

## **$\Upsilon$ – Constacyclic codes over a Frobenius ring and their application to find novel quantum codes**

Pooja Soni \*

Manju Pruthi †

*Department of Mathematics*

*Indira Gandhi University*

*Meerpur*

*Rewari 123401*

*Haryana*

*India*

Arun Kumar Yadav §

*School of Basic and Applied Sciences*

*K. R. Mangalam University*

*Sohna Road*

*Gurugram 122103*

*Haryana*

*India*

---

### **Abstract**

In this work, we use the Hermitian technique to find novel Quantum error correcting codes (QECC's) by Constacyclic codes (CCc's) over the ring  $\mathcal{R} = \mathcal{F}_{p^2}[u, v]/(u^3 - \omega^2 u, v^3 - \omega^2 v)$ , where  $p$  is a non-even prime power and  $\mathcal{F}_{p^2} = \langle \omega \rangle$ . Firstly, we express the ring in terms of "pairwise orthogonal Idempotent" elements & analyze "linear codes." We investigate ring structure and establish a one-one, onto and distance preserving Gray map,  $\emptyset : \mathcal{R}^n \rightarrow \mathcal{F}_{p^2}^{5n}$ . We provide the units of  $\mathcal{R}$ , to analyze CCc's & their generators. We also give a condition for this code to contain its Hermitian dual over  $\mathcal{R}$ . At last, we derive and tabulate some novel and efficient QECC's.

---

**Subject Classification:** 94B05, 94B15, 94B35.

**Keywords:** QECC, Hermitian, CCc, Gray map.

---

\* E-mail: [pooja.math.rs@igu.ac.in](mailto:pooja.math.rs@igu.ac.in) (Corresponding Author)

† E-mail: [manju.pruthi@yahoo.com](mailto:manju.pruthi@yahoo.com)

§ E-mail: [arun.math.rs@igu.ac.in](mailto:arun.math.rs@igu.ac.in)

## 1. Introduction

Communication is an essential part of our life. It is the exchange of information between individuals through a “noisy channel”. However, noise may create some errors in the received data. Shannon [1] claimed that appropriate encoding and decoding methods make secure information transmission possible. Quantum computation’s speed is much greater than classical computation in handling complex problems. Because quantum bits, say, qubits, can store more information than classical bits due to their superposition property. Quantum codes are crucial for safeguarding quantum information against quantum noise. Quantum codes can correct both types of errors: bit flip and phase flip. Shor [2] discovered 1<sup>st</sup> QECC. Since then, researchers’ interest in discovering new and efficient QECC’s has grown. Calderbank et al. [3] discussed a groundbreaking method for creating QECC’s using classical cyclic codes. Subsequently, researchers have focused on enhancing the effectiveness of QECC’s and extending their applicability over finite fields [4] and rings [5], [6], [7], [8], [9], [10] using Cyclic Codes. A CCc (a generalization of Cyclic Codes) is crucial for effective error correction due to its extensive algebraic structure. Recently, numerous studies have been done on the construction of QECC’s by CCc over the finite chain and non-chain rings to produce several QECC’s [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21]. Also, [22] show that complementary group codes over finite noncommutative Frobenius rings form LCD codes, including checkable codes over the same alphabet. In the present study, we generate some novel and efficient QECC’s from Hermitian dual containing CCc over the Frobenius & non-chain ring  $\mathcal{R} = \mathcal{F}_{p^2}[u, v]/(u^3 - \omega^2 u, v^3 - \omega^2 v)$ .

The outline of the study: In the first section, the introductory elements of this research study has presented. Section 2 provides a comprehensive overview of the fundamental definitions and linear codes over the field,  $\mathcal{F}_{q^2}$ , Euclidean (EIP) and Hermitian inner product (HIP) over  $\mathcal{R}$ . In section 3, we establish the structure of finite, non-chain, and Frobenius ring,  $\mathcal{R} = \mathcal{F}_{p^2}[u, v]/(u^3 - \omega^2 u, v^3 - \omega^2 v)$ . Here, we find Idempotents of  $\mathcal{R}$ , and express the ring in terms of these Idempotents. Also, we establish the distance-preserving “Gray map” over  $\mathcal{R}$ . In next section, we discuss units and some significant results related to CCc codes and the formation of QE ‘s from Y – CCc over the ring. In section 5, we construct and tabulate some novel and efficient QECC’s as an application. Last section concludes the paper.

## 2. Preliminaries

Consider the finite field  $\mathcal{F}_{p^2}$  with cardinality  $p^2$ . If a code  $C$  is a subspace of the vector space  $\mathcal{F}_{p^2}^n$ . Then,  $C$  is said to be an  $n$ -length “linear code” (LC) and the members of  $C$  are called codewords. Hamming weight of code  $C$  is described as,  $w_{\mathcal{H}}(C) = \min\{w_{\mathcal{H}}(s) = \sum_{s_i} 1 \mid s \in C, s \neq 0\}$ , and Hamming distance of  $C$ ,  $d_{\mathcal{H}}(C) = \min\{d_{\mathcal{H}}(s, l) = w_{\mathcal{H}}(s - l), s \neq l\}$ , where  $s = (s_0, s_1, \dots, s_{n-1})$ ,  $l = (l_0, l_1, \dots, l_{n-1}) \in C$ . Define Hermitian inner product of  $s$

and  $l$ ,  $\langle s, l \rangle_{\mathcal{H}} = \sum_{i'=0}^{n-1} s_{i'} l_{i'}^p$  and Hermitian dual,  $C^{\perp_{\mathcal{H}}} = \{s \in \mathcal{F}_{p^2}^n | \langle s, l \rangle_{\mathcal{H}} = 0 \forall l \in C\}$ . A  $\mathcal{F}_{p^2}$  – linear code with length  $n$  is called  $\mu'$  –CCc if  $(\mu' s_{n-1}, s_0, \dots, s_{(n-2)}) \in C \forall (s_0, s_1, \dots, s_{n-1}) \in C$ , where  $\mu' \in \mathcal{F}_{p^2}^*$ . A code  $C$  is called cyclic or negacyclic, according to  $\mu'$  is 1 or -1, respectively. Polynomial representation of  $s \in C$  is  $s_0 + s_1 y + \dots + s_{(n-1)} y^{n-1} \in \mathcal{F}_{p^2}[y]/\langle y^n - \mu' \rangle$ . An  $\mathcal{F}_{p^2}$  – linear code  $C$  with length  $n$  is called  $\mu'$  –CCc iff  $C$  is an ideal of  $\mathcal{F}_{p^2}[y]/\langle y^n - \mu' \rangle$ .

Suppose  $\gcd(n, p) = 1$ , which implies that the zeroes of  $(y^n - \mu')$  are non-repeated. Let  $\mu'$  be a primitive  $t^{\text{th}}$  root of unity and  $m$  be the least natural number such that  $p^{2m} \equiv 1 \pmod{nt}$ . Then,  $\exists$  a primitive  $nt$ .th root of unity  $\beta$  in  $\mathcal{F}_{p^{2m}}$  such that  $\beta^n = \mu'$ . Let  $\alpha = \beta^t$ , then  $\alpha$  is a primitive  $n$ .th root of unity. Then,  $y^n - \mu' = \prod_{\vartheta=0}^{(n-1)} (y - \beta^{t\vartheta+1})$ . Suppose  $\mathcal{M} = \{t\vartheta + 1 \mid \vartheta = 0 \text{ to } (n-1)\} \pmod{nt}$ . Then,  $\mathcal{W} = \{i'' \in \mathcal{M} \mid g(\beta^{i''}) = 0\}$  be the defining set of the  $\mu'$  –CCc,  $C = \langle g(y) \rangle$ .

Consider  $\tau \in \text{Aut}(\mathcal{R})$ , where  $\text{Aut}(\mathcal{R})$  is the collection of all automorphisms of a Frobenius, commutative, and finite ring  $\mathcal{R}$ . Then, we can extend it to a bijective map,  $\tau : \mathcal{R}^n \rightarrow \mathcal{R}^n$  by  $(s'_0, s'_1, \dots, s'_{n-1}) \mapsto (\tau(s'_0), \tau(s'_1), \dots, \tau(s'_{n-1}))$ . Define  $\tau$  – Inner product as,  $\langle s'', s' \rangle_{\tau} = s''_1 \tau(s'_0) + s''_2 \tau(s'_1) + \dots + s''_n \tau(s'_{n-1})$ , where  $s'' = (s''_0, s''_1, \dots, s''_{n-1})$  and  $s' = (s'_0, s'_1, \dots, s'_{n-1}) \in \mathcal{R}^n$ . When  $\mathcal{R} = \mathcal{F}_{p^2}$  and  $\tau \in \text{Aut}(\mathcal{R})$  is identity, then “ $\tau$  – inner product” becomes EIP over  $\mathcal{F}_{p^2}$ . Also, if  $\tau(b) = b^p$  for  $b \in \mathcal{F}_{p^2}$ , then “ $\tau$  – inner product” is precisely the HIP over  $\mathcal{F}_{p^2}$ . The term LC refers to a code  $C$  of length  $n$  over  $\mathcal{R}$ , if  $C$  forms an “ $\mathcal{R}$  – submodule” of  $\mathcal{R}^n$ . Dual code,  $C^{\perp_{\tau}} = \{s'' \in \mathcal{R}^n | \langle s'', s' \rangle_{\tau} = 0 \text{ for all } s' \in C\}$ .

