Palestine Journal of Mathematics

Vol 13(Special Issue II)(2024) , 9–19

Structural Properties of cyclic codes over the Ring $\mathfrak{T}_q[\mathfrak{v},\mathfrak{w}]/\langle \mathfrak{v}^2-\alpha^2,\ \mathfrak{w}^3-\beta^2\mathfrak{w},\ \mathfrak{v}\mathfrak{w}-\mathfrak{w}\mathfrak{v}\rangle$

Shakir Ali[1], Ghulam Mohammad[2], Pushpendra Sharma[3], and Mohammad Jeelani[4]

Communicated by Triloki Nath

Dedicated to Prof. B. M. Pandeya on his 78th birthday

MSC 2020 Classification: Primary 94B05; Secondary 94B15, 94B60

Keywords and phrases: Cyclic code, Gray map, Quantum code, LCD code.

Acknowledgement Authors would like to thank the reviewers for their valuable suggestions and useful comments, which helps us to improve the presentation of manuscript.

Abstract This paper aims to investigate the behaviour of cyclic codes over a finite ring, where the ring $\mathbb{S}=\mathfrak{T}_q[\mathfrak{v},\mathfrak{w}]/\langle \mathfrak{v}^2-\alpha^2,\ \mathfrak{w}^3-\beta^2\mathfrak{w},\ \mathfrak{v}\mathfrak{w}-\mathfrak{w}\mathfrak{v}\rangle$ is constructed using a field $\mathfrak{T}_q$ of order q, with q being an odd prime power, and nonzero elements α and β from $\mathfrak{T}_q$. With the help of Gray images of cyclic code over the defined ring $\mathbb{S}$, we construct LCD codes. A condition is also established for cyclic codes that contain their duals. Additionally, by using the self-orthogonal condition of cyclic codes over $\mathbb{S}$, we are able to construct quantum codes.

1 Introduction

In quantum communication and quantum computing, quantum codes are employed to safeguard quantum information from noise introduced into the channel during transmission. Following shor's [25] ground-breaking discovery, quantum error correcting(QEC) codes are fast evolving from classical error correcting (CEC) codes. Further, Calderbank et al. [8] suggested a technique for obtaining QEC codes from CEC codes. A study of QEC codes has been advanced at an incredible rate. Using classical cyclic codes over finite field $\mathfrak{T}_q$, many good QEC codes with dual or self-orthogonal containing features have been obtained (for references see [4, 11, 12, 13, 18, 19, 20, 26], where further references can be found). Firstly, Qian et al. [24] established QEC codes over the ring $\mathfrak{T}_2+u\mathfrak{T}_2$ having the condition $u^2=0$ using cyclic codes of odd length. In [23], Patel et al. establish the structure of cyclic codes over the ring $M_2(\mathfrak{T}_2+u\mathfrak{T}_2)$ and also obtained their generators. Ali et al. [2] gives the construction of cyclic codes over the class of commutative rings. In 2019, Ashraf et al. [5] obtained QEC codes over the finite nonchain ring. Motivated by these results, we construct QEC codes as well as optimal codes over the ring $\mathbb{S}$, with the help of Gray map.

A linear complementary dual code is a linear code that trivially meets its dual (abbreviated as LCD). The nearest-codeword decoding problem for LCD codes is more straightforward than it is for linear codes, and an LCD code with a potentially large minimum distance simultaneously thwarts the SCA (side-channel attack) and FIA (fault-injection attack) in a cryptosystem [9], among other advantages of LCD codes over linear codes. Keep in mind that Massey [22] introduced LCD codes. Later, LCD codes were offered by Yang and Massey [28] as cyclic codes with various limitations on their generator polynomials. Recently, authors [10] and [21] explored LCD codes over finite chain rings in order to expand these codes across finite rings. In the recent past, Yadav et al. [27] explored LCD circulant codes over a nonchain ring. In 2023, Ali et al. [1] obtained quantum and LCD codes over nonchain ring.

With the help of the self-orthogonal property, we construct QEC codes over $\mathfrak{T}_q$ from cyclic

codes over the finite ring $\mathbb{S}$ in this study. In this article, we also construct LCD codes using the Gray image. The advantage of exploring quantum codes from cyclic codes over the ring $\mathbb{S}$ is that many good quantum codes can be constructed. Our results extend and unify the results proved in [5]. The two main contributions of this study are, specifically:

(i) In this paper, we discuss LCD codes over a ring $\mathbb{S}$ which is a nonchain ring and find the optimal LCD codes from the Gray images of cyclic codes.

(ii) The article offers improved quantum codes than the old quantum codes appeared in some references.

2 Preliminaries

For an odd prime p such that $q = p^m$, where m is a positive integer. Let $\mathfrak{T}_q$ be the field of order q and consider the ring $\mathbb{S} = \mathfrak{T}_q[\mathfrak{v}, \mathfrak{w}]/\langle \mathfrak{v}^2 - \alpha^2,\ \mathfrak{w}^3 - \beta^2\mathfrak{w},\ \mathfrak{v}\mathfrak{w} - \mathfrak{w}\mathfrak{v}\rangle$, where α and β are the nonzero elements of $\mathfrak{T}_q$. Simply, we see that $\mathbb{S}$ is a semi-local, commutative, and nonchain ring. We start off by providing some fundamental definitions:

(i) The number of components that differ between two codewords $\mathbf{x} = x_1x_2\ldots x_n$ and $\mathbf{y} = y_1y_2\ldots y_n$ is known as the Hamming distance, and it is represented by the symbol d(**x,y**).

(ii) The Hamming weight of a codeword $\mathbf{x} = x_1x_2\ldots x_n$ is the number of nonzero components x_i and it is represented by $wt(\mathbf{x})$.

(iii) Let $\mathbf{x}, \mathbf{y} \in \mathfrak{T}_q^n$. The Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$ is defined as $\mathbf{x}\cdot\mathbf{y} = x_0y_0 + x_1y_1 + \ldots + x_{n-1}y_{n-1}$.

(iv) A nonempty subset $\mathfrak{E}$ of the ring $\mathbb{S}$ is known as a linear code of length n if it is an $\mathbb{S}$-submodule of $\mathbb{S}^n$ and each element in $\mathfrak{E}$ is called a codeword.

(v) A code $\mathfrak{E}$ is known as self-orthogonal if $\mathfrak{E} \subseteq \mathfrak{E}^{\perp}$, self-dual if $\mathfrak{E} = \mathfrak{E}^{\perp}$ and dual containing if $\mathfrak{E}^{\perp} \subseteq \mathfrak{E}$.

(vi) A linear code that meets its dual trivially is called linear complementary dual code (abbreviated as LCD code).

(vii) If every cyclic shift of a codeword c in $\mathfrak{E}$ is also a codeword in $\mathfrak{E}$, then the linear code $\mathfrak{E}$ of length n over $\mathbb{S}$ is said to be cyclic, i.e., if $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathfrak{E}$, then its cyclic shift $\theta(\mathbf{c}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathfrak{E}$, where the operator θ is known as cyclic shift.

(viii) A linear code $\mathfrak{E}$ is said to be reversible if $\mathbf{c}^r = (c_{n-1}, c_{n-2}, \ldots, c_0) \in \mathfrak{E}$ whenever $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathfrak{E}$.

