [6] and [11, Chapter 9]. ■

Theorem 3.2. *If f be an irreducible polynomial in $\mathbb{F}_4[x]$, then the right $\mathcal{R}$-modules of $\frac{\mathcal{R}[x]}{\langle f \rangle}$ are $\langle 0 \rangle, \langle 1 + \langle f \rangle \rangle, \langle U + \langle f \rangle \rangle, \langle 2U + \langle f \rangle \rangle, \langle (2 + Um_f) + \langle f \rangle \rangle, \langle 2 + \langle f \rangle \rangle, \langle \langle 2, U \rangle + \langle f \rangle \rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$.*

Proof. Let I be a non-zero right sub-module of $\frac{\mathcal{R}[x]}{\langle f \rangle}$ and $g(x) \in \mathcal{R}[x]$ such that $g(x) + \langle f \rangle \in I$ but $g(x) \notin \langle f \rangle$. If $gcd(\mu(g(x)),\ f(x)) = 1$, then g is invertible modulo f. So, $I = \langle 1 + \langle f \rangle \rangle = \frac{\mathcal{R}[x]}{\langle f \rangle}$.

If $gcd(\mu(g(x)), f(x)) = f(x)$, then there exist $g_1(x)$, $g_2(x)$, $g_3(x)$, $g_4(x) \in \mathbb{F}_4[x]$ such that $g(x) = g_1(x) + Ug_2(x) + 2g_3(x) + 2Ug_4(x)$ with $gcd((g_1(x)), f(x)) = f(x)$. Therefore, $g(x) + \langle f \rangle = Ug_2(x) + 2g_3(x) + 2Ug_4(x) + \langle f \rangle$.

Case 1. If $gcd(g_2(x), f(x)) = f(x)$, then $g(x) + \langle f \rangle = 2g_3(x) + 2Ug_4(x) + \langle f \rangle$. It follows that $I = \langle 2 + \langle f \rangle \rangle$.

Subcase a. $gcd(g_3(x), f(x)) = f(x)$, then $I = \langle 2U + \langle f \rangle \rangle$.

Subcase b. $gcd(g_3(x), f(x)) = 1$, then $I = \langle 2 + \langle f \rangle \rangle$.

Case 2. If $gcd(g_2(x), f(x)) = 1$, then there exists $g_2^{-1}(x) \in \mathbb{F}_4[x]$ such that $g_2(x)g_2^{-1}(x) \equiv 1 \pmod f$. Therefore, $2U = 2g(x)g_2^{-1}(x)$. Consequently, $2U + \langle f\rangle = 2g(x)g_2^{-1}(x) + \langle f\rangle \in I$. It follows that $Ug_2(x) + 2g_3(x) + \langle f\rangle = g(x) + 2Ug_4(x) + \langle f\rangle \in I$.

Subcase a. $gcd(g_3(x), f(x)) = f(x)$, then $I = \langle U + \langle f\rangle\rangle$.

Subcase b. $gcd(g_3(x), f(x)) = 1$, then $g_3^{-1}(x) \in \mathbb{F}_4[x]$ such that $g_3(x)g_3^{-1}(x) \equiv 1 \pmod f$. Hence, $2 + Ug_2(x)g_3^{-1}(x) + \langle f\rangle \in I$, i.e., $\langle 2 + Um_f + \langle f\rangle\rangle = I$, where $m_f = g_2(x)g_3^{-1}(x)$ is a unit in $\frac{\mathbb{F}_4[x]}{\langle f\rangle}$. Since $gcd(g_2(x), f(x)) = 1$, $gcd(g_3(x), f(x)) = 1$, then there exist $a_1(x)$, $a_2(x)$, $b_1(x)$, $b_2(x) \in \mathbb{F}_4[x]$ such that $g_2(x)a_1(x) + f(x)a_2(x) = 1$, $g_3(x)b_1(x) + f(x)b_2(x) = 1$. Therefore,

$$\begin{aligned} Ub_1(x) + \langle f\rangle &= (Ug_2(x) + \langle f\rangle)(a_1(x)b_1(x) + \langle f\rangle) \\ 2a_1(x) + \langle f\rangle &= (Ug_3(x) + \langle f\rangle)(a_1(x)b_1(x) + \langle f\rangle) \\ Ub_1(x) + 2a_1(x) + \langle f\rangle &= (Ug_2(x) + 2g_3(x)\langle f\rangle)(a_1(x)b_1(x) + \langle f\rangle). \end{aligned}$$

