Self-Dual Cyclic Codes over $M_2(F_2+uF_2)$

Baoni Dong
School of Mathematics and Statistics, Shandong University of Technology, China

Abstract. In this paper, we consider the self-dual cyclic codes over the matrix ring $M_2(F_2+uF_2)$ that is isomorphic to $F_4+uF_4+vF_4+uvF_4$,where $u^2=0$ and $v^2=0$. We discuss the Gray map of the ring $M_2(F_2+uF_2)$. By the Gray map, some self-dual codes over F_4 are constructed.

Key words: matrix ring; gray map; self-dual cyclic codes; self-dual codes.

Introduction

Self-dual cyclic codes (Mathematics Subject Classification, 2000: 94B15） form an important class of linear codes due to their significance in coding theory and decoding theory. Recently, there are some papers on cyclic codes over rings, these codes caught the attention of researchers. A. Hammons et al. (1994; 301-319) studied some results on Z_4 codes, and they have shown a relationship between non-linear binary codes and Z_4- linear codes. Linear codes over the Z_2- matrix ring have been studied in the survey of F. Oggier et al. (2012: 734-746). The advantage of matrix rings is that they are non-commutative. On structures of cyclic codes and their dual codes over non-commutative finite rings forms an important and new topic in coding theory in the works of modern scientists within the field (Luo and Parampalli, 2018: 1109-1117; Bhowmick et al., 2018; Alahmadi et al., 2013: 2837-2847; Pal et al., 2019). R. Luo and U. Parampalli (2018: 1109-1117) studied cyclic codes over $M_2(F_2+uF_2)$. Some optimal cyclic codes over F_4 were obtained. S. Bhowmick, S. Bagchi, R.K. Bandi (2018) studied the structures of the ring $M_2(Z_4)$and then focused on algebraic structures of cyclic codes and self-dual cyclic codes over $M_2(Z_4)$. A. Alahmadi, H. Sboui, P. Sol´e, O. Yemen (2013) characterized cyclic codes and self-dual cyclic codes over the matrix ring $M_2(F_2)$. J. Pal, S. Bhowmick, B. Satya (2019) studied some results on cyclic codes over $M_2(F_2)$.

Motivated by R. Luo and U. Parampalli (2018: 1109-1117) and Bhowmick et al., (2018), in this paper, we study self-dual cyclic codes over the matrix ring $M_2(F_2+uF_2)$. The rest of this paper is organized as follows. In section 2, we review some results on the matrix ring, give a Gray map from this ring to F_4. In section 3, we study the dual codes of cyclic codes over $M_2(F_2+uF_2)$. A necessary and sufficient condition for cyclic codes to be self-dual is given. As an application, some self-dual codes over F_4 are obtained by the Gray map.

Cyclic codes over $M_2(F_2+uF_2)$

Gray map

In this paper, we denote the ring $M_2(F_2+uF_2)$ by R,where $u^2=0$. R is a non-commutative ring of matrices of order 2 over the ring F_2+uF_2.

Lemma 1. Let $M_2(F_2+uF_2)$ be a non-commutative ring of matrices of order 2 over the ring F_2+uF_2, and $M_2(F_2)$ be a non-commutative ring of matrices of order 2 over the finite field F_2. Then $M_2(F_2+uF_2)=M_2(F_2)+uM_2(F_2)$.

Proof. Let $A=\begin{pmatrix} a+ua' & b+ub' \\ c+uc' & d+ud' \end{pmatrix}\in M_2(F_2+uF_2)$, where $a,a',b,b',c,c',d,d'\in F_2$.

Then A can be written as

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}+u\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}=B+uB'$$

,

Where $B=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_2(F_2)$ $B'=\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\in M_2(F_2)$, which implies that $B+uB'\in M_2(F_2)+uM_2(F_2)$. Hence, $A\in M_2(F_2)+uM_2(F_2)$. Thus, $M_2(F_2+uF_2)\subseteq M_2(F_2)+uM_2(F_2)$.

Inversely, let $B=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B'=\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\in M_2(F_2)$. Then

$$B+uB'=\begin{pmatrix} a+ua' & b+ub' \\ c+uc' & d+ud' \end{pmatrix}\in M_2(F_2+uF_2)$$

which implies that $M_2(F_2+uF_2)\supseteq M_2(F_2)+uM_2(F_2)$. Thus, $M_2(F_2+uF_2)=M_2(F_2)+uM_2(F_2)$.

From the survey of C. Bachoc (1997: 92–119) we know that codes over $M_2(F_2)$ reduce to codes over F_4+vF_4 in the following way. Let us call η an element of $M_2(F_2)$ of characteristic polynomial x^2+x+1,where

$$\eta=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, i=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

are elements of order 2 in R satisfying the relationship $i\eta=\eta^2 i$. Then $F_2[\eta]\cong F_4$ and $M_2(F_2)=F_2[\eta]+iF_2[\eta]$. Setting $v=1+i$ and identifying the subring $F_2[\eta]$ with F_4, then $M_2(F_2)=F_4+vF_4$.