### 3. Ring structure, Linear codes over $\mathcal{R}$ and Gray map

Consider a ring,  $\mathcal{R} = \mathcal{F}_{p^2} + u\mathcal{F}_{p^2} + u^2\mathcal{F}_{p^2} + v\mathcal{F}_{p^2} + v^2\mathcal{F}_{p^2}$  with  $u^3 = \omega^2 u$  and  $v^3 = \omega^2 v$  such that  $uv = vu = 0$ , where  $\mathcal{F}_{p^2}$  is a finite field with cardinality  $p^2$ , and  $p$  is a prime power. An element  $r \in \mathcal{R}$  be of the form,  $r = r_1 + ur_2 + u^2 r_3 + vr_4 + v^2 r_5$ , where  $r_i \in \mathcal{F}_{p^2}$ . To decompose the considered ring, let the elements of  $\mathcal{R}$  as follows:  $\varepsilon_1 = 2^{-1}(u^2 \omega^{-2} + u\omega^{-1})$ ,  $\varepsilon_2 = 2^{-1}(u^2 \omega^{-2} - u\omega^{-1})$ ,  $\varepsilon_3 = 2^{-1}(v^2 \omega^{-2} + v\omega^{-1})$ ,  $\varepsilon_4 = 2^{-1}(v^2 \omega^{-2} - v\omega^{-1})$ ,  $\varepsilon_5 = 1 - u^2 \omega^{-2} - v^2 \omega^{-2}$  such that  $\sum_{i=1}^5 \varepsilon_i = 1$ ,  $\varepsilon_i \varepsilon_j = \varepsilon_j \varepsilon_i = 0$  for  $i \neq j$ , and  $\varepsilon_i^2 = \varepsilon_i$  for all  $i, j \in \{1 \text{ to } 5\}$ . Thus,  $\mathcal{R} = \bigoplus_{i=1}^5 \varepsilon_i \mathcal{R} \cong \bigoplus_{i=1}^5 \varepsilon_i \mathcal{F}_{p^2}$ .

An element  $r = r_1 + ur_2 + u^2 r_3 + vr_4 + v^2 r_5 \in \mathcal{R}$  can be written as,  $r = r_1 + ur_2 + u^2 r_3 + vr_4 + v^2 r_5 = \varepsilon_1(r_1 + \omega r_2 + \omega^2 r_3) + \varepsilon_2(r_1 - \omega r_2 + \omega^2 r_3) + \varepsilon_3(r_1 + \omega r_4 + \omega^2 r_5) + \varepsilon_4(r_1 - \omega r_4 + \omega^2 r_5) + \varepsilon_5 r_1 = a\varepsilon_1 + b\varepsilon_2 + c\varepsilon_3 + d\varepsilon_4 + e\varepsilon_5$ , where  $r_i, a, b, c, d, e \in \mathcal{F}_{p^2}$  for all  $i \in \{1 \text{ to } 5\}$ . Define,  $C_i = \varepsilon_i C$  for all  $i \in \{1 \text{ to } 5\}$ . Then, an  $n$ -length LC,  $C$  over  $\mathcal{R}$  may be expressed as,  $C = \bigoplus_{i=1}^5 \varepsilon_i C_i$ , where  $C_i$  is an  $n$ -length  $\mathcal{F}_{p^2}$ -LC.

**Definition 1.** Define a Gray map,  $\eta: \mathcal{R} \rightarrow \mathcal{F}_{p^2}^5$  by  $\eta(a\varepsilon_1 + b\varepsilon_2 + c\varepsilon_3 + d\varepsilon_4 + e\varepsilon_5) = (a, b + c + d + e, b + c - d - e, b - c + d - e, b - c - d + e)$ , which can be extended as,  $\emptyset: \mathcal{R}^n \rightarrow \mathcal{F}_{p^2}^{5n}$  such that  $\emptyset(r'_0, r'_1, \dots, r'_{n-1}) = (\ell_1, \ell_2, \dots, \ell_5)$ , where  $\ell_1 = (a_0, a_1, \dots, a_{n-1})$ ,  $\ell_2 = ((b_0 + c_0 + d_0 + e_0), (b_1 + c_1 + d_1 + e_1), \dots, (b_{n-1} + c_{n-1} + d_{n-1} + e_{n-1}))$ ,  $\ell_3 = ((b_0 + c_0 - d_0 - e_0), (b_1 + c_1 - d_1 - e_1), \dots, (b_{n-1} + c_{n-1} - d_{n-1} - e_{n-1}))$ ,  $\ell_4 = ((b_0 - c_0 + d_0 - e_0), (b_1 - c_1 + d_1 - e_1), \dots, (b_{n-1} - c_{n-1} + d_{n-1} - e_{n-1}))$ ,  $\ell_5 = ((b_0 - c_0 - d_0 + e_0), (b_1 - c_1 - d_1 + e_1), \dots, (b_{n-1} - c_{n-1} - d_{n-1} + e_{n-1}))$ , and  $r_k = a_k\varepsilon_1 + b_k\varepsilon_2 + c_k\varepsilon_3 + d_k\varepsilon_4 + e_k\varepsilon_5 \in \mathcal{R} \forall k \in \{0 \text{ to } (n-1)\}$ .

Define lee weight of  $s' = (s'_0, s'_1, \dots, s'_{n-1}) \in \mathcal{R}^n$  as  $w_{\mathcal{L}}(s') = \sum_{k=0}^{n-1} w_{\mathcal{L}}(s'_k)$  such that  $w_{\mathcal{L}}(s'_k) = w_{\mathcal{H}}(\eta(s'_k))$ . The formula for lee distance of  $s', s'' \in \mathcal{R}^n$  is  $D_{\mathcal{L}}(s', s'') = w_{\mathcal{L}}(s' - s'') = w_{\mathcal{H}}(\emptyset(s' - s''))$ . The formula for the minimum Lee distance of  $C$  is  $D_{\mathcal{L}}(C) = \min\{D_{\mathcal{L}}(s', s'') \mid s' \neq s''\}$ . It is evident that the “Gray map”,  $\emptyset: \mathcal{R}^n \rightarrow \mathcal{F}_{p^2}^{5n}$  is distances preserving and linear. Since,  $\emptyset$  is bijective, then  $\emptyset(C)$  be an  $\mathcal{F}_{p^2}$ -LC,  $[5n, k, D_{\mathcal{H}}]_{p^2}$  where  $D_{\mathcal{H}}$  and  $k$  respectively are the Hamming distance and dimension of  $\emptyset(C)$ .

**Lemma 1:** If  $C$  is an  $n$  - length linear code over  $\mathcal{R}$ . Then,  $C^{\perp_{\tau}}$  be a linear code and  $|C||C^{\perp_{\tau}}| = |\mathcal{R}^n|$ , where  $\tau$  and  $C^{\perp_{\tau}}$  is defined in the preliminary.

**Proof:** Let  $s' = (s'_0, s'_1, \dots, s'_{n-1})$  &  $s'' = (s''_0, s''_1, \dots, s''_{n-1}) \in C^{\perp_{\tau}}$ ,  $p, q \in \mathcal{R}$ , and  $m' = (m'_0, m'_1, \dots, m'_{n-1}) \in C$ . Then,  $\langle m', ps' + qs'' \rangle_{\tau} = \sum_{k=0}^{n-1} m'_k \tau(ps'_k + qs''_k) = \tau(p) \sum_{k=0}^{n-1} m'_k \tau(s'_k) + \tau(q) \sum_{k=0}^{n-1} m'_k \tau(s''_k) = \tau(p) \langle m', s' \rangle_{\tau} + \tau(q) \langle m', s'' \rangle_{\tau} = 0$ . Thus,  $ps' + qs'' \in C^{\perp_{\tau}}$ . So,  $C^{\perp_{\tau}}$  be an LC over  $\mathcal{R}$ . Now, consider  $v'' \in C$  &  $v' \in C^{\perp_{\tau}}$ . Then,  $v' \in C^{\perp_{\tau}}$  iff  $\langle v'', v' \rangle_{\tau} = 0$  that is  $\langle v'', \tau(v') \rangle_E = 0$  iff  $\tau(v') \in C^{\perp_E}$  iff  $v' \in \tau^{-1}(C^{\perp_E})$ , where  $\langle v'', \tau(v') \rangle_E$  is Euclidean inner product of  $v''$  and  $\tau(v')$ . Also, since  $\tau: \mathcal{R}^n \rightarrow \mathcal{R}^n$  is bijective mapping. So,  $|C^{\perp_E}| = |\tau^{-1}(C^{\perp_E})| = |C^{\perp_{\tau}}|$ . For  $\mathcal{R}$ ,  $|C||C^{\perp_E}| = |\mathcal{R}^n|$ . Finally, we get,  $|C||C^{\perp_{\tau}}| = |\mathcal{R}^n|$ .