It follows that $I = \langle\langle U, 2\rangle + \langle f\rangle\rangle$. ∎

Theorem 3.3. *Let $x^n - 1 = f_1f_2f_3\cdots f_m$, where f_i's are monic basic irreducible pairwise coprime polynomials in $\mathcal{R}[x]$. Let $\hat{f}_i = \frac{x^n-1}{f_i}$. Then any ideal in $\frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$ is the sum of the right sub-modules: $\left\langle \hat{f}_i + \langle x^n - 1\rangle \right\rangle$, $\left\langle 2\hat{f}_i + \langle x^n - 1\rangle \right\rangle$, $\left\langle U\hat{f}_i + \langle x^n - 1\rangle \right\rangle$, $\left\langle 2U\hat{f}_i + \langle x^n - 1\rangle \right\rangle$, $\left\langle (2+Um_f)\hat{f}_i + \langle x^n - 1\rangle \right\rangle$, $\left\langle \langle 2, U\rangle\, \hat{f}_i + \langle x^n - 1\rangle \right\rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f\rangle}$.*

Proof. Proof of the theorem follows from the Chinese Remainder Theorem for modules and the right $\mathcal{R}$-modules of $\frac{\mathcal{R}[x]}{\langle f\rangle}$. ∎

Theorem 3.4. *Let C be a cyclic code of length n over $\mathcal{R}$. Then there exists a family of pairwise coprime monic polynomials $F_0, F_1, \ldots, F_6 \in \mathbb{F}_4[x]$ such that $F_0F_1\cdots F_6 = x^n-1$ and $C = \langle\hat{F}_1\rangle \oplus \langle U\hat{F}_2\rangle \oplus \langle 2\hat{F}_3\rangle \oplus \langle 2U\hat{F}_4\rangle \oplus \langle(2+Um_f)\hat{F}_5\rangle \oplus \left\langle\, \langle 2, U\rangle\, \hat{F}_6\right\rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f\rangle}$. Moreover, $|C| = 4^\alpha$, where $\alpha = 4degF_1 + 2degF_2 + 2degF_3 + degF_4 + 2degF_5 + 3degF_6$.*

Proof. The first part follows from a similar argument of Theorem 2 in [5].

Now, to compute $|C|$ we use the result $C = \langle\hat{F}_1\rangle \oplus \langle U\hat{F}_2\rangle \oplus \langle 2\hat{F}_3\rangle \oplus \langle 2U\hat{F}_4\rangle \oplus \langle(2 + Um_f)\hat{F}_5\rangle \oplus \left\langle\, \langle 2, U\rangle\, \hat{F}_6\right\rangle$, which implies that $|C| =| \hat{F}_1 | \cdot | U\hat{F}_2 | \cdot | 2\hat{F}_3 | \cdot | 2U\hat{F}_4 | \cdot | (2 + Um_f)\hat{F}_5 | \cdot | \langle 2, U\rangle\hat{F}_6 |$. The rest of the proof follows from the fact that $| \hat{F}_1 |= 4^{4degF_1}$, $|U\hat{F}_2| = 4^{2degF_2}$, $| 2\hat{F}_3 |= 4^{2degF_3}$, $| 2U\hat{F}_4 |= 4^{degF_4}$, $| (2 + Um_f)\hat{F}_5 |= 4^{2degF_5}$, $| \langle 2, U\rangle\hat{F}_6 |= 4^{3degF_6}$. ∎