From Lemma 1, we can see that $R=F_4+uF_4+vF_4+uvF_4$,

Where $u^2=v^2=0$ and $uv=vu$.

We define a Gray map from R to F_4^4 as follows

$\varphi: R\to F_4^4$

$$a+ub+vc+uvd \mapsto (d,c+d,b+d,a+b+c+d)$$

where $a,b,c,d\in F_4$. One can verify that the map φ is a bijection. This map can be extended to R^n.The Hamming weight w_H of $x\in F_4^n$ is defined as the number of non-zero coordinates of x. For $x=a+ub+vc+uvd\in R^n$,we define the Lee weight of x, denoted by $w_L(x)$, as

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

For any $x, y \in R^n$, the Lee distance $d_L(x,y)$ between x and y is the Lee weight *of* $x-y$, that is $d_L(x,y)=w_L(x,y)$.

Definition 1. A linear code C of length n over R is a left $R-$submodule of R^n.

The linear code C is free if C has a left $R-$basis. The Lee distance of C is denoted by $d_L(C)$ and is defined by

$$d_L(C)=\min\left\{w_L(C)=\sum_{i=0}^{n-1}w_L(c_i)\,|\,c=(c_0,c_1,...,c_{n-1})\in C\right\}.$$

By the definition of the Gray map, we have the following lemma directly.

Lemma 2. If C is a linear code over R of length n with size M and minimum Lee distance d_L, then $\varphi(C)$ is a linear code of length $4n$ with dimension $\log_4^M$ and minimum Hamming distance d_L.

The following lemma shows that the Gray map preserves the self-duality.

*Lemma 3***.** If C is a linear self-dual code over R of length n, then $\varphi(C)$ is a linear self-dual code over F_4 of length $4n$.

Proof. Let C be a linear self-dual code. Then, for any $x, y \in C$, we have

$$x\cdot y=(a+ub+vc+uvd)\cdot(a'+ub'+vc'+uvd')=aa'+uab'+vac'+uvad'+uba'+uvbc'$$
$$+vca'+uvcb'+uvda'=aa'+u(ab'+ba')+v(ac'+ca')+uv(ad'+bc'+cb'+da')=0$$

which implies that $aa'=0$, $ab'+ba'=0$, $ac'+ca'=0$, $ad'+bc'+cb'+da'=0$.

Therefore, $\varphi(x)\cdot\varphi(y)=(d,c+d,b+d,a+b+c+d)\cdot(d',c'+d',b'+d',a'+b'+c'+d')=$
$$dd'+(c+d)(c'+d')+(b+d)(b'+d')+(a+b+c+d)(a'+b'+c'+d')=aa'+(ab'+ba')$$
$$+(ac'+ca')+(ad'+bc'+cb'+da')+4dd'+2(cc'+cd'+dc+bb'+bd'+db')=0.$$

That is $\varphi(C)$ is a self-orthogonal code. Since $|C|=|\varphi(C)|$, $|C^\perp|=|\varphi(C)^\perp|$, $|C^\perp|=|C|$, it follows that $|\varphi(C)|=|\varphi(C)^\perp|$. Hence, $\varphi(C)$ is a linear self-dual code.

Cyclic codes over $M_2(F_2+uF_2)$

*Definition 2***.** Let C be a linear code over R of length n. If for any codeword $(c_0,c_1,...,c_{n-1})\in C$, $(c_{n-1},c_0,c_1,...,c_{n-2})$ is still a code word in C, then C is said to be a cyclic code of length n over R.

In this section, we use $R[x]$ to represent the polynomial ring over R.Since x^n-1 is commutative, then we can make a quotient ring $R[x]/\langle x^n-1\rangle$. Clearly, $R[x]/\langle x^n-1\rangle$ is a left module over R. Define a map

$$\pi: R^n \to R[x]/\langle x^n-1\rangle$$
$$c=(c_0,c_1,...,c_{n-1})\ \square\ c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}.$$

Clearly, π is a left $R-$module isomorphism. The cyclic shift of a code word $c=(c_0,c_1,...,c_{n-1})$ is $(c_{n-1},c_0,c_1,...,c_{n-2})$ if and only if $\pi\cdot\pi(c)\in\pi(C)$, that is C is a cyclic code of length n over R if and only if $\pi(C)$ is a left ideal of $R[x]/\langle x^n-1\rangle$. In this paper, we identify the cyclic code with the left ideal of the quotient ring $R[x]/\langle x^n-1\rangle$.

