Palestine Journal of Mathematics

Vol 13(Special Issue III)(2024) , 216–229

Skew cyclic codes over $\mathbb{F}_q[u_1, u_2, ..., u_r]/\langle u_i^3 - u_i, u_iu_j - u_ju_i\rangle_{i,j=1}^r$

Pradeep Rai, Bhupendra Singh and Ashok Ji Gupta

Communicated by Kuncham S.P.

MSC 2010 Classifications: Primary 94B05, 94B15; Secondary 11A15.

Keywords: Linear codes, Gray Map, Skew polynomial ring, Skew cyclic codes.

Abstract Our paper delves into exploring skew cyclic codes over a generalized class of rings denoted by $\mathcal{T} = T_r$. We define $T_r = \mathbb{F}_q[u_1, u_2, ..., u_r]/\langle u_i^3 - u_i, u_iu_j - u_ju_i\rangle_{i,j=1}^r$, $q = p^m$ and p is some odd prime. Our study introduces a Gray map for the ring $\mathcal{T}$ and explores its properties. Using a decomposition theorem, we analyze the structural features of skew cyclic codes over $\mathcal{T}$. Additionally, we offer a formula to find the count of skew cyclic codes of length n over the ring $\mathcal{T}$ under specific conditions. Further, we derive a criterion to get Linear Complementary Dual (LCD) codes over $\mathcal{T}$ from skew cyclic codes. Moreover, we present a technique for deriving quantum codes from a particular class of skew cyclic codes over $\mathcal{T}$ which contain their dual.

1 Introduction

The extensive algebraic features of cyclic codes make them one of the most intriguing families of codes. Hammous et al. [14] showed the existence of many good non-linear binary codes under the Gray map. Further many researchers studied cyclic codes over various chain and non-chain rings. As a generalization of cyclic codes, Boucher et al. [5] developed the idea of skew-cyclic codes or θ-cyclic codes in 2007, where θ is some automorphism of the finite field being used as code algebra. They further extended their study in [6] We know that cyclic codes of length n over $\mathbb{F}_q$ can be identified as ideals of $\mathbb{F}_q[y]/\langle y^n - 1\rangle$. Skew cyclic codes of arbitrary length were studied by Siap et al. [27]. It is interesting to observe that for an automorphism θ, skew θ-cyclic codes of length n over $\mathbb{F}_q$ can be identified as left submodules in $\mathbb{F}_q[y : \theta]/\langle y^n - 1\rangle$. Here, $\mathbb{F}_q[y : \theta]$ is a non-commutative ring in general and called a skew polynomial ring. In $\mathbb{F}_q[y : \theta]$ addition operation is the usual addition of polynomials and multiplication is defined using the rule $y * ay = \theta(a)y^2$.

Motivated by the study of skew cyclic codes over a finite field, Abualrub, and Seneviratne [1] provided a study of skew cyclic codes over the ring $\mathbf{F}_2 + v\mathbf{F}_2$, where $v^2 = v$. In 2014, Jin [19] studied skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ with $v^2 = 1$. Further, skew cyclic codes over $\mathbf{F}_q + v\mathbf{F}_q$ were investigated by Gao [11] and Gursoy et al. [13] using two different automorphisms. Dertli at al. [9] studied skew cyclic and quasi-cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Yao et al. [29] described the structural properties of skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. Moreover, they provided a formula for the number of skew cyclic codes under certain conditions. Shi et al. [24] studied skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and further Shi et al. [25] extended their study over a more general non-chain ring. Ashraf et al. [2] provided a study of skew-cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. Islam and Prakash [18] studied skew cyclic codes and skew constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. Irwansyah et al. [16] studied Θ_S-cyclic codes over a class of non-chain rings A_k. Later, a more general class of non-chain rings B_k was taken into consideration to study skew cyclic codes by Irwansyah et al. [17]. Recently, many researchers studied skew cyclic and skew constacyclic codes over various non-chain rings and provided many applications of them in the construction of LCD codes, quantum codes, DNA codes, etc. Motivated by these studies, here in this article we choose a class of finite commutative rings denoted by $\mathcal{T}$ and study skew cyclic codes over it.

Linear Complementary Dual(LCD) codes are an important class of linear codes that have many applications including in cryptography for countermeasures against side-channel attacks, fault injection attacks and in secret sharing, etc. They were first introduced by Massey [20] in 1992. A characterization of a cyclic code over a finite field to be an LCD code was discovered

by Yang and Massey [30] in 1994. Recently, Boulanour et al. [7] provided a criterion for skew constacyclic codes to be LCD. We use this criterion to characterize LCD codes from skew cyclic codes over $\mathcal{T}$.

Quantum codes were first discovered by Shor [26] in 1995. In 1998, Calderbank et al. [8] described a method to find quantum error-correcting codes (QEC) using the self-orthogonal classical linear codes over a finite field. Further many classes of quantum MDS codes over $\mathbb{F}_q$ were constructed by Grassl et al. [12]. Qian et al. introduced the initial method for constructing quantum codes from cyclic codes of odd length over the finite chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ in their work [23]. Motivated by these studies many researchers obtained quantum codes using cyclic codes which either contain their dual (dual-containing) or contained in their dual (self-orthogonal) over various chain and non-chain rings. In 2019, Özen et al. [22] derived the conditions for a skew cyclic code over $\mathbb{F}_q$ to be self-orthogonal and dual-containing. Although their criterion for dual-containing skew cyclic codes is incorrect and a correct version of the result is mentioned in [10]. We use the method mentioned in [10] to obtain dual-containing skew cyclic codes over $\mathcal{T}$ and find quantum codes from their Gray images.

In brief, the main accomplishments of this article can be summarized as::

(i) The establishment of a Gray map on $\mathcal{T}$ and an exploration of its characteristics are presented.

(ii) The examination of the attributes of linear codes over $\mathcal{T}$ is conducted using the decomposition method.

(iii) We discuss automorphisms on $\mathcal{T}$ and study skew cyclic codes over them.

(iv) A technique for deriving quantum codes from skew cyclic codes over $\mathcal{T}$ is provided by us.

(v) The skew cyclic LCD codes over $\mathcal{T}$ are characterized by us.

2 Preliminaries

Suppose that $\mathbb{F}_q$ is a finite field with q elements, where $q = p^m$, p is an odd prime and m is a positive integer. A subspace of $\mathbb{F}_q^n$ with dimension k is referred to as a linear code of length n and dimension k over $\mathbb{F}_q$ and denoted as $[n, k]_q$. Let θ be an automorphism of $\mathbb{F}_q$. Skew θ-cyclic shift of a vector $\mathbf{v} = (v_0, v_1, \ldots, v_n)$ is defined as $\sigma_\theta(\mathbf{v}) = (\theta(v_{n-1}), \theta(v_0), \theta v_1, \ldots, \theta(v_{n-2})$. A linear code C of length n over $\mathbb{F}_q$ is said to skew θ-cyclic if $\sigma_\theta(\mathbf{v}) \in C, \forall \mathbf{v} \in C$. Note that if θ is the identity map then C is cyclic code. For a vector $\mathbf{v} = (v_0, v_1, \ldots, v_n) \in \mathbb{F}_q^n, \mathbf{v} \mapsto \sum_{i=0}^{n-1} v_i y^i$ is an isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_q[y; \theta]/\langle y^n - 1\rangle$. Under this isomorphism, a linear code C is a skew cyclic code of length n if and only if it (its image) is a left submodule of $A_n = \mathbb{F}_q[y; \theta]/\langle y^n - 1\rangle$. If the order of θ divides n then A_n is a ring and a linear code C is a skew θ-cyclic code of length n if and only if it (its image) is a left ideal of A_n. The monic generator polynomial $f(y) = \sum_{i=0}^{n-k-1} f_i y^i$ of this ideal is called the generator polynomial of this code and a generator matrix (consisting of basis vectors in rows) of this code is given as:

$$G = \begin{bmatrix} f_0 & f_1 & \ldots & f_{n-k-1} & 0 & \ldots & 0 \\ 0 & \theta(f_0) & \theta(f_1) & \ldots & \theta(f_{n-k-1}) & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \theta^{k-1}(f_0) & \theta^{k-1}(f_1) & \ldots & \theta^{k-1}(f_{n-k-1}) \end{bmatrix}$$

The skew reciprocal polynomial of a polynomial $f(y) = \sum_{i=0}^{k} f_i y^i \in \mathbb{F}_q[x; \theta] \langle y^n - 1\rangle$ is defined as $f^\dagger(y) = \sum_{i_0}^{k} \theta^i(f_{k-i}) y^i \in \mathbb{F}_q[x; \theta] \langle y^n - 1\rangle$. For two vectors $\mathbf{v} = (v_0, v_1, \ldots, v_n)$ and $\mathbf{w} = (w_0, w_1, \ldots, w_n) \in \mathbb{F}_q^n$, their Euclidean inner product is defined as:

$$\mathbf{v}.{}_E\mathbf{w} = \sum_{i=0}^{n-1} v_i w_i.$$

If $q = r^2$ is an even power of some prime then Hermitian inner product of $\mathbf{v}$ and $\mathbf{w}$ is defined as:

$$\mathbf{v}._H\mathbf{w} = \sum_{i=0}^{n-1} v_i\bar{w}_i,$$

where $\bar{w}_i = w_i^r$. The Euclidean dual and Hermitian dual of a linear code $C \subseteq \mathbb{F}_q^n$ are respectively given as:

$$C^{\perp_E} = \{\mathbf{w} \in \mathbb{F}_q^n : \mathbf{v}._E\mathbf{w} = 0, \forall \mathbf{v} \in C\},$$
$$C^{\perp_H} = \{\mathbf{w} \in \mathbb{F}_q^n : \mathbf{v}._E\bar{\mathbf{w}} = 0, \forall \mathbf{v} \in C\}.$$