Theorem 3.5. *Let C be a cyclic code of length n over $\mathcal{R}$ with $C = \left\langle \hat{F_1} \right\rangle \oplus \left\langle U\hat{F_2} \right\rangle \oplus \left\langle 2\hat{F_3} \right\rangle \oplus \left\langle 2U\hat{F_4} \right\rangle \oplus \left\langle (2+Um_f)\hat{F_5} \right\rangle \oplus \left\langle \langle 2, U\rangle \hat{F_6} \right\rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f\rangle}$ and $F = \hat{F_1} + U\hat{F_2} + 2\hat{F_3} + 2U\hat{F_4} + (2+Um_f)\hat{F_5} + \langle 2, U\rangle \hat{F_6}$. Then $C = \langle F\rangle$.*

Proof. For any two distinct i, j, we have $(x^n - 1) \mid \hat{F_i}\hat{F_j}$, where $1 \leq i, j \leq 6$. So, $\hat{F_i}\hat{F_j} = 0$. Also, for any i with $1 \leq i \leq 6$, $F_i, \hat{F_i}$ are coprime and $F_i\hat{F_i} = 0$. Since $F_i, \hat{F_i}$ are coprime, there exist a_i, b_i such that $(a_1F_1 + b_1\hat{F_1})(a_2F_2 + b_2\hat{F_2})(a_3F_3 + b_3\hat{F_3})(a_4F_4 + b_4\hat{F_4})(a_5F_5 + b_5\hat{F_5}) = 1$. It shows that,

$$\begin{aligned}&a_1F_1a_2F_2a_3F_3a_4F_4a_5F_5 + b_1\hat{F_1}a_2F_2a_3F_3a_4F_4a_5F_5+\\&a_1F_1b_2\hat{F_2}a_3F_3a_4F_4a_5F_5 + a_1F_1a_2F_2b_3\hat{F_3}a_4F_4a_5F_5+\\&a_1F_1a_2F_2a_3F_3b_4\hat{F_4}a_5F_5 + a_1F_1a_2F_2a_3F_3a_4F_4b_5\hat{F_5} = 1.\end{aligned}$$

On multiplying both side by $\hat{F_6}$, we obtain $\hat{F_6}a_1F_1a_2F_2a_3F_3a_4F_4a_5F_5 = \hat{F_6}$. We have $F = \hat{F_1} + U\hat{F_2} + 2\hat{F_3} + 2U\hat{F_4} + (2+Um_f)\hat{F_5} + \langle 2, U\rangle \hat{F_6}$. As a result, we see that $Fa_1F_1a_2F_2a_3F_3a_4F_4a_5F_5 = \langle 2, U\rangle \hat{F_6}a_1F_1a_2F_2a_3F_3a_4F_4a_5F_5$, which in turn implies that $Fa_1F_1a_2F_2a_3F_3a_4F_4a_5F_5 = \langle 2, U\rangle\hat{F_6}$. Hence, $\langle 2, U\rangle\hat{F_6} \in \langle F\rangle$. Continuing this process, we obtain $\hat{F_1}$, $U\hat{F_2}$, $2\hat{F_3}$, $2U\hat{F_4}$, $(2+Um_f)\hat{F_5}$, $\langle 2, U\rangle \hat{F_6} \in \langle F\rangle$. Consequently, $C = \langle F\rangle$. ■

Let us denote $R = \frac{\mathbb{F}_4[x]}{\langle x^n - 1\rangle}$.

Theorem 3.6. *Let C be a cyclic code of length n over $\mathcal{R}$. Then there exists a family of polynomials $F, G, H, Q, T \in \mathbb{F}_4[x]$ which are the divisors of $x^n - 1$ such that $C = \langle F\rangle_R \oplus U\langle G\rangle_R \oplus 2\langle H\rangle_R \oplus 2U\langle Q\rangle_R \oplus (2+Um_f)\langle T\rangle_R$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f\rangle}$. Moreover, $|C| = 4^{5n-(degF+degG+degH+degQ+degT)}$.*

Proof. A similar argument as in [5]. ■

4. Self-dual cyclic codes over $M_2(\mathbb{Z}_4)$

For given $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathcal{R}^n$, the Euclidean scalar product (or dot product) of **x, y** is $\mathbf{x}\cdot\mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n \pmod 4$. Two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathcal{R}^n$ are called orthogonal if $\mathbf{x}\cdot\mathbf{y} = 0$. For a linear code C over $\mathcal{R}$, its dual code $C^\perp$ is the set of words over $\mathcal{R}$ that are orthogonal to all codewords of C, i.e., $C^\perp = \{\mathbf{x} \in \mathcal{R}^n \mid \mathbf{x}\cdot\mathbf{y} = 0, \forall y \in C\}$. A code C is called self-orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$.