The ring $\mathbb{S}$ can be written as $\mathbb{S} = \mathfrak{T}_q + \mathfrak{v}\mathfrak{T}_q + \mathfrak{w}\mathfrak{T}_q + \mathfrak{v}\mathfrak{w}\mathfrak{T}_q + \mathfrak{w}^2\mathfrak{T}_q + \mathfrak{v}\mathfrak{w}^2\mathfrak{T}_q$ such that $\mathfrak{v}^2 = \alpha^2$, $\mathfrak{w}^3 = \beta^2\mathfrak{w}$, $\mathfrak{v}\mathfrak{w} = \mathfrak{w}\mathfrak{v}$ and an element s of $\mathbb{S}$ is like as $s = a_1 + a_2\mathfrak{v} + a_3\mathfrak{w} + a_4\mathfrak{w}^2 + a_5\mathfrak{v}\mathfrak{w} + a_6\mathfrak{v}\mathfrak{w}^2,\ a_i \in \mathfrak{T}_q,\ 1 \le i \le 6$.

By using orthogonal idempotents, we can uniquely represent an arbitrary element of this ring as follows :

$$\mathfrak{J}_1 = \frac{(\alpha + \mathfrak{v})(\beta^2 - \mathfrak{w}^2)}{2\alpha\beta^2},$$

$$\mathfrak{J}_2 = \frac{(\alpha - \mathfrak{v})(\beta^2 - \mathfrak{w}^2)}{2\alpha\beta^2},$$

$$\mathfrak{J}_3 = \frac{(\alpha+\mathfrak{v})(\beta\mathfrak{w}+\mathfrak{w}^2)}{4\alpha\beta^2},$$

$$\mathfrak{J}_4 = \frac{(\alpha-\mathfrak{v})(\beta\mathfrak{w}+\mathfrak{w}^2)}{4\alpha\beta^2},$$

$$\mathfrak{J}_5 = \frac{(\alpha+\mathfrak{v})(-\beta\mathfrak{w}+\mathfrak{w}^2)}{4\alpha\beta^2}$$

and

$$\mathfrak{J}_6 = \frac{(\alpha-\mathfrak{v})(-\beta\mathfrak{w}+\mathfrak{w}^2)}{4\alpha\beta^2}.$$

It is straightforward to see that $\mathfrak{J}_i^2 = \mathfrak{J}_i,\ \mathfrak{J}_i\mathfrak{J}_j = 0$ and $\mathfrak{J}_1+\mathfrak{J}_2+\mathfrak{J}_3+\mathfrak{J}_4+\mathfrak{J}_5+\mathfrak{J}_6 = 1$ where $i,\ j = 1,2,3,4,5,6$ and $i \neq j$. By the orthogonal idempotent decomposition, we have $\mathbb{S} = \mathfrak{J}_1\mathbb{S} \oplus \mathfrak{J}_2\mathbb{S} \oplus \mathfrak{J}_3\mathbb{S} \oplus \mathfrak{J}_4\mathbb{S} \oplus \mathfrak{J}_5\mathbb{S} \oplus \mathfrak{J}_6\mathbb{S} \cong \mathfrak{J}_1\mathfrak{T}_q \oplus \mathfrak{J}_2\mathfrak{T}_q \oplus \mathfrak{J}_3\mathfrak{T}_q \oplus \mathfrak{J}_4\mathfrak{T}_q \oplus \mathfrak{J}_5\mathfrak{T}_q \oplus \mathfrak{J}_6\mathfrak{T}_q$. It is easy to observe that $\mathfrak{J}_i\mathbb{S} \cong \mathfrak{J}_i\mathfrak{T}_q$, where $1 \leq i \leq 6$. Each element $s \in \mathbb{S}$ can be written as $s = \mathfrak{J}_1 s_1 + \mathfrak{J}_2 s_2 + \mathfrak{J}_3 s_3 + \mathfrak{J}_4 s_4 + \mathfrak{J}_5 s_5 + \mathfrak{J}_6 s_6$, where $s_i \in \mathfrak{T}_q$ and $1 \leq i \leq 6$. Let $N \in GL_6(\mathfrak{T}_q)$ be an invertible matrix such that $NN^T = \epsilon I_6$, the transpose of the matrix N is denoted by N^T, I_6 is an identity matrix of order 6, $\epsilon \in \mathfrak{T}_q\backslash\{0\}$ for $s_i \in \mathfrak{T}_q,\ 1 \leq i \leq 6$, where $GL_6(\mathfrak{T}_q)$ is the linear group of all 6×6 invertible matrices over $\mathfrak{T}_q$.
The Gray map $\Gamma : \mathbb{S} \longrightarrow \mathfrak{T}_q^6$ is defined by $\Gamma(\mathfrak{J}_1 s_1 + \mathfrak{J}_2 s_2 + \mathfrak{J}_3 s_3 + \mathfrak{J}_4 s_4 + \mathfrak{J}_5 s_5 + \mathfrak{J}_6 s_6) = (s_1,\ s_2,\ s_3,\ s_4,\ s_5,\ s_6)N = \mathbf{sN}$, where $s = \sum_{j=0}^{6} \mathfrak{J}_j s_j \in \mathbb{S}$ for $s_j \in \mathfrak{T}_q,\ 1 \leq j \leq 6$. Here, we use $\mathbf{s}$ for the vector $(s_1,\ s_2,\ s_3,\ s_4,\ s_5,\ s_6)$.

The Gray map extended easily from $\mathbb{S}^n$ to $\mathfrak{T}_q^{6n}$, defined

$$\Gamma : \mathbb{S}^n \longrightarrow \mathfrak{T}_q^{6n}$$

by

$$\begin{aligned}\Gamma(s_0, s_1, \cdots, s_{n-1}) &= ((s_{0,1}, s_{0,2}, \cdots, s_{0,6})N, (s_{1,1}, s_{1,2}, \cdots, s_{1,6})N, \cdots, (s_{n-1,1}, s_{n-1,2}, \cdots, \\ &\quad s_{n-1,6})N) \\ &= (\mathbf{s_0}N, \mathbf{s_1}N, \cdots, \mathbf{s_{n-1}}N),\end{aligned}$$

where each $s_i = \sum_{j=0}^{6} \mathfrak{J}_j s_{i,j}$ for $0 \leq i \leq n-1$ and $1 \leq j \leq 6$.

For any element $s = \mathfrak{J}_1 s_1 + \mathfrak{J}_2 s_2 + \mathfrak{J}_3 s_3 + \mathfrak{J}_4 s_4 + \mathfrak{J}_5 s_5 + \mathfrak{J}_6 s_6 \in \mathbb{S}$, the Lee weight of s is defined as $w_L(s) = w_H(\Gamma(s))$, where w_H represents the Hamming weight for codes over $\mathfrak{T}_q$. We start this section with the following result on the Gray map:

Proposition 2.1. *The Gray map Γ is a distance preserving $\mathfrak{T}_q$-linear map from $(\mathbb{S}^n, d_L)$ to $(\mathfrak{T}_q^{6n}, d_H)$, where $d_L = d_H$.*

Proof. Let $s,\ t \in \mathbb{S}^n$ and such that

$$s = \mathfrak{J}_1 s_1 + \mathfrak{J}_2 s_2 + \mathfrak{J}_3 s_3 + \mathfrak{J}_4 s_4 + \mathfrak{J}_5 s_5 + \mathfrak{J}_6 s_6$$

$$t = \mathfrak{J}_1 t_1 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 t_5 + \mathfrak{J}_6 t_6$$

and $s_i,\ t_i \in \mathfrak{T}_q^n$ for $1 \leq i \leq 6$. Then, we have

$$\begin{aligned}\Gamma(s+t) &= \Gamma(\mathfrak{J}_1 s_1 + \mathfrak{J}_1 t_1 + \mathfrak{J}_2 s_2 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 s_3 \\ &\quad + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 s_4 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 s_5 + \mathfrak{J}_5 t_5 \\ &\quad + \mathfrak{J}_6 s_6 + \mathfrak{J}_6 t_6) \\ &= (s_1, s_2, s_3, s_4, s_5, s_6)N + (t_1, t_2, t_3, t_4, t_5, \\ &\quad t_6)N \\ &= \Gamma(s) + \Gamma(t).\end{aligned}$$

