Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 6, pp. 1949–1961
DOI : 10.47974/JDMSC-2001

Improved and Novel Quantum Codes through CSS Construction from Cyclic Codes over Commutative Non-Local Ring $\mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$

Arun Kumar Yadav *
Manju Pruthi †
Department of Mathematics
Indira Gandhi University
Meerpur
Rewari
Haryana
India

Abstract

In this study, by using CSS construction, we present the new quantum codes derived from cyclic codes over the commutative non - local ring $\mathcal{R} = \mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$, where p is an odd prime, $\alpha^3 = \alpha$. Firstly, we investigate the structure of the ring R and study linear codes by defining Lee weight over $\mathcal{R}$. We define a distance – preserving Gray map from $\mathcal{R} \to \mathcal{F}_p^4$ and discuss the cyclic codes with their dual code by Euclidean inner products on $\mathcal{R}$. Additionally, we find the quantum Singleton defect(QSD) of the quantum code, which is denoted as $n + 2 - k - 2d$. Magma Software will be employed to provide relevant illustrations for enhanced comprehension.

Subject Classification: *94B05, 94B15, 94B35, 94B60, 11T71, 14H20.*

Keywords: *Quantum codes, Gray map, Non-local ring, Cyclic codes.*

1. Introduction

In 1995, Shor achieved a significant breakthrough by fortuitously discovering the initial quantum error-correcting code [20]. Calderbank and colleagues introduced an innovative technique in 1998 [9] for producing quantum error-correcting codes through the application of classical cyclic codes.Since then, researchers have made significant strides in this area, particularly with respect to the generalization of these codes over the finite field $\mathcal{F}_q$. As a result, this field has become an active area of study, with researchers

* *E-mail:* **arunyadav0307@gmail.com (Corresponding Author)**
† *E-mail:* **manju.pruthi@yahoo.com**

© Taru Publications

exploring various approaches to improve the efficiency and effectiveness of quantum error-correcting codes[1],[5],[14],[15],[17],[18]. The domain of algebraic coding theory has advanced beyond its initial concentration on finite fields. It has broadened its investigation to diverse categories of finite rings, as demonstrated by the remarkable publication of Hammons et al.[16]. The concept of Gray maps enables the establishment of a correlation between codes over finite rings and finite fields. This correlation serves to simplify the study of codes in the context of finite rings. An extensive amount of literature is available regarding the topic of codes over rings [2],[4],[10],[11],[12],[13],[19].

In recent years, researchers have increasingly focused on examining various codes defined over the direct product of multiple finite rings. This heightened academic interest has spurred comprehensive investigations into both the theoretical and practical dimensions of these codes. In 2015, Gao performed a research study that investigated the qualities of linear codes used inside a finite non-chain ring, specifically referred to as $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p$ [15]. The aforementioned ring exhibits distinctive characteristics, as p denotes an odd prime and $\alpha^3 = \alpha$. The study presented an innovative methodology for the development of superior linear codes over finite fields, which leverages cyclic codes over a particular ring. In 2020, Ashraf et al. [3], contributed significantly to the research cyclic codes over $\mathcal{F}_p + \alpha\mathcal{F}_p$. They not only established significant achievements in this area, but they also proposed a unique method for generating self-orthogonal codes over the field $\mathcal{F}_p$. Their method included creating gray image of cyclic codes across the ring $\mathcal{F}_p + \alpha\mathcal{F}_p$. They also determined the parameters of related quantum error-correcting codes, which might be useful in the construction of efficient and trustworthy quantum computing systems. In 2019, Caliskan et al. [6] investigated the linear codes over $\mathcal{F}_2 \times (\mathcal{F}_2 + v\mathcal{F}_2)$ and their corresponding weight enumerators, subject to the condition that $v^2 = v$. Moreover, the MacWilliams identities have been verified to hold for the weight enumerators of both the complete and symmetrized codes, as well as the Lee codes. Recently, Caliskan et al.[7], cyclic codes have been established over the commutative principal ideal ring $\mathcal{F}_2 \times (\mathcal{F}_2 + v\mathcal{F}_2)$, where $v^2 = v$. The graymap representations of a cyclic code over a given ring, having a length of n, result in binary quasi-cyclic codes with an index of 3 and a length of $3n$. Furthermore, binary QECCs can be derived from cyclic codes over $\mathcal{F}_2 \times (\mathcal{F}_2 + v\mathcal{F}_2)$. In 2023, Caliskan et al. [8], examined cyclic codes, and the gray map in the ring $S = \mathcal{F}_p \times (\mathcal{F}_p + v\mathcal{F}_p)$, where p is an odd prime and $v^2 = v$. It builds cyclic and dual codes in this finite semi-local ring. The study introduces the gray map over S and applies QECCs generated from cyclic codes over S with examples. Moreover, QECCs over the ring R are examined for their properties and applications. Motivation by above work, we explore, structure and properties of $\mathcal{R} = \mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$ and obtain cyclic codes over $\mathcal{R}$ with distance preserving gray map. Also, discuss the QECCs over the ring $\mathcal{R}$.

The framework of this research is established by initially delving into the essence of the product of finite fields with finite rings in section 1. In section 2 involves presenting the ring's structure and locating the linear code across $\mathcal{R} = \mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$. Define the distance preserving Gray map $\psi : \mathcal{R} \to \mathcal{F}_p^4$ containing the generating idempotent, and give an explanation of the minimum Lee weight. In Section 3, give the cyclic and quasi-cyclic codes over $\mathcal{R} = \mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$ with some illustrations. In Section 4, the research delves into the examination of quantum error correcting codes over the ring R. We study the quantum error correcting codes over the ring $\mathcal{R}$. Finally, this paper concludes in section 5.

