On Quantum Codes over Non Local Rings

NOUREDDINE ESSAIDI[1], ABDELHAMID TADMORI[1], OSSAMA EL ABOUTI[2]

[1]Department of Mathematics and Informatics,
University Abdelmalek Essaadi, Faculty of Sciences and Technology Al Hoceima,
BP 34. Ajdir 32003 Al Hoceima,
MOROCCO

[2]Department of Physics,
University Abdelmalek Essaadi, Faculty of Sciences and Technology Al Hoceima,
BP 34. Ajdir 32003 Al Hoceima,
MOROCCO

Abstract: We study the structural properties of the ring $\mathcal{R} = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p$, where $p \neq 2$ is a prime and $u^4 = u^3$, as well as the linear codes over R. We investigate the generator's cyclic codes and their dual codes over R. An isometric Gray map from R to $\mathbb{F}_p^4$ is defined. We offer an equivalence condition that cyclic codes must satisfy over R in order to include their dual. Moreover, we establish the existence of quantum error-correcting codes based on cyclic codes over R. Finally, under various criteria such as cyclic codes length and generator polynomial degree, we build quantum error-correcting codes over $\mathcal{R}$ which their dimensions are divided by p and 2^4.

Key-Words: - Gray map, cyclic codes, non local finite rings, self-dual codes, Quantum codes

Received: May 16, 2022. Revised: August 18, 2023. Accepted: October 17, 2023. Available online: December 5, 2023.

1 Introduction

Over the past few years, quantum error-correcting codes have attracted a great deal of curiosity from researchers, especially over finite rings. Without losing meaning, we will denote them by **QECC**. A significant benefit of these codes is their exceptional adaptability to quantum physical systems of any order. In addition, finite rings make it less difficult to perform operations. The conventional error-correcting codes are necessary to prevent decoherence and other noise from destroying the classical information, but such information may also be duplicated. Similarly, the existence of QECC supplies a powerful manner to avoid decoherence and other quantum noise during quantum communication and quantum computation. We suggest the reader to [1], [2] and [3], for further information on information theory and coding theory over finite rings.

Cyclic codes have shown to be an excellent resource for developing QECC with appropriate parameters. In [4], the author led the development of the first QECC. Motivated by this discovery, the researcher, [5], gives a method of construction QECC over finite field $\mathbb{F}_q$, with hypothesis that q is a prime number power. After that, the authors, [6], proposed a technique for building QECC based on conventional error-correcting codes. Recently, QECC theory has advanced quickly. Many QECC were created by various researchers, [7], [8], [9], [10], [11], using classical codes with good parameters and properties of self-orthogonal or dual. Researchers have shown a strong interest in investigating the built of QECC over finite rings by using cyclic codes. Across a variety of finite rings, several QECC constructed from cyclic codes have been developed, more precisely, over finite non-chain ring. In [12], the author worked over $\mathbb{F}_p[v]/(v^2 - v)$ to construct linear codes. Later on, the paper, [13], examined the linear codes structure over the finite non-chain ring $\mathbb{F}_p[u]/(u^3 - u)$, where $p > 2$ is a prime, the building of QECC over $\mathbb{F}_q[v]/(v^4 - v)$ via cyclic codes, with p is assumed to be an odd prime, $(p - 1)$ is divisible by 3 and $q = p^r$, is given in [14]. Some new QECC based on cyclic codes over the finite ring $\mathbb{F}_2[u, v]/(u^2 - u, v^2 - v, uv - vu)$ are presented by the authors of the paper, [15], later on, they generalized in [16], the creating of QECC over $\mathbb{F}_2[v_1, v_2, \ldots, v_r]/(v_i^2 - v_i, v_iv_j - v_jv_i)$ where $1 \leq i, j \leq r$ for $r \geq 1$, by using cyclic codes. The building of QECC based on cyclic codes of length not divisible by two over the chain ring $\mathbb{F}_2[u]/(u^2)$ is provided in [17]. Further, [18], provided a building of QECC using cyclic codes of length not divisible by two over the ring $\mathbb{F}_4[u]/(u^2)$. Again, a building of QECC over $\mathbb{F}_2[v]/(v^2 - v)$ by utilizing cyclic codes, was established in [19].

The theory of QECC was further advanced by several scientists, whose provided the building of QECC over the finite non-chain ring $\mathbb{F}_3[u]/(u^2-1)$ basing on cyclic codes in [20]. Then, over the ring $\mathbb{F}_p[v]/(v^2-v)$, they examined QECC derived from cyclic codes and they established the construction new non-binary QECC over the ring $\mathbb{F}_q[u,v]/(u^2-u, v^2-v, uv-vu)$ in [21], [22], respectively. The authors in [23], used cyclic codes that satisfy the condition of dual-containing, to produce novel QECC over the ring $\mathbb{F}_{2^m}[u]/(u^{k+1})$, where $m > 0$ is an integer. The creation of QECC over $\mathbb{F}_{p^m}[u]/(u^2)$, where p is a prime, from linear codes is presented in [24]. Based on this studies, [25], introduced several new non-binary QECC over the ring $\mathbb{F}_q[v]/(v^3-v)$, with assumption that $q=p^r$ and $p>2$ is a prime.
Researchers have recently focused on the structural characteristics of codes over mixed alphabets (the direct product of finite rings). [26], discovered QECC and LCD codes using mixed alphabets. QECC over mixed alphabets was constructed by [27]. The researchers , [28], provide non-binary QECC across mixed alphabets. Inspired by these studies, we investigate the creation of QECC employing cyclic codes over the ring $\mathcal{R}$.
This paper's remaining sections are structured as below: In sect. 2, fundamental facts about the ring $\mathcal{R}$ are presented. In sect. 3, an equivalent condition of self-duality verified by a linear code, is provided, along with some helpful results on linear codes over this ring. In sect. 4, the definition of the Gray map is introduced and a method for representing codes that equal their dual over $\mathbb{F}_p$ to be the images of linear codes by this map over $\mathcal{R}$, is provided. In sect. 5, cyclic codes' characterisation over the ring $\mathcal{R}$ is covered, where we also provide a condition that is equivalent to dual containing verified by cyclic codes over $\mathcal{R}$. In sect. 6, we provide the characteristics of a QECC basing on cyclic codes over $\mathcal{R}$.

2 Preliminaries

In this work, consider a prime p where $p \neq 2$ and $\mathbb{F}_p$ represent a finite field, the ring $\mathbb{F}_p[u] = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p[u]$ is denoted by $\mathcal{R}$ where u is an indeterminate with $u^4 = u^3$.
The following facts provide some fundamental characteristics of $\mathcal{R}$, which will be employed in the parts that follow:

1. For any element $\alpha \in \mathcal{R}$, there exist δ, σ, ρ, $\lambda \in \mathbb{F}_p$, so we can represent α as $\alpha = \delta + \sigma u + \rho u^2 + \lambda u^3$.