Lemma 4. A linear code C of length n over R is cyclic if and only if C_1 and C_2 are cyclic codes of length n over F_4+vF_4 .

Proof. By the isomorphism of R, we have that $C=C_1+C_2$, where C_1,C_2 are linear codes over F_4+vF_4.Let $c_1+uc_2\in C$, where $c_1\in C_1$, $c_2\in C_2$.Let $C_1=\left(c_0^1,c_1^1,...,c_{n-1}^1\right)$ and $C_2=\left(c_0^2,c_1^2,...,c_{n-1}^2\right)$. Then $x\cdot\pi\left(c_1+uc_2\right)=x\cdot\pi\left(c_1\right)+ux\cdot\pi\left(c_2\right)\in C$. Therefor, $\pi\cdot\pi\left(c_1\right)\in C_1$ and $\pi\cdot\pi\left(c_2\right)\in C_2$,which implies that C_1 and C_2 are cyclic codes.

On the other hand, if C_1 and C_2 are cyclic codes, then for any $c_1+uc_2\in C$, where $c_1\in C_1$, $c_2\in C_2$, we have that $\pi\cdot\pi\left(c_1\right)\in C_1$, $\pi\cdot\pi\left(c_2\right)\in C_2$ and $x\cdot\pi\left(c_1+uc_2\right)=x\cdot\pi\left(c_1\right)+ux\cdot\pi\left(c_2\right)\in C$.Therefore C is a cyclic code.

Suppose that n is an odd positive integer in this paper. Define a map

$\mu:R[x]\to F_4[x]$

$$\sum_{i=0}^{n}a_ix^i\ \square\ \sum_{i=0}^{n}\mu(a_i)x^i,$$

where $\mu(a_i)$ denotes reduction of modulo u and v.

If $\mu(f)$ is irreducible over F_4, then the polynomial $f\in R[x]$ is called a basic irreducible polynomial. The polynomial x^n-1 factorizes uniquely into pairwise coprime irreducible polynomials over F_4. Let $x^n-1=f_1f_2f_3\cdots f_m$, where f_i are irreducible polynomials over F_4.

Lemma 5. Let $f_i\neq x^n-1$ be a basic irreducible polynomial over R. Then $R[x]/\langle f_i\rangle$ is not a ring but a left module over R.

Proof. Since $\langle f_i\rangle$ is not two sided ideal of $R[x]$, then $R[x]/\langle f_i\rangle$ is not a ring. It is only a left $R-$module.

By Lemma 5, we have the non-commutative analogy of the module's Chinese Remainder Theorem.

Lemma 6. Let n be an odd positive integer (Bhowmick et al., 2018). Then $R[x]/\langle x^n-1\rangle=\overset{m}{\underset{i=1}{\oplus}}R[x]/\langle f_i\rangle$, where $x^n-1=\prod_{r=1}^{m}f_i$ and $f_i^{'}$s are basic irreducible polynomials over R.

Lemma 7. If f is an irreducible polynomial over F_4 (Luo and Parampalli, 2018: 1109-1117), then the left $R-$submodules of $R[x]/\langle f\rangle$ are $\langle 0\rangle$, $\langle 1\rangle,\langle u\rangle,\langle v\rangle,\langle uv\rangle,\langle u\rangle+\langle v\rangle,\langle u+vh_\alpha\rangle$, where h_α is an unit in $F_4[x]/\langle f\rangle$.

Let h be a factor of x^n-1 in $F_4[x]$. From Lemmas 6 and 7, we have the follow result.

Lemma 8. Let $x^n-1=f_1f_2f_3\cdots f_m$,where $f_i^{'}$s are monic basic irreducible (Luo and Parampalli, 2018: 1109-1117) pairwise coprime polynomials in $R[x]$. Let $\hat{f}_i=\frac{x^n-1}{f_i}$. Then

any ideal in $R[x]/\langle x^n-1\rangle$ is the sum of the left $R-$submodules $\left\langle \hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle u\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle v\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle uv\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle (u+vh_\alpha)\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle (\langle u\rangle+\langle v\rangle)\hat{f}_i+\langle x^n-1\rangle \right\rangle$, where h_α is an unit in $F_4[x]/\langle f\rangle$.

Theorem 1. Let C be a cyclic code of odd length n over R.Then there exists a family of pairwise monic polynomials $F_0,F_1,F_2,F_3,F_4,F_5,F_6 \in F_4[x]$ such that

$$x^n-1=F_0F_1F_2F_3F_4F_5F_6 \text{ and}$$

$$C=\left\langle \hat{F}_1\right\rangle \oplus \left\langle u\hat{F}_2\right\rangle \oplus \left\langle v\hat{F}_3\right\rangle \oplus \left\langle uv\hat{F}_4\right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5\right\rangle \oplus \left\langle \left\langle u\hat{F}_6\right\rangle +\left\langle v\hat{F}_6\right\rangle \right\rangle,$$

where h_α is an unit in $F_4[x]/\langle x^n-1\rangle$. Furthermore, $|C|=a^\beta$, where $\beta=4\deg F_1+2\deg F_2+2\deg F_3+\deg F_4+2\deg F_5+3\deg F_6$.