2. Linear Code over the ring $\mathcal{R} = \mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$

In this section, we define a ring $\mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$, where p is an odd prime with elemental properties, where $\mathcal{F}_p$ be a finite field with p elements and the finite ring $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p = \{a + \alpha b + \alpha^2 c : a, b, c \in \mathcal{F}_p\}$ with p^3 elements.

Consider $\mathcal{R} = \mathcal{F}_p \times \left(\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p\right) = \{(x, y): x \in \mathcal{F}_p \text{ and } y \in \mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p\}$, and $\alpha^3 = \alpha$. $\mathcal{R}$ is a commutative ring with identity with characteristics p. It has three maximal ideals $\langle(0,\ \alpha)\rangle, \langle(1,\ \alpha - 1)\rangle, \langle(1,\ \alpha + 1)\rangle$. Let $(\beta, a + \alpha b + \alpha^2 c) \in \mathcal{R}$.

Now, Multiplication on $\mathcal{R}^n$ be defined as

$$(\beta, a + \alpha b + \alpha^2 c) * \boldsymbol{u} = (\beta\beta_0, aa_0 + \alpha(ba_0 + ab_0 + cb_0 + bc_0) + \alpha^2(ca_0 + bb_0 + ac_0 + cc_0), \ldots, (\beta\beta_{n-1}, aa_{n-1} + \alpha(ba_{n-1} + ab_{n-1} + cb_{n-1} + bc_{n-1}) + \alpha^2(ca_{n-1} + bb_{n-1} + ac_{n-1} + cc_{n-1})).$$

where $\boldsymbol{u} = (u_0, u_1, u_2, \ldots, u_{n-1}) \in \mathcal{R}^n$ such that $u_k = (\beta_k, a_k + \alpha b_k + \alpha^2 c_k)$, where $k = 0,1,2, \ldots, n-1$.

Let us redirect our attention to linear codes operating within the field $\mathcal{R}$. Initially, we will introduce the concept of a Lee weight for codes over $\mathcal{R}$, followed by the establishment of a distance-preserving Gray map connecting $\mathcal{R}^n$ and ${\mathcal{F}_p}^{4n}$.

Definition 1: The linear code C of length n over $\mathcal{R}$ can be expressed as an $\mathcal{R}$ - submodule of $\mathcal{R}^n$.

Result 1: To be permutation equivalent, a code C of length n over the ring $\mathcal{R}$ must be expressible as the direct product of two codes, C_1 and C_2 of length n over field $\mathcal{F}_p$ and $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p$ respectively. Hence, $C = (C_1, C_2)$ of length n over $\mathcal{R}$ is linear iff both C_1 and C_2 of length n over field $\mathcal{F}_p$ and $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p$ respectively are linear codes.

Definition 2: Let $(\beta, a + \alpha b + \alpha^2 c) \in \mathcal{R}$ with $a, b, c \in \mathcal{F}_p$ then the Lee weight of $(\beta, a + \alpha b + \alpha^2 c)$ is defined as

$$\omega_L(\beta, a + \alpha b + \alpha^2 c) = \omega_H(\beta) + \omega_H(a) + \omega_H(a + b + c) + \omega_H(a - b + c)$$

where Hamming weight, denoted by $\omega_H(t)$, of a given element t in $\mathcal{F}_p$ is the number of non-zero coordinates associated with t.

Consider two codewords $\boldsymbol{u} = (u_0, u_1, u_2, \dots, u_{n-1})$ and $\boldsymbol{v} = (v_0, v_1, v_2, \dots, v_{n-1}) \in C$. The computation of the Lee weight of $\boldsymbol{u}$ involves a rational summation of the Lee weight attributed to each individual component. The mathematical expression for the Lee distance is $d_L(\boldsymbol{u}, \boldsymbol{v}) = \omega_L(\boldsymbol{u} - \boldsymbol{v})$. The minimum non-zero weight value in code C is its minimal Lee weight. The minimal Lee distance of a code C is the smallest distance that is not zero between any two codewords in C. One interesting fact about linear codes like C is that their minimum Lee distance and weight coincide.

Gray Map over $\boldsymbol{\mathcal{R}}$

Consider any element $(\beta, a + \alpha b + \alpha^2 c)$ of $\mathcal{R}$ can be uniquely expressed as $(\beta, a + \alpha b + \alpha^2 c) = (\beta, ae_1 + (a + b + c)e_2 + (a - b + c)e_3$, where $e_1 = 1 - \alpha^2, e_2 = \frac{\alpha}{2} + \frac{\alpha^2}{2}, e_3 = -\frac{\alpha}{2} + \frac{\alpha^2}{2}$ are the orthogonal idempotent of ring $(\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$.

Define the Gray map between $\mathcal{R}$ to $\mathcal{F}_p^4$

$$\phi(\beta, a + \alpha b + \alpha^2 c) = (\beta, a, a + b + c, a - b + c),$$

Now, continuing with the extension, we introduce the mapping $\psi : \mathcal{R}^n \to \mathcal{F}_p^{4n}$ such that $\psi\big((u_0, u_1, u_2, \dots, u_{n-1})11\big) \to (\beta_0, \beta_1, \dots, \beta_{n-1}, a_0, a_1, \dots, a_{n-1}, a_0 + b_0 + c_0, a_1 + b_1 + c_1, \dots, a_{n-1} + b_{n-1} + c_{n-1}, a_0 - b_0 + c_0, a_1 - b_1 + c_1, \dots, a_{n-1} - b_{n-1} + c_{n-1})$