These definitions and concepts can be obtained in detail in any standard book of coding theory like [15]. Consider $\mathbb{F}_q[u_1, u_2, ..., u_r]/\langle u_i^3 - u_i, u_iu_j - u_ju_i\rangle$, which is a finite commutative ring. Let $T_1 = \mathbb{F}_q[u_1]\langle u_1^3 - u_1\rangle$ and $T_{j+1} = T_j[u_{j+1}]\langle u_{j+1}^3 - u_{j+1}\rangle$ then $\mathcal{T} = T_r$. Let

$$\mathcal{B}_j = \left\{\kappa_{j1} = 1 - u_j^2, \kappa_{j2} = \frac{u_j^2 - u_j}{2}, \kappa_{j3} = \frac{u_j^2 + u_j}{2}\right\}$$

Now let

$$\eta_{i_1i_2...i_r} = \Pi_{j=1}^r \kappa_{ji_j}.$$

Then we can verify that

$$\begin{aligned} \eta_{i_1i_2...i_r}^2 &= \eta_{i_1i_2...i_r} \\ \eta_{i_1i_2...i_r}\eta_{l_1l_2...l_r} &= 0 \\ \sum_{i_1,i_2,...,i_r} \eta_{i_1i_2...i_r} &= 1, \end{aligned} \tag{2.1}$$

where $\sum_{i_1,i_2,...,i_r} = \sum_{i_1=1}^3 \cdots \sum_{i_r=1}^3$. Thus by a decomposition theorem of ring theory

$$\mathcal{T} = \bigoplus_{i_1i_2...i_r} \eta_{i_1i_2...i_r}\mathcal{T} \cong \bigoplus_{i_1i_2...i_r} \eta_{i_1i_2...i_r}\mathbb{F}_q.$$

Thus any $\mathsf{v} \in \mathcal{T}$ can be expressed as

$$\mathsf{v} = \sum_{i_1,i_2,...,i_r} \eta_{i_1i_2...i_r}v_{i_1i_2...i_r}$$

in a unique way, where $v_{i_1i_2...i_r} \in \mathbb{F}_q$ and $i_j \in \{1, 2, 3\}$ for $j = 1, 2, ..., r$.

3 Gray Map

We define a Gray map $\phi : \mathcal{T} \to \mathbb{F}_q^{3^r}$ as

$$\begin{aligned} \phi(\mathsf{v}) &= (v_{i_1i_2...i_r})_{i_1,i_2,...,i_r}M \\ &= (v_{11...1}, \ldots, v_{11...r}, v_{21...1}, \ldots v_{rr...r})M \end{aligned}$$

for all $\mathsf{v} = \sum_{i_1,i_2,...,i_r} \eta_{i_1i_2...i_r}v_{i_1i_2...i_r} \in \mathcal{C}$, where $M \in GL_{3^r}(\mathbb{F}_q)$ is such that $MM^T = \lambda I_{3^r}$, for some $\lambda \in \mathbb{F}_q^*$. The Lee-weight of an element $v \in \mathcal{T}$ is defined as

$$w_L(\mathsf{v}) = w_H(\phi(\mathsf{v})),$$

where w_H denotes the Hamming weight.

We can extend ϕ to $\mathcal{T}^n$ as $\Phi : \mathcal{T}^n \mapsto \mathbb{F}_q^{3^rn}$ as

$$\Phi(\mathbf{v}) = (\phi(\mathsf{v}^0), \phi(\mathsf{v}^1), ..., \phi(\mathsf{v}^{n-1})),$$

for all $\mathbf{v} = (\mathsf{v}^0, \mathsf{v}^1, ..., \mathsf{v}^{n-1}) \in R^n$.

For any $\mathbf{v} = (\mathsf{v}^0, \mathsf{v}^1, ..., \mathsf{v}^{n-1}) \in \mathcal{T}^n$, we define its Lee-weight as

$$w_L(\mathbf{v}) = \sum_{k=0}^{n-1} w_L(v^k)$$

.

And for any two $\mathbf{v}, \mathbf{w} \in R^n$, their Lee distance is define as

$$d_L(\mathbf{v}, \mathbf{w}) = w_L(\mathbf{v} - \mathbf{w}).$$

Theorem 3.1. *The Gray map Φ is a bijective, linear map and it preserves the distance between $(\mathcal{T}^n, d_L)$ and $(\mathbb{F}_q^{3^r n}, d_H)$.*

Proof. Since ϕ is bijective and linear, Φ is also bijective and linear. For the proof of later part, let $\mathbf{r}$ and $\mathbf{t} \in \mathcal{T}^n$ be such that

$$\mathbf{r} = (\mathsf{r}^0, \mathsf{r}^1, ..., \mathsf{r}^{n-1}),\ \mathbf{t} = (\mathsf{t}^0, \mathsf{t}^1, ..., \mathsf{t}^{n-1}),$$

where

$$\mathsf{r}^i = \sum_{i_1 i_2 ... i_r} \eta_{i_1 i_2 ... i_r} r^i_{i_1 i_2 ... i_r},\ \mathsf{t}^i = \sum_{i_1 i_2 ... i_r} \eta_{i_1 i_2 ... i_r} t^i_{i_1 i_2 ... i_r}$$

Now,

$$\begin{aligned}
d_L(\mathbf{r},\ \mathbf{t}) &= wt_L(\mathbf{r} - \mathbf{t}) \\
&= wt_L(\mathsf{r}^0 - \mathsf{t}^0, \mathsf{r}^1 - \mathsf{t}^1, ..., \mathsf{r}^{n-1} - \mathsf{t}^{n-1}) \\
&= \sum_{i=0}^{n-1} wt_L(\mathsf{r}^i - \mathsf{t}^i) \\
&= \sum_{i=0}^{n-1} wt_H(\phi(\mathsf{r}^i - \mathsf{t}^i)) \\
&= \sum_{i=0}^{n-1} wt_H(\phi(\mathsf{r}^i) - \phi(\mathsf{t}^i)) \\
&= wt_H(\phi(\mathsf{r}^0) - \phi(\mathsf{t}^0), \phi(\mathsf{r}^1) - \phi(\mathsf{t}^1), ..., \phi(\mathsf{r}^{n-1}) - \phi(\mathsf{t}^{n-1})) \\
&= wt_H((\phi(\mathsf{r}^0), \phi(\mathsf{r}^1), ..., \phi(\mathsf{r}^{n-1})) - (\phi(\mathsf{t}^0), \phi(\mathsf{t}^1), ..., \phi(\mathsf{t}^{n-1}))) \\
&= wt_H(\Phi(\mathbf{r}) - \Phi(\mathbf{t})) \\
&= d_H(\Phi(\mathbf{r}),\ \Phi(\mathbf{t}))
\end{aligned}$$

Hence, Φ is distance preserving between $(\mathcal{T}^n, d_L)$ and $(\mathbb{F}_q^{3^r n}, d_H)$. □

Theorem 3.2. *For any two $\boldsymbol{c}, \boldsymbol{d} \in \mathcal{T}^n$, $\boldsymbol{c} \perp \boldsymbol{d}$ if and only if $\Phi(\boldsymbol{c}) \perp \Phi(\boldsymbol{d})$. In other words, Φ preserves orthogonality.*

Proof. Let $\mathbf{c}, \mathbf{d} \in \mathcal{T}^n$ such that $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \ldots, \mathsf{c}^{n-1})$ and $\mathbf{d} = (\mathsf{d}^0, \mathsf{d}^1, \ldots, \mathsf{d}^{n-1})$, where $\mathsf{c}^i = \sum_{i_1 i_2 ... i_r} c^i_{i_1 i_2 ... i_r} \eta_{i_1 i_2 ... i_r}$ and $\mathsf{d}^i = \sum_{i_1 i_2 ... i_r} d^i_{i_1 i_2 ... i_r} \eta_{i_1 i_2 ... i_r}$, for $i = 0, 1, 2, \ldots, n-1$. Now, using the definition of Euclidean inner product and properties of primitive orthogonal idempotents, we

get

$$\begin{aligned}
\mathbf{c.d} &= \sum_{i=0}^{n-1} \mathsf{c}^i.\mathsf{d}^i \\
&= \sum_{i=0}^{n-1}\Big(\sum_{i_1 i_2 \ldots i_r} c^i_{i_1 i_2 \ldots i_r}\eta_{i_1 i_2 \ldots i_r}\Big).\Big(\sum_{l_1 l_2 \ldots l_r} d^i_{l_1 l_2 \ldots l_r}\eta_{l_1 l_2 \ldots l_r}\Big) \\
&= \sum_{i=0}^{n-1}\Big(\sum_{i_1 i_2 \ldots i_r} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r}\eta_{i_1 i_2 \ldots i_r}\Big) \qquad (3.1) \\
&= \sum_{i_1 i_2 \ldots i_r}\Big(\sum_{i=0}^{n-1} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r}\Big)\eta_{i_1 i_2 \ldots i_r}. \qquad (3.2)
\end{aligned}$$

and

$$\begin{aligned}
\Phi(\mathbf{c}).\Phi(\mathbf{d}) &= \Phi(\mathbf{c})\Phi(\mathbf{d})^T \\
&= \sum_{i=0}^{n-1} \phi(\mathsf{c}^i)\phi(\mathsf{d}^i)^T \\
&= \sum_{i=0}^{n-1} (c^i_{11\ldots1}, \ldots, c^i_{rr\ldots r}) M M^T (d^i_{11\ldots1}, \ldots, d^i_{rr\ldots r})^T \\
&= \lambda \sum_{i=0}^{n-1}\Big(\sum_{i_1 i_2 \ldots i_r} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r}\Big) \\
&= \lambda \sum_{i_1 i_2 \ldots i_r}\sum_{i=0}^{n-1} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r} \qquad (3.3)
\end{aligned}$$

