Contemporary Mathematics
https://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER
PUBLISHER

Research Article

Construction of Quantum Codes from Constacyclic Codes Over the Class of Commutative Rings

Pushpendra Sharma[1], **Amal S. Alali**[2], **Shakir Ali**[1,3*], **Mohd Azeem**[1]

[1] Department of Mathematics, Faculty of Science, Aligarh Muslim University, Aligarh-202002, India
[2] Department of Mathematical Sciences, College of Science, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh-11671, Saudi Arabia
[3] Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada, Yogyakarta-55598, Indonesia
E-mail: shakir.ali.mm@amu.ac.in

Received: 19 May 2025; **Revised:** 22 July 2025; **Accepted:** 29 July 2025

Abstract: This paper primarily investigates the structural properties of constacyclic codes over the ring $\mathscr{R}_k$, defined as $\mathscr{R}_k = \frac{\mathscr{F}_{p^m}[w_1, w_2, \ldots, w_k]}{\langle w_i^2-1,\ w_iw_j-w_jw_i\rangle}$ where $i,\ j = 1,\ 2,\ 3,\ \ldots,\ k,$ and $k,\ m$ are positive integers. Here, $\mathscr{F}_{p^m}$ denotes a finite field of order p^m with characteristic p, an odd prime. Furthermore, we determine the necessary and sufficient conditions for the duals of constacyclic codes to exist. These findings make it easier to create new Quantum Error-Correcting (QEC) codes throughout the ring $\mathscr{R}_1$ (i.e., when $k = 1$), as well as optimal linear codes that make use of the Gray images of constacyclic codes. Additionally, Table 4 presents several Linear Complementary Dual (LCD) codes obtained using the Gray map.

***Keywords*:** constacyclic code, Kronecker product, quantum code, Gray map, Linear Complementary Dual (LCD) code

MSC: 94B05, 94B15, 94B60

1. Introduction

Constacyclic codes were initially introduced by Berlekamp [1] as an extension of cyclic and negacyclic codes. Since their introduction, extensive research has been conducted on constacyclic codes over both finite fields and finite chain rings (see [2–8] and the references therein). This class of codes plays a significant role in error-correcting code theory, as it generalizes the widely studied cyclic codes, which remain one of the most important families in coding theory.

In quantum communication and quantum computing, quantum codes are used to shield data from channel noise while it is being transmitted. This requirement has fueled significant advancements in the construction of quantum error-correcting codes and their extensions derived from classical cyclic codes. In the year 1995, Shor [9] presented the first Quantum Error-Correcting (QEC) code. The following year, Steane [10] investigated the structural aspects of fundamental QEC codes. Later, in 1998, Calderbank et al. [11] proposed an innovative approach to transform classical error-correcting codes into quantum codes. Numerous efficient QEC codes that contain dual or self orthogonal properties have since been developed over finite fields $\mathscr{F}_q$ by leveraging classical cyclic codes. The constacyclic shift property, where a shift of a codeword by one position results in multiplication by a fixed unit λ, provides an algebraic structure that facilitates efficient encoding and syndrome-based decoding. This property can be exploited to optimize algorithms by reducing complexity in

DOI: https://doi.org/10.37256/cm.6420257258

both encoding, via polynomial multiplication modulo $x^n - \lambda$, and decoding, by enabling the use of generator polynomials and syndromes in a structured manner. Such optimizations are critical when constructing large error-correcting codes for practical applications.

Qian [12] was the first to construct QEC codes from cyclic codes of odd lengths over the finite non-chain ring $\mathscr{F}_2 + u\mathscr{F}_2$, where $u^2 = 0$. Quantum codes derived from cyclic, constacyclic and skew constacyclic codes specified over odd non-chain rings were then thoroughly examined. These developments have been thoroughly studied in [13–16]. The structure of the codes over the ring $\frac{\mathscr{F}_2[w_1, w_2, w_3, \ldots, w_k]}{\langle w_i^2 - w_i, w_iw_j - w_jw_i\rangle}$ was examined by Cengellenmis et al. [17] in 2014 using the Gray map. Later in 2018, Zheng et al. [18] discovered generator polynomials for constacyclic codes over the ring $\frac{\mathscr{F}_{p^m}[u_1, u_2, \ldots, u_k]}{\langle u_i^2 - u_i, u_iu_j - u_ju_i\rangle}$ and determined the structural properties of linear codes in this context. Additionally, as reported in [19–21], a number of quantum codes over rings with even characteristics were developed. More recently, new quantum and LCD codes were built over the finite non-chain ring $\mathscr{F}_{2^m} + u\mathscr{F}_{2^m}$, where $u^2 = u$, by Islam and Prakash [22]. These advancements inspire our investigation into the properties of constacyclic codes over the ring $\mathscr{R}_k = \frac{\mathscr{F}_{p^m}[w_1, w_2, \ldots, w_k]}{\langle w_i^2 - 1, w_iw_j - w_jw_i\rangle}$ where $i, j = 1, 2, 3, \ldots, k$.

The structure of this paper is set up as follows: In the context of the ring $\mathscr{R}_k$, Section 2 introduces the Gray map and provides key concepts. In Section 3, constacyclic codes, their dual codes, and generator polynomials are studied, as well as the structure of linear codes and their duals over $\mathscr{R}_k$. We also construct sufficient and necessary requirements for the duals of constacyclic codes to be contained in this section. Improved quantum coding examples are given in Section 4. Furthermore, we create optimal codes over the ring $\mathscr{R}_1$ (i.e., when $k = 1$) by using the Gray images of cyclic codes.

2. Preliminaries

Let $\mathscr{F}_{p^m}$ be a finite field with order p^m and characteristic p, where m is a positive integer. For any positive integer k, define the ring $\mathscr{R}_k$ as $\mathscr{R}_k = \frac{\mathscr{F}_{p^m}[w_1, w_2, \ldots, w_k]}{\langle w_i^2 - 1, w_iw_j - w_jw_i\rangle}$, for $i, j = 1, 2, 3, \ldots, k$. We begin by presenting some fundamental definitions.

(i) For two vectors, $\mathbf{x} = x_1x_2 \cdots x_n$ and $\mathbf{y} = y_1y_2 \cdots y_n$, the Hamming distance between them, represented by $d(\mathbf{x}, \mathbf{y})$, is the number of coordinates in which they differ.

(ii) The number of nonzero components in $\mathbf{x}$ is the Hamming weight of a vector $\mathbf{x} = x_1x_2 \cdots x_n$, represented by $wt(\mathbf{x})$.

(iii) The Euclidean inner product of any two vectors $\mathbf{x}, \mathbf{y} \in \mathscr{F}_q^n$ is defined as follows: $\mathbf{x} \cdot \mathbf{y} = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}$.

(iv) A code of length n over a ring R is said to be a linear over R if it forms a submodule of R^n over R.

(v) If $C^\perp \subseteq C$, then a code C is dual-containing; if $C = C^\perp$, then it is self-dual; and if $C \subseteq C^\perp$, it is self-orthogonal.

(vi) The term Linear Complementary Dual (LCD) code refers to a linear code that has the condition that $C \cap C^\perp = \{0\}$, where $C^\perp$ denotes the dual code of C.

(vii) If a linear code C of length n over a ring R is closed under the constacyclic shift operator, then it is referred to as a constacyclic code. That is, for any codeword $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in C$, its constacyclic shift $\delta(\mathbf{c}) = (\lambda c_{n-1}, c_0, c_1, c_2, \ldots, c_{n-2})$ also belongs to C, where λ is a unit in R and δ denotes the constacyclic shift.

(viii) Notably, a Hilbert space of dimension q^n is formed by the n-fold tensor product $(\mathscr{K}^q)^{\otimes n} = \mathscr{K}^q \otimes \mathscr{K}^q \otimes \cdots \otimes \mathscr{K}^q$ (taken n times). Here, $\mathscr{K}^q$ represents a Hilbert space of dimension q, where the complex field is $\mathscr{K}$. The code $[[n, k, d]]_q$ denotes a quantum code of length n over the field $\mathscr{F}_q$, where q is a prime power, and k is the dimension and d is the minimum distance. Every quantum codes satisfy the Singleton bound $n - k + 2 \geq 2d$. The quantum code is Maximum Distance Separable (MDS) code if $n - k + 2 = 2d$. One or both of the following criteria must be met for one of the quantum codes $[[n, k, d]]_q$ is better than another quantum code $[[n', k', d']]_q$:

(a) $\frac{k}{n} > \frac{k'}{n'}$, where $d = d'$, indicating a higher code rate while maintaining the same minimum distadnce.

(b) $d > d'$, where $\frac{k}{n} = \frac{k'}{n'}$, meaning a greater minimum distance while preserving the same code rate.