Lemma 1: *As a distance-preserving map, the Gray map ψ upholds the connection between $\mathcal{R}^n$ (Lee distance) and $\mathcal{F}_p^{4n}$ (Hamming distance), while also being an $\mathcal{F}_p$ map, and it is also $\mathcal{F}_p - linear$.*

Proof: By the definition of Gray map ψ, if $\boldsymbol{u_1}, \boldsymbol{u_2} \in \mathcal{R}^n$ then $\psi(t_1\boldsymbol{u_1} + t_2\boldsymbol{u_2}) = t_1\psi(\boldsymbol{u_1}) + t_2\psi(\boldsymbol{u_2})$ where $t_1, t_2 \in \mathcal{F}_p$**.** Hence, ψ is $\mathcal{F}_p - linear$. It is evident that $\psi(\boldsymbol{u}, \boldsymbol{v}) = \psi(\boldsymbol{u}) - \psi(\boldsymbol{v})$ where $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{R}^n$. By definition 2 and $d_L(\boldsymbol{u}, \boldsymbol{v}) = \omega_L(\boldsymbol{u} - \boldsymbol{v})$, we have $d_L(\boldsymbol{u}, \boldsymbol{v}) = d_H(\psi(\boldsymbol{u}) - \psi(\boldsymbol{v}))$.

Lemma 2: *A linear code C over $\mathcal{R}$ of length n, the resulting code $\psi(C)$over $\mathcal{F}_p$ will have a length of $4n$ and will preserve linearity.*

Proof: The result may be deduced from the Grey map and Lemma 1.

Definition 3: *Let $\boldsymbol{u} = (u_0, u_1, u_2, \dots, u_{n-1})$ and $\boldsymbol{v} = (v_0, v_1, v_2, \dots, v_{n-1})$ be two vectors of $\mathcal{R}^n$. The Euclidean inner product(EIP) of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined as follows*

$$\langle \boldsymbol{u}.\boldsymbol{v} \rangle = \sum_{j=0}^{n-1} u_j v_j$$

Now, the EIP on $\mathcal{R}^n$ can be defined by employing the ordinary dot product "." on $\mathcal{F}_p$ and the EIP "$\langle , \rangle_E$" on $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p$ is

$\langle(\beta, a+\alpha b+\alpha^2 c)(\gamma, r+\mu s+\mu^2 t)\rangle = (\beta.\gamma, \langle a+\alpha b+\alpha^2 c,\ r+\mu s+\mu^2 t\rangle_E)$, where $\beta, a, b, c, r, s, t \in \mathcal{F}_p^n$.

The dual code is defined as $C^\perp = \{s \in \mathcal{R}^n : \langle x, y\rangle = (0,0), y \in C\}$. Using the above product, $C^\perp$ is also a linear code over $\mathcal{R}$ of length n. If $C = (C_1, C_2)$ is a linear code over $\mathcal{R}$ of length n, so is $C^\perp = ({C_1}^\perp, {C_2}^\perp)$.

Lemma 3: *In order for a code $C = (C_1, C_2)$ to exhibit self-orthogonality over $\mathcal{R}$ iff codes C_1 and C_2 meet the self-orthogonality criteria over $\mathcal{F}_p$ and $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p$.*

Proof: Let $C = (C_1, C_2)$ be an n-bit self-orthogonal code in $\mathcal{R}$. and $\boldsymbol{u} = (\beta, a+\alpha b+\alpha^2 c) \in \mathcal{R}$. We have

$$0 = \langle \boldsymbol{u}, \boldsymbol{u}\rangle = (\beta.\beta, (a+\alpha b+\alpha^2 c, a+\alpha b+\alpha^2 c)_E).$$

Then $\beta \in {C_1}^\perp$, and $a+b\alpha+c\alpha^2 \in {C_2}^\perp$, we have $C_1 \subseteq {C_1}^\perp$ and $C_2 \subseteq {C_2}^\perp$. On the other hand, if $C_1 \subseteq {C_1}^\perp$ and $C_2 \subseteq {C_2}^\perp$, then $C \subseteq C^\perp$ utilizing Result 1.

Theorem 1: *Let C is an n -length linear coder over $\mathcal{R}$ then $\psi(C^\perp) = \psi(C)^\perp$. If C is a self-dual, so $\psi(C)$ is.*

Proof: Consider $\boldsymbol{u} = (\beta, a+\alpha b+\alpha^2 c) \in C$ and $\boldsymbol{v} = (\gamma, r+\mu s+\mu^2 t) \in C^\perp$. If $\langle \boldsymbol{u}.\boldsymbol{v}\rangle = 0$, then

$$\sum_{j=0}^{n-1} \beta_j\gamma_j = 0, \qquad \sum_{j=0}^{n-1} a_j r_j = 0,$$
$$\sum_{j=0}^{n-1}(a_j s_j + b_j r_j + b_j t_j + c_j s_j) = 0$$
$$\sum_{j=0}^{n-1}(a_j t_j + c_j r_j + b_j s_j + c_j t_j) = 0$$

Therefore,

$$\langle \psi(\boldsymbol{u}), \psi(\boldsymbol{v})\rangle = (\beta, a, a+b+c, a-b+c).(\gamma, r, r+s+t, r-ls+t)$$
$$= \sum_{j=0}^{n-1} \beta_j\gamma_j + 3\sum_{j=0}^{n-1} a_j r_j + 2\sum_{j=0}^{n-1}(a_j t_j + c_j r_j + b_j s_j + c_j t_j)$$
$$= 0$$

We know that $\mathcal{R}$ is a Commutative non - local ring. We have $\psi(\boldsymbol{v}) \in \psi(C)^\perp \Rightarrow \psi(C^\perp) = \psi(C)^\perp$.