Since, $\{\eta_{i_1 i_2 \ldots i_r} : i_j \in \{1,2,3\}\}$ is a linearly independent set and $\lambda \in \mathbb{F}_q^*$, from (3.1) and (3.3), we conclude that $\mathbf{c.d} = 0$ if and only if $\Phi(\mathbf{c}).\Phi(\mathbf{d}) = 0$, i.e. $\mathbf{c} \perp \mathbf{d}$ if and only if $\Phi(\mathbf{c}) \perp \Phi(\mathbf{d})$. □

4 Linear Codes over $\mathcal{T}$

An $\mathcal{T}$-submodule of $\mathcal{T}^n$ is called a linear code over $\mathcal{T}$ having length n. For a linear code $\mathcal{C} \subseteq \mathcal{T}^n$ and for $(i_1, i_2, ..., i_r) \in \{1,2,3\}^r$, we define

$$\begin{aligned}
\mathcal{C}_{i_1 i_2 \ldots i_r} = \{w_{i_1 i_2 \ldots i_r} \in \mathbb{F}_q^n : \exists\, w_{l_1 l_2 \ldots l_r} \in \mathbb{F}_q^n, (i_1, i_2, ..., i_r) \neq (l_1, l_2, ..., l_r) \\
\textit{such that} \sum_{l_1, l_2, \ldots, l_r} \eta_{l_1 l_2 \ldots l_r} w_{l_1 l_2 \ldots l_r} \in \mathcal{C}\}.
\end{aligned}$$

Then $\mathcal{C}_{i_1 i_2 \ldots i_r} \subseteq \mathbb{F}_q^n$ are also linear $\forall i_j \in \{1,2,3\}$, $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ and $|\mathcal{C}| = \Pi_{i_1 i_2 \ldots i_r} |\mathcal{C}_{i_1 i_2 \ldots i_r}|$.

For a linear code $\mathcal{C}$ of length n over $\mathcal{T}$, its dual code $\mathcal{C}^\perp$ is defined as

$$\mathcal{C}^\perp = \{w \in \mathcal{T}^n : w.v = 0, \forall v \in \mathcal{C}\},$$

where $w.v$ denotes the usual Euclidean inner product. The code $\mathcal{C}$ is called self-orthogonal if $\mathcal{C}^\perp \subseteq \mathcal{C}$ and self-dual if $\mathcal{C}^\perp = \mathcal{C}$.

Theorem 4.1. *Let $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be an (n, q^k, d_L) linear code over $\mathcal{T}$ then*

(i) $\Phi(\mathcal{C})$ is a $[3^r n, k, d_H]$ linear code over $\mathbb{F}_q$, where $d_H = d_L$,

(ii) $\Phi(\mathcal{C})^\perp = \Phi(\mathcal{C}^\perp)$,

(iii) $\mathcal{C}^\perp = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}^\perp_{i_1 i_2 \ldots i_r}$,

(iv) $\mathcal{C}$ *is a self-orthogonal code if and only if* $\Phi(\mathcal{C})$ *is a self-orthogonal code over* $\mathbb{F}_q$,

(v) $\mathcal{C}$ *is a dual containing code if and only if* $\Phi(\mathcal{C})$ *is a dual containing code over* $\mathbb{F}_q$,

(vi) $\mathcal{C}$ *is a self-dual code if and only if* $\Phi(\mathcal{C})$ *is a self-dual code over* $\mathbb{F}_q$

Proof. Proof of part (a), follows from Theorem 3.1. Part (b) follows from Theorems 3.1 and 3.2. Part (c) follows from Theorem 3.1. Part (d), (e) and (f) can be proved using the fact Φ is bijective and linear from Theorem 3.1. □

Theorem 4.2. *If* $G_{i_1 i_2 ... i_r}$ *is some generator matrix of* $\mathcal{C}_{i_1 i_2 ... i_r}$, $i_j \in \{1, 2, 3\}$ *then*

$$G = \left[\eta_{i_1 i_2 ... i_r} G_{i_1 i_2 ... i_r}\right]_{i_1 i_2 ... i_r} = \begin{bmatrix} \eta_{11...1} G_{11...1} \\ \eta_{11...2} G_{11...1} \\ \vdots \\ \eta_{11...r} G_{11...r} \\ \vdots \\ \eta_{rr...1} G_{rr...1} \\ \vdots \\ \eta_{rr...r} G_{rr...r} \end{bmatrix}$$

and

$$\left[\Phi(\eta_{i_1 i_2 ... i_r} G_{i_1 i_2 ... i_r})\right]_{i_1 i_2 ... i_r} = \begin{bmatrix} \Phi(\eta_{11...1} G_{11...1}) \\ \Phi(\eta_{11...2} G_{11...1}) \\ \vdots \\ \Phi(\eta_{11...r} G_{11...r}) \\ \vdots \\ \Phi(\eta_{rr...1} G_{rr...1}) \\ \vdots \\ \Phi(\eta_{rr...r} G_{rr...r}) \end{bmatrix}$$

are the generator matrices of $\mathcal{C}$ *and* $\Phi(\mathcal{C})$ *respectively.*

Proof. The proof of the above results follows from the fact that Φ is bijective and linear proved in Theorem 3.1. □

5 Skew cyclic Codes over $\mathcal{T}$

This section focuses on the characteristics of skew cyclic codes over $\mathcal{T}$. We will first look at the automorphisms of $\mathcal{T}$.

Let $\Theta : \mathcal{T} \to \mathcal{T}$ be an automorphism. Then $\Theta|_{\mathbb{F}_q}$, the restriction map over $\mathbb{F}_q$ is an $\mathbb{F}_q$-automorphism. Therefore $\Theta|_{\mathbb{F}_q} = \theta_t : a \longmapsto a^{p^t}$ for some t such that $0 \leq t \leq m-1$ where $q = p^m$ and $a \in \mathbb{F}_q$. Thus for $\sum_{i_1, i_2, ..., i_r} \eta_{i_1 i_2 ... i_r} v_{i_1 i_2 ... i_r} \in \mathcal{T}$, we have

$$\Theta\Big(\sum_{i_1, i_2, ..., i_r} \eta_{i_1 i_2 ... i_r} v_{i_1 i_2 ... i_r}\Big) = \sum_{i_1, i_2, ..., i_r} \Theta(\eta_{i_1 i_2 ... i_r}) v^{p^t}_{i_1 i_2 ... i_r}.$$

From eq. 2.1, we conclude that the set $\{\eta_{i_1 i_2 ... i_r} : i_j \in \{1, 2, 3\} \; for \; j = 1, 2, ..., r\}$ is a complete set in $\mathcal{T}$. Therefore, the set $\{\Theta(\eta_{i_1 i_2 ... i_r}) : i_j \in \{1, 2, 3\} \; for \; j = 1, 2, ..., r\}$ is permutation of the set $\{\eta_{i_1 i_2 ... i_r} : i_j \in \{1, 2, 3\} \; for \; j = 1, 2, ..., r\}$. Hence, $\exists\, \gamma_j \in S_3$, the permutation group of $\{1, 2, 3\}$, for $j = 1, 2, ..., r$ such that $\Theta(\eta_{i_1 i_2 ... i_r}) = \eta_{\gamma_1(i_1)\gamma_2(i_2)...\gamma_r(i_r)}$. Therefore

$$\Theta\Big(\sum_{i_1, i_2, ..., i_r} \eta_{i_1 i_2 ... i_r} v_{i_1 i_2 ... i_r}\Big) = \sum_{i_1, i_2, ..., i_r} \eta_{\gamma_1(i_1)\gamma_2(i_2)...\gamma_r(i_r)} v^{p^t}_{i_1 i_2 ... i_r}.$$

Whenever γ_j are identity permutation for all $j = 1, 2, ..., r$ and $\Theta|_{\mathbb{F}_q} = \theta_t$ then we denote Θ by Θ_t. For any element $\alpha = (\alpha^0, \alpha^1, \ldots, \alpha^{n-1}) \in \mathcal{T}^n$, its Θ-cyclic shift is defined as:

$$\sigma_\Theta(\alpha) = (\Theta(\alpha_{n-1}), \Theta(\alpha_0), \ldots, \Theta(\alpha_{n-2}).$$

Definition 5.1. For an automorphism Θ of $\mathcal{T}$, $\mathcal{C} \subseteq \mathcal{T}^n$ is called a skew Θ-cyclic code of length n, if it is linear and $\sigma_\Theta(\alpha) \in \mathcal{C}$ whenever $\alpha \in \mathcal{C}$.

