AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(10): 24434–24445.
DOI: 10.3934/math.20231246
Received: 06 June 2023
Revised: 22 July 2023
Accepted: 06 August 2023
Published: 17 August 2023

Research article

On skew cyclic codes over $M_2(\mathbb{F}_2)$

Xuesong Si and Chuanze Niu*

School of Mathematical Sciences, Liaocheng University, Liaocheng 252059, China

* **Correspondence:** Email: niuchuanze@lcu.edu.cn.

Abstract: The algebraic structure of skew cyclic codes over $M_2(\mathbb{F}_2)$, using the $\mathbb{F}_4$-cyclic algebra, is studied in this work. We determine that a skew cyclic code with a polynomial of minimum degree $d(x)$ is a free code generated by $d(x)$. According to our findings, skew cyclic codes of odd and even lengths are cyclic and 2-quasi-cyclic over $M_2(\mathbb{F}_2)$, respectively. We provide the self-dual skew condition of Hermitian dual codes of skew cyclic codes. The generator polynomials of Euclidean dual codes are obtained. Furthermore, a spanning set of a double skew cyclic code over $M_2(\mathbb{F}_2)$ is considered in this paper.

Keywords: skew cyclic code; finite chain ring; skew polynomial rings; Gray map
Mathematics Subject Classification: 11T71, 94B05, 94B15

1. Introduction

Error-correcting codes have been a widely studied topic for the past six decades. Among all linear codes, cyclic codes have received significant attention. Boucher et al. [9] generalized the concept of cyclic codes over finite fields to skew cyclic codes. Siap et al. [25] extended their results to skew cyclic codes of arbitrary length. For the last twenty years, scholars have focused on error-correcting codes over finite rings.

There exist a host of studies on skew cyclic codes and double skew cyclic codes over finite commutative rings. Boucher et al. [10] and Jitman et al. [17] considered skew constacyclic codes over Galois rings and finite chain rings, respectively. Abualrub et al. [1] built θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Gao [13] investigated the algebraic structure of skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. Gursoy et al. [15] accomplished the construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$. The algebraic properties of skew cyclic codes over the finite semi-local ring $\mathbb{F}_{p^m} + v\mathbb{F}_{p^m}$ were studied by M. Ashraf [3]. Shi et al. [22, 23] established skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and $\mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$. Bagheri et al. [6] studied skew cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and obtained some torsion codes of skew cyclic codes. Shi et al. [24] proved the structure of skew cyclic codes over a finite non-chain ring. Recently, Prakash [21] studied the structure of skew cyclic codes over $\mathbb{F}_q[u, v, w]/\langle u^2 - 1, v^2 - 1, w^2 - 1, uv - vu, vw - wv, wu - uw\rangle$. Gao et al. [14] studied weight distribution of double cyclic codes over Galois rings. Aydogdu et al. [4] characterized the algebraic structure of double skew cyclic codes over $\mathbb{F}_q$.

Since Wood [26] proved that the finite Frobenius rings can serve as the alphabets of coding theory, many papers on cyclic codes over matrix rings have been published (see [2,7,11,16,18–20]). However, there are few papers investigating skew and double skew cyclic codes over matrix rings. In this study, we use the $\mathbb{F}_4$-cyclic algebra given in [5] to build the algebraic structure of skew cyclic codes over $M_2(\mathbb{F}_2)$. Additionally, we discuss the dual codes of skew cyclic codes and double skew cyclic codes over $M_2(\mathbb{F}_2)$.

This article is organized as follows: Section 2 provides some basic facts, and considers the algebraic structure of skew cyclic codes over $M_2(\mathbb{F}_2)$. We prove that a skew cyclic code C with a polynomial of minimum degree $d(x)$ is a free submodule generated by $d(x)$. We discuss Euclidean and Hermitian dual codes of θ-cyclic codes in Section 3. In Section 4, the spanning sets of double skew cyclic codes over $M_2(\mathbb{F}_2)$ are obtained, and Section 5 concludes this paper.

2. Skew cyclic codes over $\mathcal{R}$

Let R be a finite ring with identity $1 \neq 0$. A left (resp. right) R-module M is denoted by ${}_RM$ (resp. M_R). The socle of a module M is defined as the sum of its minimal submodules, denoted by $\mathrm{Soc}(M)$. The ring R is called a Frobenius ring if $\mathrm{Soc}({}_RR)$ (resp. $\mathrm{Soc}(R_R)$) is a principal left (resp. right) ideal. The ring R is called a local ring if R has a unique left (resp. right) maximal ideal (or equivalently, if $R/\mathrm{rad}(R)$ is a division ring). A ring R is called a left (resp. right) chain ring if the set of all left (resp. right) ideals of R is linearly ordered under the set inclusion. Lemma 2.1 describes the equivalence conditions between chain rings, principal ideal rings and local rings (cf. [12, Theorem 2.1]).

Lemma 2.1. *For any finite ring R, the following conditions are equivalent:*

(i) R is a local principal ideal ring;

(ii) R is a local ring and the unique maximal ideal M of R is principal;

(iii) R is a chain ring whose ideal are $\langle r^i\rangle$, $0 \leq i \leq N(r)$, *where* $N(r)$ *is the nilpotency index of r.*

Moreover, if R is a finite chain ring with the unique maximal ideal $\langle r\rangle$ and the nilpotency index of r is z, then the cardinality of $\langle r^i\rangle$ is $|R/\langle r\rangle|^{z-i}$ for $i = 0, 1, \cdots, z - 1$.