2. Recall that $\mathcal{R}$ and $\mathbb{F}_p[X]/(X^4 - X^3)$ are isomorphic as rings. Besides that, the finiteness and commutativity are verified by the ring $\mathcal{R}$, furthermore, it has identity and characteristic equals p. To prove this result, we need to construct a bijective ring homomorphism between them. In fact, we consider the map:

$$\begin{array}{rccc} \vartheta: & \mathbb{F}_p[X] & \longrightarrow & \mathbb{F}_p[u] \\ & P & \longmapsto & P(u). \end{array}$$

The fact that ϑ is a surjective homomorphism is obvious. It is still necessary to demonstrate that the kernel of ϑ is the ideal $(X^4 - X^3)$.
From the fact that u satisfies $u^4 = u^3$, it follows immediately that
$(X^4 - X^3) \subseteq \ker(\vartheta)$.
On other hand, Let $P \in \mathbb{F}_p[X]$ such that $\vartheta(P) = 0$ in $\mathcal{R}$. Then,
$0 = \vartheta(P) = P(u)$ which implies that P is divisible by $(X^4 - X^3)$. Therefore, $\ker(\vartheta) = (X^4 - X^3)$.
Thus, by the isomorphism theorem for rings, we have

$$\mathcal{R} \simeq \mathbb{F}_p[u],$$

where $u^4 = u^3$.

3. For any element $\alpha = \delta + \sigma u + \rho u^2 + \lambda u^3$ of $\mathcal{R}$, we have

$$\alpha \; is \; unit \Longleftrightarrow \left\{ \begin{array}{c} \delta \neq 0, \\ \delta + \sigma + \rho + \lambda \not\equiv 0 (mod\, p) \end{array} \right.$$

Moreover, from [13], we have $\mid \mathcal{R}^{\times} \mid = (p-1)^2$, where $\mathcal{R}^{\times}$ represents the group of units of $\mathcal{R}$.

4. Let $\alpha \in \mathcal{R}$, then

$$\alpha \in \mathcal{R} \backslash \mathcal{R}^{\times} \Longleftrightarrow \left\{ \begin{array}{c} \alpha = \sigma u + \rho u^2 + \lambda u^3 \\ or \\ \alpha = \delta + \sigma u + \rho u^2 - (\delta + \sigma + \rho) u^3 \end{array} \right.$$

where $(\delta, \sigma, \rho, \lambda) \in \mathbb{F}_p^4$. Basing on this fact, $\mathcal{R}$ is a semi-local ring.
Indeed, consider $\mathfrak{I}_1 = (\sigma u + \rho u^2 + \lambda u^3)$ and $\mathfrak{I}_2 = (\delta + \sigma u + \rho u^2 - (\delta + \sigma + \rho) u^3)$ to be two ideals of $\mathcal{R}$.
Since $\mathfrak{I}_1 \neq \mathcal{R}$ and $\mathfrak{I}_2 \neq \mathcal{R}$, then it is sufficient to show that $\mathfrak{I}_1 \cup \mathfrak{I}_2$ is not an ideal.
It is obvious that the elements of $\mathfrak{I}_1 \cup \mathfrak{I}_2$ are non invertible elements in $\mathcal{R}$.
Let consider $\delta, \sigma, \rho, a, b, c \in \mathbb{F}_p$, then we obtain

$$\delta + \sigma u + \rho u^2 - (\delta + \sigma + \rho) u^3 = au + bu^2 + cu^3$$

$$\Rightarrow \delta + (\sigma - a)u + (\rho - b)u^2 - (\delta + \sigma + \rho + c)u^3 = 0$$

$$\Rightarrow \left\{ \begin{array}{c} \delta = 0 \\ \sigma - a = 0 \\ \rho - b = 0 \\ \delta + \sigma + \rho + c = 0 \end{array} \right. \Rightarrow \left\{ \begin{array}{c} \delta = 0 \\ \sigma = a \\ \rho = b \\ \sigma + \rho = -c \end{array} \right.$$

As a result, we have $\mathfrak{I}_1 \cap \mathfrak{I}_2 = (au + bu^2 - cu^3)$. therefore $\mathfrak{I}_1 \cup \mathfrak{I}_2$ is not an ideal.
Consequently, $\mathfrak{I}_1$ and $\mathfrak{I}_2$ are two maximal ideals of $\mathcal{R}$. Then, we obtain the result.

5. According to ring theory, a commutative chain ring is a ring verifying that its ideals create a unique chain below the inclusion relation. Based on the previous result, we can see that the ideals of $\mathcal{R}$ do not create a chain because $\mathfrak{I}_1$ and $\mathfrak{I}_2$ are incomparable, implying that $\mathcal{R}$ is not a chain ring.

6. The ring $\mathcal{A} = \mathbb{F}_p[X]/(X^4 - X^3)$ is isomorphic to the direct product rings

$$\mathcal{A} \simeq \mathcal{A}_1 \times \mathcal{A}_2,$$

where $\mathcal{A}_1 = \mathbb{F}_p$ and $\mathcal{A}_2 = \mathbb{F}_p[v]/(v^3)$.

7. Let consider the following mapping:

$$\begin{array}{rccc} \pi_1 : & \mathcal{A} & \longrightarrow & \mathcal{A}_1 = \mathbb{F}_p \\ & \alpha = \delta + \sigma u + \rho u^2 + \lambda u^3 & \longmapsto & \delta + \sigma + \rho + \lambda \end{array}$$

and

$$\begin{array}{rccc} \pi_2 : & \mathcal{A} & \longrightarrow & \mathcal{A}_2 \\ & \alpha = \delta + \sigma u + \rho u^2 + \lambda u^3 & \longmapsto & \delta + \sigma v + \rho v^2, \end{array}$$

where $v^3 = 0$, then π_1 and π_2 are the surjective morphisms of rings.

8. Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two rings, such that

$$\mathcal{R}_1 = \{u^3.\alpha \mid \alpha \in \mathcal{A}\}$$

and

$$\mathcal{R}_2 = \{\delta + \sigma u + \rho u^2 - (\delta + \sigma + \rho)u^3 \mid (\delta, \sigma, \rho) \in \mathbb{F}_p^3\}.$$

The following mapping:

$$\begin{array}{rccc} \xi_1 : & \mathcal{R}_1 & \longrightarrow & \mathcal{A}_1 \\ & u^3.\alpha & \longmapsto & \delta + \sigma + \rho + \lambda, \end{array}$$

and

$$\xi_2 : \mathcal{R}_1 \longrightarrow \mathcal{A}_2$$
$$\delta + \sigma u + \rho u^2 - (\delta + \sigma + \rho)u^3 \longmapsto \delta + \sigma v + \rho v^2,$$

are the isomorphisms of rings.