For an automorphism Θ of $\mathcal{T}$, $\mathcal{T}[y; \Theta]$ is a non-commutative ring(in general) under usual addition of polynomials and multiplication defined as $y * ay = \Theta(a)y^2$ and it is called skew-Θ polynomial ring. Moreover, for a vector $\mathbf{v} = (\mathsf{v}^0, \mathsf{v}^1, \ldots, \mathsf{v}^{n-1}) \in \mathcal{T}^n, \mathbf{v} \mapsto \sum_{i=0}^{n-1} \mathsf{v}^i y^i$ is an isomorphism between $\mathcal{T}^n$ and $\mathcal{T}[y; \Theta]/\langle y^n - 1\rangle$. Under this isomorphism, a linear code C is a skew Θ-cyclic code of length n if and only if it (its image) is a left submodule of $A_n = \mathcal{T}[y; \Theta]/\langle y^n - 1\rangle$. If the order of Θ divides n then A_n is a ring and a linear code C is a skew Θ-cyclic code of length n if and only if it (its image) is a left ideal of A_n.

Theorem 5.2. *Suppose that $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ is a linear code of length n over $\mathcal{T}$. Then $\mathcal{C}$ is a Θ_t-skew cyclic code over $\mathcal{T}$ if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ are θ_t-skew cyclic code over $\mathbb{F}_q$, for all $i_j \in \{1, 2, 3\}$.*

Proof. Let $\mathcal{C}_{i_1 i_2 \ldots i_r}$ be skew θ_t-cyclic codes for all $i_j \in \{1, 2, 3\}$. Let $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \mathsf{c}^2, \ldots, \mathsf{c}^{n-1}) \in \mathcal{C}$. Suppose that for $l \in \{0, 1, \ldots, n-1\}$, $\mathsf{c}^l = \sum_{i_1 i_2 \ldots i_r} c^l_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}$. Then

$$(c^0_{i_1 i_2 \ldots i_r}, c^1_{i_1 i_2 \ldots i_r}, \ldots, c^{n-1}_{i_1 i_2 \ldots i_r}) \in \mathcal{C}_{i_1 i_2 \ldots i_r}.$$

Since $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is a θ_t-skew cyclic code for all $i_j \in \{1, 2, 3\}$, we have

$$\sigma_{\theta_t}((c^0_{i_1 i_2 \ldots i_r}, c^1_{i_1 i_2 \ldots i_r}, \ldots, c^{n-1}_{i_1 i_2 \ldots i_r})) = (\theta(c^{n-1}_{i_1 i_2 \ldots i_r}), \theta(c^0_{i_1 i_2 \ldots i_r}), \theta(c^1_{i_1 i_2 \ldots i_r}), \ldots, \theta(c^{n-2}_{i_1 i_2 \ldots i_r})) \in \mathcal{C}_{i_1 i_2 \ldots i_r}, \forall i_j \in \{1, 2, 3\}.$$

Thus $\sum_{i_1 i_2 \ldots i_r} (\theta(c^{n-1}_{i_1 i_2 \ldots i_r}), \theta(c^0_{i_1 i_2 \ldots i_r}), \theta(c^1_{i_1 i_2 \ldots i_r}), \ldots, \theta(c^{n-2}_{i_1 i_2 \ldots i_r})) \eta_{i_1 i_2 \ldots i_r}$
$= (\sum_{i_1 i_2 \ldots i_r} c^{n-1}_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}, \sum_{i_1 i_2 \ldots i_r} c^0_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}, \ldots, \sum_{i_1 i_2 \ldots i_r} c^{n-2}_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r})$
$= (\Theta(\mathsf{c}^{n-1}), \Theta(\mathsf{c}^0), \Theta(\mathsf{c}^1), \Theta(\mathsf{c}^2), ..., \Theta(\mathsf{c}^{n-2})) = \sigma_\Theta(\mathbf{c}) \in \mathcal{C}$. This proves that $\mathcal{C}$ is skew Θ_t-cyclic.

Next, let us assume that $\mathcal{C}$ is skew Θ_t-cyclic. Let $(c^0_{i_1 i_2 \ldots i_r}, c^1_{i_1 i_2 \ldots i_r}, \ldots, c^{n-1}_{i_1 i_2 \ldots i_r}) \in \mathcal{C}_{i_1 i_2 \ldots i_r}$., for $i_j \in \{1, 2, 3\}$ then
$\sum_{i_1 i_2 \ldots i_r} (c^0_{i_1 i_2 \ldots i_r}, c^1_{i_1 i_2 \ldots i_r}, ..., c^{n-1}_{i_1 i_2 \ldots i_r}) \eta_{i_1 i_2 \ldots i_r}$
$= (\sum_{i_1 i_2 \ldots i_r} c^0_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}, \sum_{i_1 i_2 \ldots i_r} c^1_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}, ..., \sum_{i_1 i_2 \ldots i_r} c^{n-1}_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}) \in \mathcal{C}$.
Since $\mathcal{C}$ is skew Θ_t-cyclic,
$(\Theta_t(\sum_{i_1 i_2 \ldots i_r} c^{n-1}_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}), \Theta_t(\sum_{i_1 i_2 \ldots i_r} c^0_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}), \ldots, \Theta_t(\sum_{i_1 i_2 \ldots i_r} c^{n-2}_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}))$
$= \sum_{i_1 i_2 \ldots i_r} (\theta_t(c^{n-1}_{i_1 i_2 \ldots i_r}), \theta_t(c^0_{i_1 i_2 \ldots i_r}), \theta_t(c^1_{i_1 i_2 \ldots i_r}), ..., \theta_t(c^{n-2}_{i_1 i_2 \ldots i_r})) \eta_{i_1 i_2 \ldots i_r}$
$\in \mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r}$. This implies that

$$(\theta_t(c^{n-1}_{i_1 i_2 \ldots i_r}), \theta_t(c^0_{i_1 i_2 \ldots i_r}), ..., \theta_t(c^{n-2}_{i_1 i_2 \ldots i_r})) = \sigma_{\theta_t}(c^0_{i_1 i_2 \ldots i_r}, c^1_{i_1 i_2 \ldots i_r}, ..., c^{n-1}_{i_1 i_2 \ldots i_r}) \in \mathcal{C}_{i_1 i_2 \ldots i_r},$$

for all $i_j \in \{1, 2, 3\}$ which proves that they all are skew θ_t-cyclic. □

Corollary 5.3. *If the order of Θ_t divides n, the dual code of a skew Θ_t-cyclic code of length n over $\mathcal{T}$ is also a skew Θ_t-cyclic code.*

Theorem 5.4. *Suppose that $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ is a skew Θ_t-cyclic code of length n over $\mathcal{T}$. Let $\mathcal{C}_{i_1 i_2 \ldots i_r} = \langle f_{i_1 i_2 \ldots i_r}(y)\rangle$, where $f_{i_1 i_2 \ldots i_r}(y)$ are monic right divisors of $y^n - 1$ and $i_j \in \{1, 2, 3\}$, for $j = 1, 2, ..., r$. Then $\exists$ a polynomial $f(y)$ in $\mathcal{T}[y; \theta_t]$ such that*

(i) $\mathcal{C} = \langle f(y)\rangle$

(ii) f(y) is right divisor of $y^n - 1$

(iii) $|\mathcal{C}| = q^{3^r n - \sum_{i_1, i_2, \ldots, i_r} deg(f_{i_1 i_2 \ldots i_r}(y))}$

Proof. Since $\mathcal{C}_{i_1i_2...i_r} = \langle f_{i_1i_2...i_r}(y)\rangle$, for $i_j \in \{1,2,3\}$ and $\mathcal{C} = \bigoplus_{i_1i_2...i_r} \eta_{i_1i_2...i_r}\mathcal{C}_{i_1i_2...i_r}$, then

$$\mathcal{C} = \left\{ c(y) = \sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} r_{i_1i_2...i_r}(y) f_{i_1i_2...i_r}(y) | r_{i_1i_2...i_r}(y) \in \mathbb{F}_q[y;\theta_t] \right\}.$$

Hence $\mathcal{C} \subseteq \langle \eta_{11...1}f_{11...1}(y), \ldots, \eta_{rr...r}f_{rr...r}(y)\rangle$. Conversely, for any

$$\sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} k_{i_1i_2...i_r}(y) f_{i_1i_2...i_r}(y) \in \langle \eta_{11...1}f_{11...1}(y), \ldots, \eta_{rr...r}f_{rr...r}(y)\rangle,$$

where $k_{i_1i_2...i_r}(y) \in \mathbb{F}_q[y;\theta_t]/\langle y^n - 1\rangle$, there exist $r_{i_1i_2...i_r}(y) \in \mathbb{F}_q[y;\theta_t]$ such that

$$\eta_{i_1i_2...i_r} k_{i_1i_2...i_r}(y) = \eta_{i_1i_2...i_r} r_{i_1i_2...i_r}(y)$$

. Thus $\langle \eta_{11...1}f_{11...1}(y), \ldots, \eta_{rr...r}f_{rr...r}(y)\rangle \subseteq \mathcal{C}$. Hence

$$\langle \eta_{11...1}f_{11...1}(y), \ldots, \eta_{rr...r}g_{rr...r}(y)\rangle = \mathcal{C}.$$