We denote the 2×2 matrix ring over finite field $\mathbb{F}_2$ by $M_2(\mathbb{F}_2)$. By [5], we have $M_2(\mathbb{F}_2)$ is isomorphic to the $\mathbb{F}_4$-cyclic algebra $\mathcal{R} = \mathbb{F}_4 \oplus e\mathbb{F}_4$ with $e^2 = 1$ under the map δ,

$$\delta : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto e, \quad \delta : \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \mapsto \omega,$$

where $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ and $\omega^2 + \omega + 1 = 0$. Note that $(e + 1)^2 = 0$, then $e + 1$ is a nilpotent element of order 2. The multiplication in $\mathcal{R}$ is given by $re = e\sigma(r)$ for any $r \in \mathcal{R}$, where $\sigma(r) = r^2$ is the Frobenius map on $\mathbb{F}_4$ and the addition is usual.

The set of the unit elements of $\mathcal{R}$ is $\{1, \omega, 1+\omega, e, e\omega, e(1+\omega)\}$. It is easy to know that the ring $\mathcal{R}$ has the unique maximal ideal $\langle e+1\rangle$. Since the $n\times n$ matrix ring $M_n(R)$ over a Frobenius ring R is also Frobenius, then $\mathcal{R}$ is a finite local Frobenius ring.

Define a map $\theta : \mathcal{R} \to \mathcal{R}$ by $\theta(a + eb) = \sigma(a) + e\sigma(b)$, $a, b \in \mathbb{F}_4$. One can verify that θ is an automorphism of $\mathcal{R}$ with order 2. The set $\mathbb{F}_{4,\theta} = \{0, 1, e, 1 + e\}$ is the fixed commutative subring of $\mathcal{R}$ by θ. Define the skew polynomial ring

$$\mathcal{R}[x, \theta] = \left\{ r_n x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 | r_i \in \mathcal{R}, n \in \mathbb{N} \right\}$$

with the usual polynomial addition, and the multiplication is defined by the rule $r_1x^i \cdot r_2x^j = r_1\theta^i(r_2)x^{i+j}$, $i, j \in \mathbb{N}$. Then for every $a + eb \in \mathcal{R}$,

$$x^i(a+eb) = \begin{cases} (a+eb)x^i, & \text{if } i \text{ is even,} \\ (a^2+eb^2)x^i, & \text{if } i \text{ is odd.} \end{cases}$$

Note that $\mathcal{R}[x, \theta]$ is non-commutative for multiplication, therefore, the submodules we discussed in this paper are always left. It should be noted also that $\mathcal{R}[x, \theta]$ is not a unique factorization ring, for instance, $x^2 = x \cdot x = ex \cdot ex$, $x^3 = x \cdot x \cdot x = x \cdot ex \cdot ex$. In addition, the right division can be defined.

Lemma 2.2. *Let $f(x)$, $g(x) \in \mathcal{R}[x, \theta]$, where the leading coefficient of $g(x)$ is invertible. Then there exist unique $q(x)$, $r(x) \in \mathcal{R}[x, \theta]$ such that*

$$f(x) = q(x)g(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. The polynomials $q(x)$ and $r(x)$ are called the right quotient and right remainder, respectively. The polynomial $g(x)$ is called a right divisor of $f(x)$ if $g(x)|f(x)$.

Proof. The proof is similar to that of Lemma 2.3 of [13]. □

Proposition 2.3. *The center $Z(\mathcal{R}[x, \theta])$ of $\mathcal{R}[x, \theta]$ is $\mathbb{F}_{4,\theta}[x^2]$.*

Proof. This proof is similar to that of [13, Theorem 1]. We give the proof briefly. Since $|\langle\theta\rangle| = 2$, then $x^{2i} \cdot r = (\theta^2)^i(r)x^{2i} = rx^{2i}$ with any $r \in \mathcal{R}$. Thus $x^{2i} \in Z(\mathcal{R}[x, \theta])$. It implies that $f(x) = \sum_{j=0}^{s} r_j x^{2j} \in Z(\mathcal{R}[x, \theta])$, where $r_j \in \mathbb{F}_{4,\theta}$. Conversely, for any $f_z \in Z(\mathcal{R}[x, \theta])$ and $r \in \mathcal{R}$, if $rf_z = f_z r$ and $xf_z = f_z x$, then the coefficients of f_z are all in $\mathbb{F}_{4,\theta}$ and $f_z \in \mathcal{R}[x^2, \theta]$. Therefore $f_z \in \mathbb{F}_{4,\theta}[x^2]$. □

Corollary 2.4. *We have that $x^n + 1 \in Z(\mathcal{R}[x, \theta])$ if and only if n is even.*

Let $\mathcal{R}^n$ be the set of all n-tuples over $\mathcal{R}$. Then a code C of length n over $\mathcal{R}$ is a nonempty subset of $\mathcal{R}^n$. If C is a left (resp. right) $\mathcal{R}$-submodule of $\mathcal{R}^n$, then C is called a left (resp. right) linear code of length n over $\mathcal{R}$. Every element $c = (c_0, c_1, \cdots, c_{n-1})$ in C is called a codeword.

Define the Gray map $\varphi(a+eb) = (b, a+b)$ from $\mathcal{R}$ to $\mathbb{F}_4^2$ following the method in [8]. This map φ is a linear bijection and can be extended to a map from $\mathcal{R}^n$ onto $\mathbb{F}_4^{2n}$ by concatenating the images of each component. For any element $a + eb \in \mathcal{R}$, Lee weight of $a + eb$ is defined as

$$w_L(a + eb) = w_{Ham}(b) + w_{Ham}(a + b),$$

where $w_{Ham}(*)$ stands for Hamming weight over finite fields. If $x = (x_0, x_1, \cdots, x_{n-1}) \in \mathcal{R}^n$, then Lee weight of x is defined as

$$w_L(x) = w_L(x_0) + w_L(x_1) + \cdots + w_L(x_{n-1}).$$

If C is a linear code of length n over $\mathcal{R}$, then Hamming and Lee distance of C are defined as $d_{Ham} = \min\{w_{Ham}(\mathrm{x}) | \mathrm{x} \in C\}$ and $d_L = \min\{w_L(\mathrm{x}) | \mathrm{x} \in C\}$, respectively. Analogously to [19, Theorem 7], we get the following result. It is a proposition of the image of the linear code C over $\mathcal{R}$ under the Gray map φ.