Let $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k$ be a polynomial of degree k with $a_k \neq 0$, $a_0 \neq 0$. The reciprocal $f^*(x)$ of $f(x)$ is defined by

$$f^*(x) = a_0^{-1}x^kf(x^{-1}).$$

Theorem 4.1. *Let C be a cyclic code of length n over $\mathcal{R}$ with $C = \langle \hat{F_1} \rangle \oplus \langle U\hat{F_2} \rangle \oplus \langle 2\hat{F_3} \rangle \oplus \langle 2U\hat{F_4} \rangle \oplus \langle (2+Um_f)\hat{F_5} \rangle \oplus \langle \langle 2,U \rangle \hat{F_6} \rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Then $C^{\perp} = \langle \hat{F_0^*} \rangle \oplus \langle U\hat{F_2^*} \rangle \oplus \langle 2\hat{F_3^*} \rangle \oplus \langle 2U\hat{F_6^*} \rangle \oplus \langle (2+Um_f)\hat{F_5^*} \rangle \oplus \langle \langle 2,U \rangle \hat{F_4^*} \rangle$ and $\mid C^{\perp} \mid = 4^{4degF_0+2degF_2+2degF_3+3degF_4+2degF_5+degF_6}$.*

Proof. From the Theorem 3.4, $\mid C \mid = 4^{4degF_1+2degF_2+2degF_3+degF_4+2degF_5+3degF_6}$. Since $\mid C \mid\mid C^{\perp} \mid = 4^{4n}$ and $n = degF_1 + degF_2 + degF_3 + degF_4 + degF_5 + degF_6$, so $\mid C^{\perp} \mid = 4^{4degF_0+2degF_2+2degF_3+3degF_4+2degF_5+degF_6}$.

We denote $C^* = \langle \hat{F_0^*} \rangle \oplus \langle U\hat{F_2^*} \rangle \oplus \langle 2\hat{F_3^*} \rangle \oplus \langle 2U\hat{F_6^*} \rangle \oplus \langle (2+Um_f)\hat{F_5^*} \rangle \oplus \langle \langle 2,U \rangle \hat{F_4^*} \rangle$. For $0 \le i,j \le 6$, if $i+1 = 7-j+1$, i.e., $i = 7-j$, we see that $\hat{F}_{i+1}\hat{F}^*_{7-i+1} = 0$. If $i+1 \neq 7-j+1$, i.e., $i \neq 7-j$, then we have $x^n-1 \mid \hat{F}_{i+1}\hat{F}^*_{7-i+1}$. Thus, $\hat{F}_{i+1}\hat{F}^*_{7-i+1} = 0$. Therefore, $C^* \subseteq C^{\perp}$. Note that $\mid \hat{F_0^*} \mid = 4^{4degF_0}$, $\mid U\hat{F_2^*} \mid = 4^{2degF_2}$, $\mid 2\hat{F_3^*} \mid = 4^{2degF_3}$, $\mid 2U\hat{F_6^*} \mid = 4^{degF_6}$, $\mid (2+Um_f)\hat{F_5^*} \mid = 4^{2degF_5}$, $\mid \langle 2,U \rangle \hat{F_4^*} \mid = 4^{degF_4}$. Hence $|C^*| = 4^{4degF_0+2degF_2+2degF_3+3degF_4+2degF_5+degF_6} = |C^{\perp}|$. Consequently, $C^* = C^{\perp}$. ■

Theorem 4.2. *Let C be a cyclic code of length n over $\mathcal{R}$ with C and $C^{\perp}$ mentioned as in Theorem 4.1 and denote $F^* = \hat{F_0^*} + U\hat{F_2^*} + 2\hat{F_3} + 2U\hat{F_6^*} + (2+Um_f)\hat{F_5^*} + \langle 2,U \rangle \hat{F_4^*}$. Then $C^{\perp} = \langle F^* \rangle$.*