9. From the facts above, we can deduce that

$$\mathcal{R} \simeq \mathbb{F}_p \times (\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p),$$

where $v^3 = 0$.

3 Linear codes over $\mathcal{R}$

From coding theory, a code $\mathfrak{C}$ that it is linear and its length equals n over $\mathcal{R}$, is characterized as an $\mathcal{R}$-submodule of $\mathcal{R}^n$. A codeword is every element $\mathfrak{w} \in \mathfrak{C}$.
Let $\mathfrak{w} = (\mathfrak{w}_0, \mathfrak{w}_1, \ldots, \mathfrak{w}_{n-1}) \in \mathfrak{C}$,

- The Hamming weight of $\mathfrak{w}$ is known to be $wt_H(\mathfrak{w}) = \mid \{i \mid \mathfrak{w}_i \neq 0\} \mid$, for $0 \leq i \leq n-1$.
- For an element $\alpha = \delta + \sigma u + \rho u^2 + \lambda u^3 \in \mathcal{R}$, its Lee weight can be given as $wt_L(\alpha) = wt_H(\delta, \sigma - \rho, \sigma + \rho - \lambda, \delta - \sigma + \rho + \lambda)$, where $wt_H(\gamma)$ is the Hamming weight of $\gamma = (\delta, \sigma - \rho, \sigma + \rho - \lambda, \delta - \sigma + \rho + \lambda)$ over $\mathbb{F}_p$.
- From previous definition, it can easily define the Lee weight of a vector $\mathfrak{z} = (\mathfrak{z}_0, \mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}) \in \mathcal{R}^n$ to be

$$wt_L(\mathfrak{z}) = \sum_{i=0}^{n-1} wt_L(\mathfrak{z}_i),$$

where $wt_L(\mathfrak{z}_i) = wt_L(\delta_i, \sigma_i - \rho_i, \sigma_i + \rho_i - \lambda_i, \delta_i - \sigma_i + \rho_i + \lambda_i)$ for $0 \leq i \leq n-1$.

- The number of places where two codewords $\mathfrak{x} = (\mathfrak{x}_0, \mathfrak{x}_1, \ldots, \mathfrak{x}_{n-1})$ and $\mathfrak{y} = (\mathfrak{y}_0, \mathfrak{y}_1, \ldots, \mathfrak{y}_{n-1})$ are different is called the Hamming distance, i.e $d_H(\mathfrak{x}, \mathfrak{y}) = \mid \{i \mid \mathfrak{x}_i \neq \mathfrak{y}_i\} \mid$.
- The Lee distance is provided by $d_L(\mathfrak{x}, \mathfrak{y}) = wt_L(\mathfrak{x} - \mathfrak{y})$, where $\mathfrak{x}$ and $\mathfrak{y}$ are elements of $\mathcal{R}^n$.
- The minimum Hamming distance of $\mathfrak{C}$ is $d(\mathfrak{C}) = \min\{wt_H(\mathfrak{w}) \mid 0 \neq \mathfrak{w} \in \mathfrak{C}\}$.
- The smallest $d_L(\mathfrak{x}, \mathfrak{y}) \neq 0$ present the minimum Lee distance of a code $\mathfrak{C}$, where $\mathfrak{x}, \mathfrak{y} \in \mathfrak{C}$. The minimum Lee weight, on the other hand, is the codeword with the least nonzero Lee weight.

Given that $\mathfrak{C}$ is linear, it result that there is equality between the minimum Lee distance and the minimum Lee weight.
Recall that

$$< \mathfrak{x}, \mathfrak{y} >_{\mathcal{R}^n} = \sum_{i=1}^{n} \mathfrak{x}_i \mathfrak{y}_i,$$

is the definition of the Euclidean inner product of two components $\mathfrak{x} = (\mathfrak{x}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_n)$ and $\mathfrak{y} = (\mathfrak{y}_1, \mathfrak{y}_2, \ldots, \mathfrak{y}_n)$ in $\mathcal{R}^n$.
If $< \mathfrak{x}, \mathfrak{y} >_{\mathcal{R}^n}$ equals zero, implies that they are orthogonal.
The set

$$\mathfrak{C}^{\perp} = \{\mathfrak{x} \in \mathcal{R}^n \mid < \mathfrak{x}, \mathfrak{y} >_{\mathcal{R}^n} = 0, \ \forall \mathfrak{y} \in \mathfrak{C}\},$$

represents the dual of $\mathfrak{C}$.
The condition $\mathfrak{C} \subset \mathfrak{C}^{\perp}$ implies that $\mathfrak{C}$ satisfy the self-orthogonality and verifying the self-duality if there is equality.
Now, consider a code $\mathfrak{C}$ over the product ring $\mathbb{F}_p \times (\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)$ with assumption that it is linear and its length is n. Hence, $\mathfrak{C}$ is represented to be $(\mathfrak{C}_1, \mathfrak{C}_2)$, where the codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are considered over the rings $\mathbb{F}_p$ and $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, respectively. Moreover, they are linear and their length is n.
Furthermore, $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are expressed in the manner that follow:

$$\mathfrak{C}_1 = \{\mu \in \mathbb{F}_p^n \mid (\mu, 0) \in \mathfrak{C}\}$$

and

$$\mathfrak{C}_2 = \{\nu \in (\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)^n \mid (0, \nu) \in \mathfrak{C}\}.$$

As a result, $\mathfrak{C}$ is presented by the direct sum of $\mathfrak{C}_1$ and $\mathfrak{C}_2$, with denotation $\mathfrak{C} = \mathfrak{C}_1 \oplus \mathfrak{C}_2$, and each codeword in $\mathfrak{C}$ is uniquely written as

$$\mathfrak{w} = (\mathfrak{r}, \mathfrak{s} + \mathfrak{t}v + \mathfrak{l}v^2),$$

where $\mathfrak{r}, \mathfrak{s}, \mathfrak{t}, \mathfrak{l} \in \mathbb{F}_p^n$.
The generator matrices $\mathcal{G}_1$ and $\mathcal{G}_2$ are assumed corresponding to $\mathfrak{C}_1$ and $\mathfrak{C}_2$, respectively. Since $\mathfrak{C}$ is a $\mathcal{R}$-module, hence, the matrix $\mathcal{G}$ generating $\mathfrak{C}$ is represented as follows

$$\mathcal{G} = \begin{pmatrix} \mathcal{G}_1 \\ \mathcal{G}_2 \end{pmatrix}. \tag{1}$$