Proposition 2.5. *Let C be a linear code over $\mathcal{R}$ of length n with size $\mathcal{M}$ and minimum Lee distance d_L. Then $\varphi(C)$ is a linear code over $\mathbb{F}_4$ of length $2n$ with size $\mathcal{M}$ and minimum Hamming distance d_{Ham}.*

We discuss the algebraic structure of skew cyclic codes over $\mathcal{R}$ below. Let n be a positive integer. The set $\mathcal{R}_n = \mathcal{R}[x, \theta]/\langle x^n - 1\rangle$ is a ring if n is even. When n is odd, the set $\mathcal{R}_n$ is a left $\mathcal{R}[x, \theta]$-module under the multiplication defined by

$$f_1(x)(f_2(x) + (x^n - 1)) = f_1(x)f_2(x) + (x^n - 1).$$

Denote by $\mathscr{T}$ the standard shift operator on a linear code C, i.e., $\mathscr{T}(c) = (c_{n-1}, c_0, \cdots, c_{n-2})$ for any codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in C$. A linear code C over $\mathcal{R}$ is cyclic if any cyclic shift of a codeword $c \in C$ is also a codeword, i.e., $\mathscr{T}(c) \in C$. A linear code over $\mathcal{R}$ is called quasi-cyclic of index ℓ (or ℓ-quasi-cyclic) if and only if it is invariant under $\mathscr{T}^{\ell}$. If $\ell = 1$, then it is a cyclic code. A linear code C of length n is called a skew cyclic code if and only if

$$\theta(c) = (\theta(c_{n-1}), \theta(c_0), \cdots, \theta(c_{n-2})) \in C,$$

for any codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in C$.

In a set of polynomials, a polynomial is called the polynomial of minimum degree if and only if it is not a polynomial of lower degree by removing any of its terms. Let $d(x) = x^{n-m} + \sum_{i=0}^{n-m-1} d_i x^i$ be a monic right divisor of $x^n - 1$. Then a $m \times n$ generator matrix G of the skew cyclic code $C = \langle d(x)\rangle$ is given by

$$G = \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-m-1} & 1 & 0 & \cdots & 0 & 0 \\ 0 & \theta(d_0) & \cdots & \theta(d_{n-m-2}) & \theta(d_{n-m-1}) & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \theta^2(d_{n-m-3}) & \theta^2(d_{n-m-2}) & \theta^2(d_{n-m-1}) & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & \theta^{m-2}(d_0) & \theta^{m-2}(d_1) & \theta^{m-2}(d_3) & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & \theta^{m-1}(d_0) & \theta^{m-1}(d_1) & \cdots & \theta^{m-1}(d_{n-m-1}) & 1 \end{pmatrix}.$$

Proposition 2.6 shows that skew cyclic codes with a polynomial of minimum degree over $\mathcal{R}$ are free codes. Proposition 2.9 gives a sufficient and necessary condition for a skew cyclic code over $\mathcal{R}$ to become a cyclic code. Propositions 2.7 and 2.8 describe the relationship between skew cyclic codes of length n and cyclic codes, quasi-cyclic codes, respectively.

Proposition 2.6. *Let n be a positive integer and C be a skew cyclic code of length n over $\mathcal{R}$ with a polynomial of minimum degree $d(x)$, where the leading coefficient of $d(x)$ is a unit. Then C is a free $\mathcal{R}[x, \theta]$-submodule of $\mathcal{R}_n$ such that $C = \langle d(x)\rangle$, where $d(x)$ is a right divisor of $x^n - 1$. Moreover, the code C has a basis $\mathcal{B} = \{d(x), xd(x), \cdots, x^{n-\deg(d(x))-1}d(x)\}$ and the number of codewords in C is $|\mathcal{R}|^{n-\deg(d(x))}$.*

Proof. By Lemma 2.2, any polynomial in C is divisible by $d(x)$. It implies that $d(x)|x^n - 1$ and $C = \langle d(x)\rangle$. For the second statement, let $x^n - 1 = q(x)d(x)$ for some $q(x) \in \mathcal{R}[x,\theta]$. Since the leading coefficient of $d(x)$ is a unit, then the leading coefficient of $q(x)$ is also invertible. Let m be the degree of $q(x)$, then the degree of $d(x)$ is $n - m$. Let $q(x) = \sum_{i=0}^{m} q_i x^i$, where q_m is invertible. Therefore $\sum_{i=0}^{m} q_i x^i d(x) = 0$ in $\mathcal{R}_n$. It follows that $x^j d(x)$ with $j \geq m$ can be linearly presented by the elements of the set $\mathcal{B} = \{d(x), xd(x), \cdots, x^{m-1}d(x)\}$.