Now let $f(y) = \sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} f_{i_1i_2...i_r}(y)$ then $\langle f(y)\rangle \subseteq \mathcal{C}$. Also since $\eta_{i_1i_2...i_r}f_{i_1i_2...i_r} = \eta_{i_1i_2...i_r}f_{i_1i_2...i_r}$, for all $i_j \in \{1,2,3\}$ so $\mathcal{C} \subseteq \langle f(y)\rangle$. Hence $\mathcal{C} \subseteq \langle f(y)\rangle$. Further as $f_{i_1i_2...i_r}(y)$ divides $y^n - 1 \in \mathbb{F}_q[y : \theta_t]$ and are monic as well for all $i_j \in \{1,2,3\}$. Thus $y^n - 1 = g_{i_1i_2...i_r}(y) f_{i_1i_2...i_r}(y)$ for some $g_{i_1i_2...i_r}(y) \in \mathbb{F}_q[y : \theta_t]$. Therefore,

$$\begin{aligned}
(\sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} g_{i_1i_2...i_r}(y)) f(y) &= (\sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} g_{i_1i_2...i_r}(y))(\sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} f_{i_1i_2...i_r}(y)) \\
&= \sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} g_{i_1i_2...i_r}(y) f_{i_1i_2...i_r}(y) \\
&= \sum_{i_1i_2...i_r} \eta_{i_1i_2...i_r} (y^n - 1) \\
&= y^n - 1 \in \mathcal{T}[y;\Theta_t].
\end{aligned}$$

Hence $f(y)$ divides $y^n - 1$ from right. Since $|\mathcal{C}| = \Pi_{i_1i_2...i_r} |\mathcal{C}_{i_1i_2...i_r}|$, we get

$$|\mathcal{C}| = q^{3^r n - \sum_{i_1,i_2,\ldots,i_r} deg(f_{i_1i_2...i_r}(y))}.$$

□

Example 5.5. Let $q = 5^2$ then $\mathbb{F}_q = GF[5]/\langle X^2 + 4X + 2\rangle$ and let s be a root of $X^2 + 4X + 2$. Consider the ring $\mathbb{F}_q/\langle u_1^3 - u_1, u_2^3 - u_2, u_1u_2 - u_2u_1\rangle$. Let $\theta = \theta_1$ be the Frobenius map i.e.

$$a \longmapsto a^5.$$

Then the order of θ is 2. Now consider the factorization of $x^4 - 1$ in $\mathbb{F}_q[x;\theta]$.

$$\begin{aligned}
y^4 - 1 &= (y + 2s + 1)(y + 2s + 2)(y + 4s + 4)(y + 4s + 2) \\
&= (y + 4)(y + 1)(y + 2)(y + 3) \\
&= (y + 2s + 1)(y + 2s + 2)(y + 3)(y + 2) \\
&= (y + 2s + 1)(y + 2s + 2)(y + s + 1)(y + s + 3)
\end{aligned}$$

Let $f(y) = (y + 4s + 4)(y + 4s + 2) = y^2 + (s + 1)y + 1$ which is a right divisor of $y^4 - 1$. Then for all $i_j \in \{1,2,3\}$, let $\mathcal{C}_{i_1i_2...i_r} = \langle f(x)\rangle$ is a skew cyclic code. A generator matrix of $\mathcal{C}_{i_1i_2...i_r}$ is given as:

$$\begin{bmatrix} 1 & s+1 & 1 & 0 \\ 0 & 1 & 4s^2+2 & 1 \end{bmatrix}$$

$\mathcal{C}_{i_1i_2...i_r}$ are $[4,2,3]$ skew cyclic codes over $\mathbb{F}_q$ which is MDS. Hence, $\mathcal{C} = \bigoplus_{i_1i_2...i_r} \eta_{i_1i_2...i_r}\mathcal{C}_{i_1i_2...i_r}$ is a skew cyclic code of length 4 over $\mathcal{T}$ with minimum Lee distance $d_L = 3$.

Theorem 5.6. *A skew Θ-cyclic code $\mathcal{C} \subseteq \mathcal{T}^n$ is a quasi cyclic code of index ν, where $\nu = \frac{n}{(n,O(\theta))}$.*

Proof. Suppose that $n_\Theta = (n, O(\Theta))$ and $n = n_\Theta l$. By extended Euclidean algorithm, we find two integers c' and d' satisfying $n_\theta = c'O(\Theta) + d'n$. If $d' > 0$, find $e \in \mathbb{N}$ satisfying $O(\Theta)e - d' > 0$. Then $(c' + ne)O(\Theta) = n_\Theta + (O(\Theta)e - d')n$. In this case, take $c = c' + ne$ and $d = O(\Theta)e - d'$. Otherwise if $d' < 0$, then simply take $c = c'$ and $d = -d'$. Thus we have $cO(\Theta) = n_\Theta + dn$. Let

$$\mathbf{w} = (w_{0,0}, w_{0,1}, \ldots, w_{0,n_\Theta-1}, w_{1,0}, w_{1,1}, \ldots, w_{1,n_\Theta-1}, \ldots, w_{l-1,0}, w_{l-1,1}, \ldots, w_{l-1,n_\Theta-1}) \in \mathcal{C}.$$

Say $\mathbf{w} = (\mathsf{w}^0, \mathsf{w}^1, \ldots, \mathsf{w}^{l-1})$, where $\mathsf{w}^i = (w_{i,0}, w_{i,1}, \ldots, w_{i,n_\theta-1})$. Now since $\mathcal{C}$ is a skew cyclic code, $\sigma_\Theta(\mathbf{w}), \sigma_\Theta^2(\mathbf{w}), \ldots, \sigma_\Theta^{n_\Theta}(\mathbf{w}), \ldots, \sigma_\Theta^{n_\theta+dn}(\mathbf{w}), \ldots \in \mathcal{C}$. Since $n_\Theta + dn$ is divisible by $O(\Theta)$, we have

$$\begin{aligned}\sigma_\Theta^{n_\Theta+dn} &= (\Theta^{n_\Theta+dn}(\mathsf{w}^{l-1}), \Theta^{n_\Theta+dn}(\mathsf{w}^0), \Theta^{n_\Theta+dn}(\mathsf{w}^1), \ldots, \Theta^{n_\Theta+dn}(\mathsf{w}^{l-2})) \\ &= (\mathsf{w}^{l-1}, \mathsf{w}^0, \ldots, \mathsf{w}^{l-2}) \\ &= \tau_{id,l}(\mathbf{w}) \in \mathcal{C}\end{aligned}$$

This shows that $\forall\ \mathbf{w} \in \mathcal{C}$, $\tau_{id,l}(\mathbf{w}) \in \mathcal{C}$. Hence, $\mathcal{C}$ is a quasi-cyclic code of index l. In particular, if $n_\Theta = 1$, then $n = l$ and so $\mathcal{C}$ is cyclic. □

Corollary 5.7. *Let $(n, O(\Theta_t)) = 1$ and $y^n - 1 = \Pi_{k=1}^s f_k(y)^{n_k}$, where $f_k(y)$ are irreducible factors. Then the number of skew θ_t-cyclic codes of length n over $\mathcal{T}$ is $\Pi_{k=1}^s (n_k + 1)^{3^r}$.*

Example 5.8. Let $q = 3^4$ then $\mathbb{F}_q = GF[3]/\langle X^4 + 2X^3 + 2\rangle = \mathbb{F}_3(\beta)$ where β is a root of $X^4 + 2X^3 + 2$. Further, let $r = 3$. Then $\mathcal{T} = T_3 = \mathbb{F}_{81}/\langle u_1^3 - u_1, u_2^3 - u_2, u^3 - u_3, u_1u_2 - u_2u_1, u_1u_3 - u_3u_1, u_2u_3 - u_3u_2\rangle$. Let Θ_1 be an automorphism of $\mathcal{T}$ such that $\Theta_1(\eta_{i_1i_2i_3}) = \eta_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = (23), \gamma_2 = (123)$ and $\gamma_3 = (132) \in S_3$ the permutation group of $\{1, 2, 3\}$ and $\Theta_1|_{\mathbb{F}_{81}} = \theta_1$ the Frobenius map i.e. $\theta_1 : a \longmapsto a^3$. Then the order of θ_1 is 4 and that of Θ_1, $O(\Theta_1) = lcm(2, 3, 3, 4) = 12$. Now let $n = 24$ and then from the factorization of $y^{24} - 1$ in $\mathbb{F}_{81}[x; \theta_1]$ we observe that $u(y) = y^{17} + (\beta^2 + \beta + 1)y^{16} + 2y^{13} + (2\beta^2 + 2\beta + 2)y^{12} + y^5 + (\beta^2 + \beta + 1)y^4 + 2y + 2\beta^2 + 2\beta + 2$ is a right divisor of $y^{24} - 1$. Let $\mathcal{C}_{i_1i_2i_3} = \langle u(y)\rangle$ for all $i_j \in \{1, 2, 3\}$. Thus $\mathcal{C}_{i_1i_2i_3}$ is a skew θ_1-cyclic code of length 24 and minimum distance 6. Since $gcd(24, 12) = 12 > 1$. Hence by Theorem 5 skew Θ_1-cyclic code $\mathcal{C} = \bigoplus_{i_1i_2i_3} \eta_{i_1i_2i_3}\mathcal{C}_{i_1i_2i_3}$ is a quasi-cyclic code of index $2(= 24/12)$ and $d_L = 6$.