Proof. Let $x^n-1=f_1f_2f_3\cdots f_t$ be a factorization of x^n-1 into a product of monic basic irreducible pairwise coprime polynomials. By Lemma 8, C is a sum of ideals of the form $\left\langle \hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle u\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle v\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle uv\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle (u+vh_\alpha)\hat{f}_i+\langle x^n-1\rangle \right\rangle$, $\left\langle (\langle u\rangle+\langle v\rangle)\hat{f}_i+\langle x^n-1\rangle \right\rangle$, where $1\le i\le m$. After reordering if necessary, we can assume that

$$\begin{aligned}
C=&\left\langle \hat{f}_{k_1+1}\right\rangle \oplus\cdots\oplus\left\langle \hat{f}_{k_1+k_2}\right\rangle\\
&\oplus\left\langle u\hat{f}_{k_1+k_2+1}\right\rangle\oplus\cdots\oplus\left\langle u\hat{f}_{k_1+k_2+k_3}\right\rangle\\
&\oplus\left\langle v\hat{f}_{k_1+k_2+k_3+1}\right\rangle\oplus\cdots\oplus\left\langle v\hat{f}_{k_1+k_2+k_3+k_4}\right\rangle\\
&\oplus\left\langle uv\hat{f}_{k_1+k_2+k_3+k_4+1}\right\rangle\oplus\cdots\oplus\left\langle uv\hat{f}_{k_1+k_2+k_3+k_4+k_5}\right\rangle\\
&\oplus\left\langle (u+vh_\alpha)\hat{f}_{k_1+k_2+k_3+k_4+k_5+1}\right\rangle\oplus\cdots\oplus\left\langle (u+vh_\alpha)\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6}\right\rangle\\
&\oplus\left\langle \left\langle u\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1}\right\rangle+\left\langle v\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1}\right\rangle\right\rangle\oplus\cdots\oplus\left\langle \langle u\rangle\hat{f}_t+\langle v\rangle\hat{f}_t\right\rangle,
\end{aligned}$$

where $k_1,k_2,k_3,k_4,k_5,k_6\ge 0$ and $k_1+k_2+k_3+k_4+k_5+k_6+1\le m$. Let $k_0=0$ and $k_1,k_2,\cdots,k_7$ be nonnegative integers such that $k_1+k_2+k_3+k_4+k_5+k_6+k_7=m$.

Define

$F_0 = f_{k_0+1} \cdots f_{k_0+k_1}, F_1 = f_{k_0+k_1+1} \cdots f_{k_0+k_1+k_2},$
$F_2 = f_{k_0+k_1+k_2+1} \cdots f_{k_0+k_1+k_2+k_3}, F_3 = f_{k_0+\cdots+k_3+1} \cdots f_{k_0+\cdots+k_4},$
$F_4 = f_{k_0+\cdots+k_4+1} \cdots f_{k_0+\cdots+k_5}, F_5 = f_{k_0+\cdots+k_5+1} \cdots f_{k_0+\cdots+k_6},$
$F_6 = f_{k_0+\cdots+k_6+1} \cdots f_m.$

Then, by the construction, it is clear that $F_0, F_1, \cdots, F_6$ are pairwise coprime, $x^n - 1 = F_0F_1F_2F_3F_4F_5F_6$

And

$$C = \left\langle \hat{F}_1 \right\rangle \oplus \left\langle u\hat{F}_2 \right\rangle \oplus \left\langle v\hat{F}_3 \right\rangle \oplus \left\langle uv\hat{F}_4 \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle \oplus \left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle.$$

Now, we compute the size $|C|$. We know that

$C = \left\langle \hat{F}_1 \right\rangle \oplus \left\langle u\hat{F}_2 \right\rangle \oplus \left\langle v\hat{F}_3 \right\rangle \oplus \left\langle uv\hat{F}_4 \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle \oplus \left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle$, which implies that $C = \left|\left\langle \hat{F}_1 \right\rangle\right| \cdot \left|\left\langle u\hat{F}_2 \right\rangle\right| \cdot \left|\left\langle v\hat{F}_3 \right\rangle\right| \cdot \left|\left\langle uv\hat{F}_4 \right\rangle\right| \cdot \left|\left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle\right| \cdot \left|\left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle\right|$.