Proof. The result follows from a similar argument as in the proof of Theorem 3.5 as $\hat{F_i^*}\hat{F_j^*} = 0$ and $\hat{F_i^*}, F_j^*$ are coprime for $0 \le i,j \le 6$. ■

Theorem 4.3. *Let C be a cyclic code of length n over $\mathcal{R}$. Then there exists a family of polynomials $F^*, G^*, H^*, Q^*, T^* \in \mathbb{F}_4[x]$ which are the divisors of x^n-1 such that $C^{\perp} = \langle F^* \rangle_R \oplus U \langle G^* \rangle_R \oplus 2 \langle H^* \rangle_R \oplus 2U \langle Q^* \rangle_R \oplus (2+Um_f) \langle T^* \rangle_R$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Moreover, $|C^{\perp}| = 4^{5n-(degF^*+degG^*+degH^*+degQ^*+degT^*)}$.*

Proof. Follows from Theorem 3.6. ■

We now prove the main result of this section, a condition for a cyclic code C over $\mathcal{R}$ to be self-dual. From Theorem 3.5 and Theorem 4.2, we can see that a cyclic code C is self-dual if and only if $F = F^*$. It shows that

$$\hat{F_1} = \hat{F_0^*}, \quad \hat{F_2} = \hat{F_2^*}, \quad \hat{F_3} = \hat{F_3^*}, \quad \hat{F_4} = \hat{F_6^*}, \quad \hat{F_5} = \hat{F_5^*}, \quad \hat{F_6} = \hat{F_4^*}.$$

Again since $\hat{F_i} = \frac{x^n-1}{F_i}$, $\hat{F_j^*} = \frac{x^n-1}{F_j^*}$ and $\hat{F_i} = \hat{F_j^*}$, we have $F_i = F_j^*$. Hence, we state the following results.

Theorem 4.4. *Let C be a cyclic code of length n over $\mathcal{R}$ with $C = \langle \hat{F_1} \rangle \oplus \langle U\hat{F_2} \rangle \oplus \langle 2\hat{F_3} \rangle \oplus \langle 2U\hat{F_4} \rangle \oplus \langle (2+Um_f)\hat{F_5} \rangle \oplus \langle \langle 2,U \rangle \hat{F_6} \rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Then C is a self-dual code if and only if $F_1 = F_0^*$, $F_2 = F_2^*$, $F_3 = F_3^*$, $F_4 = F_6^*$, $F_5 = F_5^*$.*

Theorem 4.5. *Let C be a cyclic code of length n over $\mathcal{R}$ with $C = \langle F \rangle_R \oplus U \langle F \rangle_R \oplus 2 \langle F \rangle_R \oplus 2U \langle F \rangle_R \oplus (2+Um_f) \langle F \rangle_R$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Then C is a self-dual code if and only if $F = F^*$, $G = G^*$, $H = H^*$, $Q = Q^*$, $T = T^*$.*

5. HERMITIAN SELF-DUAL CYCLIC CODES OVER $M_2(\mathbb{Z}_4)$

For any two codewords $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathcal{R}^n$, the Hermitian inner product is defined as

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x} \cdot \bar{\mathbf{y}} = x_1 \bar{y_1} + x_2 \bar{y_2} + \cdots + x_n \bar{y_n},$$

where "$\bar{\mathbf{y}}$" is called the conjugation of $\mathbf{y}$, for example, $\bar{0} = 0$, $\bar{1} = 1$, $\bar{w} = w^2$, $\bar{w^2} = w$. The Hermitian dual of C, denoted by $C^{\perp_H}$, is define as

$$C^{\perp_H} = \{ \mathbf{x} \in \mathcal{R}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0, \forall y \in C \}.$$

We can see that $\bar{C}^{\perp} = C^{\perp_H}$. As usual C is called Hermitian self-orthogonal and Hermitian self-dual if $C \subseteq C^{\perp_H}$ and $C = C^{\perp_H}$, respectively.