Let $\sum_{i=0}^{m-1} a_i \cdot x^i d(x) = 0$, where $a_i \in \mathcal{R}$, $i = 0, 1, \cdots, m-1$. Thus $a(x)d(x) = 0$, where $a(x) = \sum_{i=0}^{m-1} a_i x^i$. The polynomial $a(x)d(x)$ can be represented to $a(x)d(x) = \zeta(x)(x^n - 1)$ for some $\zeta(x) \in \mathcal{R}[x,\theta]$. The degree of $a(x)d(x)$ is $n-1$, while the degree of $\zeta(x)(x^n - 1)$ is greater than or equal to n if $\zeta(x) \neq 0$. This is a contradiction. Therefore, we have $\zeta(x) = a(x) = 0$, i.e. $a_i = 0$ for $i = 0, 1, \cdots, m-1$. The set $\mathcal{B} = \{d(x), xd(x), \cdots, x^{m-1}d(x)\}$ is $\mathcal{R}$-linearly independent. Consequently $\mathcal{B}$ is a basis of C and $|C| = |\mathcal{R}|^{n-\deg(d(x))}$. This completes the proof. □

Proposition 2.7. *If C is a skew cyclic code of odd length over $\mathcal{R}$, then C is a cyclic code over $\mathcal{R}$.*

Proof. Let n be odd and C be a skew cyclic code of length n over $\mathcal{R}$. There exist two integers s, t such that $2s + nt = 1$. Thus, we have $2s = 1 - nt$. If $c(x) = \sum_{i=0}^{n-1} c_i x^i$ is any codeword in C, then

$$x^{2s}c(x) = x^{1-nt}c(x) = \sum_{i=0}^{n-1} c_i x^{i+1-nt}.$$

Since $x^n = 1$, then

$$x^{2s}c(x) = \sum_{i=0}^{n-1} x^{i+1} = xc(x) \in C.$$

It follows that $(c_{n-1}, c_0, \cdots, c_{n-2}) \in C$ for any codeword $(c_0, c_1, \cdots, c_{n-1})$ in C. □

Proposition 2.8. *If C is a skew cyclic code of even length over $\mathcal{R}$, then C is a quasi-cyclic code of index 2.*

Proof. Let C be a skew cyclic code of length $2t$ over $\mathcal{R}$ and $c = (c_{0,0}, c_{0,1}, c_{1,0}, \cdots, c_{t-1,0}, c_{t-1,1}) \in C$. Since $\theta(c) \in C$ and $\theta^2 = 1$, it follows that $\theta^2(c) = (c_{t-1,0}, c_{t-1,1}, c_{0,0}, c_{0,1}, \cdots, c_{t-2,0}, c_{t-2,1}) \in C$. By the definition of quasi-cyclic codes, the code C is a 2-quasi-cyclic code of length $2t$. □

Proposition 2.9. *Let C be a skew cyclic code generated by $d(x)$ of even length n over $\mathcal{R}$, where $d(x)$ is a monic right divisor of $x^n - 1$. Then C is a cyclic code over $\mathcal{R}$ if and only if $d(x)$ is fixed by θ.*

Proof. Let $d(x) = x^l + d_{l-1}x^{l-1} + \cdots + d_1 x + d_0$, where $\theta(d_i) = d_i$, $i = 0, 1, 2, \cdots, l-1$. Then $xd(x) = d(x)x \in C$. It follows that the code $C = \langle d(x)\rangle$ is cyclic over $\mathcal{R}$.

Conversely, if C is a cyclic code of even length n over $\mathcal{R}$, then C is a left ideal of $\mathcal{R}_n$ and an ideal of $\mathcal{R}[x]/\langle x^n - 1\rangle$. Therefore, $d(x)x$ is a codeword in C. Since C is linear, we have $d(x)x - xd(x) \in C$. It implies that $\sum_{i=0}^{l-1}(d_i - \theta(d_i))x^{i+1}$ is a left multiple of $d(x)$ such that $d(x)x - xd(x) = rd(x)$ with $r \in \mathcal{R}$. Note that the constant term of $d(x)x - xd(x)$ is 0, then $d(x)x - xd(x)$ must be 0. It shows that $\theta(d_i) = d_i$, $i = 0, 1, \cdots, l-1$. The proof is done. □

Example 2.10. *There are two examples:*

(1) *Let C be a skew cyclic code of length 4 over $\mathcal{R}$ generated by the following matrix,*

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

The generated polynomial of C is $d(x) = x^2 + (e+1)x + e$. Note that $d(x)$ is a commutative right divisor of $x^4 - 1$, and all coefficients of $d(x)$ are fixed by θ. By Proposition 2.9, the code C is cyclic.

(2) *Let C_1 be a skew cyclic code of length 4 generated by the following matrix,*

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

The generated polynomial of C_1 is $d_1(x) = x+\omega$, and it is a right divisor of $x^4 - 1$. The coefficients of $d_1(x)$ are not all fixed by θ. By Propositions 2.8 and 2.9, the code C_1 is not cyclic but 2-quasi-cyclic.

3. Duals of skew cyclic codes over $\mathcal{R}$

This section investigates the dual codes of skew cyclic codes over the ring $\mathcal{R}$. For any $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \cdots, y_{n-1}) \in \mathcal{R}^n$, the Euclidean inner product on $\mathcal{R}^n$ is defined by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=0}^{n-1} x_i y_i$. If the order of the automorphism θ is 2, then the Hermitian inner product of any $\mathbf{x}, \mathbf{y} \in \mathcal{R}^n$ is defined by $\langle \mathbf{x}, \mathbf{y} \rangle_H = \sum_{i=0}^{n-1} x_i \theta(y_i)$.

The elements $\mathbf{x}, \mathbf{y} \in \mathcal{R}^n$ are called Euclidean or Hermitian orthogonal if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ or $\langle \mathbf{x}, \mathbf{y} \rangle_H = 0$, respectively. Let C be a skew cyclic code over $\mathcal{R}$. Then its Euclidean dual code $C^\perp$ is defined as $C^\perp = \{\mathbf{y} \in \mathcal{R}^n | \langle \mathbf{y}, \mathbf{x} \rangle = 0 \text{ for all } \mathbf{x} \in C\}$. The Hermitian dual code $C_H^\perp$ of C is defined as $C_H^\perp = \{\mathbf{z} \in \mathcal{R}^n | \langle \mathbf{z}, \mathbf{x} \rangle_H = 0 \text{ for all } \mathbf{x} \in C\}$. A code C is called Euclidean or Hermitian self-dual if $C = C^\perp$ or $C = C_H^\perp$, respectively.