The Kronecker product of two matrices M and N results in a block matrix of size $pm \times qn$

$$M \otimes N = \begin{bmatrix} p_{11}N & p_{12}N & \ldots & p_{1n}N \\ p_{21}N & p_{22}N & \ldots & p_{2n}N \\ \cdots & \cdots & \cdots & \cdots \\ p_{m1}N & p_{m2}N & \ldots & p_{mn}N \end{bmatrix} \tag{1}$$

Here, $M = (p_{ij})$ is a matrix of order $m \times n$ and $N = (q_{i'j'})$ is a matrix of order $p \times q$. To be more precise,

$$M \otimes N = \begin{bmatrix} p_{11}q_{11} & p_{11}q_{12} & \cdots & p_{11}q_{1q} & \cdots & \cdots & p_{1n}q_{11} & p_{1n}q_{12} & \cdots & p_{1n}q_{1q} \\ p_{11}q_{21} & p_{11}q_{22} & \cdots & p_{11}q_{2q} & \cdots & \cdots & p_{1n}q_{21} & p_{1n}q_{22} & \cdots & p_{1n}q_{2q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{11}q_{p1} & p_{11}q_{p2} & \cdots & p_{11}q_{pq} & \cdots & \cdots & p_{1n}q_{p1} & p_{1n}q_{p2} & \cdots & p_{1n}q_{pq} \\ \vdots & \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & \vdots & \vdots & & \vdots \\ p_{m1}q_{11} & p_{m1}q_{12} & \cdots & p_{m1}q_{1q} & \cdots & \cdots & p_{mn}q_{11} & p_{mn}q_{12} & \cdots & p_{mn}q_{1q} \\ p_{m1}q_{21} & p_{m1}q_{22} & \cdots & p_{m1}q_{2q} & \cdots & \cdots & p_{mn}q_{21} & p_{mn}q_{22} & \cdots & p_{mn}q_{2q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{m1}q_{p1} & p_{m1}q_{p2} & \cdots & p_{m1}q_{pq} & \cdots & \cdots & p_{mn}q_{p1} & p_{mn}q_{p2} & \cdots & p_{mn}q_{pq} \end{bmatrix} \tag{2}$$

where $1 \le i \le m$, $1 \le j \le n$, $1 \le i' \le p$, and $1 \le j' \le q$.

Additionally, utilizing the Kronecker product, we establish the Gray map within the ring $\mathscr{R}_k$. The Kronecker product exhibits the subsequent characteristics:

(i) For matrices $M = (p_{ij})_{m \times m}$ and $N = (q_{i'j'})_{n \times n}$, the following holds:

$$(M \otimes N)^{-1} = M^{-1} \otimes N^{-1}. \tag{3}$$

(ii) $(M \otimes N) \otimes C = M \otimes (N \otimes C)$ for arbitrary M, N, and C matrices.

(iii) $(M \otimes N)^T = M^T \otimes N^T$, where the transpose of matrices M and N is indicated by M^T and N^T, respectively.

The ring $\mathscr{R}_k = \frac{\mathscr{F}_{p^m}[w_1,\, w_2,\, \ldots,\, w_k]}{\langle w_i^2-1,\, w_iw_j-w_jw_i\rangle}$ may also be expressed as follows: $\mathscr{R}_k = \mathscr{F}_{p^m} + \mathscr{F}_{p^m}w_1 + \mathscr{F}_{p^m}w_2 + \mathscr{F}_{p^m}w_1w_2 + \cdots + \mathscr{F}_{p^m}w_1w_2\ldots w_k$, where, for all i, $j = 1, 2, 3, \ldots, k$, $w_iw_j = w_jw_i$ and $w_i^2 = 1$. Let $\mathscr{T}$ represent the power set of $\{1, 2, 3, \ldots, k\}$, and let $\mathscr{R}_k$ be a finite commutative ring. In this way, each element $s \in \mathscr{R}_k$ can be uniquely expressed as: $s = \sum_{T \in \mathscr{T}} \beta_T w_T$, where $\beta_T \in \mathscr{F}_q$, $w_T = \prod_{i \in T} w_i$, and $w_\phi = 1$. For $i \neq j$, where i, $j = 1, 2, 3, \ldots, 2^k$, define $e_i^k \in \{w_T \colon T \in \mathscr{T},\, w_\phi = 1\}$ so that $e_i^k \neq e_j^k$.

For $k = 1$, we have $\mathscr{R}_1 = \mathscr{F}_{p^m}[w_1]/\langle w_1^2 - 1\rangle$. This ring can be written as $\mathscr{R}_1 = \mathscr{F}_{p^m} + w_1\mathscr{F}_{p^m}$ with $w_1^2 = 1$. Therefore, a basis of $\mathscr{R}_1$ is given by $\{1, w_1\}$. Define $e_1^1 = 1$ and $e_2^1 = w_1$.

For the ring $\mathscr{R}_k$, the basis can be expressed using the Kronecker product as follows:

$$(e_1^k, e_2^k, \ldots, e_{2^k}^k) = (1, w_k) \otimes (e_1^{k-1}, e_2^{k-1}, \ldots, e_{2^{k-1}}^{k-1}) \tag{4}$$

Here, $(e_1^1, e_2^1) = (1, w_1)$. Furthermore, we obtain a set of orthogonal idempotent elements in the ring $\mathscr{R}_k$, where each ζ_i^k is defined by

$$\zeta_i^k = \prod_{j=1}^{k} \Delta_j, \tag{5}$$

with $\Delta_j \in \left\{\frac{1-w_j}{2}, \frac{1+w_j}{2}\right\}$, and for $i \neq j$, we have $\zeta_i^k \neq \zeta_j^k$, where $i, j = 1, 2, 3, \ldots, 2^k$. It is simple to verify that

$$\sum_{i=1}^{2^k} \zeta_i^k = 1, \quad (\zeta_i^k)^2 = \zeta_i^k, \quad \zeta_i^k \zeta_j^k = 0 \text{ for } i \neq j. \tag{6}$$

For this reason, the ring $\mathscr{R}_k$ also has a basis in the collection $\{\zeta_i^k \mid i = 1, 2, \ldots, 2^k\}$. In particular, for $k = 1$, we have $\zeta_1^1 = \frac{1-w_1}{2}$ and $\zeta_2^1 = \frac{1+w_1}{2}$. The equation is rewritten in the matrix form shown as

$$(\zeta_1^1, \zeta_2^1) = (e_1^1, e_2^1)P_1 \tag{7}$$

$$(\frac{1-w_1}{2}, \frac{1+w_1}{2}) = (1, w_1)P_1. \tag{8}$$

After some calculation, we get $P_1 = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$. Moreover, utilizing the properties of the Kronecker product, we obtain

$$\begin{aligned} P_k &= P_1 \otimes P_{k-1}, \\ P_k &= P_1 \otimes P_1 \otimes P_{k-2}, \\ &= \ldots \qquad \ldots \\ P_k &= \underbrace{P_1 \otimes P_1 \otimes P_1 \otimes \cdots \otimes P_1}_{(k\text{-}times)}. \end{aligned} \tag{9}$$

It is evident that P_k is an invertible matrix, with $P_k^{-1} = P_1^{-1} \otimes P_1^{-1} \otimes \cdots \otimes P_1^{-1}$. Moreover, P_k^{-1} is invertible, and its transpose satisfies $(P_k^{-1})^T = (P_1^{-1})^T \otimes (P_1^{-1})^T \otimes \cdots \otimes (P_1^{-1})^T$, where $(P_1^{-1})^T = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. Hence,

$$(\zeta_1^k, \zeta_2^k, \ldots, \zeta_{2^k}^k)P_k = (e_1^k, e_2^k, \ldots, e_{2^k}^k)\underbrace{P_1 \otimes P_1 \otimes P_1 \otimes \cdots \otimes P_1}_{(k\text{-}times)} \tag{10}$$

and

$$(e_1^k, e_2^k, \dots, e_{2^k}^k)P_k = (\zeta_1^k, \zeta_2^k, \dots, \zeta_{2^k}^k)\underbrace{(P_1^{-1})^T \otimes (P_1^{-1})^T \otimes (P_1^{-1})^T \otimes \dots \otimes (P_1^{-1})^T}_{(k\text{-}times)}. \tag{11}$$

Similarly as in Eq. (4), we have

$$(\zeta_1^k, \zeta_2^k, \dots, \zeta_{2^k}^k) = (\frac{1-w_k}{2}, \frac{1+w_k}{2}) \otimes (\zeta_1^{k-1}, \zeta_2^{k-1}, \dots, \zeta_{2^{k-1}}^{k-1}), \tag{12}$$

where $(\zeta_1^1, \zeta_2^1) = (\frac{1-w_1}{2}, \frac{1+w_1}{2})$.

Every element s in $\mathscr{R}_k$ can be uniquely represented as $s = \sum_{i=1}^{2^k} \beta_i e_i^k = \sum_{i=1}^{2^k} \gamma_i^k \zeta_i^k$, where β_i, $\gamma_i^k \in \mathscr{F}_{p^m}$ and $i = 1, 2, 3, \dots, 2^k$. The Gray map is defined using the matrix P_k as

$$\Theta_k \colon \mathscr{R}_k \longrightarrow \mathscr{F}_{p^m}^{2^k} \tag{13}$$

as follows:

$$\Theta_k(s) = \Theta_k \left(\sum_{i=1}^{2^k} \beta_i e_i^k \right) = (\beta_1, \beta_2, \dots, \beta_{2^k})(P_k^{-1})^T. \tag{14}$$

For simplicity, we write $(\beta_1, \beta_2, \dots, \beta_{2^k})(P_k^{-1})^T = (\gamma_1^k, \gamma_2^k, \dots, \gamma_{2^k}^k)$. The Gray map described above can be naturally extended to $\mathscr{R}_k^n$ as

$$\Theta_k \colon \mathscr{R}_k^n \longrightarrow \mathscr{F}_{p^m}^{2^k n}, \tag{15}$$

defined by

$$\Theta_k(s_0, s_1, s_2, \dots, s_{n-1}) = (\gamma_{i,\,j}^k)_{1 \le i \le 2^k,\ 0 \le j \le n-1}. \tag{16}$$

Here, every s_j can be written as $s_j = \sum_{i=1}^{2^k} \beta_{i,\,j} e_i^k$, and thus,

$$\Theta_k(s_j) = (\beta_{1,\,j}, \beta_{2,\,j}, \beta_{3,\,j}, \dots, \beta_{2^k,\,j})(P_k^{-1})^T = (\gamma_{1,\,j}^k, \gamma_{2,\,j}^k, \gamma_{3,\,j}^k, \dots, \gamma_{2^k,\,j}^k), \tag{17}$$

where $\beta_{i,\,j} \in \mathscr{F}_{p^m}$ for $i = 1, 2, 3, \dots, 2^k$, and $j = 0, 1, 2, \dots, n-1$.