Lemma 1 *Given a code $\mathfrak{C} = \mathfrak{C}_1 \oplus \mathfrak{C}_2$ that supposed linear and its length is n over $\mathcal{R}$. Then,*

$$\mathfrak{C}^{\perp} = \mathfrak{C}_1^{\perp} \oplus \mathfrak{C}_2^{\perp}.$$

In addition, the next propositions are equivalents:

1. *$\mathfrak{C}$ satisfy the self-orthogonality over $\mathcal{R}$.*
2. *The self-orthogonality is verified respectively by $\mathfrak{C}_1$ and $\mathfrak{C}_2$ over the rings $\mathbb{F}_p$ and $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$.*

Proof 1 *Suppose that $\mathfrak{C}_1$ satisfy the self-orthogonality over $\mathbb{F}_p$ i.e $\mathfrak{C}_1 \subseteq \mathfrak{C}_1^{\perp}$ and satisfied by $\mathfrak{C}_2$ over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ i.e $\mathfrak{C}_2 \subseteq \mathfrak{C}_2^{\perp}$. Since $\mathfrak{C}$ is expressed as $(\mathfrak{C}_1, \mathfrak{C}_2)$, moreover, $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are linear , then $\mathfrak{C} \subseteq \mathfrak{C}^{\perp}$.*
Conversely, let $\mathfrak{w} = (\mathfrak{r}, \mathfrak{s} + \mathfrak{t}v + \mathfrak{l}v^2) \in \mathfrak{C}$, assuming the self-orthogonality of $\mathfrak{C}$ over $\mathcal{R}$, we get via Euclidian inner product:

$$< \mathfrak{w}, \mathfrak{w} >_{\mathcal{R}^n} = < (\mathfrak{r}, \mathfrak{s}+\mathfrak{t}v+\mathfrak{l}v^2), (\mathfrak{r}, \mathfrak{s}+\mathfrak{t}v+\mathfrak{l}v^2) >_{\mathcal{R}^n}$$

$$= << \mathfrak{r}, \mathfrak{r} >_{\mathbb{F}_p^n}, < \mathfrak{s}+\mathfrak{t}v+\mathfrak{l}v^2, \mathfrak{s}+\mathfrak{t}v+\mathfrak{l}v^2 >_{(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)^n} >$$

$$= 0.$$

Hence, $< \mathfrak{r}, \mathfrak{r} >_{\mathbb{F}_p^n} = 0$ and $< \mathfrak{s} + \mathfrak{t}v + \mathfrak{l}v^2, \mathfrak{s} + \mathfrak{t}v + \mathfrak{l}v^2 >_{(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)^n} = 0$, which implies that $\mathfrak{r} \in \mathfrak{C}_1^{\perp}$, and $\mathfrak{s} + \mathfrak{t}v + \mathfrak{l}v^2 \in \mathfrak{C}_1^{\perp}$. Thus, $\mathfrak{C}_1 \subseteq \mathfrak{C}_1^{\perp}$ and $\mathfrak{C}_2 \subseteq \mathfrak{C}_2^{\perp}$.

From literature, we recall the definition of the dimension of $\mathfrak{C}$ over $\mathcal{R}$ as follow:
The dimension of $\mathfrak{C}$ is the maximum number of linearly independent codewords in $\mathfrak{C}$. In other words

$$|\mathfrak{C}| = \max\{|\mathcal{F}|; \mathcal{F} \subseteq \mathfrak{C}\},$$

where $\mathcal{F} = \{\mathfrak{w}_1, \mathfrak{w}_2, \ldots, \mathfrak{w}_j\}$ is a set of linearly independent codewords of $\mathfrak{C}$.

4 Gray map over $\mathcal{R}$

From section 2, every element $\alpha \in \mathcal{R}$ is represented by the expression $\alpha = \delta + \sigma u + \rho u^2 + \lambda u^3$, where $\delta, \sigma, \rho, \lambda \in \mathbb{F}_p$. The following map is known as Gray map on $\mathcal{R}$:

$$\begin{array}{rccc} \Gamma: & \mathcal{R} & \longrightarrow & \mathbb{F}_p^4 \\ & \alpha & \longmapsto & (\delta, \sigma - \rho, \sigma + \rho - \lambda, \delta - \sigma + \rho + \lambda). \end{array}$$

Clearly, Γ is linear and an $\mathbb{F}_p$-module isomorphism. Similarly, the Gray map Γ is extended naturally to $\mathcal{R}^n$ by the following manner:

$$\begin{array}{rccc} \Gamma: & \mathcal{R}^n & \longrightarrow & \mathbb{F}_p^{4n} \\ & (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) & \longmapsto & (\beta_0, \beta_1, \ldots, \beta_{n-1}), \end{array}$$

where $\alpha_i = \delta_i + \sigma_i u + \rho_i u^2 + \lambda_i u^3$ and $\beta_i = (\delta_i, \sigma_i - \rho_i, \sigma_i + \rho_i - \lambda_i, \delta_i - \sigma_i + \rho_i + \lambda_i)$ for $i = 0, 1, \ldots, n-1$.
In the same way that the matrix generating $\mathfrak{C}$ over $\mathcal{R}$ is given in (1). As a $\mathcal{R}$-module isomorphism, the following matrix generate $\Gamma(\mathfrak{C})$ (Gray image of $\mathfrak{C}$) as below:

$$\Gamma(G) = \begin{pmatrix} \Gamma(G_1) \\ \Gamma(G_2) \end{pmatrix}.$$

According to the definition of Γ on $\mathcal{R}^n$ the following facts are evident:

Lemma 2 *[13] Γ is an isometry from $\mathcal{R}^n$ (Lee distance) to $\mathbb{F}_p^{4n}$ (Hamming distance). Moreover, Γ is $\mathbb{F}_p$-linear.*

Lemma 3 *[13, 21] Consider a code $\mathfrak{C}$ that supposed linear and characterized by length n, dimension $|\mathcal{C}| = p^k$ and the minimum Lee distance d_L over $\mathcal{R}$. It result that the code $\Gamma(\mathfrak{C})$ is linear and parameterized by length $4n$, dimension k and the minimum Hamming distance d_H over $\mathbb{F}_p$, where $d_H = d_L$.*

Proof 2 *Clearly, $\Gamma(\mathfrak{C})$ is a linear code over $\mathbb{F}_p$, according to $\mathbb{F}_p$-linearity of Γ from lemma 2. Furthermore, the construction of Γ implies that $\Gamma(\mathfrak{C})$ is an*

element of $\mathbb{F}_p^{4n}$ *then its length is* $4n$. *It is evident that* Γ *is a bijective map from* $\mathcal{R}^n$ *to* $\mathbb{F}_p^{4n}$, *hence, the dimension of* $\Gamma(\mathfrak{C})$ *equals* $v_p(|\ \mathfrak{C}\ |) = k$, *where* v_p *is the* p*-adic valuation.*
From the above lemma, the preserving distance of Γ *ensure that the minimum distance of* $\Gamma(\mathfrak{C})$ *is* $d_H = d_L$.