**Definition 2:** Define a map,  $\gamma: \mathcal{R} \rightarrow \mathcal{R}$  by  $\theta'(a\varepsilon_1 + b\varepsilon_2 + c\varepsilon_3 + d\varepsilon_4 + e\varepsilon_5) = \varepsilon_1\varphi(a) + \varepsilon_2\varphi(b) + \varepsilon_3\varphi(c) + \varepsilon_4\varphi(d) + \varepsilon_5\varphi(e)$ , where  $a, b, c, d, e \in \mathcal{F}_{p^2}$ , and  $\varphi \in \text{Aut}(\mathcal{F}_{p^2})$  such that  $\varphi(b) = b^p$  for all  $b \in \mathcal{F}_{p^2}$ . Clearly,  $\theta' \in \text{Aut}(\mathcal{R})$ . The Hermitian inner product of  $s'', s'$  i.e.  $\langle s'', s' \rangle_{\mathcal{H}} = \sum_{k=0}^{n-1} s''_k \theta'(s'_k)$ , where  $s'' = (s''_0, s''_1, \dots, s''_{n-1})$  &  $s' = (s'_0, s'_1, \dots, s'_{n-1}) \in \mathcal{R}^n$ .

**Lemma 2:** Let  $C$  be an  $n$ - length linear code over  $\mathcal{R}$ . Then,  $\emptyset(C^{\perp_{\mathcal{H}}}) = \emptyset(C)^{\perp_{\mathcal{H}}}$ .

**Proof:** By lemma 1, we have  $|C||C^{\perp_{\mathcal{H}}}| = |\mathcal{R}^n|$ , and  $|\emptyset(C)||\emptyset(C)^{\perp_{\mathcal{H}}}| = |\mathcal{F}_{p^2}^{5n}|$ . Since  $\emptyset$  is bijective, so  $|C| = |\emptyset(C)|$  &  $|C^{\perp_{\mathcal{H}}}| = |\emptyset(C^{\perp_{\mathcal{H}}})|$ , gives  $|\emptyset(C^{\perp_{\mathcal{H}}})| = |\emptyset(C)^{\perp_{\mathcal{H}}}|$ . Suppose,  $s' = (s'_0, s'_1, \dots, s'_{n-1}) \in C$  &  $s'' = (s''_0, s''_1, \dots, s''_{n-1}) \in C^{\perp_{\mathcal{H}}}$ , where  $s'_k = a'_k\varepsilon_1 + b'_k\varepsilon_2 + c'_k\varepsilon_3 + d'_k\varepsilon_4 + e'_k\varepsilon_5$ , &  $s''_k = a''_k\varepsilon_1 + b''_k\varepsilon_2 +$

$c''_{\ell}\varepsilon_3 + d''_{\ell}\varepsilon_4 + e''_{\ell}\varepsilon_5$  for  $\ell \in \{0 \text{ to } (n-1)\}$ . Then,  $\langle s', s'' \rangle_{\mathcal{H}} = \sum_{\ell=0}^{n-1} s'_{\ell} \gamma(s''_{\ell})$   
 $= \varepsilon_1 \sum_{\ell=0}^{n-1} a'_{\ell} a''_{\ell} + \varepsilon_2 \sum_{\ell=0}^{n-1} b'_{\ell} b''_{\ell} + \varepsilon_3 \sum_{\ell=0}^{n-1} c'_{\ell} c''_{\ell} + \varepsilon_4 \sum_{\ell=0}^{n-1} d'_{\ell} d''_{\ell} +$   
 $\varepsilon_5 \sum_{\ell=0}^{n-1} e'_{\ell} e''_{\ell} = 0$ . Since,  $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5\}$  is the basis of  $\mathcal{R}$  over  $\mathcal{F}_{p^2}$ , so  
 $\sum_{\ell=0}^{n-1} a'_{\ell} a''_{\ell} = \sum_{\ell=0}^{n-1} b'_{\ell} b''_{\ell} = \sum_{\ell=0}^{n-1} c'_{\ell} c''_{\ell} = \sum_{\ell=0}^{n-1} d'_{\ell} d''_{\ell} = \sum_{\ell=0}^{n-1} e'_{\ell} e''_{\ell} =$   
 $0$  (eq.1). Consider,  $\langle \emptyset(s'), \emptyset(s'') \rangle_{\mathcal{H}} = \sum_{\ell=0}^{(n-1)} a'_{\ell} a''_{\ell} + \sum_{\ell=0}^{(n-1)} (b'_{\ell} + c'_{\ell} +$   
 $d'_{\ell} + e'_{\ell})(b''_{\ell} + c''_{\ell} + d''_{\ell} + e''_{\ell}) + \sum_{\ell=0}^{(n-1)} (b'_{\ell} + c'_{\ell} - d'_{\ell} - e'_{\ell})(b''_{\ell} + c''_{\ell} -$   
 $d''_{\ell} - e''_{\ell}) + \sum_{\ell=0}^{(n-1)} (b'_{\ell} - c'_{\ell} + d'_{\ell} - e'_{\ell})(b''_{\ell} - c''_{\ell} + d''_{\ell} - e''_{\ell}) +$   
 $\sum_{\ell=0}^{(n-1)} (b'_{\ell} - c'_{\ell} - d'_{\ell} + e'_{\ell})(b''_{\ell} - c''_{\ell} - d''_{\ell} + e''_{\ell}) = \sum_{\ell=0}^{(n-1)} a'_{\ell} a''_{\ell} +$   
 $4(\sum_{\ell=0}^{(n-1)} b'_{\ell} b''_{\ell} + \sum_{\ell=0}^{(n-1)} c'_{\ell} c''_{\ell} + \sum_{\ell=0}^{(n-1)} d'_{\ell} d''_{\ell} + \sum_{\ell=0}^{(n-1)} e'_{\ell} e''_{\ell}) = 0$   
 (using eq. (1)). Since  $\emptyset(s') \in \emptyset(C)$ , so  $\emptyset(s'') \in \emptyset(C)^{\perp_{\mathcal{H}}}$ . Hence,  $\emptyset(C^{\perp_{\mathcal{H}}}) \subseteq$   
 $\emptyset(C)^{\perp_{\mathcal{H}}}$ . Also, since  $|\emptyset(C^{\perp_{\mathcal{H}}})| = |\emptyset(C)^{\perp_{\mathcal{H}}}|$  so,  $\emptyset(C^{\perp_{\mathcal{H}}}) = \emptyset(C)^{\perp_{\mathcal{H}}}$ .  $\square$

To investigate the units of the ring for providing a better outline of the algebraic structure of the considered ring.

**Lemma 3:** Suppose  $Y = \sum_{i=1}^5 \varepsilon_i Y_i \in \mathcal{R}$ . Then,  $Y$  is a unit in  $\mathcal{R}$  iff  $Y_i \in \mathcal{F}_{p^2}^*$  for all  $i \in \{1 \text{ to } 5\}$ .

**Proof:** Here,  $Y \in \mathcal{R}$  may be written as  $Y = J_1 + uJ_2 + u^2J_3 + vJ_4 + v^2J_5 =$   
 $\varepsilon_1(J_1 + \omega J_2 + \omega^2J_3) + \varepsilon_2(J_1 - \omega J_2 + \omega^2J_3) + \varepsilon_3(J_1 + \omega J_4 + \omega^2J_5) + \varepsilon_4(J_1 -$   
 $\omega J_4 + \omega^2J_5) + \varepsilon_5J_1 = \sum_{i=1}^5 \varepsilon_i Y_i$ , where  $J_i \in \mathcal{F}_{p^2} \forall i \in \{1 \text{ to } 5\}$ . Suppose  
 $Y \in \mathcal{R}$  be a unit, then  $\exists Y' = \sum_{i=1}^5 \varepsilon_i Y'_i \in \mathcal{R}$  such that  $YY' = 1 = \sum_{i=1}^5 \varepsilon_i$ . So,  
 $\sum_{i=1}^5 \varepsilon_i = (\sum_{i=1}^5 \varepsilon_i Y_i)(\sum_{i=1}^5 \varepsilon_i Y'_i) = \sum_{i=1}^5 \varepsilon_i Y_i Y'_i \Rightarrow \sum_{i=1}^5 \varepsilon_i (Y_i Y'_i - 1) = 0$ .  
 Since  $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5\}$  is the basis of  $\mathcal{R}$  over  $\mathcal{F}_{p^2}$ . So,  $Y_i Y'_i = 1 \forall i$ . Therefore,  
 $Y_i$  are units  $\forall i \in \{1 \text{ to } 5\}$ . Suppose that  $Y_i$  are units for all  $i \in \{1 \text{ to } 5\}$ , then  
 $\exists Y'_i \in \mathcal{F}_{p^2}$  such that  $Y_i Y'_i = 1$ . Let  $Y' = \sum_{i=1}^5 \varepsilon_i Y'_i$ , then  $YY' = \sum_{i=1}^5 \varepsilon_i Y_i Y'_i =$   
 $\sum_{i=1}^5 \varepsilon_i = 1$ . Hence,  $Y \in \mathcal{R}$  be a unit.