Also for any $\alpha \in \mathfrak{T}_q$, we have

$$\begin{aligned}\Gamma(\alpha s) &= \Gamma(\mathfrak{J}_1\alpha s_1 + \mathfrak{J}_2\alpha s_2 + \mathfrak{J}_3\alpha s_3 + \mathfrak{J}_4\alpha s_4 + \\ &\quad \mathfrak{J}_5\alpha s_5 + \mathfrak{J}_6\alpha s_6) \\ &= \Gamma(\alpha(\mathfrak{J}_1 s_1 + \mathfrak{J}_2 s_2 + \mathfrak{J}_3 s_3 + \mathfrak{J}_4 s_4 + \mathfrak{J}_5 s_5 \\ &\quad +\mathfrak{J}_6 s_6)) \\ &= \alpha(s_1, s_2, s_3, s_4, s_5, s_6)N \\ &= \alpha\Gamma(s).\end{aligned}$$

Hence, Γ is $\mathfrak{T}_q$-linear. For second part, we know that

$$\begin{aligned}d_L(s,t) &= w_L(s-t) \\ &= w_H(\Gamma(s-t)) \\ &= w_H(\Gamma(s) - \Gamma(t)) \\ &= d_H(\Gamma(s), \Gamma(t)).\end{aligned}$$

Therefore, Γ is a distance preserving map. □

Define $\zeta_1 \otimes \zeta_2 \otimes \zeta_3 \otimes \zeta_4 \otimes \zeta_5 \otimes \zeta_6 = \{(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6) \mid \xi_i \in \zeta_i : 1 \leq i \leq 6\}$ and $\zeta_1 \oplus \zeta_2 \oplus \zeta_3 \oplus \zeta_4 \oplus \zeta_5 \oplus \zeta_6 = \{(\xi_1 + \xi_2 + \xi_3 + \xi_4 + \xi_5 + \xi_6) \mid \xi_i \in \zeta_i : 1 \leq i \leq 6\}$. Let $\mathfrak{E}$ be a linear code of length n over $\mathbb{S}$. We assume that

$$\mathfrak{E}_1 = \{t_1 \in \mathfrak{T}_q^n \mid \mathfrak{J}_1 t_1 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 t_5 + \mathfrak{J}_6 t_6 \in \mathfrak{E}, \text{ for some } t_2, t_3, t_4, t_5, t_6 \in \mathfrak{T}_q^n\},$$

$$\mathfrak{E}_2 = \{t_2 \in \mathfrak{T}_q^n \mid \mathfrak{J}_1 t_1 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 t_5 + \mathfrak{J}_6 t_6 \in \mathfrak{E}, \text{ for some } t_1, t_3, t_4, t_5, t_6 \in \mathfrak{T}_q^n\},$$

$$\mathfrak{E}_3 = \{t_3 \in \mathfrak{T}_q^n \mid \mathfrak{J}_1 t_1 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 t_5 + \mathfrak{J}_6 t_6 \in \mathfrak{E}, \text{ for some } t_1, t_2, t_4, t_5, t_6 \in \mathfrak{T}_q^n\},$$

$$\mathfrak{E}_4 = \{t_4 \in \mathfrak{T}_q^n \mid \mathfrak{J}_1 t_1 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 t_5 + \mathfrak{J}_6 t_6 \in \mathfrak{E}, \text{ for some } t_1, t_2, t_3, t_5, t_6 \in \mathfrak{T}_q^n\},$$

$$\mathfrak{E}_5 = \{t_5 \in \mathfrak{T}_q^n \mid \mathfrak{J}_1 t_1 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 t_5 + \mathfrak{J}_6 t_6 \in \mathfrak{E}, \text{ for some } t_1, t_2, t_3, t_4, t_6 \in \mathfrak{T}_q^n\},$$

and

$$\mathfrak{E}_6 = \{t_6 \in \mathfrak{T}_q^n \mid \mathfrak{J}_1 t_1 + \mathfrak{J}_2 t_2 + \mathfrak{J}_3 t_3 + \mathfrak{J}_4 t_4 + \mathfrak{J}_5 t_5 + \mathfrak{J}_6 t_6 \in \mathfrak{E}, \text{ for some } t_1, t_2, t_3, t_4, t_5 \in \mathfrak{T}_q^n\}.$$

Here, every $\mathfrak{E}_i$ is a linear code of length n over $\mathfrak{T}_q$, for $1 \leq i \leq 6$. Therefore, every linear code of length n can be shown as $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ such that $|\mathfrak{E}| = |\mathfrak{E}_1||\mathfrak{E}_2||\mathfrak{E}_3||\mathfrak{E}_4||\mathfrak{E}_5||\mathfrak{E}_6|$ over $\mathbb{S}$. If the rows of a matrix form a minimal generating set of the linear code $\mathfrak{E}$ then the matrix will be called a generator matrix of the linear code. Suppose N_i is the generator matrix for the linear code $\mathfrak{E}_i$, where $i = 1, 2, 3, 4, 5, 6$, then a generator matrix of $\mathfrak{E}$ is

$$N = \begin{pmatrix} \mathfrak{J}_1 N_1 \\ \mathfrak{J}_2 N_2 \\ \mathfrak{J}_3 N_3 \\ \mathfrak{J}_4 N_4 \\ \mathfrak{J}_5 N_5 \\ \mathfrak{J}_6 N_6 \end{pmatrix}$$

and a generator matrix of $\Gamma(\mathfrak{E})$ is

$$\Gamma(N) = \begin{pmatrix} \Gamma(\mathfrak{J}_1 N_1) \\ \Gamma(\mathfrak{J}_2 N_2) \\ \Gamma(\mathfrak{J}_3 N_3) \\ \Gamma(\mathfrak{J}_4 N_4) \\ \Gamma(\mathfrak{J}_5 N_5) \\ \Gamma(\mathfrak{J}_6 N_6) \end{pmatrix}.$$

Proposition 2.2. *Let $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ be a linear code having length n over $\mathbb{S}$. Then $\Gamma(\mathfrak{E})$ is a linear code having the parameters $[6n, \sum_{i=1}^{6} k_i, d]$ over $\mathfrak{T}_q$ for $1 \leq i \leq 6$, where each $\mathfrak{E}_i$ is $[n, k_i, d_i]$ for $d = min\{d_i\}$.*

Proposition 2.3. *Let $\mathfrak{E}$ be a linear code having length n over $\mathbb{S}$. Then $\Gamma(\mathfrak{E}) = \mathfrak{E}_1 \otimes \mathfrak{E}_2 \otimes \mathfrak{E}_3 \otimes \mathfrak{E}_4 \otimes \mathfrak{E}_5 \otimes \mathfrak{E}_6$.*

Proof. The way of proof is same as in [6]. □

Theorem 2.4. *If $\mathfrak{E}$ is a self-orthogonal linear code with length n over $\mathbb{S}$, then its Gray image $\Gamma(\mathfrak{E})$ is also a self-orthogonal linear code with length $6n$ over $\mathfrak{T}_q$.*