In particular, for $k = 1$, the Gray map is defined similarly as in Eq. (14):

$$\Theta_1 \colon \mathscr{R}_1 \longrightarrow \mathscr{F}_{p^m}^2, \tag{18}$$

given by

$$\Theta_1(\beta_1 e_1^1 + \beta_2 e_2^1) = \Theta_1(\beta_1 + \beta_2 w_1) = (\beta_1, \beta_2)(P_1^{-1})^T, \tag{19}$$

where

$$(P_1^{-1})^T = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \tag{20}$$

In the ring $\mathscr{R}_k$, the definition of the Lee weight of an element $s = \sum_{i=1}^{2^k} \beta_i e_i^k$ is as follows:

$$w_L(s) = w_H(\Theta_k(s)) = w_H(\gamma_1^k, \gamma_2^k, \gamma_3^k, \ldots, \gamma_{2^k}^k), \tag{21}$$

where w_H is the Hamming weight.

Let C be a linear code over $\mathscr{R}_k$ of length n. The linear code $\Theta_k(C)$ over $\mathscr{F}_{p^m}$ of length $2^k n$ is evident. We define

$$C_j = \left\{ \mathbf{x}_j \in \mathscr{F}_{p^m}^n \mid \sum_{i=1}^{2^k} \zeta_i^k \mathbf{x}_i \in C, \ \mathbf{x}_i \in \mathscr{F}_{p^m}^n, \ i \neq j, \text{ and } 1 \leq i \leq 2^k \right\}, \tag{22}$$

for every linear code C of length n over $\mathscr{R}_k$. This means that each C_j is a linear code of length n over $\mathscr{F}_{p^m}$.

Next, let B_i be linear codes over $\mathscr{F}_{p^m}$ for $i = 1, 2, 3, \ldots, 2^k$. We define

$$B_1 \oplus B_2 \oplus B_3 \oplus \cdots \oplus B_{2^k} = \{b_1 + b_2 + b_3 + \cdots + b_{2^k} \mid b_i \in B_i \text{ with } 1 \leq i \leq 2^k\} \tag{23}$$

and

$$B_1 \otimes B_2 \otimes B_3 \otimes \cdots \otimes B_{2^k} = \{(b_1, b_2, b_3, \ldots, b_{2^k}) \mid b_i \in B_i \text{ with } 1 \leq i \leq 2^k\}. \tag{24}$$

Consequently, it follows that the expression for the linear code C over $\mathscr{R}_k$ of length n is

$$C = \bigoplus_{i=1}^{2^k} \zeta_i^k C_i = \zeta_1^k C_1 \oplus \zeta_2^k C_2 \oplus \cdots \oplus \zeta_{2^k}^k C_{2^k}. \tag{25}$$

If the rows in a matrix G produce C, then the matrix G is referred to as a generator matrix of C. Let G_i be the generator matrix of C_i for $i = 1, 2, 3, \ldots, 2^k$. Then, a generator matrix for C is given by

$$G = \begin{bmatrix} \zeta_1^k G_1 \\ \zeta_2^k G_2 \\ \vdots \\ \zeta_{2^k}^k G_{2^k} \end{bmatrix}, \tag{26}$$

and $\Theta_k(C)$ has a generator matrix that is

$$\Theta_k(G) = \begin{bmatrix} \Theta_k(\zeta_1^k G_1) \\ \Theta_k(\zeta_2^k G_2) \\ \vdots \\ \Theta_k(\zeta_{2^k}^k G_{2^k}) \end{bmatrix} \tag{27}$$

3. Main results

In this section, we use the CSS construction to study the structural properties of cyclic codes over the ring $\mathscr{R}_k$ and present some results related to the Gray map. We also prove novel results about QEC codes.

3.1 *Results related to the Gray map*

We commence our discussions with the following result:

Proposition 1 The Gray map Θ_k is linear, bijective, and distance-preserving from $(\mathscr{R}_k^n,\, d_L)$ to $(\mathscr{F}_{p^m}^{2^k n},\, d_H)$, where $d_L = d_H$.

Proof. Suppose $\mathbf{c}_1,\, \mathbf{c}_2 \in \mathscr{R}_k^n$. It is straightforward to verify that

$$\Theta_k(\mathbf{c}_1 + \mathbf{c}_2) = \Theta_k(\mathbf{c}_1) + \Theta_k(\mathbf{c}_2). \tag{28}$$

Additionally, for any $\delta \in \mathscr{F}_{p^m}$, we have

$$\Theta_k(\delta \mathbf{c}_1) = \delta \Theta_k(\mathbf{c}_1). \tag{29}$$

Therefore, Θ_k is a linear. Next, we demonstrate the bijection of Θ_k. We have

$$\Theta_k(\mathbf{c_1}) = \Theta_k(\mathbf{c_2})$$

$$\Theta_k(\sum_{i=1}^{2^k} \beta_i e_i^k) = \Theta_k(\sum_{i=1}^{2^k} \delta_i e_i^k) \tag{30}$$

$$(\beta_1,\, \beta_2,\, \dots,\, \beta_{2^k})(P_k^{-1})^T = (\delta_1,\, \delta_2,\, \dots,\, \delta_{2^k})(P_k^{-1})^T$$

where, for $1 \leq i \leq 2^k$, β_i, $\delta_i \in \mathscr{F}_{p^m}$. This suggests that

$$\beta_1 = \delta_1, \ldots, \beta_{2^k} = \delta_{2^k}. \tag{31}$$

Then $\mathbf{c}_1 = \mathbf{c}_2$. From this, it follows that Θ_k is injective. Now, consider any $(\beta_1, \beta_2, \ldots, \beta_{2^k})(P_k^{-1})^T \in \mathscr{F}_{p^m}^{2^k}$. Then, $\Theta_k(\mathbf{c}) = (\beta_1, \ldots, \beta_{2^k})$, where $\mathbf{c} \in \mathscr{R}_k^n$ is a corresponding element. This makes Θ_k surjective. Since Θ_k is bijective, we obtain

$$\begin{aligned} d_L(\mathbf{c_1}, \mathbf{c_2}) &= w_L(\mathbf{c_1} - \mathbf{c_2}) \\ &= w_H(\Theta_k(\mathbf{c_1} - \mathbf{c_2})) \\ &= w_H(\Theta_k(\mathbf{c_1}) - \Theta_k(\mathbf{c_2})) \\ &= d_H(\Theta_k(\mathbf{c_1}), \Theta_k(\mathbf{c_2})). \end{aligned} \tag{32}$$

Therefore, the map Θ_k preserve distance. □

Proposition 2 Let C be a linear code over the ring $\mathscr{R}_k$ of length n. Then $|\Theta_k(C^\perp)| = |\Theta_k(C)^\perp|$, and $\Theta_k(C)$ is self-orthogonal iff C is a self orthogonal code. Moreover, $\Theta_k(C)$ is self dual iff C is a self dual code.

Proof. Given two elements $\mathbf{s}$, $\mathbf{t} \in \mathscr{R}_k^n$, let us say that

$$\begin{aligned} \mathbf{s} &= (s_0, s_1, \ldots, s_{n-1}) \\ \mathbf{t} &= (t_0, t_1, \ldots, t_{n-1}), \end{aligned} \tag{33}$$

where $s_j = \sum\limits_{i=1}^{2^k} p_{i,j}\zeta_i^k$ and $t_j = \sum\limits_{i=1}^{2^k} r_{i,j}\zeta_i^k$ for $i = 1, 2, \ldots, 2^k$ and $j = 1, 2, \ldots, n-1$, with $p_{i,j}$, $r_{i,j} \in \mathscr{F}_{p^m}$. Next, assume that $\mathbf{s} \cdot \mathbf{t} = 0$. Then, we have

$$\begin{aligned} &\sum_{i=1}^{n-1} s_j t_j = 0 \\ \Longrightarrow &\sum_{j=0}^{n-1} (\sum_{i=0}^{2^k} p_{i,j}\zeta_i^k)(\sum_{i=0}^{2^k} r_{i,j}\zeta_i^k) = 0. \end{aligned} \tag{34}$$

Since $(\zeta_i^k)^2 = \zeta_i^k$, we have

$$\sum_{j=0}^{n-1} \sum_{i=0}^{2^k} p_{i,j} r_{i,j} \zeta_i^k \ = \ \sum_{i=0}^{2^k} \sum_{j=0}^{n-1} p_{i,j} r_{i,j} \zeta_i^k \ = \ 0. \tag{35}$$

Therefore,

$$\sum_{j=0}^{n-1} p_{i,\,j} r_{i,\,j} \;=\; 0, \tag{36}$$

where $i = 1, 2, 3, \ldots, 2^k$. Also,

$$\begin{aligned}\Theta_k(\mathbf{s})\Theta_k(\mathbf{t}) &= \sum_{j=0}^{n-1}\sum_{i=0}^{2^k} p_{i,\,j} r_{i,\,j}\\ &= \sum_{i=0}^{2^k}\sum_{j=0}^{n-1} p_{i,\,j} r_{i,\,j}\\ &= 0.\end{aligned} \tag{37}$$

This implies that,

$$\Theta_k(C^{\perp}) \;\subseteq\; \Theta_k(C)^{\perp}. \tag{38}$$

Since Θ_k is a one-to-one correspondence, it follows that $|\Theta_k(C^{\perp})| = |\Theta_k(C)^{\perp}|$. Consequently, $\Theta_k(C^{\perp}) = \Theta_k(C)^{\perp}$. Moreover, C is a self-orthogonal code iff $C \subseteq C^{\perp}$, which implies that $\Theta_k(C) \subseteq \Theta_k(C^{\perp}) = \Theta_k(C)^{\perp}$ iff $\Theta_k(C)$ is self-orthogonal. Similarly, C is a self-dual code iff $\Theta_k(C)$ is self-dual. □

Proposition 3 Let $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i$ be a linear code over the ring $\mathscr{R}_k$ having length n. Then,

(i) $\Theta_k(C) = C_1 \otimes C_2 \otimes C_3 \otimes \cdots \otimes C_{2^k}$. Additionally, $|C| = |C_1||C_2||C_3|\cdots|C_{2^k}|$.