#### 4. Novel Q ECC's through CCc's over $\mathcal{R}$

Here, we establish some important results to construct Q ECC's by Hermitian dual containing CCc's.

**Definition 3:** A Q ECC,  $[[n, K', d'']]_q$  is defined as “a  $q^{K'}$ -dimensional subspace” of “a  $q^n$ -dimensional complex Hilbert space,”  $\underbrace{\mathbb{C}^q \otimes \mathbb{C}^q \otimes \dots \otimes \mathbb{C}^q}_{n \text{ times}}$ ,

where  $q$  is a prime power and  $d''$  is the minimum Hamming distance of Q ECC. A Q ECC can correct up to  $\lfloor (d'' - 1)/2 \rfloor$  errors. Q ECC is represented by  $[[n, k, D]]_p$ , where  $n, k, D$  are respectively its length, dimension, and minimum Hamming distance over  $\mathcal{F}_p$ . Q ECC's parameters satisfy Quantum singleton bound (Qsb) =  $n - k + 2 \geq 2D$ .

**Theorem 1:** *The necessary and sufficient condition for an LC,  $C = \sum_{i=1}^5 \varepsilon_i C_i$  to be a  $Y-CCc$  with length  $n$  over  $\mathcal{R}$  is that  $C_i$  is a  $Y_i-CCc$  with length  $n$  over  $\mathcal{F}_{p^2}$ .*

**Proof:** Let  $C = \sum_{i=1}^5 \varepsilon_i C_i$  be  $n$ -length,  $Y-CCc$  over  $\mathcal{R}$  &  $\mu = (\mu_0, \mu_1, \dots, \mu_{n-1}) \in C$ , where  $\mu_{\ell} = \varepsilon_1 \mu_{1\ell} + \varepsilon_2 \mu_{2\ell} + \varepsilon_3 \mu_{3\ell} + \varepsilon_4 \mu_{4\ell} + \varepsilon_5 \mu_{5\ell}$ ,  $\mu_{i\ell} \in \mathcal{F}_{p^2}$ . Clearly,  $(\mu_{i0}, \mu_{i1}, \dots, \mu_{i(n-1)}) \in C_i \forall i \in \{1 \text{ to } 5\}$ ,  $\ell \in \{0 \text{ to } (n-1)\}$ . Since  $C$  is  $Y-CCc$  with length  $n$  over  $\mathcal{R}$ , we have  $(Y\mu_{(n-1)}, \mu_0, \dots, \mu_{(n-2)}) \in C$ . Furthermore,  $Y = \sum_{i=1}^5 \varepsilon_i Y_i \Rightarrow \varepsilon_{\ell} Y = \varepsilon_{\ell} Y_{\ell}$  for all  $\ell$ . Thus,  $(Y\mu_{(n-1)}, \mu_0, \dots, \mu_{(n-2)}) = (Y(\varepsilon_1 \mu_{1(n-1)} + \varepsilon_2 \mu_{2(n-1)} + \dots + \varepsilon_5 \mu_{5(n-1)}), (\varepsilon_1 \mu_{10} + \varepsilon_2 \mu_{20} + \varepsilon_3 \mu_{30} + \varepsilon_4 \mu_{40} + \varepsilon_5 \mu_{50}), \dots, (\varepsilon_1 \mu_{1(n-2)} + \varepsilon_2 \mu_{2(n-2)} + \dots + \varepsilon_5 \mu_{5(n-2)})) = \sum_{i=1}^5 \varepsilon_i (Y_i \mu_{i(n-1)}, \mu_{i0}, \dots, \mu_{i(n-2)}) \in C$ , we have  $(Y_i \mu_{i(n-1)}, \mu_{i0}, \dots, \mu_{i(n-2)}) \in C_i$ . Hence,  $C_i$  is a  $Y_i-CCc$  with length  $n$  over  $\mathcal{F}_{p^2}$  for all  $i \in \{1 \text{ to } 5\}$ . The reverse aspect can be demonstrated similarly.

The below findings are employed to find the generators of  $Y-CCc$  over  $\mathcal{R}$ .

**Theorem 2:** *Consider an  $n$ -length,  $Y-CCc$ ,  $C = \sum_{i=1}^5 \varepsilon_i C_i$  over  $\mathcal{R}$ . Then,  $C = \langle \varepsilon_1 g_1(y), \varepsilon_2 g_2(y), \varepsilon_3 g_3(y), \varepsilon_4 g_4(y), \varepsilon_5 g_5(y) \rangle = \langle g(y) \rangle$  and  $g(y) | (y^n - Y)$ , where  $g(y) = \varepsilon_1 g_1(y) + \varepsilon_2 g_2(y) + \dots + \varepsilon_5 g_5(y)$ ,  $g_i(y)$  is a generator polynomial of  $Y_i-CCc$ ,  $C_i$  over  $\mathcal{F}_{p^2}$ .*

**Proof:** Let  $C = \{f(y) | f(y) = \sum_{i=1}^5 \varepsilon_i f_i(y), f_i(y) \in C_i; i = \{1 \text{ to } 5\}\}$ . Then,  $C \subseteq \langle \varepsilon_1 g_1(y), \varepsilon_2 g_2(y), \dots, \varepsilon_5 g_5(y) \rangle$ . Consider,  $\sum_{i=1}^5 \varepsilon_i g_i(y) h_i(y) \in \langle \varepsilon_1 g_1(y), \varepsilon_2 g_2(y), \dots, \varepsilon_5 g_5(y) \rangle$  such that  $h_i(y) \in \frac{\mathcal{R}[y]}{\langle y^n - Y \rangle}$  and hence  $\varepsilon_i h_i(y) = \varepsilon_i f'_i(y)$ , where  $f'_i(y) \in \frac{\mathcal{F}_{p^2}[y]}{\langle y^n - Y_i \rangle}$  for  $i = 1 \text{ to } 5$ . So,  $\sum_{i=1}^5 \varepsilon_i g_i(y) h_i(y) = \sum_{i=1}^5 \varepsilon_i g_i(y) f'_i(y) \in C$ . Thus,  $\langle \varepsilon_1 g_1(y), \varepsilon_2 g_2(y), \dots, \varepsilon_5 g_5(y) \rangle \subseteq C \Rightarrow C = \langle \varepsilon_1 g_1(y), \varepsilon_2 g_2(y), \dots, \varepsilon_5 g_5(y) \rangle$ . Another part can be proved as follows: Suppose,  $g(y) = \varepsilon_1 g_1(y) + \varepsilon_2 g_2(y) + \dots + \varepsilon_5 g_5(y)$ . Then,  $\langle g(y) \rangle \subseteq C = \langle \varepsilon_1 g_1(y), \varepsilon_2 g_2(y), \dots, \varepsilon_5 g_5(y) \rangle$ . Also,  $\varepsilon_i g_i(y) = \varepsilon_i g(y)$  implies  $\langle \varepsilon_1 g_1(y), \varepsilon_2 g_2(y), \dots, \varepsilon_5 g_5(y) \rangle = C \subseteq \langle g(y) \rangle$ . The expression,  $g_i(y) | (y^n - Y_i) \Rightarrow g_i(y) h'_i(y) = (y^n - Y_i) \Rightarrow g_i(y) h'_i(y) \varepsilon_i = (y^n - Y_i) \varepsilon_i$  for  $h'_i(y) \in \frac{\mathcal{F}_{p^2}[y]}{\langle y^n - Y_i \rangle}$ , where  $i = 1 \text{ to } 5$ . Now,  $(y^n - Y) = y^n - (\sum_{i=1}^5 \varepsilon_i Y_i) = \sum_{i=1}^5 (y^n - Y_i) \varepsilon_i = \sum_{i=1}^5 g_i(y) h'_i(y) \varepsilon_i = (\sum_{i=1}^5 \varepsilon_i g_i(y)) \sum_{i=1}^5 h'_i(y) \varepsilon_i$ . Hence,  $g(y) | (y^n - Y)$ .