Jitman et al. [17] described the algebraic structure of skew constacyclic codes over finite chain rings, and provided the generators of Euclidean and Hermitian dual codes of such codes. The ring $\mathcal{R} = \mathbb{F}_4 \oplus e\mathbb{F}_4$ can be alternatively represented as $\mathbb{F}_4 \oplus u\mathbb{F}_4$ with $u^2 = (e+1)^2 = 0$. This indicates that $\mathcal{R}$ is a finite chain ring under the change of basis.

In this section, Proposition 3.2 delineates a sufficient and necessary condition for Hermitian dual code of a skew cyclic code with length n over $\mathcal{R}$. Proposition 3.3 is the self-dual skew condition of Hermitian dual code. Propositions 3.2 and 3.3 can be seen as corollaries of Theorems 3.7 and 3.8 of [17], respectively. The main work of this section is to depict the structure of Euclidean dual codes of skew cyclic codes over $\mathcal{R}$. Proposition 3.6 illustrates that the Euclidean dual codes of skew cyclic codes of even length generated by a monic polynomial over $\mathcal{R}$ are also free and gives their generator polynomials.

By Lemmas 3.1 and 3.5 of [17], we acquire the following statement.

Lemma 3.1. *Let C be a linear code of length n over $\mathcal{R}$.*

(i) *For any integer n, the code C is a skew cyclic code if and only if $C^\perp$ is skew cyclic.*

(ii) For even integer n, the code C is a skew cyclic code if and only if $C_H^{\perp}$ is skew cyclic.

From [17], the ring automorphism ρ on $\mathcal{R}[x,\theta]$ is given as

$$\rho(\sum_{i=0}^{t} r_i x^i) = \sum_{i=0}^{t} \theta(r_i) x^i.$$

By Theorems 3.7 and 3.8 of [17], we have the following results.

Proposition 3.2. *Let n be even. If $d(x)$ is a monic right divisor of $x^n - 1$ and $\hat{d}(x) = \frac{x^n-1}{d(x)}$, then C is a free skew cyclic code generated by $d(x)$ if and only if $C_H^{\perp}$ is a skew cyclic code generated by*

$$d^{\perp}(x) = \rho(x^{\deg(\hat{d}(x))}\phi(\hat{d}(x))),$$

where $\phi : \mathcal{R}[x,\theta] \to \mathcal{R}[x,\theta]\mathcal{S}^{-1}$ is the anti-monomorphism of rings defined by

$$\phi(\sum_{i=0}^{t} r_i x^i) = \sum_{i=0}^{t} x^{-i} r_i$$

with $\mathcal{S} = \{x^i | i \in \mathbb{N}\}$.

Proposition 3.3. *Let $n = 2k$. If $d(x) = x^k + \sum_{i=0}^{k-1} d_i x^i$ is a right divisor of $x^n - 1$, then the skew cyclic code $C = \langle d(x)\rangle$ is a Hermitian self-dual code if and only if*

$$(x^k + \sum_{i=0}^{k-1} d_i x^i)(\theta^{-k-1}(d_0^{-1})) + \sum_{i=1}^{k-1} \theta^{i-k-1}\left((d_0^{-1} d_{k-i})x^i + x^k\right) = x^n - 1.$$

This is called the self-dual skew condition.

Next, we discuss the algebraic properties of Euclidean dual codes of skew cyclic codes over $\mathcal{R}$.

Lemma 3.4. *Let $d(x), q(x) \in \mathcal{R}[x,\theta]$, where the leading coefficient of $q(x)$ is a unit. If $d(x)q(x) \in Z(\mathcal{R}[x,\theta])$ is a monic polynomial, then $d(x)q(x) = q(x)d(x)$.*

Proof. It is easy to prove by $q(x)(d(x)q(x)) = (d(x)q(x))q(x)$ and Lemma 2.2. □

Lemma 3.5. *Let n be even and $x^n - 1 = q(x)d(x)$, where the leading coefficient of $q(x)$ is a unit. If $C = \langle d(x)\rangle$ is a skew cyclic code of length n over $\mathcal{R}$, then $c(x) \in \mathcal{R}_n$ is in C if and only if $c(x)q(x) = 0$ in $\mathcal{R}_n$.*

Proof. Let $c(x) \in C$. Then $c(x) = r(x)d(x)$ for some $r(x) \in \mathcal{R}[x,\theta]$. Since $x^n - 1 = q(x)d(x) \in Z(\mathcal{R}[x,\theta])$, we have $q(x)d(x) = d(x)q(x)$. Hence $c(x)q(x) = r(x)d(x)q(x) = r(x)q(x)d(x) = 0$ in $\mathcal{R}_n$.