The rest follows from the fact that $\left|\left\langle \hat{F}_1 \right\rangle\right| = 4^{4\deg F_1}, \left|\left\langle u\hat{F}_2 \right\rangle\right| = 4^{2\deg F_2}, \left|\left\langle v\hat{F}_3 \right\rangle\right| = 4^{2\deg F_3},$

$$\left|\left\langle uv\hat{F}_4 \right\rangle\right| = 4^{\deg F_4}, \left|\left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle\right| = 4^{2\deg F_5}, \left|\left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle\right| = 4^{3\deg F_6}.$$

Theorem 2. Let C be a cyclic code of odd length n over R with $C = \left\langle \hat{F}_1 \right\rangle \oplus \left\langle u\hat{F}_2 \right\rangle \oplus \left\langle v\hat{F}_3 \right\rangle \oplus \left\langle uv\hat{F}_4 \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle \oplus \left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle$, where h_α is an unit in $F_4[x]/\langle x^n - 1\rangle$.Let $C = \hat{F}_1 + u\hat{F}_2 + v\hat{F}_3 + uv\hat{F}_4 + (u+vh_\alpha)\hat{F}_5 + u\hat{F}_6 + v\hat{F}_6$. Then $C = \langle F \rangle$.

Proof. For any two distinct integers i and j, $0 \le i, j \le 6$, we have that $(x^n - 1) \mid \hat{F}_i\hat{F}_j$.

So $\hat{F}_i\hat{F}_j = 0$.Further, for any i with $0 \le i \le 6$, F_i and $\hat{F}_i$ are coprime with $\hat{F}_i\hat{F}_i = 0$. Since F_i and $\hat{F}_i$ are coprime, then, for $1 \le i \le 5$, there exist a_i, b_i such that $\left(a_1F_1 + b_1\hat{F}_1\right)\left(a_2F_2 + b_2\hat{F}_2\right)\left(a_3F_3 + b_3\hat{F}_3\right)\left(a_4F_4 + b_4\hat{F}_4\right)\left(a_5F_5 + b_5\hat{F}_5\right) = 1$,which implies that

$a_1F_1a_2F_2a_3F_3a_4F_4a_5F_5 + b_1\hat{F}_1a_2F_2a_3F_3a_4F_4a_5F_5 + a_1F_1b_2\hat{F}_2a_3F_3a_4F_4a_5F_5$.

$+ a_1F_1a_2F_2a_3F_3a_4F_4a_5F_5 + b_1\hat{F}_1a_2F_2a_3F_3a_4F_4a_5F_5 + a_1F_1b_2\hat{F}_2a_3F_3a_4F_4a_5F_5\hat{F}_3a_4F_4a_5F_5$

$+ a_1F_1a_2F_2a_3F_3b_4\hat{F}_4a_5F_5 + a_1F_1a_2F_2a_3F_3a_4F_4b_5\hat{F}_5 = 1$. Multiplying both sides by $\hat{F}_6$, we obtain $\hat{F}_6a_1F_1a_2F_2a_3F_3a_4F_4a_5F_5 = \hat{F}_6$.

Let $F=\hat{F}_1+u\hat{F}_2+v\hat{F}_3+uv\hat{F}_4+(u+vh_\alpha)\hat{F}_5+u\hat{F}_6+v\hat{F}_6$. Then $Fa_1F_1a_2F_2a_3F_3a_4F_4a_5F_5=\left(u\hat{F}_6+v\hat{F}_6\right)a_1F_1a_2F_2a_3F_3a_4F_4a_5F_5$, which implies that $Fa_1F_1a_2F_2a_3F_3a_4F_4a_5F_5=u\hat{F}_6+v\hat{F}_6$. Therefore, $u\hat{F}_6+v\hat{F}_6\in\langle F\rangle$.

Repeat the above progress, we have that $\hat{F}_1,u\hat{F}_2,v\hat{F}_3,uv\hat{F}_4,(u+vh_\alpha)\hat{F}_5,u\hat{F}_6+v\hat{F}_6\in\langle F\rangle$. Thus, $C=\langle F\rangle$.

Self-dual cyclic codes over $M_2(F_2+uF_2)$

Let $x=(x_1,x_2,...,x_n)$, $y=(y_1,y_2,...,y_n)\in R_n$. The Euclidean inner product of x and y is given *by* $x\cdot y=x_1y_1+x_2y_2+\cdots+x_ny_n$. Two vectors x and y in R_n are called orthogonal if $x\cdot y=0$. For a linear code R over R, its dual code $C^\perp$ is the set of words over R that are orthogonal to all code words of R, that is $C^\perp=\{x\in R^n\mid x\cdot y=0,\forall y\in C\}$. A code C is called self-orthogonal if $C\subseteq C^\perp$ 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, where $a_k\neq 0$ and a_0 is an unit of R. The reciprocal $f^*(x)$ of $f(x)$ is defined by $f^*(x)=a_0^{-1}x^kf(x^{-1})$.