**Theorem 3:** [19] *Suppose  $C$  is an  $\mathcal{F}_{p^2}$ -linear code with parameters  $[n, \mathbb{K}, D]_{p^2}$ . If  $C^{\perp_H} \subseteq C$ , then  $\exists$  a  $QEC$  having parameters  $[[n, 5\mathbb{K} - n, D]]_p$ .*

**Lemma 4:** Suppose  $C_i$  be a  $Y_i - CCc$  with length  $n$  and the defining set  $\mathcal{W}_i$  over  $\mathcal{F}_{p^2}$ , where  $Y_i \in \mathcal{F}_{p^2}^*$  is the primitive  $t_i - th$  root of unity such that  $t_i | (p+1)$ . Then,  $C_i^{\perp_{\mathcal{H}}} \subseteq C_i \Leftrightarrow \mathcal{W}_i \cap \mathcal{W}_i^{-p}$  is the empty set, where  $\mathcal{W}_i^{-p} = \{-p w \pmod{n t} | w \in \mathcal{W}_i\}$ .

**Theorem 4:** The necessary and sufficient condition for  $C^{\perp_{\mathcal{H}}} \subseteq C$  to be  $C_i^{\perp_{\mathcal{H}}} \subseteq C_i$ , where  $C = \bigoplus_{i=1}^5 \varepsilon_i C_i$  be a  $Y - CCc$  with length  $n$  over  $\mathcal{R}$ .

**Proof:** Firstly, suppose  $C_i^{\perp_{\mathcal{H}}} \subseteq C_i$ , then  $\varepsilon_i C_i^{\perp_{\mathcal{H}}} \subseteq \varepsilon_i C_i \Rightarrow \bigoplus_{i=1}^5 \varepsilon_i C_i^{\perp_{\mathcal{H}}} \subseteq \bigoplus_{i=1}^5 \varepsilon_i C_i$ . Therefore,  $C^{\perp_{\mathcal{H}}} \subseteq C$ . Similarly,  $C^{\perp_{\mathcal{H}}} \subseteq C \Rightarrow C_i^{\perp_{\mathcal{H}}} \subseteq C_i, i = 1$  to  $5$ .

**Theorem 5:** Consider an  $n - length, Y - CCc, C = \bigoplus_{i=1}^5 \varepsilon_i C_i$  over  $\mathcal{R}$ . If  $C^{\perp_{\mathcal{H}}} \subseteq C$ , then  $\exists$  a QECc,  $[[5n, 2k - 5n, D_{\mathcal{H}}]]_p$ .

**Proof:** Let  $u' \in \emptyset(C^{\perp_{\mathcal{H}}}) \subseteq \emptyset(C)^{\perp_{\mathcal{H}}}$ , then  $\exists u'' \in C^{\perp_{\mathcal{H}}}$  such that  $u' = \emptyset(u'')$ . Since,  $C^{\perp_{\mathcal{H}}} \subseteq C$ , then  $u'' \in C$  &  $u' = \emptyset(u'') \in \emptyset(C)$ , which gives  $\emptyset(C)^{\perp_{\mathcal{H}}} \subseteq \emptyset(C)$ . Therefore,  $\emptyset(C)$  be a Hermitian dual containing LC,  $[5n, k, D_{\mathcal{H}}]_{p^2}$  over  $\mathcal{F}_{p^2}$ . Hence, by theorem 3,  $\exists$  QECc with parameters  $[[5n, 2k - 5n, D_{\mathcal{H}}]]_p$ .

## 5. Application of CCc to construct novel Quantum codes

Using the above-discussed results, we explain 3 different examples (Ex.) for 3 different scenarios to get some novel Qecc. In Ex. 1, the least natural number that satisfies  $p^{2^m} \equiv 1 \pmod{nt}$  is 1 for each  $C_j$  that is, both splitting and base fields are the same. In Ex. 2<sup>nd</sup>,  $m$  is 1 for  $C_j; j = 1, 5$  and  $m$  is not 1 for  $C_j, j = 2, 3, 4$ , that is, the splitting field and base field are not same for ring  $\mathcal{R}$ . In Ex. 3,  $m$  is not 1 for each  $C_j$  that is, the splitting field and base field are not same for ring  $\mathcal{R}$ .

**Example 1:** Suppose  $\mathcal{F}_{11^2}^* = \langle \omega \rangle$  that is  $\omega^{120} = 1$ , then  $\mathcal{R} = \mathcal{F}_{11^2} + u\mathcal{F}_{11^2} + u^2\mathcal{F}_{11^2} + v\mathcal{F}_{11^2} + v^2\mathcal{F}_{11^2}$  with  $u^3 = \omega^2 u$  &  $v^3 = \omega^2 v$ . Let  $C$  be  $Y - CCc$  such that  $Y = -1 + (2u^2 + v^2)\omega^{118} + v\omega^{119}$ , then  $(Y_1, Y_2, \dots, Y_5) = (1, 1, 1, -1, -1)$ . Here,  $y^{10} - 1 = (y+1)(y+2) \dots (y+10)$ . As  $Y_1 = Y_2 = Y_3 = 1$  are 1<sup>st</sup> primitive root of unity, so  $t = 1$ . Smallest natural no  $m$  that satisfies  $p^{2^m} \equiv 1 \pmod{nt}$  that is  $121^m \equiv 1 \pmod{10}$  is 1. Let  $\beta_j = 2$  such that  $\beta_j^{10} = 1 \Rightarrow \beta_j$  is 10<sup>th</sup> primitive root of unity for  $j = 1, 2, 3$ . The roots of  $y^{10} - 1$  are  $\beta_j^{(1+\vartheta)}$ ,  $\vartheta = 0$  to  $9$ , that is, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 in  $\mathcal{F}_{11^2}$ . Therefore,  $\mathcal{M} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \pmod{10}$ . Suppose,  $C_j = \langle g_j(y) \rangle$  is a  $Y_j - CCc$ , where:  $g_1(y) = (y+2)(y+3)$ , the defining set of  $C_1$  is  $\mathcal{W}_1 = \{6, 3\}$ , and  $\mathcal{W}_1^{-11} = \{4, 10\}$ ;  $g_2(y) = (y+5)$ , the defining set of  $C_2$  is  $\mathcal{W}_2 = \{9\}$ , and  $\mathcal{W}_2^{-11} = \{1\}$ ;  $g_3(y) = (y+7)$ , the defining set of  $C_3$  is  $\mathcal{W}_3 = \{2\}$ , &  $\mathcal{W}_3^{-11} = \{8\}$ . Here,  $\mathcal{W}_j^{-11} = \{-11w \pmod{10} | w \in \mathcal{W}_j\}$  and  $\mathcal{W}_j \cap \mathcal{W}_j^{-p} = \emptyset \Rightarrow C_j^{\perp_{\mathcal{H}}} \subseteq C_j$  for all  $j = 1, 2, 3$ . Here,  $y^{10} + 1 = (y +$

$\omega^6)(y + \omega^{18})(y + \omega^{30})(y + \omega^{42})(y + \omega^{54})(y - \omega^6)(y - \omega^{18})(y - \omega^{30})(y - \omega^{42})(y - \omega^{54})$ . As  $Y_4 = Y_5 = -1$  are 2<sup>nd</sup> primitive root of unity, so  $t = 2$ . Smallest natural no  $m$  that satisfies  $p^{2m} \equiv 1 \pmod{n t}$  that is  $121^m \equiv 1 \pmod{20}$  is 1. Let  $\beta_j = \omega^6$  such that  $\beta_j^{10} = -1$  that is  $\beta_j$  is the 20<sup>th</sup> primitive root of unity for  $j = 4, 5$ . The roots of  $y^{10} + 1$  are  $\beta_j^{(1+2\vartheta)}$ ,  $\vartheta = 0$  to 9 that is, the roots are  $\omega^6, \omega^{18}, \dots, \omega^{114}$  in  $\mathcal{F}_{11^2}$ . Therefore,  $\mathcal{M} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\} \pmod{20}$ .

Suppose,  $C_j = \langle g_j(y) \rangle$  be  $Y_j - \text{CCc}$ , where  $g_4(y) = (y + \omega^6)(y + \omega^{18})$ , defining set of  $C_4$  is  $\mathcal{W}_4 = \{11, 13\}$ ,  $\mathcal{W}_4^{-11} = \{19, 17\}$ ,  $g_5(y) = (y + \omega^{18})$ , defining set of  $C_5$  is  $\mathcal{W}_5 = \{13\}$ ,  $\mathcal{W}_5^{-11} = \{17\}$ . Here,  $\mathcal{W}_j^{-11} = \{-11w \pmod{20} | w \in \mathcal{W}_j\}$ , and  $\mathcal{W}_j \cap \mathcal{W}_j^{-11} = \emptyset \Rightarrow C_j^{\perp_{\mathcal{H}}} \subseteq C_j$  for all  $j = 4, 5$ . Hence, by theorem 4,  $C^{\perp_{\mathcal{H}}} \subseteq C$ . So,  $\emptyset(C)$  be an LC having parameters  $[50, 43, 4]_{11^2}$  over  $\mathcal{F}_{11^2}$ , and by theorem 5,  $\exists$  a Q ECC having parameters  $[[50, 36, 4]]_{11}$ .