Proof. Let us consider that $x, y \in \Gamma(\mathfrak{E})$ such that $x = (x_0, x_1, ..., x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$. We will show that $x \cdot y = 0$. Then there exists $x' = (x'_0, x'_1, ..., x'_{n-1})$ and $y = (y'_0, y'_1, ..., y'_{n-1}) \in \mathfrak{E}$ and $N \in GL_6(\mathfrak{T}_q)$ such that $x = \Gamma(x') = (x'_0N, x'_1N, ..., x'_{n-1}N)$ and $y = \Gamma(y') = (y'_0N, y'_1N, ..., y'_{n-1}N)$, where $NN^T = \lambda I_6$, $\lambda \in \mathfrak{T}_q \backslash \{0\}$ Now,

$$\begin{aligned} x \cdot y &= xy^T \\ &= \sum_{j=0}^{n-1} x'_j N N^T {y'_j}^T \\ &= \sum_{j=0}^{n-1} x'_j \epsilon I_6 {y'_j}^T \\ &= \epsilon \sum_{j=0}^{n-1} x'_j y'_j. \end{aligned}$$

Since x and y are arbitrary and $\mathfrak{E}$ is self orthogonal, then we have $x' \cdot y' = \sum_{j=0}^{n-1} x'_j y'_j = 0$. Hence $x \cdot y = 0$. Consequently $\Gamma(\mathfrak{E})$ self-orthogonal linear code having length $6n$ over $\mathfrak{T}_q$. □

3 Structural Properties of Cyclic Codes Over $\mathbb{S}$

This section will examine the particular structure of cyclic codes over the defined ring $\mathbb{S}$ and give some results. We start with the theorem over cyclic codes.

Theorem 3.1. *Let $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ be a linear code of length n over $\mathbb{S}$. Then, $\mathfrak{E}$ is cyclic code over $\mathbb{S}$ if and only if each $\mathfrak{E}_i$ is cyclic code over $\mathfrak{T}_q$, where $1 \leq i \leq 6$.*

Proof. Let s be any codeword in $\mathfrak{E}$ such that $s = (s_0, s_1, ..., s_{n-1})$, we can write its components as $s_j = \mathfrak{J}_1 s_j^1 + \mathfrak{J}_2 s_j^2 + \mathfrak{J}_3 s_j^3 + \mathfrak{J}_4 s_j^4 + \mathfrak{J}_5 s_j^5 + \mathfrak{J}_6 s_j^6$, where $s_j^1, s_j^2, s_j^3, s_j^4, s_j^5, s_j^6 \in \mathfrak{T}_q$ and $0 \leq j \leq n-1$. Let

$$s_1 = (s_0^1, s_1^1, ..., s_{n-1}^1),$$
$$s_2 = (s_0^2, s_1^2, ..., s_{n-1}^2),$$

$$s_3 = (s_0^3,\ s_1^3,\ ...,\ s_{n-1}^3),$$

$$s_4 = (s_0^4,\ s_1^4,\ ...,\ s_{n-1}^4),$$

$$s_5 = (s_0^5,\ s_1^5,\ ...,\ s_{n-1}^5),$$

$$s_6 = (s_0^6,\ s_1^6,\ ...,\ s_{n-1}^6),$$

where $s_1 \in \mathfrak{E}_1,\ s_2 \in \mathfrak{E}_2,\ s_3 \in \mathfrak{E}_3,\ s_4 \in \mathfrak{E}_4,\ s_5 \in \mathfrak{E}_5,\ s_6 \in \mathfrak{E}_6$. Next, let us consider that $\mathfrak{E}_1,\ \mathfrak{E}_2,\ \mathfrak{E}_3,\ \mathfrak{E}_4,\ \mathfrak{E}_5$ and $\mathfrak{E}_6$ are cyclic codes over $\mathfrak{T}_q$. This implies that

$$\theta(s_1) = (s_{n-1}^1,\ s_0^1,\ ...,\ s_{n-2}^1) \in \mathfrak{E}_1,$$

$$\theta(s_2) = (s_{n-1}^2,\ s_0^2,\ ...,\ s_{n-2}^2) \in \mathfrak{E}_2,$$

$$\theta(s_3) = (s_{n-1}^3,\ s_0^3,\ ...,\ s_{n-2}^3) \in \mathfrak{E}_3,$$

$$\theta(s_4) = (s_{n-1}^4,\ s_0^4,\ ...,\ s_{n-2}^4) \in \mathfrak{E}_4,$$

$$\theta(s_5) = (s_{n-1}^5,\ s_0^5,\ ...,\ s_{n-2}^5) \in \mathfrak{E}_5,$$

$$\theta(s_6) = (s_{n-1}^6,\ s_0^6,\ ...,\ s_{n-2}^6) \in \mathfrak{E}_6.$$

Thus $\mathfrak{J}_1\theta(s_1) + \mathfrak{J}_2\theta(s_2) + \mathfrak{J}_3\theta(s_3) + \mathfrak{J}_4\theta(s_4) + \mathfrak{J}_5\theta(s_5) + \mathfrak{J}_6\theta(s_6) \in \mathfrak{E}$. It can be easily seen that $\mathfrak{J}_1\theta(s_1) + \mathfrak{J}_2\theta(s_2) + \mathfrak{J}_3\theta(s_3) + \mathfrak{J}_4\theta(s_4) + \mathfrak{J}_5\theta(s_5) + \mathfrak{J}_6\theta(s_6) = \theta(s)$. Hence, $\theta(s) \in \mathfrak{E}$. From here, $\mathfrak{E}$ will be a cyclic code over the ring $\mathbb{S}$.
For the converse part, we assume that $\mathfrak{E}$ is a cyclic code over $\mathbb{S}$. Let $s_j = \mathfrak{J}_1 s_j^1 + \mathfrak{J}_2 s_j^2 + \mathfrak{J}_3 s_j^3 + \mathfrak{J}_4 s_j^4 + \mathfrak{J}_5 s_j^5 + \mathfrak{J}_6 s_j^6$, where $s_1 = (s_0^1,\ s_1^1,\ ...,\ s_{n-1}^1)$, $s_2 = (s_0^2,\ s_1^2,\ ...,\ s_{n-1}^2)$, $s_3 = (s_0^3,\ s_1^3,\ ...,\ s_{n-1}^3)$, $s_4 = (s_0^4,\ s_1^4,\ ...,\ s_{n-1}^4)$, $s_5 = (s_0^5,\ s_1^5,\ ...,\ s_{n-1}^5)$ and $s_6 = (s_0^6,\ s_1^6,\ ...,\ s_{n-1}^6)$. Then, $s_1 \in \mathfrak{E}_1,\ s_2 \in \mathfrak{E}_2,\ s_3 \in \mathfrak{E}_3,\ s_4 \in \mathfrak{E}_4,\ s_5 \in \mathfrak{E}_5$ and $s_6 \in \mathfrak{E}_6$. Now again, $s = (s_0,\ s_1,\ \dots, s_{n-1}) \in \mathfrak{E}$, then by the hypothesis $\theta(s) \in \mathfrak{E}$. We have $\mathfrak{J}_1\theta(s_1) + \mathfrak{J}_2\theta(s_2) + \mathfrak{J}_3\theta(s_3) + \mathfrak{J}_4\theta(s_4) + \mathfrak{J}_5\theta(s_5) + \mathfrak{J}_6\theta(s_6) \in \mathfrak{E}$. Here $\theta(s_1) \in \mathfrak{E}_1,\ \theta(s_2) \in \mathfrak{E}_2,\ \theta(s_3) \in \mathfrak{E}_3,\ \theta(s_4) \in \mathfrak{E}_4,\ \theta(s_5) \in \mathfrak{E}_5$ and $\theta(s_6) \in \mathfrak{E}_6$. Consequently, $\mathfrak{E}_1,\ \mathfrak{E}_2,\ \mathfrak{E}_3,\ \mathfrak{E}_4,\ \mathfrak{E}_5$ and $\mathfrak{E}_6$ are cyclic codes over $\mathfrak{T}_q$. □