Theorem 3. Let $C=\langle\hat{F}_1\rangle\oplus\langle u\hat{F}_2\rangle\oplus\langle v\hat{F}_3\rangle\oplus\langle uv\hat{F}_4\rangle\oplus\langle(u+vh_\alpha)\hat{F}_5\rangle\oplus\langle\langle u\hat{F}_6\rangle+\langle v\hat{F}_6\rangle\rangle$ be a cyclic code of odd length n over R,where h_α is an unit in $F_4[x]/\langle x^n-1\rangle$. Then $C^\perp=\langle\hat{F}_0^*\rangle\oplus\langle u\hat{F}_2^*\rangle\oplus\langle v\hat{F}_3^*\rangle\oplus\langle uv\hat{F}_6^*\rangle\oplus\langle(u+vh_\alpha)\hat{F}_5^*\rangle\oplus\langle\langle u\hat{F}_4^*\rangle+\langle v\hat{F}_4^*\rangle\rangle$ and

$$C^\perp=4^{4\deg F_0+2\deg F_2+2\deg F_3+3\deg F_4+2\deg F_5+3\deg F_6}.$$

Proof. Denote

$$C^*=\langle\hat{F}_0^*\rangle\oplus\langle u\hat{F}_2^*\rangle\oplus\langle v\hat{F}_3^*\rangle\oplus\langle uv\hat{F}_6^*\rangle\oplus\langle(u+vh_\alpha)\hat{F}_5^*\rangle\oplus\langle\langle u\hat{F}_4^*\rangle+\langle v\hat{F}_4^*\rangle\rangle.$$

For i,j, $0\le i,j\le 5$, if $i+1=6-j+1$, that $i=6-j$,we can see that $u^2\hat{F}_{i+1}\left(\hat{F}_{6-j+1}^*\right)^*=0$, $v^2\hat{F}_{i+1}\left(\hat{F}_{6-j+1}^*\right)^*=0$, $2uv\hat{F}_{i+1}\left(\hat{F}_{6-j+1}^*\right)^*=0$.if $i+1\neq 6-j+1$, i.e. $i\neq 6-j$, then we have $x^n-1\mid\hat{F}_{i+1}\left(\hat{F}_{6-j+1}^*\right)^*$. Therefore, $\hat{F}_{i+1}\left(\hat{F}_{6-j+1}^*\right)^*=0$. Thus, $C^*\subseteq C^\perp$. From Theorem 1,

$C = 4^{4\deg F_0 + 2\deg F_2 + 2\deg F_3 + 3\deg F_4 + 2\deg F_5 + 3\deg F_6}$. Since $|C| \cdot |C^{\perp}| = 4^{4n}$ and $n = \deg F_1 + \deg F_2 + \deg F_3 + \deg F_4 + \deg F_5 + \deg F_6$, then

$$C^{\perp} = 4^{4\deg F_0 + 2\deg F_2 + 2\deg F_3 + 3\deg F_4 + 2\deg F_5 + \deg F_6}.$$

Note that $\left|\left\langle \hat{F}_0^* \right\rangle\right| = 4^{4\deg F_0}, \left|\left\langle u\hat{F}_2^* \right\rangle\right| = 4^{2\deg F_2}, \left|\left\langle v\hat{F}_3^* \right\rangle\right| = 4^{2\deg F_3}, \left|\left\langle uv\hat{F}_4^* \right\rangle\right| = 4^{\deg F_6}$, $\left|\left\langle uv\hat{F}_4^* \right\rangle\right| = 4^{\deg F_6}, \left|\left\langle (u+vh_\alpha)\hat{F}_5^* \right\rangle\right| = 4^{2\deg F_5}, \left|\left\langle \left\langle u\hat{F}_6^* \right\rangle + \left\langle v\hat{F}_6^* \right\rangle \right\rangle\right| = 4^{\deg F_4}$. Therefore, $|C^*| = 4^{4\deg F_0 + 2\deg F_2 + 2\deg F_3 + 3\deg F_4 + 2\deg F_5 + \deg F_6} = |C^{\perp}|$,

which implies that $C^* = C^{\perp}$.

Corollary 1. Let C be a cyclic code of odd length n over R and

$$F^* = \hat{F}_0^* + u\hat{F}_2^* + v\hat{F}_3^* + uv\hat{F}_6^* + (u+vh_\alpha)\hat{F}_5^* + u\hat{F}_4^* + v\hat{F}_4^*,$$

where h_α is an unit in $F_4[x]/\langle x^n - 1\rangle$. Then $C^{\perp} = \langle F^* \rangle$.

Proof. The result follows from Theorem 2 and Theorem 3.