Theorem 1 *[13] Let a code* $\mathfrak{C}$ *that supposed linear over* $\mathcal{R}$ *and characterized as in Lemma 3. Then*

$$\begin{array}{c} \mathfrak{C}\ satisfy\ the\ self-duality\ over\ \mathcal{R} \\ \Downarrow \\ \Gamma(\mathfrak{C})\ satisfy\ the\ self-duality\ over\ \mathbb{F}_p. \end{array}$$

Moreover, the dual of $\Gamma(\mathfrak{C})$ *equals* $\Gamma(\mathfrak{C}^{\perp})$.

5 Cyclic codes over $\mathcal{R}$

Now, we introduce a few essential structural facts about cyclic codes over $\mathcal{R}$, that will be useful in building of the appropriate QECC.
A code $\mathfrak{C}$ that it is linear and its length is n over $\mathcal{R}$ is known as cyclic if it satisfies the following condition: for each codeword $\mathfrak{w} = (\mathfrak{w}_0, \mathfrak{w}_1, \ldots, \mathfrak{w}_{n-1}) \in \mathfrak{C}$, the codeword $\widehat{\mathfrak{w}} = (\mathfrak{w}_{n-1}, \mathfrak{w}_0, \ldots, \mathfrak{w}_{n-2}) \in \mathfrak{C}$.
From literature, the fact that $\mathfrak{C}$ is a cyclic code of length n over $\mathcal{R}$ equivalent to $\mathfrak{C}$ is viewed as an ideal in the polynomial ring $\widetilde{\mathcal{R}} = \mathcal{R}[\varepsilon]/(\varepsilon^n - 1)$ by the following $\mathcal{R}$-module isomorphism:

$$\begin{array}{rccc} \varphi: & \mathcal{R}^n & \to & \widetilde{\mathcal{R}} = \mathcal{R}[\varepsilon]/(\varepsilon^n - 1) \\ & \mathfrak{w} & \mapsto & \mathfrak{w}_0 + \mathfrak{w}_1\varepsilon + \ldots + \mathfrak{w}_{n-1}\varepsilon^{n-1} + (\varepsilon^n - 1) \end{array}$$

In fact, it is sufficient that we write each $\mathfrak{w} = (\mathfrak{w}_0, \mathfrak{w}_1, \ldots, \mathfrak{w}_{n-1}) \in \mathfrak{C}$ as polynomial $\mathfrak{w}(\varepsilon) = \mathfrak{w}_0 + \mathfrak{w}_1\varepsilon + \ldots + \mathfrak{w}_{n-1}\varepsilon^{n-1} \in \mathcal{R}[\varepsilon]$, which called the associated polynomial of $\mathfrak{C}$. Then, we can write $\widehat{\mathfrak{w}} = (\mathfrak{w}_{n-1}, \mathfrak{w}_0, \ldots, \mathfrak{w}_{n-2})$ as $\widehat{\mathfrak{w}}(\varepsilon) = \mathfrak{w}_{n-1} + \mathfrak{w}_0\varepsilon + \ldots + \mathfrak{w}_{n-2}\varepsilon^{n-1} \in \mathcal{R}[\varepsilon]$ and we obtain $\widehat{\mathfrak{w}}(\varepsilon) = \mathfrak{w}(\varepsilon)\varepsilon - \mathfrak{w}_{n-1}(\varepsilon^n - 1)$, it results that

$$\widehat{\mathfrak{w}}(\varepsilon) \equiv \mathfrak{w}(\varepsilon)\varepsilon\ mod\ (\varepsilon^n - 1).$$

Furthermore, it is easily seen that

$$\mathfrak{w}(\varepsilon) \in \mathfrak{C} mod(\varepsilon^n - 1) \Longleftrightarrow \mathfrak{w}(\varepsilon)\varepsilon \in \mathfrak{C} mod(\varepsilon^n - 1).$$

We repeat this procedure, we get

$$\mathfrak{w}(\varepsilon)\varepsilon \in \mathfrak{C} mod(\varepsilon^n - 1) \Longleftrightarrow \mathfrak{w}(\varepsilon)\varepsilon^2 \in \mathfrak{C} mod(\varepsilon^n - 1).$$

By induction steps, it results that $\mathfrak{w}(\varepsilon)\varepsilon^i \in \mathfrak{C}\ mod\ (\varepsilon^n - 1)$, for all $i \in \mathbb{N}$.
This leads us to the conclusion that a code $\mathfrak{C}$ with assumption that it is linear and its length is n, is considered cyclic over $\mathcal{R}$ equivalent to $\varphi(\mathfrak{C})$ is an ideal of $\widetilde{\mathcal{R}}$.
The following results are required for the next part.

Lemma 4 *Consider a code* $\mathfrak{C} = \mathfrak{C}_1 \oplus \mathfrak{C}_2$ *with assumption that it is linear and its length is* n *over* $\mathcal{R}$. *Hence, the following equivalence holds:*

$$\begin{array}{c} \mathfrak{C}\ is\ cyclic\ over\ \mathcal{R} \\ \Updownarrow \\ \left\{ \begin{array}{c} The\ codes\ \mathfrak{C}_1\ and\ \mathfrak{C}_2\ are\ cyclic\ over\ the \\ rings\ \mathbb{F}_p\ and\ \mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p,\ resp. \end{array} \right. \end{array}$$