**Example 2:** Suppose  $\mathcal{F}_{3^2}^* = \langle \omega \rangle$  that is  $\omega^8 = 1$ , then  $\mathcal{R} = \mathcal{F}_{3^2} + u\mathcal{F}_{3^2} + u^2\mathcal{F}_{3^2} + v\mathcal{F}_{3^2} + v^2\mathcal{F}_{3^2}$  with  $u^3 = \omega^2 u$  and  $v^3 = \omega^2 v$ . Let  $C$  be  $Y - \text{CCc}$  such that  $Y = 1 + u\omega^7 - (u^2 + 2v^2)\omega^6$ , then  $(Y_1, Y_2, \dots, Y_5) = (1, -1, -1, -1, 1)$ . Here,  $y^8 - 1 = (y + 1)(y + \omega)(y + \omega^2)(y + \omega^3)(y + 2)(y + \omega^5)(y + \omega^6)(y + \omega^7)$ . As  $Y_1 = Y_5 = 1$  are 1<sup>st</sup> primitive root of unity, so  $t = 1$ . Smallest natural no  $m$  that satisfies  $p^{2m} \equiv 1 \pmod{n t}$  that is  $9^m \equiv 1 \pmod{8}$  is 1. Let  $\beta_j = \omega$  such that  $\beta_j^8 = 1$  that is  $\beta_j$  is the 8<sup>th</sup> primitive root of unity for  $j = 1, 5$ . The roots of  $y^8 - 1$  are  $\beta_j^{(1+\vartheta)}$ ,  $\vartheta = 0$  to 7, that is, the roots are  $\omega, \omega^2, \dots, \omega^7, 1$ . Therefore,  $\mathcal{M} = \{1, 2, 3, 4, 5, 6, 7, 8\} \pmod{8}$ .

Suppose,  $C_j = \langle g_j(y) \rangle$  is a  $Y_j - \text{CCc}$ , where  $g_1(y) = (y + \omega)(y + \omega^3)$ , the defining set of  $C_1$  is  $\mathcal{W}_1 = \{5, 7\}$ , &  $\mathcal{W}_1^{-3} = \{1, 3\}$ ,  $g_5(y) = (y + \omega^7)(y + \omega^5)$ , the defining set of  $C_5$  is  $\mathcal{W}_5 = \{3, 1\}$ , &  $\mathcal{W}_5^{-3} = \{7, 5\}$ . Here,  $\mathcal{W}_j^{-3} = \{-3w \pmod{8} | w \in \mathcal{W}_j\}$  and,  $\mathcal{W}_j \cap \mathcal{W}_j^{-3} = \emptyset \Rightarrow C_j^{\perp_{\mathcal{H}}} \subseteq C_j$  for all  $j = 1, 5$ . Here,  $y^8 + 1 = (y^2 + \omega)(y^2 + \omega^3)(y^2 + \omega^5)(y^2 + \omega^7)$ . As  $Y_2 = Y_3 = Y_4 = -1$  are 2<sup>nd</sup> primitive root of unity, so  $t = 2$ . Smallest natural no  $m$  that satisfies  $p^{2m} \equiv 1 \pmod{n t}$  that is  $9^m \equiv 1 \pmod{16}$  is 2. So,  $y^8 + 1$  splits in  $\mathcal{F}_{9^2}$ . Let  $\mathcal{F}_{9^2}^* = \langle \zeta \rangle$  that is  $\zeta^{80} = 1$  and  $\beta_j = \zeta^5$  such that  $\beta_j^8 = -1 \Rightarrow \beta_j$  is 16<sup>th</sup> primitive root of unity for  $j = 2, 3, 4$ . The roots of  $y^8 + 1$  are  $\beta_j^{(1+2\vartheta)}$  that is  $\zeta^{(5+10\vartheta)}$ ,  $\vartheta = 0$  to 7. Note:  $\omega = \zeta^{10}$ . Therefore,  $\mathcal{M} = \{1, 3, 5, 7, 9, 11, 13, 15\} \pmod{16}$ . Suppose,  $C_j = \langle g_j(y) \rangle$  is a  $Y_j - \text{CCc}$  over  $\mathcal{F}_{3^2}$ , where  $g_2(y) = (y^2 + \omega)$  with roots in  $\mathcal{F}_{9^2}$  are  $\zeta^{65}, \zeta^{75}, \zeta^{25}, \zeta^{35}$ , the defining set of  $C_2$  is  $\mathcal{W}_2 = \{5, 7, 13, 15\}$ , &  $\mathcal{W}_2^{-3} = \{1, 11, 9, 3\}$ ;  $g_3(y) = (y^2 + \omega^3)$  with roots in  $\mathcal{F}_{9^2}$  are  $\zeta^{25}, \zeta^{35}$ ; the defining set of  $C_3$  is  $\mathcal{W}_3 = \{13, 15\}$ , &  $\mathcal{W}_3^{-3} = \{9, 3\}$ ;  $g_4(y) = (y^2 + \omega^5)$  with roots in  $\mathcal{F}_{9^2}$  are  $\zeta^{45}, \zeta^5$ , the defining set of  $C_4$  is  $\mathcal{W}_4 = \{1, 9\}$ ,  $\mathcal{W}_4^{-3} = \{13, 5\}$ . Here,  $\mathcal{W}_j^{-3} = \{-3w \pmod{16} | w \in \mathcal{W}_j\}$ , and

Table 1  
QECC's by CCc's over  $\mathcal{R}$

| $n$ | $\gamma_1, \gamma_2, \dots, \gamma_5$ | $\beta_1, \beta_2, \dots, \beta_5$                                              | $\theta_1(\gamma)$                             | $\theta_2(\gamma)$                 | $\theta_3(\gamma)$                | $\theta_4(\gamma)$                   | $\theta_5(\gamma)$                             | $\emptyset(C)$         | QECC's                |
|-----|---------------------------------------|---------------------------------------------------------------------------------|------------------------------------------------|------------------------------------|-----------------------------------|--------------------------------------|------------------------------------------------|------------------------|-----------------------|
| 12  | 1, 1, 1, -1, -1                       | $2, 2, 2, \omega^6, \omega^6$                                                   | 168                                            | 1(12)84                            | 119                               | $1\omega^7 \cdot 1\omega^{21}$       | $1\omega^7 \cdot 1\omega^{35} \cdot 1\omega^2$ | $[60, 48, 4]_{13^2}$   | $[[60, 36, 4]]_{13}$  |
| 12  | 1, 1, 1, -1, -1                       | $2, 2, 2, \omega^6, \omega^6$                                                   | 168                                            | 119                                | 16                                | $1\omega^{35} \cdot 1\omega^7$       | $1\omega^7 \cdot 1\omega^{21}$                 | $[60, 51, 3]_{13^2}$   | $[[60, 42, 3]]_{13}$  |
| 16  | 1, 1, -1, -1, -1                      | $3, 3, \omega^9, \omega^9, \omega^9$                                            | 18(15)                                         | 1(10)4                             | $1\omega^9 \cdot 1\omega^{27}$    | $1\omega^{153} \cdot 1\omega^{189}$  | $1\omega^{171} \cdot 1\omega^{189}$            | $[80, 70, 4]_{17^2}$   | $[[80, 60, 4]]_{17}$  |
| 15  | 1, 1, 1, 1, -1                        | $\omega^8, \omega^8, \omega^8, \omega^8, \omega^4$                              | $1\omega^4 \cdot 1\omega^{28} \cdot 17$        | $1\omega^{52} \cdot 1\omega^{44}$  | $1\omega^{76} \cdot 1\omega^{68}$ | $1\omega^{28} \cdot 1\omega^4$       | $1\omega^8 \cdot 1\omega^{64}$                 | $[75, 64, 4]_{11^2}$   | $[[75, 53, 4]]_{11}$  |
| 39  | 1, 1, 1, -1, -1                       | $\zeta^{16}, \zeta^{16}, \zeta^{16}, \zeta^8, \zeta^8$                          | $1\omega^2 \omega^8$                           | $1\omega^3 \omega^{16}$            | $1\omega^7 \omega^{16}$           | $1\omega \omega^{16}$                | $1\omega^{15} \omega^{16}$                     | $[195, 185, 3]_{5^2}$  | $[[195, 175, 3]]_5$   |
| 24  | 1, 1, 1, 1, -1                        | $\omega^2, \omega^2, \omega^2, \omega^2, \omega$                                | $1\omega^2 \cdot 1\omega^4 \cdot 1\omega^{14}$ | $1\omega^2 \cdot 1\omega^4$        | $1\omega^{20}$                    | $1\omega^{26}$                       | $1\omega \cdot 1\omega^3 \cdot 1\omega^5$      | $[120, 110, 3]_{7^2}$  | $[[120, 100, 3]]_7$   |
| 24  | 1, 1, 1, -1, -1                       | $\omega, \omega, \omega, \zeta^{13}, \zeta^{13}$                                | $1\omega^7 \cdot 1\omega^2$                    | $1\omega^1 \cdot 1\omega^{13}$     | $1\omega^{21}$                    | $1\omega^{17}$                       | $10\omega^{19}$                                | $[120, 111, 3]_{5^2}$  | $[[120, 102, 3]]_5$   |
| 8   | 1, 1, 1, -1, -1                       | $\omega^{45}, \omega^{45}, \omega^{45}, \omega^{45}, \omega^{45}, \zeta^{8145}$ | $1\omega^{45}$                                 | $1\omega^{135} \cdot 1\omega^{45}$ | $1\omega^{225}$                   | $10\omega^{45}$                      | $10\omega^{135} \cdot 10\omega^{45}$           | $[40, 30, 4]_{19^2}$   | $[[40, 20, 4]]_{19}$  |
| 8   | 1, 1, -1, -1, -1                      | $\omega^{45}, \omega^{45}, \zeta^{8145}, \zeta^{8145}, \zeta^{8145}$            | $1\omega^{135}$                                | $1\omega^{135} \cdot 1\omega^{45}$ | $10\omega^{225}$                  | $10\omega^{135}$                     | $10\omega^{45}$                                | $[40, 31, 4]_{19^2}$   | $[[40, 22, 4]]_{19}$  |
| 24  | 1, 1, -1, -1, -1                      | $\omega^{15}, \omega^{15}, \zeta^{2715}, \zeta^{2715}, \zeta^{2715}$            | $1\omega^{15}$                                 | $1\omega^{15} \cdot 1\omega^{30}$  | $10\omega^{15}$                   | $10\omega^{75} \cdot 10\omega^{105}$ | $10\omega^{15} \cdot 10\omega^{45}$            | $[120, 107, 4]_{19^2}$ | $[[120, 94, 4]]_{19}$ |