Again Let Θ_2 be another automorphism of $\mathcal{T}$ such that $\Theta_2(\eta_{i_1i_2i_3}) = \eta_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = \gamma_2 = \gamma_3 = id$, the identity permutation and $\Theta_2|_{\mathbb{F}_{81}} = \theta_1$ the Frobenius map i.e. $\theta_1 : a \longmapsto a^3$. Then $O(\Theta_2) = lcm(1, 1, 1, 4) = 4$. Suppose that $n = 15$ then $gcd(15, 4) = 1$ and hence by Theorem 5 any skew Θ_2-cyclic code is cyclic. Thus $y^n - 1$ has a unique factorization as:

$$y^{15} - 1 = (y^4 + y^3 + y^2 + y + 1)^3(y + 2)^3.$$

Hence by Corollary 5.7, there are $(3 + 1)^{27} \times (3 + 1)^{27} = 4^{54}$ skew Θ_2-cyclic codes over $\mathcal{T}$ in total.

Finally Let Θ_3 be an automorphism of $\mathcal{T}$ where $\gamma_1 = (12), \gamma_2 = (13)$ and $\gamma_3 = (23) \in S_3$ and $\Theta_3|_{\mathbb{F}_{81}} = \theta_2$ i.e. $\theta_2 : a \longmapsto a^{3^2} = a^9$. Now $o(\gamma_1) = o(\gamma_2) = o(\gamma_3) = o(\theta_2) = 2$ and so $O(\Theta_3) = lcm(2, 2, 2, 2) = 2$. If we take $n = 8$ then by Theorem 5, any skew Θ_3-cyclic code is a quasi-cyclic code of index 4 and any skew Θ_3-cyclic code over $\mathcal{T}$ of odd length is cyclic.

Example 5.9. Let $q = 5^3$ then $\mathbb{F}_q = GF[5]/\langle X^3 + 3X + 3\rangle = \mathbb{F}_3(\delta)$ where δ is a root of $X^3 + 3X + 3$. Further, let $r = 2$. Then $\mathcal{T} = T_2 = \mathbb{F}_{125}/\langle u_1^3 - u_1, u_2^3 - u_2, u_1u_2 - u_2u_1\rangle$. Let Θ_1 be an automorphism of $\mathcal{T}$ such that $\Theta_1(\eta_{i_1i_2i_3}) = \eta_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = (123), \gamma_2 = (132)$ and $\gamma_3 = (123) \in S_3$ the permutation group of $\{1, 2, 3\}$ and $\Theta_1|_{\mathbb{F}_{125}} = \theta_1$ the Frobenius map i.e. $\theta_1 : a \longmapsto a^5$. Then the order of θ_1 is 3 and that of Θ_1, $O(\Theta_1) = lcm(3, 3, 3, 3) = 3$. Now let $n = 18$ and then from the factorization of $y^{18} - 1$ in $\mathbb{F}_{125}[x; \theta_1]$ we observe that $u(y) = y^{12} + y^9 + 4y^3 + 4$ is a right divisor of $y^{18} - 1$. Let $\mathcal{C}_{i_1i_2i_3} = \langle u(y)\rangle$ for all $i_j \in \{1, 2, 3\}$. Thus $\mathcal{C}_{i_1i_2i_3}$ is a skew θ_1-cyclic code of length 18 and minimum distance 4. Since $gcd(18, 3) = 3 > 1$.

Hence by Theorem 5, the skew Θ_1-cyclic code $\mathcal{C} = \bigoplus_{i_1 i_2 i_3} \eta_{i_1 i_2 i_3} \mathcal{C}_{i_1 i_2 i_3}$ is a quasi-cyclic code of index $6(= 18/3)$ and $d_L = 4$.

Again Let Θ_2 be another automorphism of $\mathcal{T}$ such that $\Theta_2(\eta_{i_1 i_2 i_3}) = \eta_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = \gamma_2 = \gamma_3 = id$, the identity permutation and $\Theta_2|_{\mathbb{F}_{125}} = \theta_2$ i.e. $\theta_2 : a \longmapsto a^{10}$. Then $O(\Theta_2) = lcm(1, 1, 1, 3) = 3$. Suppose that $n = 20$ then $gcd(20, 3) = 1$ and hence by Theorem 5, any skew Θ_2-cyclic code is cyclic. Thus $y^n - 1$ has a unique factorization as:

$$y^{20} - 1 = (y + 4)^5 (y + 2)^5 (y + 3)^5 (y + 1)^5.$$

Hence by Corollary 5.7, there are $(5+1)^9 \times (5+1)^9 \times (5+1)^9 \times (5+1)^9 = 6^{36}$ skew Θ_2-cyclic codes over $\mathcal{T}$ in total.

6 Construction of Quantum Codes

The focus of this section is on building quantum codes from skew cyclic codes over $\mathcal{T}$. We begin by revisiting the definition of quantum codes and the CSS construction. We also revisit a criterion for identifying dual-containing skew cyclic codes over $\mathbb{F}_q$, which we leverage to characterize dual-containing skew cyclic codes over $\mathcal{T}$. We then present an approach to generate quantum codes from dual-containing skew cyclic codes over $\mathcal{T}$, and we use this method to construct a novel quantum code.

Definition 6.1. (Quantum Codes) Let H be a q-dimensional Hilbert space over the field of complex numbers $\mathbb{C}$. Then n-fold tensor product of H defined as $H^{\otimes n} = H \otimes H \otimes ... \otimes H$ $(n\ times)$ is a q^n-dimensional Hilbert space. A k- dimensional subspace of $H^{\otimes n}$ is called an $[[n, k]]_q$ quantum code.

Lemma 6.2. ***(CSS Construction)*** *([8], Theorem 3) Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ such that $C^{\perp} \subseteq C$, then there exists a $[[n, 2k - n, d]]_q$ QECC (quantum error correcting code).*

Lemma 6.3. *([10], Corollary 5.7) Let C be skew θ-cyclic code of length n over $\mathbb{F}_q$ such that $ord(\theta) \mid n$. If $f(y)$ is the generator polynomial of C such that $g(y)f(y) = y^n - 1$. Then C contains its dual if and only if $g^{\dagger}(y)g(y)$ is divisible by $y^n - 1$ from the right.*

Theorem 6.4. *Let $\mathcal{C} = \bigoplus_{i_1 i_2 ... i_r} \eta_{i_1 i_2 ... i_r} \mathcal{C}_{i_1 i_2 ... i_r}$ be a skew Θ_t-cyclic code of length n over $\mathcal{T}$ such that $ord(\Theta_t) \mid n$ and $f_{i_1 i_2 ... i_r}(y)$ is the generator polynomial of $\mathcal{C}_{i_1 i_2 ... i_r}$ and $g_{i_1 i_2 ... i_r} f_{i_1 i_2 ... i_r}(y) = y^n - 1, \forall i_j \in \{1, 2, 3\}$.*

(i) $\mathcal{C}$ contains its dual if and only if $g^{\dagger}_{i_1 i_2 ... i_r}(y) g_{i_1 i_2 ... i_r}(y)$ is divisible by $y^n - 1$ from right, $\forall\ i_j \in \{1, 2, 3\}$.

(ii) If $g^{\dagger}_{i_1 i_2 ... i_r}(y) g_{i_1 i_2 ... i_r}(y)$ is divisible by $y^n - 1$ from right, $\forall\ i_j \in \{1, 2, 3\}$ then there exist a quantum code of dimension $[[N, K, d]]_q$, where $K = 3^r n - 2\sum_{i_1 i_2 ... i_r} deg(f_{i_1 i_2 ... i_r}(y))$, $N = 3^r n$ and $D = d_L$, the Lee distance of $\mathcal{C}$.

Proof. Proof of part(i) follows from part(iii) of Theorem 4.1 and Lemma 6.3. Combining part (i) and Lemma 6.2, part(ii) follows. □

Example 6.5. Let $q = 25$ and $r = 1$ then $\mathcal{T} = \mathbb{F}_{25}/\langle u_1^3 - u_1\rangle$. Let θ_1 be the Frobenius automorphism and $\gamma_1 = id$ the identity permutation. So $\Theta : \mathcal{T} \to \mathcal{T}$ defined as

$$w_1\eta_1 + w_2\eta_2 + w_3\eta_3 \longmapsto w_1^5\eta_1 + w_2^5\eta_2 + w_3^5\eta_3$$

is an automorphism. Let $n = 8$. Consider two factorisations of $y^n - 1 \in \mathbb{F}_{25}[y; \theta_1]$ as:
$y^8 - 1 = (y+3w+3)(y+3w+4)(y+w+2)^2(y+4w+2)(y+4w+4)(y+4w+1)(y+4w) = (y + 2w + 1)(y + 2w + 2)(y + 2w)(y + 2w + 3)(y + 4w + 1)(y + w + 1)(y + 2w + 4)(y + 3)$, where w is a primitive of $\mathbb{F}_{25}$.
Let us take $f_1(y) = y+4w$, $f_2(y) = 1$ and $f_3(y) = (y+2w+4)(y+3) = y^2+(2w+2)y+w+2$ and $y^n - 1 = g_i(y)f_i(y)$. Then $g_i^*(y)g_i(y)$ is divisible by $y^n - 1$ for all $i = 1, 2, 3$. Take

$$M = \begin{bmatrix} 3 & 3 & 1 \\ 1 & 3 & 3 \\ 2 & 4 & 2 \end{bmatrix}$$

then $MM^T = 4I_3$. Let $\mathcal{C}_i = \langle f_i(y) \rangle$ and $\mathcal{C} = \bigoplus_{i=1}^{3} \eta_i \mathcal{C}_i$ then $\Phi(\mathcal{C})$ is a dual-containing $[24, 21, 3]_{25}$ code. Hence by Theorem 6.4, there exists a $[[24, 18, 3]]_{25}$ quantum code which is a new code as per database [4].