(ii) $C^{\perp} = \oplus_{i=1}^{2^k} \zeta_i^k C_i^{\perp}$. Moreover, each C_i is self-orthogonal iff C is a self-orthogonal code, and each C_i is self-dual iff C is a self-dual code.

Proof. (i) Assume that $\mathbf{w} = (\gamma_{1,\,0}^k,\ \gamma_{1,\,1}^k,\ \ldots,\ \gamma_{1,\,n-1}^k,\ \gamma_{2,\,0}^k,\ \gamma_{2,\,1}^k,\ \ldots,\ \gamma_{2,\,n-1}^k,\ \ldots,\ \gamma_{2^k,\,0}^k,\ \ldots,\ \gamma_{2^k,\,1}^k,\ \ldots,\ \gamma_{2^k,\,n-1}^k)$ for $j = 0,\ 1,\ 2,\ \ldots,\ n-1$. Consequently, $\mathbf{s} = (s_0,\ s_1,\ s_2,\ \ldots,\ s_{n-1}) \in C$. The map Θ_k is bijective, therefore for any $i = 1,\ 2,\ 3,\ \ldots,\ 2^k$, $(\gamma_{i,\,0}^k,\ \gamma_{i,\,1}^k,\ \ldots,\ \gamma_{i,\,n-1}^k) \in C_i$. This implies $\mathbf{w} \in C_1 \otimes C_2 \otimes C_3 \otimes \cdots \otimes C_{2^k}$ according to the definition of C_i. Thus, $\Theta_k(C) \subseteq C_1 \otimes C_2 \otimes C_3 \otimes \cdots \otimes C_{2^k}$.

Conversely, suppose $\mathbf{w} = (\gamma_{1,\,0}^k, \gamma_{1,\,1}^k, \ldots, \gamma_{1,\,n-1}^k, \gamma_{2,\,0}^k, \gamma_{2,\,1}^k, \ldots, \gamma_{2,\,n-1}^k, \ldots, \gamma_{2^k,\,0}^k, \gamma_{2^k,\,1}^k, \ldots, \gamma_{2^k,\,n-1}^k) \in C_1 \otimes C_2 \otimes C_3 \otimes \cdots \otimes C_{2^k}$. Then, $(\gamma_{i,\,0}^k, \gamma_{i,\,1}^k, \ldots, \gamma_{i,\,n-1}^k) \in C_i$ for each $i = 1, 2, \ldots, 2^k$. Define $s_j = \sum\limits_{i=1}^{2^k} \gamma_{i,\,j}^k \zeta_i^k$ for $j = 0, 1, 2, \ldots, n-1$. Then, $\mathbf{s} = (s_0, s_1, s_2, s_3, \ldots, s_{n-1}) \in C$ and hence $\Theta_k(\mathbf{s}) = \mathbf{w}$. Thus, $\mathbf{w} \in \Theta_k(C)$. It follows that $C_1 \otimes C_2 \otimes C_3 \otimes \cdots \otimes C_{2^k} \subseteq \Theta_k(C)$.

Since Θ_k is one-one and onto, we have $|C| = |\Theta_k(C)|$. Thus,

$$|C| = |C_1 \otimes C_2 \otimes C_3 \otimes \cdots \otimes C_{2^k}| = |C_1|\,|C_2|\,|C_3| \cdots |C_{2^k}|. \tag{39}$$

(ii) Let us define

$$U_j = \left\{ \mathbf{r_j} \in \mathscr{F}_{p^m}^n \mid \sum_{i=1}^{2^k} \zeta_i^k \mathbf{r_i} \in C^\perp, \text{ for } \mathbf{r_i} \in \mathscr{F}_{p^m}^n, \; i \neq j \text{ with } 1 \leq i, j \leq 2^k \right\}. \tag{40}$$

The unique expression for $C^\perp$ can then be

$$C^\perp = \zeta_1^k U_1 \oplus \zeta_2^k U_2 \oplus \zeta_3^k U_3 \oplus \cdots \oplus \zeta_{2^k}^k U_{2^k}. \tag{41}$$

Consider

$$U_1 = \left\{ \mathbf{r_1} \in \mathscr{F}_{p^m}^n \mid \sum_{i=1}^{2^k} \zeta_i^k \mathbf{r_i} \in C^\perp, \text{ for } \mathbf{r_i} \in \mathscr{F}_{p^m}^n, \; i \neq 1 \text{ with } 1 \leq i \leq 2^k \right\} \tag{42}$$

It is evident that $C_1 U_1 = 0$, implying $U_1 \subseteq C_1^\perp$.
Conversely, let $\mathbf{c_1} \in C_1^\perp$. Then $\mathbf{c_1} \mathbf{x_1} = 0$ for any $\mathbf{c} = \sum_{i=1}^{2^k} \zeta_i^k \mathbf{x_i} \in C$. Thus,

$$\zeta_1^k \mathbf{c_1} \mathbf{c} = \zeta_1^k \mathbf{c_1} \mathbf{x_1} = 0, \tag{43}$$

which implies that $\zeta_1^k \mathbf{c_1} \in C^\perp$. Therefore, by the uniqueness of the representation of $C^\perp$, we deduce $\mathbf{c_1} \in U_1$, hence $C_1^\perp \subseteq U_1$. Thus, $C_1^\perp = U_1$.

Similarly, for each $j = 2, 3, \ldots, 2^k$, we can demonstrate that $C_j^\perp = U_j$. Therefore,

$$C^\perp = \bigoplus_{i=1}^{2^k} \zeta_i^k C_i^\perp. \tag{44}$$

Furthermore, $C \subseteq C^\perp$ iff C is self-orthogonal. This yields

$$\zeta_1^k C_1 \oplus \cdots \oplus \zeta_{2^k}^k C_{2^k} \subseteq \zeta_1^k C_1^\perp \oplus \cdots \oplus \zeta_{2^k}^k C_{2^k}^\perp \iff C_i \subseteq C_i^\perp, \tag{45}$$

for each $i = 1, 2, 3, \ldots, 2^k$. In a similar manner, it is evident that C is a self-dual code iff each C_i is self-dual code. □

Proposition 4 Let $C = \bigoplus_{i=1}^{2^k} \zeta_i^k C_i$ be a linear code over the ring $\mathscr{R}_k$ with parameters $[n, k, d_L]$. Then, $\Theta_k(C)$ is a linear code over $\mathscr{F}_{p^m}$ with parameters $[2^k n, \sum_{i=1}^{2^k} k_i, d_H]$, where $i = 1, 2, 3, \ldots, 2^k$ and $d_L = d_H$.

3.2 *Constacyclic codes over the ring $\mathscr{R}_k$*

In this section, several important conclusions about constacyclic codes over the ring $\mathscr{R}_k$ are presented. We also study the dual codes of λ-constacyclic codes and discuss about their generators.

Let $\lambda \in \mathscr{R}_k$ be expressed as $\lambda = \sum_{i=1}^{2^k} \lambda_i \zeta_i^k$, where each $\lambda_i \in \mathscr{F}_{p^m}$ for $i = 1, 2, \ldots, 2^k$.

$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_{2^k})(P_k^{-1})^T \begin{pmatrix} \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_{2^k} \end{pmatrix} = (\kappa_1, \kappa_2, \kappa_3, \dots, \kappa_{2^k}) \begin{pmatrix} \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_{2^k} \end{pmatrix}$. Noteworthy is the fact that $\lambda = \lambda \sum_{i=1}^{2^k} \zeta_i^k = \sum_{i=1}^{2^k} \kappa_i \zeta_i^k$ and $(\kappa_1, \kappa_2, \kappa_3, \dots, \kappa_{2^k}) = (\lambda_1, \lambda_2, \dots, \lambda_{2^k})(P_k^{-1})^T$.

Proposition 5 Suppose that $\lambda = \sum_{i=1}^{2^k} \lambda_i \zeta_i$ is an element of $\mathscr{R}_k$, and let $(\kappa_1, \kappa_2, \dots, \kappa_{2^k}) = (\lambda_1, \lambda_2, \dots, \lambda_{2^k})(P_k^{-1})^T$. Then, λ is a unit in $\mathscr{R}_k$ iff each κ_i is a unit in $\mathscr{F}_{p^m}$ for all $1 \le i \le 2^k$.