Conversely, if $c(x)q(x) = 0$ in $\mathcal{R}_n$ for some $c(x) \in \mathcal{R}[x,\theta]$, then there exists $r(x) \in \mathcal{R}[x,\theta]$ such that $c(x)q(x) = r(x)(x^n - 1) = r(x)q(x)d(x) = r(x)d(x)q(x)$, i.e., $c(x) = r(x)d(x) \in C$. □

Proposition 3.6. *Let $C = \langle d(x)\rangle$ be a skew cyclic code of even length n over $\mathcal{R}$, where $d(x)$ is a monic right divisor of $x^n - 1$. Let $x^n - 1 = q(x)d(x)$, $q(x) = x^m + \sum_{j=0}^{m-1} q_j x^j$ and $d(x) = x^{n-m} + \sum_{i=0}^{n-m-1} d_i x^i$. Then $C^{\perp}$ is generated by the polynomial $q^*(x) = 1 + \sum_{i=0}^{m} \theta^i(q_{m-i})x^i$.*

Proof. Let $c(x) = \sum_{i=0}^{n-1} c_i x^i$ be a codeword in C. Then $c(x)q(x) = 0$ in $\mathcal{R}_n$ by Lemma 3.5. The coefficients of $x^m, x^{m+1}, \cdots, x^{n-1}$ are all zeros in $c(x)q(x)$. Therefore, we have

$$\begin{aligned} c_0 + c_1\theta(q_{m-1}) + c_2\theta^2(q_{m-2}) + \cdots c_m\theta^m(q_0) &= 0, \\ c_1 + c_2\theta^2(q_{m-1}) + c_3\theta^3(q_{m-2}) + \cdots c_{m+1}\theta^{m+1}(q_0) &= 0, \\ c_2 + c_3\theta^3(q_{m-1}) + c_4\theta^4(q_{m-2}) + \cdots c_{m+2}\theta^{m+2}(q_0) &= 0, \\ &\vdots \\ c_{n-m-1} + c_{n-m}\theta^{n-m}(q_{m-1}) + c_{n-m-1}\theta^{n-m}(q_{m-2}) + \cdots c_{n-1}\theta^{n-1}(q_0) &= 0. \end{aligned}$$

We set

$$Q^* = \begin{pmatrix} 1 & \theta(q_{m-1}) & \theta^2(q_{m-2}) & \dots & \theta^{m-1}(q_1) & \theta^m(q_0) & \dots & 0 \\ 0 & 1 & \theta^2(q_{m-1}) & \dots & \theta^{m-1}(q_2) & \theta^m(q_1) & \dots & 0 \\ 0 & 0 & 1 & \dots & \theta^{m-1}(q_3) & \theta^m(q_2) & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \theta^{n-m}(q_{m-1}) & \dots & \theta^{n-1}(q_0) \end{pmatrix}.$$

It is easy to know that each row vector of Q^* is orthogonal to every codeword in C. Thus, all the row vectors of Q^* are in $C^\perp$. Since C is a Frobenius ring and $\deg(d(x)) = n - m$, then $|C||C^\perp| = |\mathcal{R}|^n$, $|C| = |\mathcal{R}|^m$ and $|C^\perp| = |\mathcal{R}|^{n-m}$. Note that the rows of Q^* are linearly independent. Consequently, the cardinality of the row spanning of Q^* is $|\mathcal{R}|^{n-m}$. It follows that Q^* is a generator matrix of $C^\perp$. Observe that Q^* is a circular matrix, then the corresponding polynomial $q^*(x) = 1 + \sum_{i=0}^{m} \theta^i(q_{m-i})x^i$ is a generator polynomial of $C^\perp$. The proof is done. □

Example 3.7. *Let $C_1 = \langle d_1(x)\rangle$ be a skew cyclic code of length 4 over $\mathcal{R}$. With the same notation as in Example 2.10, by Proposition 3.6, we have that the generated polynomial of dual code $C_1^\perp$ of C_1 is $q_1^*(x) = \omega x^3 + x^2 + \omega x$. The generated matrix of $C_1^\perp$ is*

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

4. Double skew cyclic codes over $\mathcal{R}$

Both double cyclic codes and double skew cyclic codes are good linear codes because of their specific closure properties under the standard shift and addition operations. Double cyclic codes can be extended to double skew cyclic codes. We investigate double skew cyclic codes over $\mathcal{R}$ in this section.

A code C of length n is called double skew linear code if any codeword in C is partitioned into two blocks of lengths n_1 and n_2 such that the set of the first blocks of n_1 symbols and the set of second blocks of n_2 symbols form skew linear codes of lengths n_1 and n_2 over $\mathcal{R}$, respectively.

For any $r \in \mathcal{R}$ and $c = (u_0, u_1, \cdots, u_{n_1-1}, v_0, v_1, \cdots, v_{n_2-1}) \in \mathcal{R}^{n_1+n_2}$, we define

$$rc = (ru_0, ru_1, \cdots, ru_{n_1-1}, rv_0, rv_1, \cdots, rv_{n_2-1}).$$

It implies that $\mathcal{R}^{n_1+n_2}$ is an $\mathcal{R}$-module under the multiplication and a double skew linear code is an $\mathcal{R}$-submodule of $\mathcal{R}^{n_1+n_2}$.

A double linear code C of length $n = n_1 + n_2$ over $\mathcal{R}$ is called double cyclic code if

$$(u_0, u_1, \cdots, u_{n_1-1}, v_0, v_1, \cdots, v_{n_2-1}) \in C$$

implies

$$(u_{n_1-1}, u_0, \cdots, u_{n_1-2}, v_{n_2-1}, v_0, \cdots, v_{n_2-2}) \in C.$$

A double skew linear code C of length $n_1 + n_2$ over $\mathcal{R}$ is called a double skew cyclic code if and only if

$$(\theta(u_{n_1-1}), \theta(u_0), \cdots, \theta(u_{n_1-2}), \theta(v_{n_2-1}), \theta(v_0), \cdots, \theta(v_{n_2-2})) \in C$$

for any codeword

$$c = (u_0, u_1, \cdots, u_{n_1-1}, v_0, v_1, \cdots, v_{n_2-1}) \in C.$$

We denote the codeword $c = (u_0, u_1, \cdots, u_{n_1-1}, v_0, v_1, \cdots, v_{n_2-1}) \in C$ by $c(x) = (c_1(x)|c_2(x))$, where

$$c_1(x) = \sum_{i=0}^{n_1-1} u_i x^i \in \mathcal{R}[x, \theta]/\langle x^{n_1} - 1\rangle$$

and

$$c_2(x) = \sum_{j=0}^{n_2-1} v_j x^j \in \mathcal{R}[x, \theta]/\langle x^{n_2} - 1\rangle.$$