Let $f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + a_k x^k$ be a polynomial of degree k with $a_k \neq 0$, $a_0 \neq 0$. The reciprocal $f^*(x)$ of $f(x)$ is defined by

$$f^*(x) = a_0^{-1} x^k f(x^{-1}).$$

We denote $\bar{f}(x) = a_0^2 + a_1^2 x + \cdots + a_{k-1}^2 x^{k-1} + a_k^2 x^k$. It is easy to check that $(\bar{f^*})(x) = (\bar{f})^*(x)$. All the theorems proved in previous section are true with respect to Hermitian inner product as well. So, we state them here without narrating the proofs elaborately.

Theorem 5.1. *Let C be a cyclic code of length n over $\mathcal{R}$ with $C = \langle \hat{F}_1 \rangle \oplus \langle U\hat{F}_2 \rangle \oplus \langle 2\hat{F}_3 \rangle \oplus \langle 2U\hat{F}_4 \rangle \oplus \langle (2+Um_f)\hat{F}_5 \rangle \oplus \langle \langle 2, U \rangle \hat{F}_6 \rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Then $C^{\perp_H} = \langle \hat{\bar{F}}_0^* \rangle \oplus \langle U\hat{\bar{F}}_2^* \rangle \oplus \langle 2\hat{\bar{F}}_3^* \rangle \oplus \langle 2U\hat{\bar{F}}_6^* \rangle \oplus \langle (2+Um_f)\hat{\bar{F}}_5^* \rangle \oplus \langle \langle 2, U \rangle \hat{\bar{F}}_4^* \rangle$ and $\mid C^{\perp_H} \mid = 4^{4degF_0+2degF_2+2degF_3+3degF_4+2degF_5+degF_6}$.*

Theorem 5.2. *Let C be a cyclic code of length n over $\mathcal{R}$ with C and $C^{\perp}$ as referred in Theorem 5.1, and $\bar{F}^* = \hat{\bar{F}}_0^* + U\hat{\bar{F}}_2^* + 2\hat{\bar{F}}_3 + 2U\hat{\bar{F}}_6^* + (2+Um_f)\hat{\bar{F}}_5^* + \langle 2, U \rangle \hat{\bar{F}}_4^*$. Then $C^{\perp_H} = \langle \bar{F}^* \rangle$.*

Theorem 5.3. *Let C be a cyclic code of length n over $\mathcal{R}$. Then there exists a family of polynomials $\bar{F}^*, \bar{G}^*, \bar{H}^*, \bar{Q}^*, \bar{T}^* \in \mathbb{F}_4[x]$ which are the divisors of $x^n - 1$ such that $C^{\perp_H} = \langle \bar{F}^* \rangle_R \oplus U \langle \bar{G}^* \rangle_R \oplus 2 \langle \bar{H}^* \rangle_R \oplus 2U \langle \bar{Q}^* \rangle_R \oplus (2+Um_f) \langle \bar{T}^* \rangle_R$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Moreover, $|C^{\perp_H}| = 4^{5n-(degF^*+degG^*+degH^*+degQ^*+degT^*)}$.*

Theorem 5.4. *Let C be a cyclic code of length n over $\mathcal{R}$ with $C = \langle \hat{F}_1 \rangle \oplus \langle U\hat{F}_2 \rangle \oplus \langle 2\hat{F}_3 \rangle \oplus \langle 2U\hat{F}_4 \rangle \oplus \langle (2+Um_f)\hat{F}_5 \rangle \oplus \langle \langle 2, U\rangle \hat{F}_6 \rangle$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Then C is a Hermitian self-dual code if and only if*

$$\hat{F}_1 = \hat{\bar{F}}_0^*, \quad \hat{F}_2 = \hat{\bar{F}}_2^*, \quad \hat{F}_3 = \hat{\bar{F}}_3^*, \quad \hat{F}_4 = \hat{\bar{F}}_6^*, \quad \hat{F}_5 = \hat{\bar{F}}_5^*, \quad \hat{F}_6 = \hat{\bar{F}}_4^*.$$