Proof. It is known that $\lambda = \sum_{i=1}^{2^k} \kappa_i \zeta_i$, where the κ_i are defined as above. Consequently, in the ring $\mathscr{R}_k$, λ is a unit iff there exists an element $x = \sum_{i=1}^{2^k} \beta_i \zeta_i$ in $\mathscr{R}_k$ such that

$$1 = \lambda x = \left(\sum_{i=1}^{2^k} \kappa_i \zeta_i \right) \left(\sum_{i=1}^{2^k} \beta_i \zeta_i \right) = \sum_{i=1}^{2^k} \kappa_i \beta_i \zeta_i. \tag{46}$$

Here, the set $\{\zeta_i \mid 1 \le i \le 2^k\}$ is linearly independent over $\mathscr{F}_{p^m}$ and $\sum_{i=1}^{2^k} \zeta_i = 1$. Therefore, λ is a unit iff $\kappa_i \beta_i = 1$ for each $1 \le i \le 2^k$. □

Theorem 1 Let $C = \bigoplus_{i=1}^{2^k} \zeta_i^k C_i$ be a linear code over the ring $\mathscr{R}_k$ of length n, where $\lambda \in U(\mathscr{R}_k)$. Then, the code C is a λ-constacyclic over $\mathscr{R}_k$ of length n iff each C_i is a κ_i-constacyclic code over the field $\mathscr{F}_{p^m}$ of length n, where $i = 1, 2, 3, \dots, 2^k$.

Proof. Let C be a linear code over the ring $\mathscr{R}_k$ of length n. Consider any codeword $\mathbf{c} = (c_0, c_1, c_3, \dots, c_{n-1}) \in C$ where each c_j can be written as $c_j = \sum_{i=1}^{2^k} \zeta_i^k c_{i,j}$ with $c_{i,j} \in \mathscr{F}_{p^m}$ for $i = 1, 2, 3, \dots, 2^k$ and $j = 0, 1, 2, \dots, n-1$. Let $\mathbf{y_i} = (c_{i,0}, c_{i,1}, \dots, c_{i,n-1}) \in C_i$ for each i, where $\mathbf{y_i}$ belongs to the code C_i. The λ-constacyclic code C over $\mathscr{R}_k$ gives us $\delta_\lambda(\mathbf{c}) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$, where $\delta_\lambda(\mathbf{c})$ indicates the λ-constacyclic shift of $\mathbf{c}$. Observe that

$$\lambda c_{n-1} = \lambda \sum_{i=1}^{2^k} c_{i,n-1} \zeta_i^k = \sum_{i=1}^{2^k} \lambda c_{i,n-1} \zeta_i^k = \sum_{i=1}^{2^k} \kappa_i c_{i,n-1} \zeta_i^k. \tag{47}$$

Hence, we have

$$\delta_\lambda(\mathbf{c}) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) = \sum_{i=1}^{2^k} (\kappa_i c_{i,n-1}, c_{i,0}, c_{i,1}, \dots, c_{i,n-2}) \zeta_i^k. \tag{48}$$

Therefore, $\delta_\lambda(\mathbf{c}) \in C$ iff $\delta_\lambda(\mathbf{y_i}) = (\kappa_i c_{i,n-1}, c_{i,0}, \dots, c_{i,n-2}) \in C_i$ for each $i = 1, 2, 3, \dots, 2^k$. Thus, C is a λ-constacyclic code of length n over $\mathscr{R}_k$ iff each C_i is a κ_i-constacyclic code over $\mathscr{F}_{p^m}$ of length n. □

Theorem 2 Let $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i$ be a λ-constacyclic code of length n over the ring $\mathscr{R}_k$, where $g_i(y)$ is the monic generator polynomial of the κ_i-constacyclic code C_i such that $g_i(y)$ divides $y^n - \kappa_i$ for all $i = 1, 2, 3, \dots, 2^k$. Then:

(i) The code C can be expressed as $C = \langle g_1(y)\zeta_1^k,\ g_2(y)\zeta_2^k,\ \dots,\ g_{2^k}(y)\zeta_{2^k}^k \rangle$ and its size is $|C| = (p^m)^{2^k n - \sum_{i=1}^{2^k} \deg(g_i(y))}$.

(ii) Moreover, C can also be generated by a single polynomial $g(y) = \sum_{i=1}^{2^k} g_i(y)\zeta_i^k$, where $g(y)$ divides $y^n - \lambda$ in $\mathscr{R}_k[y]$.

Proof. (i) According to Theorem 1, for $i = 1, 2, 3, \dots, 2^k$, each C_i is a κ_i-constacyclic code over $\mathscr{F}_{p^m}$ of length n. Given that the generator polynomial (monic) of C_i is $g_i(y)$ and over the ring $\mathscr{R}_k$, C is a λ-constacyclic code, we obtain

$$C_i = \langle g_i(y) \rangle \subseteq \frac{\mathscr{F}_{p^m}[y]}{\langle y^n - \kappa_i \rangle}. \tag{49}$$

Hence, it follows that

$$C = \langle g_1(y)\zeta_1^k,\ g_2(y)\zeta_2^k, \ldots,\ g_{2^k}(y)\zeta_{2^k}^k \rangle. \tag{50}$$

Moreover, we obtain $|\Theta_k(C)| = |C|$ since the Gray map Θ_k is one-one and onto. According to Proposition 3, this means that

$$\begin{aligned} |C| &= |C_1||C_2||C_3|\cdots|C_{2^k}| \\ &= (p^m)^{n-\deg(g_1(y))} \cdot (p^m)^{n-\deg(g_2(y))} \cdots (p^m)^{n-\deg(g_{2^k}(y))} \\ &= (p^m)^{2^k n - \sum\limits_{i=1}^{2^k} \deg(g_i(y))}. \end{aligned} \tag{51}$$

(ii) By part (i), we have

$$C = \langle g_1(y)\zeta_1^k,\ g_2(y)\zeta_2^k, \ldots,\ g_{2^k}(y)\zeta_{2^k}^k \rangle. \tag{52}$$

Define

$$D = g_1(y)\zeta_1^k + g_2(y)\zeta_2^k + \cdots + g_{2^k}(y)\zeta_{2^k}^k. \tag{53}$$

Clearly, $D \subseteq C$. Since $(\zeta_i^k)^2 = \zeta_i^k$ and $\zeta_i^k \zeta_j^k = 0$ for $i \neq j$, it follows that

$$g_i(y)\zeta_i^k = \left(\sum_{j=1}^{2^k} g_j(y)\zeta_j^k \right) \zeta_i^k. \tag{54}$$

This shows that $C \subseteq D$. Consequently, $C = D$, where

$$g(y) = \sum_{i=1}^{2^k} g_i(y)\zeta_i^k. \tag{55}$$

Since each $g_i(y)$ is the monic generator polynomial of C_i, we have $g_i(y)$ divides $y^n - \kappa_i$, i.e.,

$$y^n - \kappa_i = h_i(y)g_i(y), \tag{56}$$

which implies that

$$(y^n - \kappa_i)\zeta_i^k = h_i(y)g_i(y)\zeta_i^k \tag{57}$$

for each $i = 1, 2, 3, \ldots, 2^k$. Thus,

$$\begin{aligned} y^n - \lambda &= y^n\left(\sum_{i=1}^{2^k}\zeta_i^k\right) - \sum_{i=1}^{2^k}\kappa_i\zeta_i^k \\ &= \sum_{i=1}^{2^k}(y^n - \kappa_i)\zeta_i^k \\ &= \sum_{i=1}^{2^k}h_i(y)g_i(y)\zeta_i^k \\ &= \left(\sum_{i=1}^{2^k}h_i(y)\zeta_i^k\right)\left(\sum_{i=1}^{2^k}g_i(y)\zeta_i^k\right) \\ &= \left(\sum_{i=1}^{2^k}h_i(y)\zeta_i^k\right)g(y). \end{aligned} \tag{58}$$

Hence, we have that $g(y)$ divides $y^n - \lambda$. □

Corollary 1 Let $C = \bigoplus_{i=1}^{2^k}\zeta_i C_i$ denote a λ-constacyclic code over the ring $\mathscr{R}_k$ of length n, where $\lambda = \sum_{i=1}^{2^k}\kappa_i\zeta_i$ is a unit in the ring $\mathscr{R}_k$. Then,

(i) $C^\perp = \bigoplus_{i=1}^{2^k}\zeta_i C_i^\perp$ forms a λ^{-1}-constacyclic code over the ring $\mathscr{R}_k$ of length n, where each $C_i^\perp$ is a κ_i^{-1}-constacyclic code over $\mathscr{F}_{p^m}$ of length n, for $1 \leq i \leq 2^k$.

(ii) Let the monic generator polynomial of the κ_i-constacyclic code C_i be $g_i(y)$, where $g_i(y)$ divides $y^n - \kappa_i$ for each i with $1 \leq i \leq 2^k$. Then,

(a) $C^\perp = \langle h_1^*(y)\zeta_1,\ h_2^*(y)\zeta_2,\ h_3^*(y)\zeta_3, \ldots, h_{2^k}^*(y)\zeta_{2^k}\rangle$ and $|C^\perp| = (p^m)^{\sum_{i=1}^{2^k} deg(g_i(y))}$.

(b) $C^\perp = \langle h^{'}(y)\rangle$, where $h^{'}(y) = \sum_{i=1}^{2^k}h_i^*(y)\zeta_i$.