$\mathcal{W}_j \cap \mathcal{W}_j^{-3} = \phi \Rightarrow C_j^{\perp \mathcal{H}} \subseteq C_j$  for all  $j = 2, 3, 4$ . Hence, by theorem 4,  $C^{\perp \mathcal{H}} \subseteq C$ . So,  $\emptyset(C)$  be an LC,  $[40, 30, 4]_{3^2}$  over  $\mathcal{F}_{3^2}$  and by theorem 5,  $\exists$  a QECC having parameter  $[[40, 20, 4]]_3$ .

**Example 3:** Suppose  $\mathcal{F}_{5^2}^* = \langle \omega \rangle$  that is  $\omega^{24} = 1$  then,  $\mathcal{R} = \mathcal{F}_{5^2} + u\mathcal{F}_{5^2} + u^2\mathcal{F}_{5^2} + v\mathcal{F}_{5^2} + v^2\mathcal{F}_{5^2}$  with  $u^3 = \omega^2u$  and  $v^3 = \omega^2v$ . Let  $C$  be  $Y - \text{CCc}$  such that  $Y = -1 + 2u^2\omega^{22}$ , then  $(Y_1, Y_2, \dots, Y_5) = (1, 1, -1, -1, -1)$ . Here,  $y^{39} - 1 = (y + \omega^4)(y + 4)(y + \omega^{20})(y^2 + \omega y + 1)(y^2 + \omega^2 y + 1)(y^2 + \omega^2 y + \omega^8)(y^2 + \omega^3 y + \omega^{16})(y^2 + \omega^5 y + 1)(y^2 + \omega^7 y + \omega^{16})(y^2 + \omega^9 y + \omega^{16})(y^2 + \omega^{10} y + 1)(y^2 + \omega^{10} y + \omega^{16})(y^2 + \omega^{11} y + \omega^8)(y^2 + \omega^{13} y + \omega^{16})(y^2 + \omega^{15} y + \omega^8)(y^2 + \omega^{17} y + \omega^8)(y^2 + 3y + \omega^8)(y^2 + 3y + \omega^{16})(y^2 + \omega^{19} y + 1)(y^2 + \omega^{21} y + \omega^8)(y^2 + \omega^{23} y + 1)$ . As  $Y_1 = Y_2 = 1$  are 1<sup>st</sup> primitive root of unity, so  $t = 1$ . Smallest natural no  $m$  that satisfies  $p^{2m} \equiv 1 \pmod{nt}$  that is  $25^m \equiv 1 \pmod{39}$  is 2. So,  $y^{39} - 1$  splits in  $\mathcal{F}_{25^2}$ . Let  $\mathcal{F}_{25^2}^* = \langle \varsigma \rangle$  that is  $\varsigma^{624} = 1$  and  $\beta_j = \varsigma^{16}$  such that  $\beta_j^{39} = 1 \Rightarrow \beta_j$  is 39<sup>th</sup> primitive root of unity for  $j = 1, 2$ . The roots of  $y^{39} - 1$  are  $\beta_j^{(1+\vartheta)}$  that is  $\varsigma^{(16+16\vartheta)}$ ,  $\vartheta = 0$  to 38. (Note:  $\omega = \varsigma^{26}$ ). Therefore,  $\mathcal{M} = \{1, 2, \dots, 39\}x \pmod{16}$ . Suppose,  $C_j = \langle g_j(y) \rangle$  is a  $Y_j - \text{CCc}$  over  $\mathcal{F}_{5^2}$ , where  $g_1(y) = (y^2 + \omega^3 y + \omega^{16})$  with roots in  $\mathcal{F}_{25^2}$  are  $\varsigma^{448}, \varsigma^{592}$ , the defining set of  $C_1$  is  $\mathcal{W}_1 = \{28, 37\}$ , &  $\mathcal{W}_1^{-5} = \{16, 10\}$ . Let  $g_2(y) = (y^2 + \omega^9 y + \omega^{16})$  with roots in  $\mathcal{F}_{25^2}$  are  $\varsigma^{352}, \varsigma^{64}$ , the defining set of  $C_2$  is  $\mathcal{W}_2 = \{22, 4\}$ , &  $\mathcal{W}_2^{-5} = \{7, 19\}$ . Here,  $\mathcal{W}_j^{-5} = \{-5\ell \pmod{39} | \ell \in \mathcal{W}_j\}$ , and  $\mathcal{W}_j \cap \mathcal{W}_j^{-5} = \phi \Rightarrow C_j^{\perp \mathcal{H}} \subseteq C_j$  for all  $j = 1, 2$ . Here,  $y^{39} + 1 = (y + 1)(y + \omega^8)(y + \omega^{16})(y^2 + \omega y + \omega^{16})(y^2 + \omega^3 y + \omega^8)(y^2 + \omega^5 y + \omega^8)(y^2 + 2y + \omega^8)(y^2 + 2y + \omega^{16})(y^2 + \omega^7 y + 1)(y^2 + \omega^9 y + \omega^8)(y^2 + \omega^{11} y + 1)(y^2 + \omega^{13} y + 1)(y^2 + \omega^{14} y + 1)(y^2 + \omega^{14} y + \omega^8)(y^2 + \omega^{15} y + \omega^{16})(y^2 + \omega^{17} y + 1)(y^2 + \omega^{19} y + \omega^{16})(y^2 + \omega^{21} y + \omega^{16})(y^2 + \omega^{22} y + 1)(y^2 + \omega^{22} y + \omega^{16})(y^2 + \omega^{23} y + \omega^8)$ . As  $Y_3 = Y_4 = Y_5 = -1$  are 2nd primitive root of unity, so  $t = 2$ . Smallest natural no  $m$  that satisfies  $p^{2m} \equiv 1 \pmod{nt}$  that is  $25^m \equiv 1 \pmod{78}$  is 2. So,  $y^{39} + 1$  splits in  $\mathcal{F}_{25^2}$ . Let  $\mathcal{F}_{25^2}^* = \langle \varsigma \rangle$ , where  $\varsigma^{624} = 1$  &  $\beta_j = \varsigma^8$ , such that  $\beta_j^{39} = -1$ . That is  $\beta_j$  is 78<sup>th</sup> primitive root of unity for  $j = 3, 4, 5$ . The roots of  $y^{39} + 1$  are  $\beta_j^{(1+2\vartheta)}$  that is  $\varsigma^{(8+16\vartheta)}$ ,  $\vartheta = 0$  to 38. Note:  $\omega = \varsigma^{26}$ . Therefore,  $\mathcal{M} = \{1, 3, \dots, 77\} \pmod{78}$ . Suppose,  $C_j = \langle g_j(y) \rangle$  is a  $Y_j - \text{CCc}$  over  $\mathcal{F}_{25^2}$ , where  $g_3(y) = y^2 + \omega^{21} y + \omega^{16}$  with roots in  $\mathcal{F}_{25^2}$  are  $\varsigma^{376}, \varsigma^{40}$ , the defining set of  $C_3$  is  $\mathcal{W}_3 = \{47, 5\}$ , &  $\mathcal{W}_2^{-3} = \{77, 53\}$ ;  $g_4(y) = y^2 + \omega^3 y + \omega^8$  whose roots in  $\mathcal{F}_{25^2}$  are  $\varsigma^{56}, \varsigma^{152}$ , defining set of  $C_4$  is  $\mathcal{W}_4 = \{7, 19\}$ ,  $\mathcal{W}_4^{-3} = \{43, 61\}$ ;  $g_5(y) = y^2 + \omega^{15} y + \omega^{16}$  whose roots in  $\mathcal{F}_{25^2}$  are  $\varsigma^{136}, \varsigma^{280}$ , the defining set of  $C_5$  is  $\mathcal{W}_5 = \{17, 35\}$ ,  $\mathcal{W}_5^{-5} = \{71, 59\}$ . Here,  $\mathcal{W}_j^{-5} = \{-5w \pmod{78} | w \in \mathcal{W}_j\}$  and  $\mathcal{W}_j \cap \mathcal{W}_j^{-5} = \phi \Rightarrow C_j^{\perp \mathcal{H}} \subseteq C_j$  for all  $j = 3, 4, 5$ . Hence, by theorem 4,  $C^{\perp \mathcal{H}} \subseteq C$ . So,  $\emptyset(C)$  be an LC,  $[195, 185, 4]_{5^2}$  over  $\mathcal{F}_{5^2}$  and by theorem 5,  $\exists$  a QECC having parameters