We now give a condition for a cyclic code to be self-dual. From Theorem 2 and Corollary 1, we can see that a cyclic code C is self-dual if and only if $F = F^*$, which implies that

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

Since $\hat{F}_i = \frac{x^n - 1}{F_i}$, $\hat{F}_j^* = \frac{x^n - 1}{F_j^*}$ and $\hat{F}_i^* = \hat{F}_j^*$, $F_i = F_j^*$. So the following result is proved.

Theorem 4. Let C be a cyclic code of odd length n over R. Then if

$$C = \left\langle \hat{F}_1 \right\rangle \oplus \left\langle u\hat{F}_2 \right\rangle \oplus \left\langle v\hat{F}_3 \right\rangle \oplus \left\langle uv\hat{F}_4 \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle \oplus \left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle,$$

where h_α is an unit in $F_4[x]/\langle x^n - 1\rangle$. Then C *i*s self-dual if and only if $F_1 = F_0^*$, $F_2 = F_2^*$, $F_3 = F_3^*$, $F_4 = F_6^*$, $F_5 = F_5^*$.

Proof. Let $C = \left\langle \hat{F}_1 \right\rangle \oplus \left\langle u\hat{F}_2 \right\rangle \oplus \left\langle v\hat{F}_3 \right\rangle \oplus \left\langle uv\hat{F}_4 \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle \oplus \left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle$, where h_α is an unit in $F_4[x]/\langle x^n - 1\rangle$. if C *i*s self-dual, then $C = C^{\perp}$. Therefore, by Theorem 3, we have that

$$\left\langle \hat{F}_0^* \right\rangle \oplus \left\langle u\hat{F}_2^* \right\rangle \oplus \left\langle v\hat{F}_3^* \right\rangle \oplus \left\langle uv\hat{F}_6^* \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5^* \right\rangle \oplus \left\langle \left\langle u\hat{F}_4^* \right\rangle + \left\langle v\hat{F}_4^* \right\rangle \right\rangle = \left\langle \hat{F}_1 \right\rangle \oplus \left\langle u\hat{F}_2 \right\rangle \oplus \left\langle v\hat{F}_3 \right\rangle \oplus \left\langle uv\hat{F}_4 \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle \oplus \left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle,$$

i.e. $F_1 = F_0^*$, $F_2 = F_2^*$, $F_3 = F_3^*$, $F_4 = F_6^*$, $F_5 = F_5^*$.

Inversely, if $F_1 = F_0^*$, $F_2 = F_2^*$, $F_3 = F_3^*$, $F_4 = F_6^*$, $F_5 = F_5^*$, then

$$C = \left\langle \hat{F}_1 \right\rangle \oplus \left\langle u\hat{F}_2 \right\rangle \oplus \left\langle v\hat{F}_3 \right\rangle \oplus \left\langle uv\hat{F}_4 \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5 \right\rangle \oplus \left\langle \left\langle u\hat{F}_6 \right\rangle + \left\langle v\hat{F}_6 \right\rangle \right\rangle = \left\langle \hat{F}_0^* \right\rangle \oplus$$

$$\left\langle u\hat{F}_2^* \right\rangle \oplus \left\langle v\hat{F}_3^* \right\rangle \oplus \left\langle uv\hat{F}_6^* \right\rangle \oplus \left\langle (u+vh_\alpha)\hat{F}_5^* \right\rangle \oplus \left\langle \left\langle u\hat{F}_4^* \right\rangle + \left\langle v\hat{F}_4^* \right\rangle \right\rangle = C^\perp$$

. Hence, C is a self-dual code.

In the following, we give some examples to illustrate the main results in this paper. In these examples, some self-dual codes over F_4 are constructed by self-dual cyclic codes over R and the Gray map.

Example 1. Consider the factorization $x^3 - 1 = (x+1)(x+w)(x+w^2)$ over F_4. Let $f_1 = (x+1)$, $f_2 = (x+w)$ and $f_3 = (x+w^2)$. Then $f_1 = f_1^*$, $f_2 = f_3^*$ and $f_3 = f_2^*$.

The cyclic codes $\langle f_1, f_2, tf_2f_3 \rangle$ and $\langle f_1, f_3, tf_2f_3 \rangle$, where $t \in \{v, u\}$, of length 3 over R are self-dual codes and their Gray images are self-dual codes over F_4 with parameters [12, 6, 4].

Example 2. Consider the factorization $x^5 - 1 = (x+1)(x^2+wx+1)(x^2+w^2x+1)$ over F_4. Let $f_1 = (x+1)$, $f_2 = (x^2+wx+1)$ and $f_3 = (x^2+w^2x+1)$. Then $f_1 = f_1^*$, $f_2 = f_3^*$ and $f_3 = f_2^*$ .The cyclic codes $\langle f_1, f_2, tf_2f_3 \rangle$ and $\langle f_1, f_3, tf_2f_3 \rangle$, where $t \in \{v, u\}$, of length 5 over R are self-dual codes and their Gray images are self-dual codes over F_4 with parameters [20, 10, 6].