Proof. A cyclic code C is Hermitian self-dual if and only if $C = C^{\perp_H}$. Therefore, the desired result is an immediate consequence of Theorem 3.5 and Theorem 5.2. ∎

Theorem 5.5. *Let C be a cyclic code of length n over $\mathcal{R}$ with $C = \langle F \rangle_R \oplus U \langle F \rangle_R \oplus 2 \langle F \rangle_R \oplus 2U \langle F \rangle_R \oplus (2+Um_f) \langle F \rangle_R$, where m_f is a unit in $\frac{\mathbb{F}_4[x]}{\langle f \rangle}$. Then C is a Hermitian self-dual code if and only if*

$$F = \bar{F}^*, \quad G = \bar{G}^*, \quad H = \bar{H}^*, \quad Q = \bar{Q}^*, \quad T = \bar{T}^*.$$

Proof. A cyclic code C is Hermitian self-dual if and only if $C = C^{\perp_H}$. Thus, the required result can be proved by comparing Theorem 3.6 with Theorem 5.3. ∎

Example 5.1. The factorization of $x^7 - 1$ is $(x-1)(x^3+x+1)(x^3+x^2+1)$ over $\mathbb{F}_4$. Let $f_1 = (x-1)$, $f_2 = (x^3+x+1)$ and $f_3 = (x^3+x^2+1)$, then $f_1 = f_1^*$, $f_2 = f_3^*$ and $f_3 = f_2^*$. The following cyclic codes of length 7 over $\mathcal{R}$ are self-dual (Euclidean) codes and their Gray images $\Phi(C)$ have the parameter $[28, 14, 4]$ over $\mathbb{F}_4$.

$$\begin{array}{lllll} \langle f_1 f_2, & r f_2 f_3 \rangle, & \langle f_1 f_3, & r f_2 f_3 \rangle, & \text{where } r \in \{U, 2, 2+U\}, \\ \langle 2U f_1 f_3, & 2 f_1 f_2, & U f_1 f_3, & s f_2 f_3 \rangle, & \text{where } s \in \{2, 2+U\}, \\ \langle 2U f_1 f_2, & 2 f_1 f_3, & U f_1 f_3, & t f_2 f_3 \rangle, & \text{where } t \in \{2, 2+U\}. \end{array}$$

Example 5.2. The factorization of $x^5 - 1$ is $(x-1)(x^2+wx+1)(x^2+w^2x+1)$ over $\mathbb{F}_4$. Let $f_1 = (x-1)$, $f_2 = (x^2+wx+1)$ and $f_3 = (x^2+w^2x+1)$, then $f_1 = \bar{f}_1^*$, $f_2 = \bar{f}_3^*$ and $f_3 = \bar{f}_2^*$. The following cyclic codes of length 5 over $\mathcal{R}$ are self-dual (Hermitian) codes and their Gray images $\Phi(C)$ have the parameter $[20, 10, 4]$ over $\mathbb{F}_4$.

$$\begin{array}{lllll} \langle f_1 f_2, & r f_2 f_3 \rangle, & \langle f_1 f_3, & r f_2 f_3 \rangle, & \text{where } r \in \{U, 2, 2+U\}, \\ \langle 2U f_1 f_3, & 2 f_1 f_2, & U f_1 f_3, & s f_2 f_3 \rangle, & \text{where } s \in \{2, 2+U\}, \\ \langle 2U f_1 f_2, & 2 f_1 f_3, & U f_1 f_3, & t f_2 f_3 \rangle, & \text{where } t \in \{2, 2+U\}. \end{array}$$

Example 5.3. The factorization of $x^3 - 1$ is $(x+1)(x+w)(x+w^2)$ over $\mathbb{F}_4$. Let $f_1 = x+1$, $f_2 = x+w$ and $f_3 = x+w^2$. Some cyclic codes of length 3 over $\mathcal{R}$ with their Gray images $\Phi(C)$ are given below.