Here $y^n - \kappa_i = g_i(y)h_i(y)$ for some $h_i(y) \in \mathscr{F}_{p^m}[y]$ and $h_i(y) = \beta_0 + \beta_1 y + \cdots + \beta_{n-r}y^{n-r}$. Then $h_i^*(y) = \beta_{n-r} + \beta_{n-r-1}y + \cdots + \beta_0 y^{n-r}$ and $h_i^*(y)$ generates the dual κ_i^{-1}-constacyclic code $C_i^\perp$.

Proposition 6 Let $C = \oplus_{i=1}^2\zeta_i C_i$ be a λ-constacyclic code of length n over the ring $\mathscr{R}_1$. Then, the following statements hold.

(i) The code C is a cyclic of length n over the ring $\mathscr{R}_1$ iff each C_i is a cyclic code for $i = 1, 2$ of length n over $\mathscr{F}_{p^m}$.

(ii) If $\lambda = u_1$, then C is a λ-constacyclic code iff C_1 is a negacyclic code and C_2 is a cyclic code, both of length n over $\mathscr{F}_{p^m}$.

(iii) If $\lambda = -u_1$, then C is a λ-constacyclic code iff C_1 is a cyclic code and C_2 is a negacyclic code, both of length n over $\mathscr{F}_{p^m}$.

3.3 Quantum codes

Quantum codes are essential for shielding quantum information from noise while it travels across several channels in quantum computing and communication. The creation of QEC codes based on classical codes, initially presented by Calderbank et al. [11], is a noteworthy advancement in this field. From cyclic codes that contain their duals, we develop quantum codes using the Calderbank-Shor-Steane (CSS) structure [23]. By using this technique, we can create quantum codes with better parameters than those that are currently in use. Furthermore, we establish the condition necessary for constacyclic codes to contain their duals in the ring $\mathscr{R}_k$ by using a criteria developed over finite fields in [11]. The necessary and sufficient condition for a constacyclic code to include its counterpart is established by our first finding.

Lemma 1 [11] Let C be a λ-constacyclic code over $\mathscr{F}_{p^m}$ with generator polynomial $g(y)$. Then, C contains its dual iff

$$y^n - \lambda \equiv 0 \pmod{g(y)g^*(y)}, \tag{59}$$

where $\lambda = \pm 1$ and $g^*(y)$ represent the reciprocal polynomial of $g(y)$.

Lemma 2 [23] [CSS Construction] If C is an $[n, k, d]$ linear code over $\mathscr{F}_{p^m}$ satisfying $C^{\perp} \subseteq C$, then there exists a QEC code with parameters $[[n, 2k-n, d]]$ over $\mathscr{F}_{p^m}$.

Theorem 3 Let $C = \oplus_{i=1}^{2^k} \zeta_i C_i$ be a λ-constacyclic code over the ring $\mathscr{R}_k$ of length n such that $\lambda = \sum\limits_{i=1}^{2^k} \kappa_i \zeta_i$ with $\kappa_i = \pm 1$. Then, $C^{\perp} \subseteq C$ iff

$$y^n - \kappa_i \equiv 0\, mod(g_i(y)g_i^*(y)), \tag{60}$$

where, the reciprocal polynomial of $g_i(y)$ is $g_i^*(y)$, for $1 \leq i \leq 2^k$.

Proof. Let $C = \bigoplus_{i=1}^{2^k} \zeta_i C_i$ be a λ-constacyclic code over the ring $\mathscr{R}_k$ of length n, where each $C_i = \langle g_i(y) \rangle$ for $1 \leq i \leq 2^k$. Suppose that

$$y^n - \kappa_i \equiv 0 \pmod{g_i(y)g_i^*(y)}, \tag{61}$$

then it follows that $C_i^{\perp} \subseteq C_i$ for all i with $1 \leq i \leq 2^k$. Consequently, we have $\zeta_i C_i^{\perp} \subseteq \zeta_i C_i$ for each i. This implies

$$\zeta_1 C_1^{\perp} \oplus \zeta_2 C_2^{\perp} \oplus \cdots \oplus \zeta_{2^k} C_{2^k}^{\perp} \subseteq \zeta_1 C_1 \oplus \zeta_2 C_2 \oplus \cdots \oplus \zeta_{2^k} C_{2^k}, \tag{62}$$

that is, $C^{\perp} \subseteq C$.

On the other hand, if $C^{\perp} \subseteq C$, then

$$\zeta_1 C_1^{\perp} \oplus \zeta_2 C_2^{\perp} \oplus \cdots \oplus \zeta_{2^k} C_{2^k}^{\perp} \subseteq \zeta_1 C_1 \oplus \zeta_2 C_2 \oplus \cdots \oplus \zeta_{2^k} C_{2^k}. \tag{63}$$

Since each $\zeta_i C_i$ is congruent to C modulo ζ_j for $i \neq j$ with $i, j \in \{1, 2, 3, \ldots, 2^k\}$, we have that $C_i^{\perp} \subseteq C_i$ for all i. Therefore,

$$y^n - \kappa_i \equiv 0 \pmod{g_i(y)g_i^*(y)}. \tag{64}$$

□

Corollary 2 Let $C = \bigoplus_{i=1}^{2^k} \zeta_i C_i$ be a λ-constacyclic code of length n over the ring $\mathscr{R}_k$, where $\lambda = \sum_{i=1}^{2^k} \kappa_i \zeta_i$ with each $\kappa_i = \pm 1$. Then, $C^{\perp} \subseteq C$ holds if and only if $C_i^{\perp} \subseteq C_i$ for all i with $1 \leq i \leq 2^k$.

Proof. The proof is obvious by Theorem 3. □

Theorem 4 Let $C = \bigoplus_{i=1}^{2^k} \zeta_i C_i$ be a λ-constacyclic code of length n over the ring $\mathscr{R}_k$, where each $C_i = \langle g_i(y) \rangle$ for $i = 1, 2, \ldots, 2^k$. Then, $\Theta_k(C)$ has parameters $[2^k n, \sum_{i=1}^{2^k} k_i, d_H]$.

(i) If $C^{\perp} \subseteq C$, then there exists a quantum code with parameters $[[2^k n, \sum_{i=1}^{2^k} k_i - 2^k n, d_H]]$ over $\mathscr{F}_{p^m}$.

(ii) If for each $i = 1, 2, \ldots, 2^k$, we have

$$y^n - \kappa_i \equiv 0 \pmod{g_i(y)g_i^*(y)}, \tag{65}$$

where $g_i^*(y)$ denotes the reciprocal polynomial of $g_i(y)$, then a quantum code with parameters $[[2^k n, 2\sum_{i=1}^{2^k} k_i - 2^k n, d_H]]$ over $\mathscr{F}_{p^m}$ can be constructed.

Proof. (i) First, assume that $C \subseteq C^{\perp}$. We get $\Theta_k(C^{\perp}) = \Theta_k(C)^{\perp}$ from Proposition 2, and hence $\Theta_k(C)^{\perp} \subseteq \Theta_k(C)$. This implies that $\Theta_k(C)$ is a linear code over $\mathscr{F}_{p^m}$ that contains duals. Consequently, a QEC with parameters $[[2^k n, 2\sum_{i=1}^{2^k} k_i - 2^k n, d_H]]$ over $\mathscr{F}_{p^m}$ exists according to Lemma 2.

(ii) Assume that $y^n - \kappa_i \equiv 0 \pmod{g_i(y)g_i^*(y)}$ for each $i = 1, 2, 3, \ldots, 2^k$, where, the reciprocal polynomial of $g_i(y)$ is $g_i^*(y)$. Then, by Theorem 3, we have that $C^{\perp} \subseteq C$. Therefore, using part (i) of this theorem, there exists a QEC with parameters $[[2^k n, 2\sum_{i=1}^{2^k} k_i - 2^k n, d_H]]$ over $\mathscr{F}_{p^m}$. □

4. Applications

In this section, we construct new quantum codes over the ring $\mathscr{R}_1$ $(k = 1)$ by utilising the dual-containing property of constacyclic codes. All computations in the forthcoming examples were carried out using the Magma computational algebra system [24]. We begin with the following:

Example 1 For $n = 3$, $m = 1$, and $p = 3$, consider the ring $\mathscr{R}_1 = \mathscr{F}_3[w_1]/\langle w_1^2 - 1 \rangle$. In $\mathscr{F}_3[x]$, we have

$$x^3 - 1 = (x+1)^3, \quad x^3 + 1 = (x+2)^3. \tag{66}$$

Let $g_1(x) = (x+2)^2$ and $g_2(x) = (x+1)$ be polynomials over $\mathscr{F}_3$. Then, C forms a constacyclic code of length 3 over $\mathscr{R}_1$. Proposition 4 states that the parameters of the Gray image $\Theta_1(C)$ are $[16, 10, 4]$ over $\mathscr{F}_3$. According to the database, this code is ideal [25].

Example 2 For $n = 8$, $m = 1$, and $p = 3$, consider the ring $\mathscr{R}_1 = \mathscr{F}_3[w_1]/\langle w_1^2 - 1 \rangle$. In $\mathscr{F}_3[y]$, we observe that

$$y^9 - 1 = (y+2)^9. \tag{67}$$

Let $g_1(y) = (y+2)^4$ and $g_2(y) = (y+2)$ be two polynomials over $\mathscr{F}_3$. Then, a cyclic code of length 9 is formed by C over $\mathscr{R}_1$. The gray image $\Theta_1(C)$ has parameters [18, 13, 3] over $\mathscr{F}_3$ according to Proposition 4. Moreover, since $y^9 - 1 \equiv 0 \pmod{g_i(y)g_i^*(y)}$ for $i = 1, 2$, Theorem 3 implies that $C^\perp \subseteq C$. Consequently, by Theorem 4, there exists a quantum code with parameters $[[18, 8, 3]]_4$. According to the database [26], this quantum code is new.