It gives a bijection between $\mathcal{R}^{n_1+n_2}$ and $\mathcal{R}_{n_1,n_2} = \mathcal{R}[x, \theta]/\langle x^{n_1} - 1\rangle \times \mathcal{R}[x, \theta]/\langle x^{n_2} - 1\rangle$. Define the multiplication of any $r(x) \in \mathcal{R}[x, \theta]$ and $(c_1(x)|c_2(x)) \in \mathcal{R}_{n_1,n_2}$ as

$$r(x)(c_1(x)|c_2(x)) = (r(x)c_1(x)|r(x)c_2(x)).$$

Under the multiplication, we have that $\mathcal{R}_{n_1,n_2}$ is a left $\mathcal{R}[x, \theta]$-module. If $c(x) = (c_1(x)|c_2(x))$ is a codeword in C, then $xc(x)$ is the standard skew cyclic shift of c.

Propositions 4.1 to 4.3 depict the structural properties of double skew cyclic codes of length $n_1 + n_2$ over $\mathcal{R}$.

Proposition 4.1. *A code C is a double skew cyclic code over $\mathcal{R}$ if and only if C is a $\mathcal{R}[x, \theta]$-submodule of $\mathcal{R}_{n_1,n_2}$.*

Proof. Let C be a double skew cyclic code and $c = (c_1(x)|c_2(x)) \in C$. Notice that $xc(x) \in C$ and C is linear, then $r(x)c(x) \in C$ for any $r(x) \in \mathcal{R}[x, \theta]$. Therefore C is a left $\mathcal{R}[x, \theta]$-submodule of the left module $\mathcal{R}_{n_1,n_2}$. The converse is trivial. □

Proposition 4.2. *A double skew cyclic code of length $n_1 + n_2$ is a double cyclic code if n_1 and n_2 are both odd.*

Proof. The proof follows by Proposition 2.7. □

Proposition 4.3. *Let $x^{n_1} - 1 = q_1(x)d_1(x)$ and $x^{n_2} - 1 = q_2(x)d_2(x)$, where $d_1(x)$ and $d_2(x)$ are two monic polynomials. If $C_1 = \langle d_1(x)\rangle$ and $C_2 = \langle d_2(x)\rangle$ are two free skew cyclic codes of length n_1 and n_2 over $\mathcal{R}$, respectively, then the code C generated by $d(x) = (d_1(x)|d_2(x))$ is a double skew cyclic code. Furthermore, $\mathcal{A} = \{d(x), xd(x), \cdots, x^{l-1}d(x)\}$ is a spanning set of C, where $l = \deg(q(x))$ and $q(x) = \mathrm{lcm}\{q_1(x), q_2(x)\} = \sum_{i=0}^{l} q_i x^i$.*

Proof. By the definition of double skew cyclic codes, it is clear that $C = \langle d(x)\rangle$ is a double skew cyclic code. The first statement follows. For the second statement, since $q(x)$ is the least common multiple of $q_1(x)$ and $q_2(x)$, we have $q(x)d(x) = q(x)(d_1(x)|d_2(x)) = 0$ and $x^j d(x)$ with $j \geq l$ can be linearly represented by the elements of the set $\mathcal{A} = \{d(x), xd(x), \cdots, x^{l-1}d(x)\}$. Now let $c(x) \in C$ be any non-zero codeword in C. Then $c(x) = a(x)d(x)$ for some $a(x) \in \mathcal{R}[x,\theta]$. If $\deg(a(x)) \geq l$, then $a(x) = p(x)q(x) + r(x)$ by Lemma 2.2, where $r(x) = 0$ or $\deg(r(x)) < \deg(q(x))$. It follows that $c(x) = a(x)d(x) = r(x)d(x)$. Since $r(x) = 0$ or $\deg(r(x)) \leq l - 1$, then any non-zero codeword in C is a linear combination of the elements in $\mathcal{A}$. The proof is done. □

5. Conclusions

In this paper, we examine the structure of skew cyclic codes over $M_2(\mathbb{F}_2)$. All skew cyclic codes of length n over $M_2(\mathbb{F}_2)$ can be identified as left $\mathcal{R}[x,\theta]$-submodules of left module $\mathcal{R}_n = \mathcal{R}[x,\theta]/\langle x^n - 1\rangle$. Our results show that a skew cyclic code C with a polynomial of minimum degree $d(x)$ is a free submodule $\langle d(x)\rangle$. We prove that a skew cyclic code of odd or even length over $M_2(\mathbb{F}_2)$ is a cyclic or 2-quasi-cyclic code. We give the self-dual skew condition of the Hermitian dual code and the generator of Euclidean dual code of a skew cyclic code, respectively. Furthermore, a spanning set of a double skew cyclic code over $M_2(\mathbb{F}_2)$ is obtained.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported by the Natural Science Foundation of Shandong Province, China (Grant number ZR2019BA011) and by the National Natural Science Foundation of China (Grant number 11401285).

Conflict of interest

The authors declare no conflicts of interest.

References

1. T. Abualrub, N. Aydin, P. Seneviratne, On θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, *Australas. J. Comb.*, **54** (2012), 115–126.