Theorem 3.2. *Let $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ be a cyclic code of length n over $\mathbb{S}$ and $h_i(s)$ is the generator polynomial of $\mathfrak{E}_i$. Then $\mathfrak{E} = \langle h(s)\rangle$ and $|\mathfrak{E}| = q^{6n-\sum_{i=0}^{6} deg(h_i(s))}$, where $h(s) = \mathfrak{J}_1h_1(s) + \mathfrak{J}_2h_2(s) + \mathfrak{J}_3h_3(s) + \mathfrak{J}_4h_4(s) + \mathfrak{J}_5h_5(s) + \mathfrak{J}_6h_6(s)$ and $1 \le i \le 6$.*

Proof. Given $\mathfrak{E}_i = \langle h_i(s)\rangle$, where $1 \le i \le 6$ and $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$. Suppose $c \in \mathfrak{E}$ such that $c = \{c(s) \mid \mathfrak{J}_1h_1(s) + \mathfrak{J}_2h_2(s) + \mathfrak{J}_3h_3(s) + \mathfrak{J}_4h_4(s) + \mathfrak{J}_5h_5(s) + \mathfrak{J}_6h_6(s)\}$ for $h_i(s) \in \mathfrak{E}_i$. Therefore, $\mathfrak{E} \subseteq \langle \mathfrak{J}_1h_1(s),\ \mathfrak{J}_2h_2(s),\ \mathfrak{J}_3h_3(s), \mathfrak{J}_4h_4(s), \mathfrak{J}_5h_5(s), \mathfrak{J}_6h_6(s)\rangle \subseteq \mathbb{S}[s]/\langle s^n - 1\rangle$. Now again $\mathfrak{J}_1q_1(s)h_1(s) + \mathfrak{J}_2q_2(s)h_2(s) + \mathfrak{J}_3q_3(s)h_3(s) + \mathfrak{J}_4q_4(s)h_4(s) + \mathfrak{J}_5q_5(s)h_5(s) + \mathfrak{J}_6q_6(s)h_6(s) \in \langle \mathfrak{J}_1h_1(s) + \mathfrak{J}_2h_2(s) + \mathfrak{J}_3h_3(s) + \mathfrak{J}_4h_4(s) + \mathfrak{J}_5h_5(s) + \mathfrak{J}_6h_6(s)\rangle \subseteq \mathbb{S}[s]/\langle s^n - 1\rangle$, where $q_i(s) \in \mathbb{S}[s]/\langle s^n - 1\rangle$, there are $h_i(s) \in \mathfrak{T}_q[s]/\langle s^n - 1\rangle$ such that

$$\mathfrak{J}_i q_i(s) = \mathfrak{J}_i h_i(s),$$

where $1 \le i \le 6$. Hence $\langle \mathfrak{J}_1h_1(s), \mathfrak{J}_2h_2(s), \mathfrak{J}_3h_3(s), \mathfrak{J}_4h_4(s), \mathfrak{J}_5h_5(s), \mathfrak{J}_6h_6(s)\rangle \subseteq \mathfrak{E}$. This implies $\langle \mathfrak{J}_1h_1(s), \mathfrak{J}_2h_2(s),\ \mathfrak{J}_3h_3(s), \mathfrak{J}_4h_4(s), \mathfrak{J}_5h_5(s), \mathfrak{J}_6h_6(s)\rangle = \mathfrak{E}$. But $|\mathfrak{E}| = |\mathfrak{E}_1||\mathfrak{E}_2||\mathfrak{E}_3|$ $|\mathfrak{E}_4||\mathfrak{E}_5||\mathfrak{E}_6|$, we find that

$$|\mathfrak{E}| = q^{6n-\sum_{i=0}^{6} deg(h_i(s))}.$$

□

Theorem 3.3. *Let $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ be a cyclic code of length n over $\mathbb{S}$. Then, there exists a polynomial $h(s) \in \mathbb{S}[s]$ such that $\mathfrak{E} = \langle h(s)\rangle$ and $h(s)$ divides $(s^n - 1)$.*

Proof. Here $\mathfrak{E} = \langle \mathfrak{J}_1 h_1(s),\ \mathfrak{J}_2 h_2(s),\ \mathfrak{J}_3 h_3(s), \mathfrak{J}_4 h_4(s),\ \mathfrak{J}_5 h_5(s),\ \mathfrak{J}_6 h_6(s)\rangle$, where $h_i(s)$ is the generator polynomial of $\mathfrak{E}_i$ and $1 \leq i \leq 6$. Let $h(s) = \mathfrak{J}_1 h_1(s) + \mathfrak{J}_2 h_2(s) + \mathfrak{J}_3 h_3(s) + \mathfrak{J}_4 h_4(s) + \mathfrak{J}_5 h_5(s) + \mathfrak{J}_6 h_6(s)$. From here, $\langle h(s)\rangle \subseteq \mathfrak{E}$. Now $\mathfrak{J}_i h_i(s) = \mathfrak{J}_i h(s)$ and $1 \leq i \leq 6$, so $\mathfrak{E} \subseteq \langle h(s)\rangle$, hence $\mathfrak{E} = \langle h(s)\rangle$. Since $h_i(s)$ is the right divisor of $(s^n - 1)$, $p_i(s) \in \mathfrak{T}_q[s]/\langle s^n - 1\rangle$, where $1 \leq i \leq 6$, such that $s^n - 1 = p_1 h_1(s) = p_2 h_2(s) = p_3 h_3(s) = p_4 h_4(s) = p_5 h_5(s) = p_6 h_6(s)$. This shows that $s^n - 1 = [\mathfrak{J}_1 p_1(s) + \mathfrak{J}_2 p_2(s) + \mathfrak{J}_3 p_3(s) + \mathfrak{J}_4 p_4(s) + \mathfrak{J}_5 p_5(s) + \mathfrak{J}_6 p_6(s)]h(s)$, i.e., $h(s)|(s^n - 1)$. Here, each $h_i(s)$ is unique, and hence $h(s)$ is unique. □

Theorem 3.4. *Suppose $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ is a cyclic code having length n over $\mathbb{S}$. Then, $\mathfrak{E}^\perp = \mathfrak{J}_1\mathfrak{E}_1^\perp \oplus \mathfrak{J}_2\mathfrak{E}_2^\perp \oplus \mathfrak{J}_3\mathfrak{E}_3^\perp \oplus \mathfrak{J}_4\mathfrak{E}_4^\perp \oplus \mathfrak{J}_5\mathfrak{E}_5^\perp \oplus \mathfrak{J}_6\mathfrak{E}_6^\perp$ is also a cyclic code having length n over $\mathbb{S}$.*