Proof 3 *Let* $(\mathfrak{r}_0, \mathfrak{r}_1, \ldots, \mathfrak{r}_{n-1}) \in \mathfrak{C}_1$ *and* $(\mathfrak{s}_0 + \mathfrak{t}_0 v + \mathfrak{l}_0 v^2, \mathfrak{s}_1 + \mathfrak{t}_1 v + \mathfrak{l}_1 v^2, \ldots, \mathfrak{s}_{n-1} + \mathfrak{t}_{n-1} v + \mathfrak{l}_{n-1} v^2) \in \mathfrak{C}_2$. *Assume that the cyclicity is verified by* $\mathfrak{C}_1$ *over* $\mathbb{F}_p$ *and by* $\mathfrak{C}_2$ *over* $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$. *We consider an element* $\mathfrak{w} = (\mathfrak{w}_0, \mathfrak{w}_1, \ldots, \mathfrak{w}_{n-1})$ *of* $\mathfrak{C}$, *where* $\mathfrak{w}_i = (\mathfrak{r}_i, \mathfrak{s}_i + \mathfrak{t}_i v + \mathfrak{l}_i v^2)$, *for* $i = 0, 1, \ldots, n-1$. *We deduce that*
$(\mathfrak{w}_{n-1}, \mathfrak{w}_0, \ldots, \mathfrak{w}_{n-2}) = (\mathfrak{r}_{n-1}, \mathfrak{r}_0, \ldots, \mathfrak{r}_{n-2}) + (\mathfrak{s}_{n-1} + \mathfrak{t}_{n-1} v + \mathfrak{l}_{n-1} v^2, \mathfrak{s}_0 + \mathfrak{t}_0 v + \mathfrak{l}_0 v^2, \ldots, \mathfrak{s}_{n-2} + \mathfrak{t}_{n-2} v + \mathfrak{l}_{n-2} v^2)$.
Since $(\mathfrak{r}_{n-1}, \mathfrak{r}_0, \ldots, \mathfrak{r}_{n-2}) \in \mathfrak{C}_1$ *and* $(\mathfrak{s}_{n-1} + \mathfrak{t}_{n-1} v + \mathfrak{l}_{n-1} v^2, \mathfrak{s}_0 + \mathfrak{t}_0 v + \mathfrak{l}_0 v^2, \ldots, \mathfrak{s}_{n-2} + \mathfrak{t}_{n-2} v + \mathfrak{l}_{n-2} v^2) \in \mathfrak{C}_2$, *then*

$$(\mathfrak{w}_{n-1}, \mathfrak{w}_0, \ldots, \mathfrak{w}_{n-2}) \in \mathfrak{C}_1 \oplus \mathfrak{C}_2 = \mathfrak{C},$$

as a result, $\mathfrak{C}$ *is a cyclic code over* $\mathcal{R}$.
On other hand, suppose that $\mathfrak{w}_i = (\mathfrak{r}_i, \mathfrak{s}_i + \mathfrak{t}_i v + \mathfrak{l}_i v^2)$, *for* $i = 0, 1, \ldots, n-1$. *Then* $(\mathfrak{w}_0, \mathfrak{w}_1, \ldots, \mathfrak{w}_{n-1})$ *is an element of* $\mathfrak{C}$. *According to the hypothesis,* $\mathfrak{C}$ *is a cyclic code over* $\mathcal{R}$, *hence* $(\mathfrak{w}_{n-1}, \mathfrak{w}_0, \ldots, \mathfrak{w}_{n-2}) \in \mathfrak{C}$. *Furthermore,*
$(\mathfrak{w}_{n-1}, \mathfrak{w}_0, \ldots, \mathfrak{w}_{n-2}) = (\mathfrak{r}_{n-1}, \mathfrak{r}_0, \ldots, \mathfrak{r}_{n-2}) + (\mathfrak{s}_{n-1} + \mathfrak{t}_{n-1} v + \mathfrak{l}_{n-1} v^2, \mathfrak{s}_0 + \mathfrak{t}_0 v + \mathfrak{l}_0 v^2, \ldots, \mathfrak{s}_{n-2} + \mathfrak{t}_{n-2} v + \mathfrak{l}_{n-2} v^2)$.
It results that $(\mathfrak{r}_{n-1}, \mathfrak{r}_0, \ldots, \mathfrak{r}_{n-2}) \in \mathfrak{C}_1$ *and* $(\mathfrak{s}_{n-1} + \mathfrak{t}_{n-1} v + \mathfrak{l}_{n-1} v^2, \mathfrak{s}_0 + \mathfrak{t}_0 v + \mathfrak{l}_0 v^2, \ldots, \mathfrak{s}_{n-2} + \mathfrak{t}_{n-2} v + \mathfrak{l}_{n-2} v^2) \in \mathfrak{C}_2$, *which ensure the result.*

In the following parts, we set a code $\mathfrak{C} = \mathfrak{C}_1 \oplus \mathfrak{C}_2$ over $\mathcal{R}$ that supposed cyclic and its length equals n. The result below gives the polynomial generating $\mathfrak{C}$ over $\mathcal{R}$.

Theorem 2 *A unique polynomial* $\chi(\varepsilon) \in \mathcal{R}[\varepsilon]$ *exists and generating* $\mathfrak{C}$ *as:*

$$\begin{array}{rcl} \mathfrak{C} & = & (\chi(\varepsilon)) \\ & = & (\chi_1(\varepsilon), \chi_2(\varepsilon) + v\chi_3(\varepsilon) + v^2\chi_4(\varepsilon)), \end{array}$$

where the polynomial $\chi_1(\varepsilon)$ *generate* $\mathfrak{C}_1$ *over* $\mathbb{F}_p$ *and the polynomial* $\chi_2(\varepsilon) + v\chi_3(\varepsilon) + v^2\chi_4(\varepsilon)$ *generate* $\mathfrak{C}_2$ *over* $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$. *Additionally,* $\varepsilon^n - 1$ *is divided by* $\chi(\varepsilon)$ *over* $\mathcal{R}$.

Proof 4 *The existence and uniqueness of* $\chi(\varepsilon)$ *are ensured by that of* $\chi_1(\varepsilon)$, $\chi_2(\varepsilon)$, $\chi_3(\varepsilon)$ *and* $\chi_4(\varepsilon)$.
In fact, we know there are unique polynomials $\chi_1(\varepsilon)$,

$\chi_2(\varepsilon)$, $\chi_3(\varepsilon)$ and $\chi_4(\varepsilon)$ in $\mathbb{F}_p[\varepsilon]$ such that $\mathfrak{C}_1 = (\chi_1(\varepsilon))$ and $\mathfrak{C}_2 = (\chi_2(\varepsilon)+v\chi_3(\varepsilon)+v^2\chi_4(\varepsilon))$ where $\chi_i(\varepsilon)$ divides the polynomial ε^n-1 in $\mathbb{F}_p[\varepsilon]$ for $i = 1,2,3,4$ and $\chi_2(\varepsilon)+v\chi_3(\varepsilon)+v^2\chi_4(\varepsilon)$ divides the polynomial ε^n-1 in $(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)[\varepsilon]$. Hence

$$\begin{aligned}\mathfrak{C} &= (\mathfrak{C}_1, \mathfrak{C}_2)\\ &= (\chi_1(\varepsilon), \chi_2(\varepsilon)+v\chi_3(\varepsilon)+v^2\chi_4(\varepsilon))\\ &= (\chi(\varepsilon)),\end{aligned}$$

In conclusion, $\chi(\varepsilon)$ divides ε^n-1 over $\mathcal{R}$.