2. A. Alahmadi, H. Sboui, P. Solé, O. Yemen, Cyclic codes over $M_2(\mathbb{F}_2)$, *J. Franklin Inst.*, **350** (2013), 2837–2847. https://doi.org/10.1016/j.jfranklin.2013.06.023
3. M. Ashraf, G. Mohammad, On skew cyclic codes over a semi-local ring, *Discrete Math. Algorit. Appl.*, **7** (2015), 1550042. https://doi.org/10.1142/S1793830915500421
4. I. Aydogdu, R. M. Hesari, K. Samei, Double skew cyclic codes over $\mathbb{F}_q$, *Comput. Appl. Math.*, **41** (2022), 126. https://doi.org/10.1007/s40314-022-01833-2
5. C. Bachoc, Applications of coding theory to the construction of modular lattices, *J. Comb. Theory, Ser. A*, **78** (1997), 92–119. https://doi.org/10.1006/jcta.1996.2763
6. S. Bagheri, R. M. Hesari, H. Rezaei, K. Samei, Skew cyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, *Iran. J. Sci. Technol. Trans. Sci.*, **46** (2022), 1469–1475. https://doi.org/10.1007/s40995-022-01352-z
7. S. Bhowmick, S. Bagchi, R. Bandi, Self-dual cyclic codes over $M_2(\mathbb{Z}_4)$, *Discuss. Math.-Gen. Algebra Appl.*, **42** (2022), 349–362. https://doi.org/10.7151/dmgaa.1395
8. A. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inf. Theory*, **45** (1999), 1250–1255. https://doi.org/10.1109/18.761278
9. D. Boucher, W. Geiselmann, F. Ulmer, Skew-cyclic codes, *Appl. Algebra Eng. Commun. Comput.*, **18** (2007), 379–389. https://doi.org/10.1007/s00200-007-0043-z
10. D. Boucher, P. Solé, F. Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, **2** (2008), 273–292. https://doi.org/10.3934/amc.2008.2.273
11. Q. H. Dinh, A. Gaur, P. Kumar, M. K. Singh, A. K. Singh, Cyclic codes over rings of matrices, *Adv. Math. Commun.*, 2022. https://doi.org/10.3934/amc.2022073
12. Q. H. Dinh, S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inf. Theory*, **50** (2004), 1728–1744. https://doi.org/10.1109/TIT.2004.831789
13. J. Gao, Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, *J. Appl. Math. Inf.*, **31** (2013), 337–342. https://doi.org/10.14317/jami.2013.337
14. J. Gao, X. Meng, F. Fu, Weight distribution of double cyclic codes over Galois rings, *Des. Codes Cryptogr.*, **90** (2022), 2529–2549. https://doi.org/10.1007/s10623-021-00914-3
15. F. Gursoy, I. Siap, B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q+v\mathbb{F}_q$, *Adv. Math. Commun.*, **8** (2014), 313–322. https://doi.org/10.3934/amc.2014.8.313
16. H. Islam, O. Prakash, D. Bhunia, On the structure of cyclic codes over $M_2(\mathbb{F}_p + u\mathbb{F}_p)$, *Indian J. Pure Appl. Math.*, **53** (2022), 153–161. https://doi.org/10.1007/s13226-021-00014-x
17. S. Jitman, S. Ling, P. Udomkavanich, Skew constacyclic codes over finite chain rings, *Adv. Math. Commun.*, **6** (2012), 39–63. https://doi.org/10.3934/amc.2012.6.39
18. R. Luo, U. Parampalli, Cyclic codes over $M_2(\mathbb{F}_2+u\mathbb{F}_2)$, *Cryptogr. Commun.*, **10** (2018), 1109–1117. https://doi.org/10.1007/s12095-017-0266-1
19. J. Pal, S. Bhowmick, S. Bagchi, Cyclic codes over $M_4(\mathbb{F}_2)$, *J. Appl. Math. Comput.*, **60** (2019), 749–756. https://doi.org/10.1007/s12190-018-01235-w
20. S. Patel, O. Prakash, H. Islam, Cyclic codes over $M_4(\mathbb{F}_2 + u\mathbb{F}_2)$, *Cryptogr. Commun.*, **14** (2022), 1021–1034. https://doi.org/10.1007/s12095-022-00572-9

21. O. Prakash, S. Patel, Skew cyclic codes over $\mathbb{F}_q[u,v,w]/\langle u^2-1, v^2-1, w^2-1, uv-vu, vw-wv, wu-uw\rangle$, *Discrete Math. Algorit. Appl.*, **14** (2022), 2150113. https://doi.org/10.1142/S1793830921501135

22. M. Shi, T. Yao, A. Alahmadi, P. Solé, Skew cyclic codes over $\mathbb{F}_q+v\mathbb{F}_q+v^2\mathbb{F}_q$, *IEICE T. Fund. Electr., Commun. Comput. Sci.*, **98** (2015), 1845–1848. https://doi.org/10.1587/transfun.E98.A.1845

23. M. Shi, P. Solé, Skew cyclic codes over $\mathbb{F}_q+v\mathbb{F}_q+\cdots+v^{m-1}\mathbb{F}_q$, *Proceedings International Workshop on the Arithmetic of Finite Fields*, 2015.

24. M. Shi, T. Yao, P. Solè, Skew cyclic codes over a non-chain ring, *Chin. J. Electron.*, **26** (2017), 544–547. https://doi.org/10.1049/cje.2017.03.008

25. I. Siap, T. Abualrub, N. Aydin, P. Seneviratne, Skew cyclic codes of arbitrary length, *Int. J. Inf. Coding Theory*, **2** (2011), 10–20. https://doi.org/10.1504/IJICOT.2011.044674

26. J. A. Wood, Code equivalence characterizes finite Frobenius rings, *Proc. Amer. Math. Soc.*, **136** (2008), 699–706. https://doi.org/10.1090/S0002-9939-07-09164-2