Clearly,

$$|\psi(C^\perp)| = \frac{p^{4n}}{|\psi(C)|} = \frac{p^{4n}}{|C|} = |C^\perp|$$

In addition, if C is self-dual, we obtain $\psi(C) = \psi(C)^\perp$. Also, $\psi(C)$ is a self-dual.

Corollary 1: *Let C be an n -length linear code over $\mathcal{R}$. If C is self-orthogonal, then so is $\psi(C)$.*

3. Cyclic Codes over the ring $\mathcal{R} = \mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$

The primary focus of this section is to provide readers with clear definitions and a collection of properties of cyclic codes over the ring $\mathcal{R}$.

We define a map $\tau : \mathcal{R}^n \to \mathcal{R}^n$ define as

$$\tau\big((t_0, t_1, t_2, \dots, t_{n-1})\big) = (t_{n-1}, t_0, t_1, t_2, \dots, t_{n-2})$$

where $(t_0, t_1, t_2, \dots, t_{n-1}) \in \mathcal{R}^n$. The cyclic shift map, known as τ, enables the establishment of cyclic codes.

Lemma 4: *If both C_1 and C_2 are n - length cyclic codes over $\mathcal{F}_p$ and $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p$ iff $C = (C_1, C_2)$ is $n-$length cyclic code over $\mathcal{R}$.*

Lemma 5: *Consider a n length cyclic code C over $\mathcal{R}$, its dual code $C^{\perp}$ is also cyclic.*

Proof: Consider $\boldsymbol{u} = (u_0, u_1, u_2, \dots, u_{n-1}) \in C$ and $\boldsymbol{v} = (v_0, v_1, v_2, \dots, v_{n-1}) \in C^{\perp}$. $\langle \boldsymbol{u}.\boldsymbol{v} \rangle = 0$. As C is a cyclic code over $\mathcal{R}$, $\tau^t(\boldsymbol{u})$ is in C for all t. Now, for $t = n-1$, We get

$$0 = \langle \tau^{n-1}(\boldsymbol{u}), \boldsymbol{v} \rangle = u_0 v_{n-1}, u_1 v_0,\ u_2 v_1, \dots, u_{n-1} v_{n-2} = \langle \boldsymbol{u}, \tau(\boldsymbol{v}) \rangle$$

$\Rightarrow \tau(\boldsymbol{v})) \in C^{\perp}$. Consequently, orthogonal of C is cyclic.

We will now direct our attention to examining the way codewords are represented in polynomial form within a cyclic code. Since a vector $\boldsymbol{\vartheta} = (\vartheta_0, \vartheta_1, \vartheta_2, \dots \vartheta_{n-1}) \in \mathcal{R}^n$ can be considered as the polynomial $\boldsymbol{\vartheta}(y) = (\vartheta_0, \vartheta_1 y, \vartheta_2 y^2, \dots, \vartheta_{n-1} y^{n-1}) \in \mathcal{R}[y]$,

In this context, a codeword in the cyclic code C over the ring $\mathcal{R}$, represented as $\boldsymbol{c} = (c_0, c_1, c_2, \dots, c_{n-1})$, can be expressed as the polynomial $\boldsymbol{c}(y) = c_0 + c_1 y + c_2 y^2 + \cdots + c_{n-1} y^{n-1} \in \mathcal{R}_n = \mathcal{R}[y]/\langle \mathbf{1}y^n - \mathbf{1} \rangle$.. Here, the element **1** = (1, 1) ∈ $\mathcal{R}$. The polynomial representation maps cyclic codes over $\mathcal{R}$ to ideals of $\mathcal{R}_n$ and vice versa.

Theorem 2: *Let $C = (C_1, C_2)$ be n length cyclic code over $\mathcal{R}$. There exist a unique generator polynomial $\varphi(y) = (\varphi_1(y), e_1\varphi_2(y) + e_2\varphi_3(y) + e_3\varphi_4(y))$ with $C = \langle \varphi(y) \rangle$ and $|C| = p^{4n - \sum_{k=1}^{4} deg(\varphi_k(y))}$, where $\varphi_k / y^n - 1 in\ \mathcal{F}_p[y]$ for $k = 1,2,3,4$ and $e_1\varphi_2(y) + e_2\varphi_3(y) + e_3\varphi_4(y)/y^n - 1 in\ (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)[y]$.*

Proof: Using Lemma 4, ∃ unique polynomials $\varphi_1(y)\varphi_2(y)\varphi_3(y)$ and $\varphi_4(y)$ such that $C_1 = \langle \varphi_1(y) \rangle$ and $C_2 = \langle e_1\varphi_2(y) + e_2\varphi_3(y) + e_3\varphi_4(y) \rangle$ with $e_1\varphi_2(y) + e_2\varphi_3(y) + e_3\varphi_4(y)/y^n - 1$ and $\varphi_k(y)/y^n - 1$ for $k = 1,2,3,4$. Therefore, we have

$$C = \langle \varphi_1(y), e_1\varphi_2(y) + e_2\varphi_3(y) + e_3\varphi_4(y) \rangle$$

Further, since $|C| = |C_1||C_2|$, we obtain that

$$|C| = p^{n - \deg(\varphi_1(y))}.p^{3n - \deg(\varphi_1(y)) - \deg(\varphi_2(y)) - \deg(\varphi_3(y))}$$

$$|C| = p^{4n-\sum_{k=1}^{4}\deg(\varphi_k(y))}$$

To demonstrate the above outcome, we now provide the following example below.