Remark 1 *The fact that $\mathfrak{C} = \mathfrak{C}_1 \oplus \mathfrak{C}_2$ and $\mathfrak{C}_1 = (\chi_1(\varepsilon))$ and $\mathfrak{C}_2 = (\chi_2(\varepsilon)+v\chi_3(\varepsilon)+v^2\chi_4(\varepsilon))$, allows us to note that:*

1. $$\begin{aligned}|\ \mathfrak{C}\ | &= |\ \mathfrak{C}_1\ ||\ \mathfrak{C}_2\ |\\ &= p^{n-deg(\chi_1(\varepsilon))}p^{3n-deg(\chi_2(\varepsilon))-deg(\chi_3(\varepsilon))-deg(\chi_4(\varepsilon))}\\ &= p^{4n-deg(\chi_1(\varepsilon))-deg(\chi_2(\varepsilon))-deg(\chi_3(\varepsilon))-deg(\chi_4(\varepsilon))}\end{aligned}$$
2. *From the existence and uniqueness of $\chi(\varepsilon)$, we can deduce that every ideal of $\widetilde{\mathcal{R}}$ is principal, $\widetilde{\mathcal{R}}$ is principal.*

Recall that, the polynomial:

$$\phi^*(\varepsilon) = \varepsilon^{deg(\phi(\varepsilon))}\phi(\varepsilon^{-1}),$$

present the reciprocal of the polynomial $\phi(\varepsilon) = e_0 + e_1\varepsilon + \ldots + e_m\varepsilon^m$, where $e_i \in$ R for $0 \leq i \leq m$. Moreover, $\phi(\varepsilon)$ is called self-reciprocal if $\phi(\varepsilon) = \phi^*(\varepsilon)$.

Corollary 1 *[13] There exist polynomials $\phi_i(\varepsilon)$ divides ε^n-1, i.e. $\phi_i(\varepsilon)\chi_i(\varepsilon) = \varepsilon^n-1$ in $\mathbb{F}_p[\varepsilon]$, for $i = 1,2,3,4$, such that*

$$\begin{aligned}\mathfrak{C}^{\perp} &= (\phi(\varepsilon))\\ &= (\phi_1^*(\varepsilon), \phi_2^*(\varepsilon)+v\phi_3^*(\varepsilon)+v^2\phi_4^*(\varepsilon)),\end{aligned}$$

and $|\ \mathfrak{C}^{\perp}\ | = p^{deg(\chi_1(\varepsilon))+deg(\chi_2(\varepsilon))+deg(\chi_3(\varepsilon))+deg(\chi_4(\varepsilon))}$, where, $\phi_i^*(\varepsilon)$ is the reciprocal polynomials of $\phi_i(\varepsilon)$, for $i = 1,2,3,4$.

6 QECC from cyclic codes over $\mathcal{R}$

We start this part by presenting the CSS construction, which is a fundamental structure of QECC and was presented by Calderbank, Shor and Steane. Next, we give our contribution regarding QECC over $\mathcal{R}$.
The following arguments explain why creating QECC from cyclic codes over $\mathcal{R}$ is preferable: The ring $\mathcal{R}$ has some similar characteristics as the finite field $\mathbb{F}_p$. Furthermore, the ring $\mathcal{R}$ may be used to generate optimal cyclic codes. Since every ideal over $\tilde{\mathcal{R}}$ is principal, QECC of any length may be simply created. The number of cyclic codes over $\mathcal{R}$ for a particular length n is substantially more than those over finite field $\mathbb{F}_p$. In addition, cyclic codes over $\mathcal{R}$ can result in good QECC. We anticipate that cyclic codes over $\mathcal{R}$ will be an excellent source for creating excellent QECC.

Lemma 5 *[3] Consider two codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$, with assumption that they are linear over $\mathbb{F}_p$, where p is a prime and parameterized by $[n,k_1,d_1]_p$ and $[n,k_2,d_2]_p$, respectively, and satisfying the condition $\mathfrak{C}_2^{\perp} \subseteq \mathfrak{C}_1$. Moreover, let $d = \min\{wt(x) \mid x \in (\mathfrak{C}_1 \backslash \mathfrak{C}_2^{\perp}) \cup (\mathfrak{C}_2 \backslash \mathfrak{C}_1^{\perp})\}$ with $d \geq \min\{d_1,d_2\}$.
It result, the existence of a QECC over $\mathbb{F}_p$ is guaranteed and parameterized by length n, dimension k_1+k_2-n and minimum distance d.
Furthermore, if $\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1$, hence there exist a QECC over $\mathbb{F}_q$ characterized by length n, dimension $n-2k_1$ and minimum distance d_1, where $d_1 = \min\{wt(x) \mid x \in (\mathfrak{C}_1^{\perp} \backslash \mathfrak{C}_1)\}$.*

Calderbank and colleagues have provided an essential conclusion that establishes the equivalence condition verified by cyclic codes over finite fields of dual containing as follows:

Lemma 6 *[6] Consider a cyclic code $\mathfrak{C}_1$ over the finite field $\mathbb{F}_p$ and generated by the polynomial $\chi_1(\varepsilon)$. Then,*

$$\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1 \Longleftrightarrow \varepsilon^n-1 \equiv 0\ (mod\ \chi_1(\varepsilon)\chi_1^*(\varepsilon)),$$

where $\chi_1^*(\varepsilon)$ is the reciprocal polynomial of $\chi_1(\varepsilon)$.

In a similar manner, we can derive the following conclusion:

Lemma 7 *Consider a cyclic code $\mathfrak{C}_2$ over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ and generated by the polynomial $\chi_2(\varepsilon)+v\chi_3(\varepsilon)+v^2\chi_4(\varepsilon)$. Then,*

$$\mathfrak{C}_2^{\perp} \subseteq \mathfrak{C}_2 \Longleftrightarrow \varepsilon^n-1 \equiv 0\ (mod\ \chi_i(\varepsilon)\chi_i^*(\varepsilon)),$$

where $\chi_i^*(\varepsilon)$ is the reciprocal polynomial of $\chi_i(\varepsilon)$ for $i = 2,3,4$.