$[[195, 175, 4]]_5$ . Table 1, below, represents the new and better  $QECC$  in the 10<sup>th</sup> column (col.). Here, 1<sup>st</sup> col. gives length  $n$ , 2<sup>nd</sup> col. gives units, 3<sup>rd</sup> col. gives  $\beta_j$  (primitive  $nt$ .th root of unity), and the following five columns give generator polynomials of  $C_j$ , in the form of their coefficients, for instance,  $y^2 + 12y + \omega^8$  and  $(y + \omega^8)(y + \omega^2)$  is written in the form  $1(12)\omega^8$  and  $1\omega^8. 1\omega^2$  respectively.

## 6. Conclusion and next plan

This manuscript discusses the construction of novel and efficient  $QECC$ 's by CCc's over the ring  $\mathcal{R} = \mathcal{F}_{p^2}[u, v]/(u^3 - \omega^2 u, v^3 - \omega^2 v)$ , where  $p$  is a prime (other than two) power. Here, we explore Idempotent elements, linear codes, units, and generator polynomials of Hermitian dual-containing CCc over the considered ring. As an application of this study, we explain three different types of examples to construct  $QECC$ 's. Example (Ex.) 1 presents the scenario when the splitting and base field of the ring are the same. Ex. 3 presents the scenario when the splitting and base field are different, and example 2 presents the mixed case. Here, many novel and effective  $QECC$ 's are found (in the 10th column of Table 1). In the future, we will extend this work to construct more efficient and new  $QECC$ 's and MDS codes, by Skew CCc's over the ring.

## References

- [1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379-423 (1948).
- [2] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. 2493-2496 (1995).
- [3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF (4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp.1369-1387(1998).
- [4] A. R. Calderbank, and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A - At. Mol. Opt. Phys*, vol. 54, no. 2, pp.1098-1105 (1996).
- [5] A. Mohammad, and M. Ghulam, "Quantum codes from cyclic codes over  $F_q + uF_q + vF_q + uvF_q$ ," *Quantum Inf. Process.*, vol. 15, no. 10, pp. 4089-4098 (2016).
- [6] A. Mohammad, and M. Ghulam, "Construction of quantum codes from cyclic codes over  $F_p + vF_p$ ," *Int. J. Inf. Coding Theory*, vol. 3, no. 2, pp. 137-144 (2015).

- [7] M. Gü'zeltepe, M. Sari, "Quantum codes from codes over the ring  $F_q + \alpha F_q$ ," *Quantum Inf. Process.*, vol. 18, no. 365, pp. 1-21 (2019).
- [8] P. Soni, M. Pruthi, and A. K. Yadav, "New Quantum Codes Derived from the Direct Product of Rings, using Cyclic Codes over the Ring," *Rep. Math. Phys.*, vol. 93, no. 2, pp. 213-229 (2024).
- [9] D. Suprijanto, and H. C. Tang, "Quantum codes constructed from cyclic codes over the ring  $F_q + vF_q + v^2 F_q + v^3 F_q + v^4 F_q$ ," arXiv:2112.13488v2[cs.IT], pp. 1-14 (2021).
- [10] A.K. Yadav, and M. Pruthi, "Improved and Novel Quantum Codes through CSS Construction from Cyclic Codes over Commutative Non-Local Ring  $F_p \times (F_p + \alpha F_p + \alpha^2 F_p)$ ," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 6, 1949-1961, Doi: 10.47974/JDMSC-2001 (2024).
- [11] T. Bag, H.Q. Dinh, K. Abdukhalikov, A.K. Upadhyay, and Y.Woraphon, "Constacyclic codes over  $\mathbb{F}_{q^2}[u]/\langle u^2 - w^2 \rangle$  and their application in Quantum code construction," *J. Appl. Math. Comput.*, vol. 68, pp. 3821-3834 (2022).
- [12] H. Q. Dinh, T. Bag, S. Pathak, A. K. Upadhyay, and W. Chinnakum, "Quantum codes obtained from constacyclic codes over a family of finite rings  $F_p[u_1, u_2, \dots, u_s]$ ," *IEEE Access*, vol. 8, pp. 194082-194091 (2020).
- [13] H. Q. Dinh, T. Bag, A. K. Upadhyay, M. Ashraf, and W. Chinnakum, "Constacyclic codes over  $F_{q^2}[u]/\langle u^2 - \omega^2 \rangle$  and their application in quantum code construction," *J. Appl. Math. Comput.*, vol. 68, pp. 3821-3834 (2022).
- [14] J. Gao, and Y. Wang, "u-Constacyclic codes over  $F_p + uF_p$  and their applications of constructing new non-binary quantum codes," *Quantum Inf. Process.*, vol. 17, no. 1 (2018).
- [15] K. Gowdhaman, C. Mohan, et al, "Construction of quantum codes from  $\lambda$ -constacyclic codes over the ring  $F_p[u, v]/\langle v^3 - v, u^3 - u, uv - vu \rangle$ ," *J. Appl. Math. Comput.*, pp. 1-12 (2020).
- [16] H. Islam, O. Prakash, "New quantum codes from constacyclic and additive constacyclic Codes," *Quantum Inf. Process.*, vol. 19, no. 9, pp. 1-17 (2020).
- [17] B. Kong, and X. Zheng, "Quantum codes from constacyclic codes over  $S_k$ ," *EPJ Quantum Technol.*, vol. 10, no. 3, pp. 1-16 (2023).

- [18] F. Ma, J. Gao, and F. Fu, “New non-binary quantum codes from constacyclic codes over  $F_q[u,v]/\langle u^2 - 1, v^2 - v, uv - vu \rangle$ ,” *Adv. Math. Commun.*, vol. 13, no. 2, pp. 421-434 (2019).
- [19] P. Soni, M. Pruthi, “New optimized Lcd codes and quantum codes using constacyclic codes over a non-local collection of rings  $A_k$ ,” *Quantum Inf. Process.*, vol. 23, no. 303, pp. 302- 316 (2024).
- [20] A. Ashikhmin, and E. Knill, “Nonbinary quantum stabilizer codes,” *IEEE Trans. Inf. Theory*, vol. 47, pp. 3065–3072 (2001).
- [21] K.Gowdhaman, T. A. Gulliver, C. Mohan, and D. Chinnappillai, “Constacyclic codes over the non-chain finite commutative ring  $Z_4[u,v]/\langle u^2 - u, v^2, uv \rangle$ ,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 6, pp. 1867–1885 (2024), Doi: 10.47974/JDMSC-1873.
- [22] S. Bhowmick, J. de la Cruz, E. Martínez-Moro, and A. Sharma, “On LCP and checkable group codes over finite non-commutative Frobenius rings,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 3, 891–905 (2025), Doi: 10.47974/JDMSC-2187.

*Received February, 2025*