Example 3 For $n = 10$, $m = 1$, and $p = 5$, consider the ring $\mathscr{R}_1 = \mathscr{F}_5[w_1]/\langle w_1^2 - 1\rangle$. In $\mathscr{F}_5[y]$, we have

$$y^{10} - 1 = (y+1)^5(y+4)^5, \quad y^{10} + 1 = (y+2)^5(y+3)^5. \tag{68}$$

Let $g_1(y) = (y+4)^2$ and $g_2(y) = (y+2)$ be polynomials over $\mathscr{F}_5$. Then, C_1 is a cyclic code with parameters [10, 8, 3] over $\mathscr{F}_5$, and C_2 is a negacyclic code with parameters [10, 9, 2] over $\mathscr{F}_5$. Therefore, the Gray image of C has parameters $[20, 17, 3]_5$. Since $g_1(y)g_1^*(y)$ divides $y^{10} - 1$ and $g_2(y)g_2^*(y)$ divides $y^{10} + 1$, Theorem 3 implies that $C^\perp \subseteq C$. Thus, by Theorem 4, there exists a quantum error-correcting code with parameters $[[20, 14, 3]]_5$. According to the database [26], this is a new quantum code.

Table 1. Gray images of cyclic codes of length n over $\mathscr{R}_1$

p^m $(m=1)$	n	$g_1(y)$	$g_2(y)$	$\Theta_1(C)$	Remarks
3	3	$(y+2)^2$	$(y+1)$	$[6, 3, 3]_3$	Optimal
3	4	$(y+1)(y^2+1)$	(y^2+y+2)	$[8, 3, 5]_3$	Optimal
3	4	y^2+1	(y^2+2y+2)	$[8, 4, 4]_3$	Optimal
3	6	$(y+1)^3$	(y^2+1)	$[12, 7, 4]_3$	Optimal
3	6	$(y+1)$	(y^2+2y+4)	$[12, 9, 3]_3$	Optimal
5	15	$(y^2+y+1)(y+4)^2$	$(y+1)$	$[30, 25, 3]_2$	...
13	6	$y+1$	$y+2$	$[12, 10, 3]_{13}$	Optimal
13	12	$y+1$	y^2+1	$[24, 21, 3]_{13}$	Optimal
17	8	$y+1$	$y+5$	$[16, 14, 3]_{17}$	Optimal
29	14	$y+4$	$y+3$	$[28, 26, 3]_{29}$	Optimal

Table 2. Quantum codes from cyclic codes over the ring $\mathscr{R}_1$

n	$g_1(y)$	$g_2(y)$	$\Theta_1(C)$	$[[n, k, d]]_{p^m}$	New Quantum Code (NQC)
9	$(y+2)^4$	$y+2$	[18, 13, 3]	$[[18, 8, 3]]_3$	NQC
10	$(y+1)^2(y+4)$	$y+1$	[20, 16, 3]	$[[20, 12, 3]]_5$	NQC
15	$(y+4)^2(y^2+y+1)$	$y+4$	[30, 25, 3]	$[[30, 20, 3]]_5$	...
20	$(y+1)^2(y+2)$	$y+1$	[40, 36, 3]	$[[40, 32, 3]]_5$	$[[40, 32, 2]]_5$ [26]
25	$(y+1)^6$	$y+4$	[50, 43, 3]	$[[50, 36, 3]]_5$	NQC
80	$(y+1)(y^4+3)$	$y+1$	[160, 154, 3]	$[[160, 148, 3]]_5$	$[[160, 146, 3]]_5$ [26]
7	$(y+6)^3$	$y+6$	[14, 10, 4]	$[[14, 6, 4]]_7$	NQC
12	$(y+2)(y^2+2)$	$y+2$	[24, 20, 3]	$[[24, 16, 3]]_7$	...
14	$(y+1)^3(y+6)$	$y+1$	[28, 23, 4]	$[[28, 18, 4]]_7$	NQC
21	$(y+3)^3(y+5)(y+6)$	$y+3$	[42, 36, 4]	$[[42, 30, 4]]_7$	NQC
28	$(y+1)^3(y^2+1)$	$y+1$	[56, 50, 4]	$[[56, 44, 4]]_7$	...

Table 3. Quantum codes from w_1-constacyclic codes over the ring $\mathscr{R}_1$

n	$g_1(y)$	$g_2(y)$	$\Theta_1(C)$	$[[n, k, d]]_{p^m}$	New Quantum Code (NQC)
5	$(y+4)^2$	$y+1$	[10, 7, 3]	$[[10, 4, 3]]_5$	NQC
10	$(y+4)^2$	$(y+2)$	[20, 17, 3]	$[[20, 14, 3]]_5$	NQC
30	(y^2+y+1)	$(y+2)^2$	[60, 56, 3]	$[[60, 52, 3]]_5$	NQC
35	$y^6+y^5+y^4+y^3+y^2+y+1$	$(y+1)^2$	[70, 62, 3]	$[[70, 54, 3]]_5$	NQC
40	$(y+4)^2$	y^4+2	[80, 74, 3]	$[[80, 68, 3]]_5$	NQC
21	$(y+3)^2$	$y+2$	[42, 39, 3]	$[[42, 36, 3]]_7$	...
28	$(y+1)^2$	y^2+3y+2	[56, 52, 3]	$[[56, 48, 3]]_7$	NQC
22	$(y+1)^3(y+10)$	y^2+1	[44, 38, 4]	$[[44, 32, 4]]_{11}$	NQC
33	$(y+10)^3$	$y^2+10y+1$	[66, 61, 4]	$[[66, 56, 4]]_{11}$	NQC
17	$(y+16)^3$	$y+1$	[34, 32, 4]	$[[34, 26, 4]]_{17}$	NQC

In Table 1, we list the optimal codes identified according to the database [25]. New quantum error-correcting codes built from cyclic and constacyclic codes of the form $C = \langle \oplus_{i=1}^{2^k} \zeta_i g_i(y) \rangle$ of length n over the ring $\mathscr{R}_k$ are shown in Tables 2 and 3, where each $C_i = \langle g_i(y) \rangle$ satisfies the condition $y^n - \kappa_i \equiv 0 \pmod{g_i(y) g_i^*(y)}$ for $i = 1, 2, \ldots, 2^k$.

5. LCD codes

In this section, we discuss LCD codes. If we take $\lambda = 1$ in λ-constacyclic code, then the λ-constacyclic code is cyclic code.

Definition 1 ([27]) If $C \cap C^\perp = \{0\}$, then LCD is a linear code C of length n over R.

Lemma 3 ([28]) Let C be a cyclic code of length n over $\mathscr{F}_q$ produced by a polynomial $h(y)$, where $k_1 \geq 0$, $n = p^{k_1} t$, and p and t are coprime. For C to be an LCD code, $h(y)$ must be self-reciprocal and every monic irreducible factor of $h(y)$ must have the same multiplicity in both $h(y)$ and $y^n - 1$, and conversely.

Definition 2 If, for each codeword $(c_0, c_1, c_2, \ldots, c_{n-1}) \in C$, its reverse $(c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$ also belongs to C, then a linear code C of length n over R is *reversible*.

Lemma 4 ([28]) Let C be a cyclic code over $\mathscr{F}_q$ of length n with $\gcd(n, p) = 1$. Then, C is a reversible code iff it is an LCD code.

The proofs of Theorems 5-7, Corollary 4, and Lemma 5 follow similar arguments to those presented in [29].

Theorem 5 Let $C = \oplus_{i=1}^{2^k} \zeta_i C_i$ be a cyclic code of length n over $\mathscr{R}_k$. Then, C is an LCD code iff each C_i is an LCD code of length n over $\mathscr{F}_{p^m}$ for all $i = 1, 2, 3, \ldots, 2^k$.

Proof. The proof directly follows from the fact that $C \cap C^\perp = \{0\}$ if and only if $C_i \cap C_i^\perp = \{0\}$ for $i = 1, 2, 3, \ldots, 2^k$. □

As an immediate consequence of Theorem 5, we have the following corollary:

Corollary 3 Let $n = p^t m$ such that $\gcd(m, p) = 1$. Consider $C = \oplus_{i=1}^{2^k} \zeta_i C_i$ to be a cyclic code of length n over $\mathscr{R}_k$, where each $C_i = \langle h_i(z) \rangle$ with $h_i(z) \in \mathscr{F}_{p^m}$ and $h_i(z)$ dividing $z^n - 1$ for $i = 1, 2, 3, 4$. Then, C is an LCD code iff each $h_i(z)$ is self-reciprocal, and every monic irreducible factor of $h_i(z)$ has the same multiplicity in both $h_i(z)$ and $z^n - 1$ for all $i = 1, 2, 3, 4$.

Theorem 6 Let $C = \oplus_{i=1}^{2^k} \zeta_i C_i$ be a cyclic code of length n over $\mathscr{R}_k$ with $\gcd(n, p) = 1$. Then, C is an LCD code iff each of C_1, C_2, C_3, and C_4 is a reversible code of length n over $\mathscr{F}_{p^m}$.