Example 3. Consider the factorization $x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1)$ over F_4. Let $f_1 = (x+1)$, $f_2 = (x^3+x+1)$ and $f_3 = (x^2+x^2+1)$. Then $f_1 = f_1^*$, $f_2 = f_3^*$ and $f_3 = f_2^*$ .The cyclic codes $\langle f_1, f_2, tf_2f_3 \rangle$ and $\langle f_1, f_3, tf_2f_3 \rangle$, where $t \in \{v, u\}$, of length 7 over R are self-dual codes and their Gray images are self-dual codes over F_4 with parameters [28, 14, 6].

In Table 1, some more self-dual codes over F_4 are constructed.

Table 1. Self-dual codes over F_4

Codes length n	Factorization of $x^n - 1$	Reciprocal polynomials	Self-dual cyclic codes	Gray images
9	$f_1 = x+1$, $f_2 = x+w$, $f_3 = x+w^2$, $f_4 = x^3+w$, $f_5 = x^3+w^2$	$f_1 = f_1^*$ $f_2 = f_3^*$, $f_3 = f_2^*$, $f_4 = f_5^*$, $f_5 = f_4^*$	$\langle f_1 f_2 f_4, uf_2f_3f_4f_5 \rangle$	[36,18,9]
11	$f_1 = x+1$, $f_2 = x^5+wx^4+x^3+x^2+w^2x+1$, $f_2 = x^5+w^2x^4+x^3+x^2+wx+1$	$f_1 = f_1^*$, $f_2 = f_3^*$, $f_3 = f_2^*$	$\langle f_1, f_2, uf_2f_3 \rangle$	[44,22,11]

13	$f_1 = x+1$, $f_2 = x^6 + wx^5 + w^2x^3 + wx + 1$, $f_2 = x^6 + w^2x^5 + wx^3 + w^2x + 1$	$f_1 = f_1^*$, $f_2 = f_3^*$, $f_3 = f_2^*$	$\langle f_1, f_2, uf_2f_3 \rangle$	[52,26,12]
17	$f_1 = x+1$, $f_2 = x^4 + x^3 + wx^2 + x + 1$, $f_3 = x^4 + x^3 + w^2x^2 + x + 1$, $f_4 = x^4 + wx^3 + x^2 + wx + 1$, $f_5 = x^4 + w^2x^3 + x^2 + w^2x + 1$	$f_1 = f_1^*$ $f_2 = f_2^*$, $f_3 = f_3^*$, $f_4 = f_4^*$, $f_5 = f_5^*$	$\langle f_1f_2f_3, uf_2f_3f_4f_5 \rangle$	[68,34,16]

Conclusion

In this paper, we study some structural properties of self-dual cyclic codes over the matrix ring $M_2(F_2+uF_2)$. The ring $M_2(F_2+uF_2)$ is isomorphic to $F_4 + uF_4 + vF_4 + uvF_4$. We also give a Gray map from this ring to F_4. By the Gary map, some self-dual codes over F_4 are obtained.

References

Alahmadi, A., Sboui, H., Sol´e, P., Yemen, O. (2013). Cyclic codes over $M_2(F_2)$, J. Frankl. Inst., 350(9), 2837–2847.

Bachoc, C.: Applications of coding theory to the construction of modular lattices, J. Combinatorial Theory A 78(1), 92–119 (1997)

Bhowmick, S., Bagchi, S., Bandi, R.K. (2018). Self-dual cyclic codes over $M_2(Z_4)$, arXiv:1807.04913

Hammons, A., Kumar, P., Calderbank, A., Sloane, N.J.A., Sol´e, P. (1994). The Z_4- linearity of kerdock, preparata, goethals, and related codes. IEEE Trans. Inf. Theory, 40, 301-319.

Luo, R., Parampalli, U. (2018). Cyclic codes over $M_2(F_2+uF_2)$. Cryptogr. Commun, 10, 1109- 1117 (2018)

Mathematics Subject Classification (2000). 94B15. Available at: http://www.mat.ucm.es/~arrondo/classification-AMS.pdf

Oggier, F., Sol´e, P., Belfiore, J.-C. (2012). Codes over matrix rings for space-time coded modulations, IEEE Trans. Inf. Theory, 58, 734-746.

Pal, J., Bhowmick, S., Satya, B. (2019). Cyclic codes over $M_4(F_2)$. J. Appl. Math. Computing. Available at: https://doi.org/10.1007/s12190-018-01235-w