Generators	$\Phi(C)$
$\langle 2f_1, Uf_1, (2+U)f_2f_3\rangle$	[12, 8, 4]
$\langle 2f_1, Uf_1, 2Uf_2f_3\rangle$	[12, 7, 4]
$\langle f_3, 2f_1, Uf_1\rangle$	[12, 11, 2]
$\langle uf_1, (2+U)f_2f_3\rangle$	[12, 10, 2]

Example 5.4. The factorization of $x^6-1=(x^3-1)^2$ is $(x+1)^2(x+w)^2(x+w^2)^2$ over $\mathbb{F}_4$. Let $f_1=(x+1)^2$, $f_2=(x+w)^2$ and $f_3=(x+w^2)^2$. Some cyclic codes of length 6 over $\mathcal{R}$ with their Gray images $\Phi(C)$ are given below.

Generators	$\Phi(C)$
$\langle 2f_1, Uf_1, (2+U)f_2f_3\rangle$	[24, 19, 4]
$\langle f_3, 2f_1, Uf_1\rangle$	[24, 23, 2]

6. Conclusion

In 2013, Alahmadi *et al.* developed cyclic codes over finite matrix ring $M_2(\mathbb{F}_2)$ and their duals as right ideals in terms of two generators. Also, the structure of cyclic codes over $M_2(\mathbb{F}_2)$ has made the existence of infinitely many nontrivial cyclic codes for the Euclidean product. All this was derived for odd length codes. In our paper, we have taken the structure of $M_2(\mathbb{Z}_4)$ and constructed cyclic dual codes and cyclic self-dual codes over it which are even length codes over $M_2(\mathbb{F}_2)$. On the ring structures of [1] [5], it is not possible to construct negacyclic codes, as the characteristic of those rings is 2. But in our construction one can form negacyclic codes. Also, we welcome the readers to construct even length codes over $M_2(\mathbb{Z}_4)$. Another useful direction for further research is to consider LCD codes over $M_2(\mathbb{Z}_4)$.

Acknowledgments

The first author Sanjit Bhowmick is thankful to MHRD for financial support. Also, the authors would like to thank the anonymous referee for carefully reading our manuscript and giving valuable suggestions to improve the draft.

References

[1] A. Alahmadi, H. Sboui, P. Solé and O. Yemen, *Cyclic codes over $M_2(\mathbb{F}_2)$*, J. Franklin Institute **350** (9) (2013) 2837–2847.
https://doi.org/10.1016/j.jfranklin.2013.06.023

[2] C. Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Combin. Theory A **78** (1997) 92–119.
https://doi.org/10.1006/jcta.1996.2763

[3] M. Greferath and S.E. Schmidt, *Linear codes and rings of matrices*, Proceedings of AAECC 13, Hawaii, Springer, LNCS **1719** (1999) 160–169.
https://doi.org/10.1007/3-540-46796-3_16

[4] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory **40** (1994) 301–319.
https://doi.org/10.1109/18.312154

[5] R. Luo and U. Parampalli, *Cyclic codes over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$*, Cryptography and Communications **10** (6) (2018) 1109–1117.
https://doi.org/10.1007/s12095-017-0266-1

[6] F. Oggier, P. Solé and J.C. Belfiore, *Codes over matrix rings for space-time coded modulations*, IEEE Trans. Inform. Theory **58** (2) (2012) 734–746.
https://doi.org/10.1109/TIT.2011.2173732

[7] J. Pal, S. Bhowmick and S. Bagchi, *Cyclic codes over $\mathcal{M}_4(\mathbb{F}_2)$*, J. Appl. Math. Comput. **60** (2019) 749–756.
https://doi.org/10.1007/s12190-018-01235-w

[8] V. Pless, P. Solé and Z. Qian, *Cyclic self-dual $\mathbb{Z}_4$-codes*, Finite Fields and Their Appl. **3** (1997) 48–69.
https://doi.org/10.1006/ffta.1996.0172

[9] V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **42** (5) (1996) 1594–1600.
https://doi.org/10.1109/18.532906

[10] P. Solé, Codes Over Rings (Singapore, World Scientific, 2009).
https://doi.org/10.1142/7140

[11] R. Wisbauer, Foundations of Module and Ring Theory (Gordon and Breach, 1991).
https://doi.org/10.1201/9780203755532

Received 31 October 2020
Revised 24 March 2021
Accepted 25 May 2022