Proof. $\mathfrak{E}^\perp$ is a cyclic codes of length n over $\mathbb{S}$, because $\mathfrak{E}$ is a cyclic code of length n over $\mathbb{S}$. Next, we have to prove that $\mathfrak{E}^\perp = \mathfrak{J}_1\mathfrak{E}_1^\perp \oplus \mathfrak{J}_2\mathfrak{E}_2^\perp \oplus \mathfrak{J}_3\mathfrak{E}_3^\perp \oplus \mathfrak{J}_4\mathfrak{E}_4^\perp \oplus \mathfrak{J}_5\mathfrak{E}_5^\perp \oplus \mathfrak{J}_6\mathfrak{E}_6^\perp$. Here $\mathfrak{E}$ is a cyclic code over $\mathbb{S}$. This shows that $\mathfrak{E}$ is a linear code. Next, let us consider $T_1 = \{t_1 \in \mathfrak{T}_q^n \mid \exists\ t_2,\ t_3,\ t_4,\ t_5,\ t_6$ such that $\sum_{i=1}^{6} t_i\mathfrak{J}_i \in \mathfrak{E}^\perp\}$. Hence, $\mathfrak{E}^\perp$ is exclusively expressed as $\mathfrak{E}^\perp = \oplus_{i=1}^{6}\mathfrak{J}_i T_i$. This shows that, $T_1 \subseteq \mathfrak{E}_1^\perp$. Conversely assume that $q \in \mathfrak{E}_1^\perp$. This means $q \cdot s_1 = 0\ \forall\ s_1 \in \mathfrak{E}_1$. Consider $y = \sum_{i=1}^{6}\mathfrak{J}_i s_i \in \mathfrak{E}$. Now, $\mathfrak{J}_1 q \cdot y = \mathfrak{J}_1 s_1 \cdot q = 0$. This implies that $\mathfrak{J}_1 q \in \mathfrak{E}_1^\perp$. From the unique expression of $\mathfrak{E}^\perp$, we get $q \in T_1$. From here, $\mathfrak{E}^\perp \subseteq T_1$. Therefore, $\mathfrak{E}_1^\perp = T_1$. In the same manner, $\mathfrak{E}_i^\perp = T_i$ for $i = 1,\ 2,\ 3,\ 4,\ 5,\ 6$. Hence, $\mathfrak{E}^\perp = \mathfrak{J}_1\mathfrak{E}_1^\perp \oplus \mathfrak{J}_2\mathfrak{E}_2^\perp \oplus \mathfrak{J}_3\mathfrak{E}_3^\perp \oplus \mathfrak{J}_4\mathfrak{E}_4^\perp \oplus \mathfrak{J}_5\mathfrak{E}_5^\perp \oplus \mathfrak{J}_6\mathfrak{E}_6^\perp$. □

4 Quantum and LCD codes

In this section, we use the CSS(Calderbank-Shor-Steane) construction [14] to construct quantum error correcting codes. We can construct better quantum codes than existing quantum codes in recent references. Lemma 4.1 applies a condition over finite fields to study the necessity of cyclic codes containing their duals. In [28], Massey introduced linear codes with complementary duals, sometimes known as LCD codes. In this section, we also obtain LCD codes. The set of n-fold tensor product $(\mathbb{K}^q)^{\otimes n} = \mathbb{K}^q \otimes \mathbb{K}^q \otimes ... \otimes \mathbb{K}^q$ (n- times), where $\mathbb{K}^q$ is the Hilbert space of dimension q over the complex field $\mathbb{K}$, is a Hilbert space having dimension q^n. A quantum code of length n and dimension q^k is denoted by $[[n, k, d]]_q$, where d is the minimum distance. The singleton bound, $n + 2 \geq 2d + k$, holds true for every quantum code. A quantum code is considered to be MDS (maximum distance separable) if it satisfies the singleton bound. A quantum code $[[n, k, d]]_q$ is superior to another quantum code $[[n', k', d']]_q$ if either one or both of the following conditions are met:

(i) $\frac{k}{n} > \frac{k'}{n'}$ and $d = d'$ (higher code rate with the same distance)

(ii) $d > d'$ and $\frac{k}{n} = \frac{k'}{n'}$ (higher distance with the same code rate).

Lemma 4.1. *[14] [CSS Construction] Let $\mathfrak{E} = \langle h(s)\rangle$ be an $[n, k, d]$ linear code with $\mathfrak{E}^\perp \subseteq \mathfrak{E}$ over the finite field $\mathfrak{T}_q$, then there exists a QEC code with parameters $[[n, 2k - n, d]]_q$ over $\mathfrak{T}_q$.*

Lemma 4.2. *[8] A cyclic code $\mathfrak{E}$ of length n over $\mathfrak{T}_q$ with generator polynomial $h(s)$ contains its dual if and only if*

$$s^n - 1 \equiv 0\ mod(h(s)h^*(s)),$$

where $h^*(s)$ is the reciprocal polynomial of $h(s)$.

In view of Lemma 4.2, in the following theorem, we derive a condition for cyclic codes to contain their duals.

Theorem 4.3. *Let $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ be a cyclic code of length n over $\mathbb{S}$ and $\mathfrak{E} = \langle h(s)\rangle = \sum_{i=1}^{6}\mathfrak{J}_i h_i(s)$, where $h_i(s)$ is the generator polynomial of $\mathfrak{E}_i$. Then $\mathfrak{E}^\perp \subseteq \mathfrak{E}$ if and only if*

$$s^n - 1 \equiv 0\ mod(h_i(s)h_i^*(s)),$$

where reciprocal polynomial of $h_i(s)$ is represented by $h_i^*(s)$ for $i = 1,\ 2,\ 3,\ 4,\ 5,\ 6$.

Proof. Let $s^n - 1 \ \equiv \ 0\, mod(h_i(s)h_i^*(s))$ for $1 \leq i \leq 6$. Then, by Lemma 4.2, we have $\mathfrak{E}_i^{\perp} \subseteq \mathfrak{E}_i$. Hence, this shows that $\mathfrak{J}_i\mathfrak{E}_i^{\perp} \subseteq \mathfrak{J}_i\mathfrak{E}_i$ for $1 \leq i \leq 6$. Similarly, $\mathfrak{E}^{\perp} = \sum_{i=0}^{6} \mathfrak{J}_i\mathfrak{E}_i^{\perp} \subseteq \sum_{i=0}^{6} \mathfrak{J}_i\mathfrak{E}_i = \mathfrak{E}$. Conversely, let $\mathfrak{E}^{\perp} \subseteq \mathfrak{E}$ and $\sum_{i=0}^{6} \mathfrak{J}_i\mathfrak{E}_i^{\perp} \subseteq \sum_{i=0}^{6} \mathfrak{J}_i\mathfrak{E}_i$, but each $\mathfrak{E}_i$ is a cyclic code over $\mathfrak{T}_q$ such that $\mathfrak{J}_i\mathfrak{E}_i \equiv \mathfrak{E}(mod\mathfrak{J}_i)$. This implies that $\mathfrak{E}_i^{\perp} \subseteq \mathfrak{E}_i$, where $1 \leq i \leq 6$. By Lemma 4.2, we get

$$s^n - 1 \ \equiv \ 0\, mod(h_i(s)h_i^*(s)),$$

where reciprocal polynomial of $h_i(s)$ is represented by $h_i^*(s)$ for $1 \leq i \leq 6$.

□

Corollary 4.4. *Suppose $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ is a cyclic code of length n over $\mathbb{S}$. Then, $\mathfrak{E}^{\perp} \subseteq \mathfrak{E}$ if and only if $\mathfrak{E}_i^{\perp} \subseteq \mathfrak{E}_i$ and $1 \leq i \leq 6$.*

Theorem 4.5. *Suppose $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ is a cyclic code having length n over the ring $\mathbb{S}$ and its Gray image is $[6n, k, d_H]$. If $\mathfrak{E}^{\perp} \subseteq \mathfrak{E}$, then there exists a QEC code $[[6n, 2k - 6n, d_H]]_q$.*

Lemma 4.6. *[28] Let $\mathfrak{E} = \langle h(s) \rangle$ be a cyclic code having length n over the finite field $\mathfrak{T}_q$.*

(i) Suppose $n = p^{\lambda_1} \cdot t$ and $gcd(p, t) = 1$. Then $\mathfrak{E}$ is a linear complementary dual code if and only if $h(s)$ is self-reciprocal polynomial and all monic irreducible factors of that polynomial, i.e., $h(s)$ have the same multiplicity in $h(s)$ and in $(s^n - 1)$.