Examples 1: For a cyclic code C of length 12 over $\mathcal{R} = \mathcal{F}_3 \times (\mathcal{F}_3 + \alpha\mathcal{F}_3 + \alpha^2\mathcal{F}_3)$ with $\alpha^3 = \alpha$, we have

$$y^{12} - 1 = (y+1)^3(y+6)^3(y^2+1)^3$$

Let $f_i(y) = y + 1$ and $f_j(y) = y + 6$, where $i = 1,3\ and\ j = 2,4$ the generating polynomial of cyclic codes C_i for $i = 1\ to\ 4$. We get $C = \langle y + 1,\ (1 + 2\alpha)y + 2\alpha\rangle$ with code words 3^8, Where $(1 + 2\alpha)y + 2\alpha$ is a factor of this polynomial $y^{12} - 1$ in $(\mathcal{F}_3 + \alpha\mathcal{F}_3 + \alpha^2\mathcal{F}_3)[y]$.

Examples 2: For a cyclic code C of length 45 over $\mathcal{R} = \mathcal{F}_5 \times (\mathcal{F}_5 + \alpha\mathcal{F}_5 + \alpha^2\mathcal{F}_5)$ with $\alpha^3 = \alpha$, we have

$$y^{45} - 1 = (y+4)^5(y^2+y+1)^5(y^6+y^3+1)^5$$

Let $f_i(y) = y^2 + y + 1$ and $f_j(y) = y + 4$, where $i = 1,3\ and\ j = 2,4$ the generating polynomial of cyclic codes C_i for $i = 1\ to\ 4$. We get $C = \langle y^2 + y + 1,\ 3(\alpha^2 + \alpha)y^2 + y + 4(\alpha^2 + 1)\rangle$ with code words 5^{14}, Where $3(\alpha^2 + \alpha)y^2 + y + 4(\alpha^2 + 1)$ is a factor of this polynomial $y^{12} - 1$ in $(\mathcal{F}_5 + \alpha\mathcal{F}_5 + \alpha^2\mathcal{F}_5)[y]$.

A cyclic code over $\mathcal{R}$ has its generator polynomials determined in Theorem 2. Based on the previous result, we are able to compute the generator polynomials for the dual code of a cyclic code over $\mathcal{R}$. It is also shown that $\varphi^*(y) = y^{\deg(\varphi(y))}\varphi(y^{-1})$ is the reciprocal polynomial of $\varphi(y)$.

Corollary 1: *Let* $C = \langle \varphi_1(y), e_1\varphi_2(y) + e_2\varphi_3(y) + e_3\varphi_4(y)\rangle$ *be a cyclic code over* $\mathcal{R}$ *of length* n *and* $y^n - 1 = \varphi_k(y)\xi_k(y)$ *for* $k = 1\ to\ 4$. *We get* $C^{\perp} = \langle \xi_1^*(y), e_1\xi_2^*(y) + e_2\xi_3^*(y) + e_3\xi_4^*(y)\rangle$. *Furthermore,* $|C^{\perp}| = p^{\sum_{k=1}^{4} deg(\varphi_k(y))}$.

3.1 *Quasi – Cyclic Codes over* $\boldsymbol{\mathcal{F}_p}$

In this subsection, Quasi-cyclic codes of length rn and index r are made available across the field $\mathcal{F}_p$ and characterize the Grey image of a cyclic code over $\mathcal{R}$. For every positive integer r, let $\boldsymbol{\beta} \in \mathcal{F}_p^{rn}$

$$\boldsymbol{\beta} = (\beta_0, \beta_1, \dots, \beta_{rn-1}) = \left(\beta^{(1)} \middle| \beta^{(2)} \middle| \dots \dots \middle| \beta^{(r)}\right),$$

where $\beta^{(k)}$ is in $\mathcal{F}_p^{rn}$ for $1 \le k \le r$. The map given as

$$\tau_r : \mathcal{F}_p^{rn} \to \mathcal{F}_p^{rn},\ \tau_r(\boldsymbol{\beta}) = \left(\tau(\beta^{(1)}) \middle| \tau\left(\beta^{(2)}\right) \middle| \dots \dots \middle| \tau\left(\beta^{(r)}\right)\right)$$

The operation carried out on $\mathcal{F}_p^{rn}$, denoted as the quasi-cyclic shift, involves utilizing the cyclic shift operator τ.

Definition 4: A quasi-cyclic code of index r over $\mathcal{F}_p$ of length rn states that a code C is considered quasi-cyclic if the cyclic shift of r positions, denoted by τ_r, applied to C results in the same code C (i.e. $\tau_r(C) = C$).

According to the description of a quasi-cyclic code, the following outcome can be derived.

Corollary 2: *Consider a cyclic code C of length n over $\mathcal{R}$. The code $\psi(C)$ is a quasi-cyclic code over $\mathcal{F}_p$, as per the given scenario. The length of $\psi(C)$is precisely $4n$, and its index is 4.*

Theorem 3: *Let the Gray map on $\mathcal{R}^n$ as ψ, the cyclic shift operator on $\mathcal{R}^n$ as τ, and the quasi-cyclic shift operator on $\mathcal{F}_p^{4n}$ of index 4 as τ_4, it is shown that the association $\psi\tau = \tau_4\psi$ is valid.*

Proof: Let β, a, b *and* c be four elements of $\mathcal{F}_p^{4n}$. The Gray map

$$\psi(\beta, a + b\alpha + c\alpha^2) = (\beta, a, a + b + c, a - b + c)$$

Thus, we obtain

$$\tau_4(\psi(\beta, a + b\alpha + c\alpha^2)) = (\tau(\beta), \tau(a), \tau(a + b + c), \tau(a - b + c))$$

On the other hand, we have

$$\tau(\beta, a + b\alpha + c\alpha^2) = \tau(\beta), \tau(a) + \alpha\tau(b) + \alpha^2\tau(c))$$

Then

$$\psi(\tau(\beta, a + b\alpha + c\alpha^2)) = (\tau(\beta), \tau(a), \tau(a + b + c), \tau(a - b + c))$$

Hence, $\psi\tau = \tau_4\psi$

4. Quantum error-correcting codes over $\mathcal{R}$

An $n-$length $p-$ary QECC can be thought as a subspace of a p^n-dimensional Hilbert space, written as $(C^p)^{\otimes n}$ with dimension p^k, where p is a prime power. The QECC is represented by the notation $[[n, k, d]]_p$, where d denotes the minimum distance. The theorem below can be utilized to derive Quantum Error-Correcting Codes (QECCs) from linear codes over finite fields. Additionally, it is essential to observe the CSS structure.