7 LCD Codes

In this section, our focus is on LCD codes over $\mathcal{T}$. We begin by reviewing essential criteria established by Boulanour et al. [7] that identify when a skew cyclic code over a finite field is LCD. We then present a technique for deriving LCD codes from skew cyclic codes over $\mathcal{T}$, based on these criteria and a decomposition method for skew cyclic codes. The section concludes with illustrative examples.

Definition 7.1. ([20]) A linear code $\mathcal{C}$ whose Hull is trivial, is called a Linear Complementary Dual (LCD) code.

In [7], Boulanour et al. provided a criterion for skew constacyclic codes to be LCD. We state a particular case ($\lambda = 1$) of Theorem 2 from [7].

Lemma 7.2. *([7]) Let θ_t be an automorphism of $\mathbb{F}_q$ and C be an skew θ_t-cyclic code of length n over $\mathbb{F}_q$ such that $f \in \mathbb{F}_q[y; \theta_t]$ is generator polynomial of C. Further assume that $g \in \mathbb{F}_q[y; \theta_t]$ is such that $\theta_t^n(g).f = y^n - 1$.*

(i) C is Euclidean LCD if and only if $GCRD(f, g^\dagger) = 1$.

(ii) C is Hermitian LCD if and only if $GCRD(f, \bar{g}^\dagger) = 1$.

Theorem 7.3. *Let $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be a linear code of length n over $\mathcal{T}$ then $\mathcal{C}$ is an LCD code if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ are LCD codes of length n over $\mathbb{F}_q$ $\forall i_j \in \{1, 2, 3\}$.*

Proof. Since, $\mathcal{C}^\perp = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}^\perp_{i_1 i_2 \ldots i_r}$, we have

$$\begin{aligned}
\mathcal{C} \cap \mathcal{C}^\perp &= \Big(\bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r} \Big) \cap \Big(\bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r} \Big)^\perp \\
&= \Big(\bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r} \Big) \cap \Big(\bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}^\perp_{i_1 i_2 \ldots i_r} \Big) \\
&= \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} (\mathcal{C}_{i_1 i_2 \ldots i_r} \cap \mathcal{C}^\perp_{i_1 i_2 \ldots i_r})
\end{aligned}$$

Thus $Hull(\mathcal{C}) = \{0\}$ if and only if $Hull(\mathcal{C}_{i_1 i_2 \ldots i_r}) = \{0\}$ $\forall i_j \in \{1, 2, 3\}$. Hence the result follows. □

Theorem 7.4. *Let order of Θ_t divides n and $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be a skew Θ_t-cyclic code of length n over $\mathcal{T}$ and $f_{i_1 i_2 \ldots i_r}(y)$ be the generator polynomial of $\mathcal{C}_{i_1 i_2 \ldots i_r}$, for $i_j \in \{1, 2, 3\}$. Further assume that $g_{i_1 i_2 \ldots i_r} \in \mathbb{F}_q[y; \theta_t]$ is such that $g_{i_1 i_2 \ldots i_r}(y).f_{i_1 i_2 \ldots i_r}(y) = y^n - 1$.*

(i) C is Euclidean LCD if and only if $GCRD(f_{i_1 i_2 \ldots i_r}, g^\dagger_{i_1 i_2 \ldots i_r}) = 1$.

(ii) C is Hermitian LCD if and only if $GCRD(f_{i_1 i_2 \ldots i_r}, \bar{g}^\dagger_{i_1 i_2 \ldots i_r}) = 1$.

Proof. Combining Lemma 7.2 and Theorem 7.3, the proof follows. □

Lemma 7.5. *For a linear code $\mathcal{C}$ of length n over $\mathcal{T}$, $\Phi(Hull(\mathcal{C})) = Hull(\Phi(\mathcal{C}))$.*

Proof. Let $\mathbf{w} \in \Phi(Hull(\mathcal{C}))$. Since Φ is onto, $\exists$ $\mathbf{v} \in Hull(\mathcal{C})$ such that $\Phi(\mathbf{v}) = \mathbf{w})$. As $\mathbf{v} \in Hull(\mathcal{C})$, $\mathbf{v} \in \mathcal{C}$ and $\mathbf{v} \in \mathcal{C}^\perp$. Therefore, $\mathbf{w} \in \Phi(\mathcal{C})$, and $\mathbf{w} \in \Phi(\mathcal{C}^\perp)$ and so $\mathbf{w} \in \Phi(\mathcal{C}) \cap \Phi(\mathcal{C}^\perp)$. Since, $\mathbf{w} \in \Phi(\mathcal{C} \cap \mathcal{C}^\perp)$ is arbitrary, we have, $\Phi(Hull(\mathcal{C})) \subseteq Hull(\Phi(\mathcal{C}))$.

Again let $\mathbf{w} \in Hull(\Phi(\mathcal{C}))$, i.e. $\mathbf{w} \in \Phi(\mathcal{C})$, and $\mathbf{w} \in \Phi(\mathcal{C}^\perp)$. Then $\exists$ $\mathbf{u} \in \mathcal{C}$ and $\exists$ $\mathbf{v} \in \mathcal{C}^\perp$ such that $\Phi(\mathbf{u}) = \mathbf{w})$ and $\Phi(\mathbf{v}) = \mathbf{w})$. Since, Φ is one-one as well, we have, $\mathbf{u} = \mathbf{v}$ and so $\mathbf{u}(= \mathbf{v}) \in \mathcal{C} \cap \mathcal{C}^\perp$. Therefore, $\mathbf{w} \in \Phi(\mathcal{C} \cap \mathcal{C}^\perp)$. Since, $\mathbf{w} \in \Phi(\mathcal{C}) \cap \Phi(\mathcal{C}^\perp)$ is arbitrary, we have, $Hull(\Phi(\mathcal{C})) \subseteq \Phi(Hull(\mathcal{C}))$. Hence, $\Phi(Hull(\mathcal{C})) = Hull(\Phi(\mathcal{C}))$.. □

Theorem 7.6. *A linear code of length n over $\mathcal{T}$ is LCD code if and only if its Gray image is a q-ary LCD code of length $3^r n$.*

Proof. Suppose that $\mathcal{C}$ is an LCD code of length n over the ring $\mathcal{T}$. Then by definition, $Hull(\mathcal{C} = \{0\}$. By Lemma 7.5, we get $Hull(\Phi(\mathcal{C})) = \Phi(Hull(\mathcal{C})) = \Phi(\{0\}) = \{0\}$ which concludes that $\Phi(\mathcal{C})$ is an LCD of length $3^r n$ over $\mathcal{T}$. Conversely, suppose that $\Phi(\mathcal{C})$ is an LCD of length $3^r n$ over $\mathbb{F}_q$ then $Hull(\Phi(\mathcal{C})) = \{0\}$. Therefore, by Lemma 7.5, we have $\Phi(Hull(\mathcal{C})) = Hull(\Phi(\mathcal{C})) = \{0\}$ which implies that $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$, as Φ is one-one. Hence, $\mathcal{C}$ is an LCD code of length n over $\mathcal{T}$. □

Now, we utilize the results obtained in this section to provide some examples of LCD codes over $\mathcal{T}$. For computation purposes, SageMath [28] and MAGMA [3] software are used.