(ii) For $gcd(p, t) = 1$, then $\mathfrak{E}$ is a linear complementary dual code if and only if $\mathfrak{E}$ is a reversible code.

All proofs run parallel as in [16].

Theorem 4.7. *Suppose $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ is a cyclic code having length n over $\mathbb{S}$.*

(i) Then, $\mathfrak{E}$ is a linear complementary dual code if $\mathfrak{E}_1$, $\mathfrak{E}_2$,$\mathfrak{E}_3$,$\mathfrak{E}_4$,$\mathfrak{E}_5$ and $\mathfrak{E}_6$ are linear complementary dual codes over the finite field $\mathfrak{T}_q$.

(ii) For $gcd(n, p) = 1$, then $\mathfrak{E}$ is a linear complementary dual code if and only if $\mathfrak{E}_1$, $\mathfrak{E}_2$, $\mathfrak{E}_3$,$\mathfrak{E}_4$, $\mathfrak{E}_5$, and $\mathfrak{E}_6$ are reversible codes of length n over the finite field $\mathfrak{T}_q$.

Corollary 4.8. *Let $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ be a cyclic code having length n over $\mathbb{S}$.*

(i) For $n = p^t m$, $gcd(m, p) = 1$ and $\mathfrak{E}_i$ is generated by $h_i(s)$ such that $h_i(s) \in \mathfrak{T}_q$ and $h_i(s)|(s^n - 1)$ for $i = 1, 2, 3, 4, 5, 6$. Then, $\mathfrak{E}$ is a linear complementary dual or in short LCD code if and only if $h_i(s)$ is self-reciprocal polynomial and each monic irreducible factor of $h_i(s)$ has the same multiplicity in $h_i(s)$ and in $s^n - 1$ for $i = 1, 2, 3, 4, 5, 6$.

(ii) Suppose $gcd(n, p) = 1$. Then, $\mathfrak{E}$ is a linear complementary dual code if and only if $h_i(s)$ is a self-reciprocal polynomial in $\mathfrak{T}_q$ for $i = 1, 2, 3, 4, 5, 6$.

Lemma 4.9. *Let $\mathfrak{E}$ be a linear code over $\mathbb{S}$ having length n.*

(i) Then $\Gamma(\mathfrak{E} \cap \mathfrak{E}^{\perp}) = \Gamma(\mathfrak{E}) \cap \Gamma(\mathfrak{E})^{\perp}$.

(ii) Then, $\mathfrak{E}$ is a complementary dual code if and only if $\Gamma(\mathfrak{E})$ is a linear complementary dual code having length $6n$ over $\mathfrak{T}_q$.

5 Examples

In this section, we obtain many better quantum codes than existing quantum codes collected from different references and we also obtain linear complementary dual codes from Gray images of cyclic codes. In these examples, we use the Magma computation system [7] for all of the calculations.

Example 5.1. Suppose $\mathbb{S} = \mathfrak{T}_7[\mathfrak{v}, \mathfrak{w}]/\langle \mathfrak{v}^2 - 1,\ \mathfrak{w}^3 - \mathfrak{w},\ \mathfrak{v}\mathfrak{w} - \mathfrak{w}\mathfrak{v}\rangle$, $n = 14$ and $\alpha = \beta = 1$. Then $s^{14} - 1 = (s+1)^7(s+6)^7 \in \mathfrak{T}_7[s]$.
Take $h_1(s) = (s+1)^3(s+6)$, $h_2(s) = h_3(s) = h_4(s) = h_5(s) = s+1$, $h_6(s) = 1$ and

$$N = \begin{bmatrix} 1 & 3 & 3 & 3 & 3 & 3 \\ 3 & 1 & 3 & 3 & 3 & 3 \\ 3 & 3 & 1 & 3 & 3 & 3 \\ 3 & 3 & 3 & 1 & 3 & 3 \\ 3 & 3 & 3 & 3 & 1 & 3 \\ 3 & 3 & 3 & 3 & 3 & 1 \end{bmatrix}$$

and fulfil the condition that $NN^T = 4I_{6\times 6}$, where $N \in GL_6(\mathfrak{T}_7)$ and $I_{6\times 6}$ is an identity matrix. Hence, $\mathfrak{E} = \mathfrak{J}_1\mathfrak{E}_1 \oplus \mathfrak{J}_2\mathfrak{E}_2 \oplus \mathfrak{J}_3\mathfrak{E}_3 \oplus \mathfrak{J}_4\mathfrak{E}_4 \oplus \mathfrak{J}_5\mathfrak{E}_5 \oplus \mathfrak{J}_6\mathfrak{E}_6$ is a cyclic code having length 14 and its Gray image $\Gamma(\mathfrak{E})$ is $[84,\ 76,\ 4]$ over $\mathfrak{T}_7$. But

$$s^{14} - 1 \equiv 0\ mod(h_i(s)h_i^*(s)),$$

for $1 \leq i \leq 6$. In view of Theorem 4.5, there exists a quantum code $[[84,\ 68,\ 4]]_7$, which has the greater code rate as well as greater minimum distance than the code $[[84, 60, 3]]_7$ appeared in [17].

Example 5.2. Suppose $\mathbb{S} = \mathfrak{T}_5[\mathfrak{v}, \mathfrak{w}]/\langle \mathfrak{v}^2 - 1,\ \mathfrak{w}^3 - \mathfrak{w},\ \mathfrak{v}\mathfrak{w} - \mathfrak{w}\mathfrak{v}\rangle$, $n = 6$ and $\alpha = 1, \beta = 1$. Then $s^6 - 1 = (s+1)(s+4)(s^2+s+1)(s^2+4s+1) \in \mathfrak{T}_5[s]$.
Take $h_1(s) = (s+1)(s^2+s+1)(s^2+4s+1)$, $h_2(s) = h_3(s) = h_4(s) = h_5(s) = s+1$, $h_6(s) = 1$ and

$$N = \begin{bmatrix} 1 & 2 & 2 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 & 2 & 2 \\ 2 & 2 & 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 1 & 2 & 2 \\ 2 & 2 & 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 2 & 2 & 1 \end{bmatrix}$$

and fulfil the condition that $NN^T = I_{6\times 6}$, where $N \in GL_6(\mathfrak{T}_5)$ and $I_{6\times 6}$ is an identity matrix. Since each $h_i(s)$ is self-reciprocal polynomial, then $\mathfrak{E}$ is an LCD code by Corollary 4.8. By Lemma 4.9, $\Gamma(\mathfrak{E})$ is an LCD code having the parameters $[36, 27, 4]_5$.