Theorem 4 [9]: *Consider a linear code C over a finite field $GF(p)$ with parameters $[n, k, d]$.The existence of a $[[n, 2k - n, d]]_p$ Quantum Error-Correcting Code System can be inferred if the dual code of C is contained within it.*

The subsequent lemma provides the requisite and complete criterion for cyclic codes that contain their duals over (p).

Lemma 6 [9]: *Consider $C = \langle\varphi_1(y)\rangle$ be length n cyclic code over $GF(p)$. Then $C^{\perp} \subseteq C$ iff $\varphi_1(y)\varphi_1{}^*(y)|y^n - 1$.*

Theorem 5 [3]: *Consider $C = \langle\varphi(y)\rangle$ be $n-$length cyclic code over $\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p$, Here $\varphi(y) = e_1\varphi_2(y) + e_2\varphi_3(y) + e_3\varphi_4(y)$. C contains its dual*

iff $\varphi_k(y)\varphi_k{}^*(y)|y^n-1$ *for* $k=2,3,4$, *where* $\varphi_k{}^*(y)$ *is the reciprocal polynoamial of* $\varphi_k(y)$.

Theorem 6: *Consider* $C=\langle\varphi(y)\rangle$ *be* $n-length$ *cyclic code over* $\mathcal{R}$ *as in theorem 2.* C *contains its dual iff* $\varphi_k(y)\varphi_k{}^*(y)|y^n-1$ *for* $k=1\ to\ 4$.

Proof: By utilizing result 1, along with Lemma 6 and Theorem 5, one can derive the desired result.

Corollary 3: *Let* $C=(C_1,C_2)$ *be a cyclic code over* $\mathcal{R}$. ${C_1}^{\perp}\subseteq C_1$ *and* ${C_2}^{\perp}\subseteq C_2$ *iff* $C^{\perp}\subseteq C$.

Theorem 7: *A QECC with the parameters* $[4n,2k-4n,d]_p$, *exists if* $n-$*length cyclic code* C *over* $\mathcal{R}$ *with the minimal Lee weight* d *includes its counterpart code.*

Proof: Suppose that $\boldsymbol{u}\in\psi(C^{\perp})$ then there exists $\boldsymbol{v}\in C^{\perp}$ such that $\boldsymbol{u}=\psi(\boldsymbol{v})$. Also, $\boldsymbol{v}\in C$ as $C^{\perp}\subseteq C$. Therefore, we have $=\psi(\boldsymbol{v})\in\psi(C)\Rightarrow\psi(C^{\perp})\subseteq\psi(C)$. Using Theorem 1, we attain $\psi(C^{\perp})\subseteq\psi(C)$. Theorem 4 proves that the parameters of the minimal Hamming weight d of $\psi(C)$ correspond to a QECC with the parameters $[4n,2k-4n,d]_p$.

5. Computatonal Work

Now, to clarify the findings in this section, we will provide several illustrations.

Examples 3: For a cyclic code C of length 12 over $\mathcal{R}=\mathcal{F}_3\times(\mathcal{F}_3+\alpha\mathcal{F}_3+\alpha^2\mathcal{F}_3)$ with $\alpha^3=\alpha$, we have

$$y^{12}-1=(y^2+1)^3(y+1)^3(y+6)^3$$

Let $f_1(y)=y^2+1$ and $f_i(y)=y+1$, where $i=2,3,4$ the generating polynomial of cyclic codes C_i, $i=1\ to\ 4$. Then $C=\langle y^2+1,\ y+1\rangle$. Now, the Gray image $\psi(C)$ with parameter $[48,43,2]_3$. Since $y^{12}-1\equiv 0\ mod\ (\varphi_k(y)\varphi_k(y)^*)$ for $k=1\ to\ 4$ then $C^{\perp}\subseteq C$. consequently, by theorem 7, the QECCs associated with $\psi(C)$ has parameter $\left[[48,38,2]\right]_3$ and singleton defect 3.

Examples 4: For a cyclic code C of length 45 over $\mathcal{R}=\mathcal{F}_5\times(\mathcal{F}_5+\alpha\mathcal{F}_5+\alpha^2\mathcal{F}_5)$ with $\alpha^3=\alpha$, we have

$$y^{45}-1=(y+4)^5(y^2+y+1)^5(y^6+y^3+1)^5$$

Let $f_1(y)=y^2+y+1$ and $f_i(y)=y+4$, where $i=2,3,4$ the generating polynomial of cyclic codes C_i for $i=1\ to\ 4$. We get $C=\langle y^2+y+1,\ y+4\rangle$. Now, the Gray image $\psi(C)$ with parameter $[179,171,2]_5$. Since $y^{45}-1\equiv 0\ mod\ (\varphi_k(y)\varphi_k(y)^*)$ for $k=1\ to\ 4$, then $C^{\perp}\subseteq C$.

consequently, by theorem 7, the QECCs associated with $\psi(C)$ has a parameter $\left[[179,163,4]\right]_5$ and singleton defect 14.