Example 7.7. Let $q = 25$ and $r = 2$ then $\mathcal{T} = \mathbb{F}_{25}/\langle u_1^3 - u_1, u_2^3 - u_2, u_1 u_2 - u_1 u_2\rangle$. Let θ_1 be the Frobenius automorphism and $\gamma_1 = id$ the identity permutation. So $\Theta_1 : \mathcal{T} \to \mathcal{T}$ defined as

$$\sum_{i_1 i_2} w_{i_1 i_2} \eta_{i_1 i_2} \longmapsto \sum_{i_1 i_2} w_{i_1 i_2}^5 \eta_{i_1 i_2}$$

is an automorphism. Let $n = 4$. Factorisation of $y^n - 1 \in \mathbb{F}_{25}[y; \theta_1]$ is given as:

$$y^n - 1 = (y + 1)(y + 4)(y + 3)(y + 2)$$

Let us take $f_{11}(y) = y + 1$ and $f_{i_1 i_2}(y) = 1$ if $(i_1, i_2) \neq (1, 1)$ and $y^n - 1 = g_{i_1 i_2}(y) f_{i_1 i_2}(y)$. Then $GCRD(g_{i_1 i_2}^{\dagger}(y), f_{i_1 i_2}(y)) = 1$. Take

$$M = \begin{bmatrix} 2 & 1 & 1 & 2 & 1 & 1 & 4 & 2 & 2 \\ 4 & 3 & 4 & 4 & 3 & 4 & 3 & 1 & 3 \\ 1 & 1 & 2 & 1 & 1 & 2 & 2 & 2 & 4 \\ 4 & 2 & 2 & 2 & 1 & 1 & 2 & 1 & 1 \\ 3 & 1 & 3 & 4 & 3 & 4 & 4 & 3 & 4 \\ 2 & 2 & 4 & 1 & 1 & 2 & 1 & 1 & 2 \\ 3 & 4 & 4 & 1 & 3 & 3 & 3 & 4 & 4 \\ 1 & 2 & 1 & 2 & 4 & 2 & 1 & 2 & 1 \\ 4 & 4 & 3 & 3 & 3 & 1 & 4 & 4 & 3 \end{bmatrix}$$

then $MM^T = I_9$. Let $\mathcal{C}_i = \langle f_i(y)\rangle$ and $\mathcal{C} = \bigoplus_{i=1}^{3} \eta_i \mathcal{C}_i$ then $\mathcal{C}$ is an LCD code of length $n = 4$ and $d_L = 2$ over $\mathcal{T}$. Hence $\Phi(\mathcal{C})$ is a $[36, 35, 2]$ LCD code over $\mathbb{F}_{25}$ which is optimal.

Example 7.8. Let $q = 9$ then $\mathbb{F}_9 = \mathbb{F}_3[X]/\langle X^2 - X - 1\rangle = \mathbb{F}_3(\alpha)$, where $\alpha^2 = \alpha + 1$. Let $\theta_1 : b \mapsto b^3$, which is Frobenius automorphism. Further take $r = 1$ so that $\mathcal{T} = \mathbb{F}_9[u_1]/\langle u_1^3 - u_1\rangle$. Then $\Theta_1 : \mathcal{T} \to \mathcal{T}$ defined as:

$$\Theta_1(\eta_1 w_1 + \eta_2 w_2 + \eta_3 w_3) = \eta_1 \theta_1(w_1) + \eta_2 \theta_1(w_2) + \eta_3 \theta_1(w_3)$$

is an automorphism of $\mathcal{T}$. Take $n = 6$ and consider the factorisation in $\mathbb{F}_9[y]$ as

$$y^6 - 1 = (y + 2\alpha + 2)(y + 2)(y + 2\alpha + 2)(y + 2\alpha + 2)(y + 1)(y + 2\alpha + 2).$$

Take

$$\begin{aligned} f_1(y) = f_2(y) = f_3(y) &= (y + 2\alpha + 2)(y + 1)(y + 2\alpha + 2) \\ &= y^3 + (\alpha + 2)y^2 + y + 2 \end{aligned}$$

so that

$$\begin{aligned} g_1(y) = g_2(y) = g_3(y) &= (y + 2\alpha + 2)(y + 2)(y + 2\alpha + 2) \\ &= y^3 + \alpha y^2 + y + 1 \end{aligned}$$

Then $g_i^{\dagger}(y) = y^3 + y^2 + \alpha^3 y + 1$ and $\bar{g}_i^{\dagger}(y) = y^3 + y^2 + \alpha y + 1$. Since $GCRD(f_i(y), \bar{g}_i^{\dagger}(y)) = 1$, for all $i = 1, 2, 3$. Hence by Theroem 7.2, $\mathcal{C} = \bigoplus_{i=1}^{3} \eta_i \mathcal{C}_i$ is a Hermitian LCD code of length 6 with $d_L = 4$ over $\mathcal{T}$.

8 Conclusion

We discussed the structural properties of skew cyclic codes over a class of finite commutative rings $\mathcal{T} = T_r$. We provided a Gray map on $\mathcal{T}$ and used the decomposition method to study skew cyclic codes. Moreover, we provided a formula to find the number of skew-cyclic codes under a particular situation. We derived methods to obtain LCD codes and quantum codes from skew cyclic codes over $\mathcal{T}$.

References

[1] T. Abualrub and P. Seneviratne, Skew codes over rings, Proc. IMECS, Hong Kong, II (2010).

[2] M. Ashraf and G. Mohammad, Skew-cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. Asian Eur. J. Math, (2018).

[3] W. Bosma, J. Cannon, Handbook of magma functions, University of Sydney (1995) http://magma.maths.usyd.edu.au/magma/

[4] N. Aydin, P. Liu and B. Yoshino, A database of quantum codes. Online available at http://quantumcodes.info/.

[5] D. Boucher, W. Geiselmann and F. Ulmer, Skew cyclic codes. Appl. Algebra Eng. Commun. Comput. **18**(4), 379–389 (2007).

[6] D. Boucher and F. Ulmer, Coding with skew polynomial ring, J. Symb. Comput. **44**(12), 1644-1656 (2009).

[7] R. Boulanouar, A. Batouland D. Boucher, An Overview on Skew Constacyclic Codes and their Subclass of LCD Codes, Adv. Math. Commun. **15**(4), 611-632 (2021).

[8] A.R. Calderbank, E.M. Rains, P.M. Shor and N.J.A. Sloane, Quantum error-correction via codes over $GF(4)$, IEEE Trans. Inf. Theory **44**, 1369–1387 (1998).

[9] A. Dertli, Y. Cengellenmis, and S. Eren, On skew cyclic and quasi-cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Palest. J. Math. **4**(1), 540-546 (2015).

[10] H. Q. Dinh, T. Bag, A.K. Upadhyay, R. Bandi and R. Tansuchat, A class of skew cyclic codes and application in quantum codes construction, Discrete Math. **344**(2), 112189 (2021).

[11] J. Gao, F. Ma, F. Fu, Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$, Appl. Comput. Math. **6**(3), 286-295 (2017).

[12] M. Grassl, T. Beth, M. Roetteler, On optimal quantum codes. Int. J. Quantum Inf. **2**(1), 55–64 (2004).

[13] F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, Adv. Math. Commun. **8**(3), 313-322 (2014).

[14] A. R. Hammous, Jr P. V. Kumar, A. R. Calderbark, J. A. Sloame and P. Solé, The $\mathbb{Z}_4$-linearity of Kordock, Preparata, Goethals, and related codes. IEEE Trans. Inform. The. **40**, 301-319 (1994)

[15] W. C. Huffman, J. L. Kim and P. Solé, Concise Encyclopedia of Coding Theory. Chapman and Hall/CRC (2021)

[16] Irwansyah, A. Barra, S. T. Dougherty, A. Muchlis, I. Muchtadi-Alamsyah, P. Solé and O. Yemen, Θ_S-cyclic codes over A_k, Int. J. Comput. Math. Comput. Syst. Theory, **1**(1), 14-31 (2016).

[17] Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis and D. Suprijanto, Skew-cyclic codes over B_k. J. Appl. Math. Comput. **57** (2018), 69–84.

[18] H. Islam and O. Parkash, Skew cyclic codes and skew $(\alpha_1 + u\alpha_2 + v\alpha_3 + uv\alpha_4)$-constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, Int. J. Inf. Coding Theory **5**(2), 101-116 (2018).

[19] L. Jin, Skew cyclic codes over ring $\mathbb{F}_p + v\mathbb{F}_p$, J. Electron. (China) **31**(3), 227-231 (2014).

[20] J.L. Massey, Linear codes with complementary duals, Discrete Math. **106**(107), 337–342 (1992).

[21] B.R. McDonald, Finite Rings with Identity, Marcel Dekker Inc., New York (1974)

[22] M. Özen, N. Tuğba, Özzaim and H. İnce, Skew quasi cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, J. Algebra Appl. **18**(4), 1950077 (2019).

[23] J. Qian, W. Ma and W. Gou, Quantum codes from cyclic codes over finite ring, Int. J. Quantum Inf. **7**, 1277-1283 (2009).

[24] M. Shi, T. Yao, A. Alahmadi and P. Solé, Skew Cyclic Codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **98**(8), 1845-1848 (2015).

[25] M. Shi, T. Yao and P. Solé, Skew cyclic codes over a non-chain ring, Chin. J. Electron. **26**(3), 544-547 (2017)

[26] P.W. Shor, Scheme for reducing decoherence in quantum memory, Phys. Rev. A. **52**, 2493-2496 (1995).

[27] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, Skew cyclic codes of arbitrary length, Int. J. Inf. Coding Theory **2**(1), 10-20 (2011).

[28] A. William and Stein et al., Sage Mathematics Software (Version 9.2), The Sage Development Team, (2021), http://www.sagemath.org.

[29] T. Yao, M. Shi and P. Solé, Skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, J. Algebra Comb. Discrete Appl. **2**(3), 163-168 (2015).

[30] X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, Discrete Math. **126**(1-3), 391–393 (1994).

Author information

Pradeep Rai, Department of Mathematical Sciences, IIT(BHU), Varanasi– 221005, Uttar Pradesh, India.
E-mail: pradeeprai.rs.mat19@itbhu.ac.in

Bhupendra Singh, CAIR Lab, DRDO, C.V. Raman Nagar, Bengaluru– 560093, Karnataka, India.
E-mail: bhusinghdrdo@gmail.com

Ashok Ji Gupta, Department of Mathematical Sciences, IIT(BHU), Varanasi– 221005, Uttar Pradesh, India.
E-mail: agupta.apm@itbhu.ac.in