Table 1. Quantum codes from cyclic code over $\mathbb{S}$

n	$h_1(s)$	$h_2(s)$	h_3	$h_4(s)$	$h_5(s)$	h_6	$\Gamma(\mathscr{C})$	$[[n, k, d]]_q$	$[[n', k', d']]_q$
10	11	1	1	1	1	1	[60, 59, 2]	$[[60, 58, 2]]_5$	$[[60, 48, 2]]_5$[5]
11	124114	124114	124114	124114	124114	1	[66, 41, 5]	$[[66, 16, 5]]_5$	$[[66, 6, 2]]_5$[5]
15	14041	14	14	14	14	1	[90, 82, 3]	$[[90, 74, 3]]_5$	$[[90, 72, 2]]_5$[5]
22	124114	124114	124114	124114	124114	1	[132, 107, 4]	$[[132, 82, 4]]_5$	$[[132, 72, 2]]_5$[5]
24	1344	12	12	12	12	1	[144, 137, 3]	$[[144, 130, 3]]_5$	$[[144, 120, 3]]_5$[5]
30	13341	14	14	14	14	1	[180, 172, $3]_5$	$[[180, 164, 3]]_5$	$[[180, 156, 3]]_5$[5]
35	140000041	14	14	14	14	1	[210, 198, 3]	$[[210, 186, 3]]_5$	$[[210, 150, 2]]_5$[5]
14	12056	11	11	11	11	1	$[84, 76, 4]_7$	$[[84, 68, 4]]_7$	$[[84, 60, 3]]_7$[17]
38	1131	1026	1131	1026	1131	1	[228, 213, 4]	$[[228, 198, 4]]_7$	$[[228, 198, 3]]_7$[3]
42	1104	11	11	11	11	1	[252, 245, 3]	$[[252, 238, 3]]_7$	$[[252, 228, 3]]_7$[3]

In Table 1, we compare our QEC codes from existing QEC codes. With the help of Table 1, we show that our QEC codes are better than the existing quantum codes that have appeared in some references. In Table 2, by using Gray images of cyclic codes, we obtain LCD codes. Two codes are optimal in Table 2 according to the database [15].

Table 2. LCD codes of length n over $\mathbb{S}$

n	$h_1(s)$	$h_2(s)$	h_3	$h_4(s)$	$h_5(s)$	h_6	$\Gamma(\mathscr{C})$	$Remarks$
4	11	1	1	1	1	1	$[24, 23, 2]_5$	$optimal$
6	111111	11	11	11	11	1	$[36, 27, 4]_5$	...
8	110011	11	11	11	11	1	$[48, 39, 4]_5$	...
12	11211	11	11	11	11	1	$[72, 64, 4]_5$	...
6	11	1	1	1	1	1	$[36, 35, 2]_7$	$optimal$
18	111111	11	11	11	11	1	$[108, 97, 4]_7$	...
8	1551	11	11	11	11	1	$[48, 41, 4]_7$	...
12	11322	11	11	11	11	1	$[72, 64, 4]_7$	...

6 Conclusion

In this article, we studied some structural properties of cyclic codes over the defined ring $\mathbb{S} = \mathfrak{T}_q[\mathfrak{v}, \mathfrak{w}]/\langle \mathfrak{v}^2 - \alpha^2,\ \mathfrak{w}^3 - \beta^2\mathfrak{w},\ \mathfrak{v}\mathfrak{w} - \mathfrak{w}\mathfrak{v}\rangle$, where α and β are the nonzero elements of finite field $\mathfrak{T}_q$ and obtained many QEC codes using their properties as well as we obtained optimal codes.

References

[1] Ali, S., Alali, A. S., Jeelani, M., Kurulay, M., Oztas, E. S., & Sharma, P.: On the construction of quantum and LCD codes from cyclic codes over the finite commutative rings. Axioms **12**(4), 367, (2023).

[2] Ali, S., Alali, A. S., Oztas, E. S., & Sharma, P.: Construction of quantum codes over the class of commutative rings and their applications to DNA codes. Mathematics **11**(6), 1430, 2023.

[3] Ali, S., Mohammad, G., Jeelani, M., Khan, N., & Sharma, P.: On quantum and LCD Codes Over The Ring $F_q + vF_q + v^2F_q$. Quantum Inf. Process. **21**(9), 1-17 (2022).

[4] Aly, S. A., Klappenecker, A., Sarvepalli, P. K.: On quantum and classical BCH codes. IEEE Trans. Inform. Theory **53**, 1183-1188 (2007).

[5] Ashraf, M., Mohammad, G.: Quantum codes over Fp from cyclic codes over $F_p[u, v]/\langle u^2 - 1,\ v^3 - v,\ uv - vu\rangle$. Cryptogr. Commun. **11**, 325-335 (2019).

[6] Bag, T., Upadhyay, A. K.: Study on negacyclic codes over the ring $Z_p[u]/\langle u^{k+1} - u\rangle$. J. Appl. Math. Comput. (2018). https://doi.org/10.1007/s12190-018-1197-5.

[7] Bosma, W., Cannon, J.: Handbook of magma functions. University of sydney (1995).

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

[9] Carlet, C. & Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. 2016, **10**(1), 131-150. doi: 10.3934/amc.2016.10.131.

[10] Durgun, Y.: On LCD codes over finite chain rings. Bull. Korean Math. Soc. 2020, **57**(1), 37-50. doi: 10.4134/BKMS.b181173.

[11] Feng, K., Ling, S., Xing, C.: Asymtotic bounds on quantum codes from algebraic geometry codes. IEEE Trans. Inform. Theory **52**, 986-991 (2006).

[12] Gaurdia, G., Palazzo Jr, R.: Constructions of new families of nonbinary CSS codes. Discrete Math. **310**, 2935-2945 (2010).

[13] Gottesman, D.: An introduction to quantum error-correction. Proc. Symp. Appl. Math. Amer. Math. Soc. **68**, 13-58 (2010).

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

[15] Grassl, M.: Code Tables: Bounds on the parameters of various types of codes available at http://www.codetables.de/ accessed on 20/04/2021.

[16] Islam, H.; Prakash, O. Construction of LCD and new quantum codes from cyclic codes over a finite non chain ring. Cryptogr. Commun. **14**, 59–73, 2022. https://doi.org/10.1007/s12095-021-00516-9.

[17] Islam, H., Prakash, O., Verma, R.K.: Quantum codes from the cyclic codes over $F_P[v, w]/\langle v^2 - 1, w^2 - 1, vw - wv\rangle$. Springer Proc. Math. Stat. **307**. https://doi.org/10.1007/978-981-15-1157-8-6 (2019).

[18] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P. K.: Nonbinary quantum stabilizer codes over finite fields. IEEE Trans. Inform. Theory **52**, 4892-4914 (2006).

[19] Li, R., Xu, Z., Li, X.: Binary construction of quantum codes of minimum distance three and four. IEEE Trans. Inform. Theory **50**, 1331-1335 (2004).

[20] Li, R., Xu, Z.: Construction of $[[n, n-4, 3]]_q$ quantum codes for odd prime power q. Phys. Rev. A **82**, 1-4 (2010).

[21] Liu, X. & Liu, H. LCD codes over finite chain rings. Finite Fields Appl. **34**, 1-19, 2015. doi: 10.1016/j.ffa.2015.01.004.

[22] Massey, J. L. Linear codes with complementary duals. Discrete Math. **106**(/107) 337-342, 1992. doi: 10.1016/0012-365X(92)90563-U.

[23] Patel, S., Prakash, O., & Islam, H.: Cyclic codes over $M_4(\mathbb{F}_2 + u\mathbb{F}_2)$. Cryptogr. Commun. **14**(5), 1021-1034, 2022.

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

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

[26] Steane, A. M.: Simple QEC codes. Phys. Rev. A **54**, 4741-4751 (1996).

[27] Yadav, S., Islam, H., Prakash, O. & Sole, P.: Self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. J. Appl. Math. Comput., 2021, doi: 10.1007/s12190-021-01499-9.

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

Author information

Shakir Ali[1], Ghulam Mohammad[2], Pushpendra Sharma[3], and Mohammad Jeelani[4], [1,2,3]Department of Mathematics, Faculty of Science, Aligarh Muslim University, Aligarh, India; [4] Department of Computer Application, Faculty of Science, Integral University, Lucknow, India.
E-mail: shakir.ali.mm@amu.ac.in, mohdghulam202@gmail.com, sharmapushpendra52@gmail.com and jeelani.0018@gmail.com