Examples 5: For a cyclic code C of length 8 over $\mathcal{R} = \mathcal{F}_7 \times (\mathcal{F}_7 + \alpha\mathcal{F}_7 + \alpha^2\mathcal{F}_7)$ with $\alpha^3 = \alpha$, we have

$$y^8 - 1 = (y+1)(y+6)(y^2+1)(y^2+3y+1)(y^2+4y+1)$$

Let $f_1(y) = y^2 + 4y + 1$ and $f_i(y) = y + 6$, where $i = 2,3,4$ the generating polynomial of cyclic codes C_i for $i = 1,2,3,4$. Then $C = \langle y^2 + 4y + 1\ , y + 6\rangle$. Now, the Gray image $\psi(C)$ with parameter $[32, 27, 2]_7$. Since $y^8 - 1 \equiv 0\ mod\ (\varphi_k(y)\varphi_k(y)^*)$ for $k = 1\ to\ 4$, then $C^\perp \subseteq C$. consequently, by theorem 7, the QECCs associated with $\psi(C)$ has parameter $\left[[32, 22, 2]\right]_7$ and singleton defect 8.

Examples 6: For a cyclic code C of length 32 over $\mathcal{R} = \mathcal{F}_{11} \times (\mathcal{F}_{11} + \alpha\mathcal{F}_{11} + \alpha^2\mathcal{F}_{11})$ with $\alpha^3 = \alpha$, we have

$$y^{32} - 1 = (y+1)(y+10)(y^2+1)(y^2+3y+10)(y^2+8y+10)(y^4+3y^2+5)(y^4+8y^2+10)(y^8+3y^4+10)(y^8+8y^4+10)$$

Let $f_1(y) = y^4 + 8y^2 + 10$ and $f_i(y) = y^2 + 1$, where $i = 2,3,4$ the generating polynomial of cyclic codes C_i for $i = 1,2,3,4$. Then $C = \langle y^4 + 8y^2 + 10,\ y^2 + 1\rangle$. Now, the Gray image $\psi(C)$ with parameter $[128, 114, 2]_{11}$. Since $y^{32} - 1 \equiv 0\ mod\ (\varphi_k(y)\varphi_k(y)^*)$ for $k = 1\ to\ 4$ then $C^\perp \subseteq C$. consequently, by theorem 7, the QECCs associated with $\psi(C)$ has parameter $\left[[128, 100, 2]\right]_{11}$ and singleton defect 26.

In Table 1, we've meticulously devised a set of *QECC's* denoted as $\left[[n', k', d']\right]_q$ showcasing significant improvements in their parameters, which are thoughtfully presented in the 4th column. The 3th column, meanwhile, provides insights into the construction of the $\chi(C)$ dual, housing a linear code designated as $[n, k, d]$. The first column gracefully encapsulates the code length n, while the 2nd column expressively lay out the generator polynomial. For example, we express the generator polynomial $(x^4 + x^3 + x^2 + x - 1)(x + 2)$ as $(1,0)y^4 + (1,0)y^3 + (1,0)y^2 + (1,1)y + (1,2)$.

Table 1
Improved QECC's Codes over finite field *p*

n	**Generating polynomial**	**ψ(*C*)**	**QECC's $[[n, k, d]]_p$**	**Q.S.D**
12	$(1,0)y^2 + (0,1)y + (1,1)$	[48,43,3]	$\left[[48, 38, 3]\right]_3$	6
15	$(1,0)y^4 + (1,0)y^3 + (1,0)y^2 + (1,1)y + (1,2)$	[60,53,5]	$\left[[60, 46, 5]\right]_3$	6
18	$(0,1)y + (2,1)$	[72,68,3]	$\left[[72, 64, 3]\right]_3$	0
10	$(1,1)y + (4,1)$	[40,36,3]	$\left[[40, 32, 3]\right]_5$	6

Contd...

15	$(1,0)y^2 + (1,1)y + (1,14)$	[60,56,4]	$\left[[60,52,4]\right]_5$	2
20	$(1,1)y + (3,1)$	[80,76,3]	$\left[[80,72,3]\right]_5$	4
35	$(1,0)y^2 + (0,1)y + (5,2)$	[160,155,4]	$\left[[160,150,4]\right]_5$	4
14	$(1,1)y + (6,1)$	[56,52,3]	$\left[[56,48,3]\right]_7$	4
18	$(1,0)y^3 + (0,1)y + (5,6)$	[72,66,4]	$\left[[72,60,4]\right]_7$	6
28	$(0,1)y^2 + (1,0)y + (1,1)$	[112,105,4]	$\left[[112,98,4]\right]_7$	8
35	$(1,0)y^4 + (1,0)y^3 + (1,0)y^2 + (1,1)y + (1,6)$	[140,133,5]	$\left[[140,126,5]\right]_7$	10
42	$(1,1)y + (6,3)$	[168,164,3]	$\left[[168,160,3]\right]_7$	4
5	$(1,1)y + (8,2)$	[20,16,3]	$\left[[20,12,3]\right]_{11}$	4
8	$(1,1)y^2 + (8,0)y + (10,1)$	[32,24,4]	$\left[[32,16,4]\right]_{11}$	10
15	$(1,1)y^2 + (3,9)y + (1,4)$	[60,52,4]	$\left[[60,44,4]\right]_{11}$	10
22	$(1,1)y + (1,10)$	[88,84,3]	$\left[[88,80,3]\right]_{11}$	4
28	$(0,1)y^2 + (1,1)y + (10,1)$	[132,125,4]	$\left[[132,118,4]\right]_{11}$	8
12	$(1,1)y + (1,2)$	[48,44,3]	$\left[[48,40,3]\right]_{13}$	4
26	$(1,1)y + (1,2)$	[104,100,3]	$\left[[104,96,3]\right]_{13}$	4
39	$(1,1)y + (12,4)$	[156,152,3]	$\left[[156,148,3]\right]_{13}$	4