Proof. The proof is follows by [23, Theorem 5]. □

Corollary 4 If $gcd(n, p) = 1$, and let $C = \oplus_{i=1}^{2^k} \zeta_i C_i$ be a cyclic code of length n over $\mathscr{R}_k$, where C_i, for $i = 1, 2, 3, \ldots, 2^k$ are cyclic codes of length n over $\mathscr{F}_{p^m}$. Then, C is an LCD code iff $g_i(y)$ is a self-reciprocal polynomial in $\mathscr{F}_{p^m}$ for $i = 1, 2, 3, \ldots, 2^k$.

In light of [23, Lemma 3], we have the following result:

Lemma 5 Let C be a linear code over the ring $\mathscr{R}_k$ of length n. Then, $\eta(C \cap C^{\perp}) = \eta(C) \cap \eta(C)^{\perp}$.

Theorem 7 Let C be a linear code over the ring $\mathscr{R}_k$ of length n. Then, C is an LCD code iff its Gray image $\eta(C)$ is an LCD code over $\mathscr{F}_{p^m}$ of length $4n$.

Proof. The proof follows immediately from [23, Theorem 6]. □

Table 4. According to the database [25], here we find some optimal and near-optimal LCD codes over $\mathscr{R}_1$

n	$g_1(y)$	$g_2(y)$	$\phi(C)$	Remark
8	$(y+2)(y^2+2y+2)$	$y+1$	$[16, 12, 3]_3$	Optimal
12	$y+1$	$y+1$	$[24, 22, 2]_3$	Optimal
36	$y+1$	$y+1$	$[72, 70, 2]_3$	Optimal
6	$(y+1)(y^2+y+1)$	$y+1$	$[12, 8, 4]_5$	Optimal
27	$y+1$	$y+1$	$[54, 52, 2]_5$	Optimal
32	$y+1$	$y+1$	$[64, 62, 2]_7$	Optimal
28	$(y+1)(y^6+8y^5+3y^4+8y^3+3y^2+8y+1$	$(y+1)(y^6+8y^5+3y^4+8y^3+3y^2+8y+1$	$[56, 42, 4]_{19}$	$\cdots$
35	$(y^2+15y+1y^6+2y^5+6y^4+12y^3+6y^2+12y+1)$	$(y^2+15y+1y^6+12y^5+13y^4+3y^3+13y^2+12y+1)$	$[70, 54, 5]_{19}$	$\cdots$

6. Conclusion

This paper investigated constacyclic codes over the ring $\mathscr{R}_k = \mathscr{F}_{p^m}[w_1, w_2, \ldots, w_k]/\langle w_i^2 - 1, w_i w_j - w_j w_i \rangle$, where p is an odd prime and m is a positive integer, for all $1 \leq i, j \leq k$. We derived generators for constacyclic codes over $\mathscr{R}_k$ and, utilising their self-orthogonal property, constructed new quantum codes from constacyclic codes over the ring $\mathscr{R}_1$ $(k = 1)$. Additionally, Table 4 lists a few of the best LCD codes found using the database [25].

The main contributions of this work lie in establishing necessary conditions and algebraic structures that enable the construction of dual-containing constacyclic codes suitable for quantum error correction via the CSS construction. Compared to previous results focusing only on constacyclic codes over finite fields, our study extends these results to a broader class of rings, thus enriching the theory and expanding the pool of applicable codes for quantum coding. Moreover, constacyclic codes possess a well-defined algebraic structure, being ideals in polynomial quotient rings. This structure is crucial as it ensures efficient implementation of encoding algorithms using polynomial multiplication modulo $x^n - \lambda$, which is computationally less intensive. In measurable theoretical parameters, the constructed codes demonstrate efficacy through their dual-containing property and minimum distances, which guarantee strong error detection and correction capabilities, while their ideal structure enhances effectiveness by supporting efficient encoding and practical implement ability. This problem can be further generalized for skew-constacyclic codes, potentially yielding additional classes of quantum codes with similar advantages in algebraic structure, efficiency, and applicability to quantum error correction systems.

Acknowledgement

The authors thank to the anonymous reviewers for their valuable suggestions and comments which significantly improved both the quality and the presentation of this paper. The authors extend their appreciation to Princess Nourah bint Abdulrahman University (PNU), Riyadh, Saudi Arabia, for funding this research under Researchers Supporting Project Number (PNURSP2025R231).

Authors contributions

Each author contributed equally.

Data availability

The findings of this study are theoretical, and no data were required to support them.

Conflict of interest

The authors declare no competing financial interest.

References

[1] Berlekamp ER. *Algebraic Coding Theory*. New York: McGraw-Hill Book Company; 1968.

[2] Alabiad S, Alkhamees Y. Constacyclic codes over finite chain rings of characteristic p. *Axioms*. 2021; 10(4): 303.

[3] Bakshi GK, Raka M. A class of constacyclic codes over a finite field. *Finite Fields and Their Applications*. 2012; 18(2): 362-377.

[4] Cao Y. On constacyclic codes over finite chain rings. *Finite Fields and Their Applications*. 2013; 24: 124-135.

[5] Chen B, Fan Y, Lin L, Liu H. Constacyclic codes over finite fields. *Finite Fields and Their Applications*. 2012; 18(6): 1217-1231.

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

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

[8] Ji Z, Zhang S. Constacyclic codes over $\mathscr{F}_q[u_1, u_2, \ldots, u_k]/\langle u_i^3 - u_i,\ u_iu_j - u_ju_i\rangle$ and their applications of constructing quantum codes. *Quantum Information Processing*. 2022; 22(1): 31.

[9] Shor PW. Scheme for reducing decoherence in quantum memory. *Physical Review A*. 1995; 52: 2493-2496.

[10] Steane AM. Simple quantum error correcting codes. *Physical Review A*. 1996; 54: 4741-4751.

[11] Calderbank AR, Rains EM, Shor PM, Sloane NJA. Quantum error-correction via codes over $GF(4)$. *IEEE Transactions on Information Theory*. 1998; 44: 1369-1387.

[12] Qian J, Ma W, Gou W. Quantum codes from cyclic codes over finite ring. *International Journal of Quantum Information*. 2009; 7: 1277-1283.

[13] Ashraf M, Mohammad G. Quantum codes over $\mathscr{F}_p$ from cyclic codes over $\mathscr{F}_p[u, v]/\langle u^2 - 1,\ v^3 - v,\ uv - vu\rangle$. *Cryptography and Communications*. 2019; 11: 325-335.

[14] Bag T, Upadhyay AK, Ashraf M, Mohammad G. Quantum code from cyclic code over the ring $\mathscr{F}_p[u]/\langle u^3 - u\rangle$. *Asian-European Journal of Mathematics*. 2020; 13(1): 2050008.

[15] Gao Y, Gao J, Fu FW. Quantum codes from cyclic codes over the ring $\mathscr{F}_q + v_1\mathscr{F}_q + \cdots + v_r\mathscr{F}_q$. *Applicable Algebra in Engineering, Communication and Computing*. 2019; 30: 161-174.

[16] Islam H, Prakash O, Verma RK. Quantum codes from the cyclic codes over $\mathscr{F}_p[v, w]/\langle v^2-1, w^2-1, vw-wv\rangle$. *Springer Proceedings in Mathematics & Statistics*. 2020; 307: 67-74.

[17] Cengellenmis Y, Dertli A, Dougherty ST. Codes over an infinite family of rings with a Gray map. *Designs, Codes and Cryptography*. 2014; 72: 559-580.

[18] Zheng X, Kong B. Constacyclic codes over $\mathscr{F}_{p^m}[u_1, u_2, \ldots, u_k]/\langle u_i^2-u_i, u_iu_j-u_ju_i\rangle$. *Open Mathematics*. 2018; 16: 490-497.

[19] Dertli A, Cengellenmis Y, Eren S. On quantum codes obtained from cyclic codes over A_2. *International Journal of Quantum Information*. 2015; 13(3): 1550031.

[20] Kai X, Zhu S. Quaternary construction of quantum codes from cyclic codes over $\mathscr{F}_4+u\mathscr{F}_4$. *International Journal of Quantum Information*. 2011; 9: 689-700.

[21] Qian J. Quantum codes from cyclic codes over $\mathscr{F}_2+v\mathscr{F}_2$. *Journal of Information and Computational Science*. 2013; 10: 1715-1722.

[22] Islam H, Prakash O. New quantum and LCD codes over finite fields of even characteristic. *Defence Science Journal*. 2021; 71(5): 656-661.

[23] Grassl M, Beth T. On optimal quantum codes. *International Journal of Quantum Information*. 2004; 2(1): 55-64.

[24] Bosma W, Cannon J. *Handbook of Magma Functions*. Sydney: University of Sydney; 1995.

[25] Grassl M. Code Tables: Bounds on the parameters of various types of codes. *Online, Codetables*. 2007. Available from: http://www.codetables.de/ [Accessed 18th February 2024].

[26] Aydin N, Liu P, Yoshino B. A database of quantum codes. *arXiv:210803567*. 2021. Available from: http://quantumcodes.info/2021 [Accessed 18th February 2024].

[27] Massey JL. Linear codes with complementary duals. *Discrete Mathematics*. 1992; 106: 337-342.

[28] Yang X, Massey JL. The condition for a cyclic code to have a complementary dual. *Discrete Mathematics*. 1994; 126: 391-393.

[29] Islam H, Prakash O. Construction of LCD and new quantum codes from cyclic codes over a finite non chain ring. *Cryptography and Communications*. 2022; 14: 59-73.