6. Conclusion

The primary objective of this research is to leverage the computer algebra system Magma for the generation of quantum error-correcting codes (QECCs) exhibiting parameters $\left[[n,k,d]\right]_p$ derived from cyclic codes over $\mathcal{R}$. The code's quantum Singleton bound (QSB) is defined as $2d \leq n + 2 - k$, while the quantum Singleton defect is computed as $n + 2 - k - 2d$. Consequently, the evaluation of the quantum codes is based on their quantum Singleton defect across $\mathcal{F}_p \times (\mathcal{F}_p + \alpha\mathcal{F}_p + \alpha^2\mathcal{F}_p)$, as illustrated in Tables 1 for p values of 3, 5, 7, 11, and 13.

References

[1] Aly, Salah A., Andreas Klappenecker, and Pradeep Kiran Sarvepalli. "On quantum and classical BCH codes." *IEEE Transactions on Information Theory* 53, no. 3, 1183-1188 (2007).

[2] Ashraf, Mohammad, and Ghulam Mohammad. "Quantum codes from cyclic codes over $F_3 + vF_3$." *International Journal of Quantum Information* 12, no. 06, 1450042 (2014).

[3] Ashraf, Mohammad, and Ghulam Mohammad. "Construction of quantum codes from cyclic codes over $F_p + vF_p$." *International Journal of Infor. and Coding Theory* 3, no. 2, 137-144 (2015).

[4] Bag, Tushar, Ashish K. Upadhyay, Mohammad Ashraf, and Ghulam Mohammad. "Quantum codes from cyclic codes over the ring $F_p\ [u]/\langle u^3 - u\rangle$." *Asian-European Journal of Mathematics* 12, no. 07, 2050008 (2019).

[5] Bosma, Wieb, John Cannon, and Catherine Playoust. "The Magma algebra system I: The user language." *Journal of Symbolic Computation* 24, no. 3-4, 235-265 (1997).

[6] Çalışkan, Fatma, and Refia Aksoy. "Linear codes over $F_2 \times (F_2 + vF_2)$ and the MacWilliams identities." *Applicable Algebra in Engineering, Communication and Computing* 31, no. 2 : 135-147 (2020).

[7] Calıskana, Fatma, and Refia Aksoyb. "Cyclic codes over $F_2 \times (F_2 + vF_2)$ and binary quantum codes." *Filomat* 37, no. 15, 5137-5147 (2023).

[8] Çalışkan, Fatma, Tülay Yıldırım, and Refia Aksoy. "Non-Binary Quantum Codes from Cyclic Codes over $F_p \times (F_p + vF_p)$." *International Journal of Theoretical Physics* 62, no. 2, 29 (2023).

[9] Calderbank, A. Robert, Eric M. Rains, Peter M. Shor, and Neil JA Sloane. "Quantum error correction via codes over GF (4)." *IEEE Transactions on Information Theory* 44, no. 4, 1369-1387 (1998).

[10] Dinh, Hai Q. "Constacyclic codes of length p^s over $F_{p^m} + uF_{p^m}$." *Journal of Algebra* 324, no. 5 940-950 (2010).

[11] Gao, Jian. "Quantum codes from cyclic codes over $F_q + vF_q + v^2 F_q + v^3 F_q$." *International Journal of Quantum Information* 13, no. 08, 1550063 (2015).

[12] Gao, Yun, Jian Gao, and Fang-Wei Fu. "Quantum codes from cyclic codes over the ring $F_q + v_1 F_q + v_2 F_q + ... + v_r F_q$." *Applicable Algebra in Engineering, Communication and Computing* 30, 161-174 (2019).

[13] Gao, Jian, and Yongkang Wang. "u-Constacyclic codes over $F_p + vF_p$ and their applications of constructing new non-binary quantum codes." *Quantum Information Processing* 17, 1-9 (2018).

[14] Gao, Jian, and Yongkang Wang. "New non-binary quantum codes derived from a class of linear codes." *IEEE Access* 7, 26418-26421 (2019).

[15] Gao, Jian. "Some results on linear codes over $F_p + uF_p + u^2 F_p$." *Journal of Applied Mathematics & Computing* 47, no. 1-2, 473 (2015).

[16] Hammons, A. Roger, P. Vijay Kumar, A. Robert Calderbank, Neil JA Sloane, and Patrick Solé. "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes." *IEEE Transactions on Information Theory* 40, no. 2, 301-319 (1994).

[17] H. Islam, O. Prakash, and D. K. Bhunia, "Algebraic structure of cyclic codes over M3(Fp)," *J. Discret. Math. Sci. Cryptogr.,* 27, no. 1, pp. 189–201 (2024).

[18] La Guardia, Giuliano G., and Reginaldo Palazzo Jr. "Constructions of new families of nonbinary CSS codes." *Discrete mathematics* 310, no. 21, 2935-2945 (2010).

[19] Mohammed, Mohanad Ali, Ameer J. Munshid, and Mehdi Alaeiyan. "Cyclic codes of length p_n over Z_{p^m}" *Journal of Discrete Mathematical Sciences and Cryptography* 24, no. 2, 579-588 (2021).

[20] Shor, Peter W. "Scheme for reducing decoherence in quantum computer memory." *Physical review* A 52, no. 4, R2493 (1995).

Received October, 2023