Proof 5 *The proof can be given by using the method in [6].*

Using the fact that $\mathfrak{C} = \mathfrak{C}_1 \oplus \mathfrak{C}_2$, the next theorem provides an equivalence condition satisfied by cyclic code of dual containing over $\mathcal{R}$.

Theorem 3 *Let $\mathcal{C}$ generated by the polynomial $\chi(\varepsilon)$. Then the following equivalence is established,*

$$\mathfrak{C}^{\perp} \subseteq \mathfrak{C} \Longleftrightarrow \begin{cases} \varepsilon^n-1 \equiv 0\ (mod\ \chi_1(\varepsilon)\chi_1^*(\varepsilon)) \\ \quad and \\ \varepsilon^n-1 \equiv 0\ (mod\ \chi_2(\varepsilon)\chi_2^*(\varepsilon)) \\ \quad and \\ \varepsilon^n-1 \equiv 0\ (mod\ \chi_3(\varepsilon)\chi_3^*(\varepsilon)) \\ \quad and \\ \varepsilon^n-1 \equiv 0\ (mod\ \chi_4(\varepsilon)\chi_4^*(\varepsilon)), \end{cases}$$

where $\chi_i^*(\varepsilon)$ is the reciprocal polynomial of $\chi_i(\varepsilon)$ for $i = 1, 2, 3, 4$.

Proof 6 *Via using Theorem 2, Lemma 6 and Lemma 7, the proof can be easily obtained.*

Definition 1 *A QECC $\mathcal{Q}$ over $\mathcal{R}$ of length n is a subspace of the tensor product $\mathcal{R}^{\otimes n}$. The encoding process is represented by an encoding map:*

$$\mathcal{E} : \mathcal{R}^{\otimes k} \longrightarrow \mathcal{Q},$$

which encodes k logical qubits into n physical qubits.

Based on lemma 5 and theorem 3, the next QECC construction can be derived.

Theorem 4 *Let $\Gamma(\mathfrak{C})$ the Gray image of $\mathfrak{C}$ characterized by length $4n$, dimension k and minimum distance d_L.*
Suppose that $\mathfrak{C}^{\perp} \subset \mathfrak{C}$, then the existence of a QECC over $\mathcal{R}$ is ensured and parameterized by length $4n$, dimension $2k - 4n$ and minimum distance d_L, where d_L denotes the minimum Lee distance of $\mathfrak{C}$.
We can denote the parameters of this QECC by $[4n, 2k - 4n, d_L]$ over $\mathcal{R}$.

Example 1 *Let $\mathcal{R} = \mathbb{F}_3 \times (\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_5)$, where $v^3 = 0$ and $n = 2^4$. Then, $\varepsilon^{2^4} - 1 = (\varepsilon + 1)(\varepsilon + 2)(\varepsilon^2 + 1)(\varepsilon^2 + \varepsilon + 2)(\varepsilon^2 + 2\varepsilon + 2)(\varepsilon^4 + \varepsilon^2 + 2)(\varepsilon^4 + 2\varepsilon^2 + 2)$ over $\mathbb{F}_3[\varepsilon]$. Let $\chi(\varepsilon) = (\chi_1(\varepsilon), \chi_2(\varepsilon) + v\chi_3(\varepsilon) + v^2\chi_4(\varepsilon))$ where $\chi_1(\varepsilon) = (\varepsilon^2 + 1)$ and $\chi_2(\varepsilon) = \chi_3(\varepsilon) = \chi_4(\varepsilon) = (\varepsilon^2 + \varepsilon + 2)$ and let a code $\mathfrak{C}$ that it is linear over $\mathcal{R}$, where*

$$\begin{aligned} \mathfrak{C} &= (\chi(\varepsilon)) \\ &= ((\chi_1(\varepsilon), \chi_2(\varepsilon) + v\chi_3(\varepsilon) + v^2\chi_4(\varepsilon))). \end{aligned}$$

Clearly, the code $\mathfrak{C}$ is cyclic, generated by $\chi(\varepsilon)$ over $\mathcal{R}$ and characterized by length 2^4, dimension $3^{2^3.3}$ and $d_L = 2$. Therefore, the code $\Gamma(\mathfrak{C})$ satisfy the linearity and parameterized by $[2^6, 2^3.3, 2]$ over $\mathbb{F}_3$. From Corollary 1, we can represent the dual code $\mathfrak{C}^{\perp}$ by

$$\mathfrak{C}^{\perp} = ((\phi_1^*(\varepsilon), \phi_2^*(\varepsilon) + v\phi_3^*(\varepsilon) + v^2\phi_4^*(\varepsilon))).$$

It result that $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$. Then, by Theorem 4, it is possible to construct a QECC parameterized by $[2^6, 2^4.3, 2]$ over $\mathbb{F}_3 \times (\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3)$.

Example 2 *Let $\mathcal{R} = \mathbb{F}_5 \times (\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5)$, where $v^3 = 0$ and $n = 2^6$. Then, $\varepsilon^{2^6} - 1 = (\varepsilon + 1)(\varepsilon + 2)(\varepsilon + 3)(\varepsilon + 4)(\varepsilon^2 + 2)(\varepsilon^2 + 3)(\varepsilon^4 + 2)(\varepsilon^4 + 3)(\varepsilon^8 + 2)(\varepsilon^8 + 3)(\varepsilon^{16} + 2)(\varepsilon^{16} + 3)$ over $\mathbb{F}_5[\varepsilon]$. Let $\chi(\varepsilon) = (\chi_1(\varepsilon), \chi_2(\varepsilon) + v\chi_3(\varepsilon) + v^2\chi_4(\varepsilon))$ where $\chi_1(\varepsilon) = (\varepsilon^2 + 2)$ and $\chi_2(\varepsilon) = \chi_3(\varepsilon) = \chi_4(\varepsilon) = (\varepsilon^2 + 3)$ and let a code $\mathfrak{C}$ that it is linear over $\mathcal{R}$, where*

$$\begin{aligned} \mathfrak{C} &= (\chi(\varepsilon)) \\ &= ((\chi_1(\varepsilon), \chi_2(\varepsilon) + v\chi_3(\varepsilon) + v^2\chi_4(\varepsilon))). \end{aligned}$$

Clearly, the code $\mathfrak{C}$ is cyclic, generated by $\chi(\varepsilon)$ over $\mathcal{R}$ and characterized by length 2^6, dimension $3^{2^3.31}$ and $d_L = 2$. Therefore, the code $\Gamma(\mathfrak{C})$ satisfy the linearity and parameterized by $[2^8, 2^3.31, 2]$ over $\mathbb{F}_5$. From Corollary 1, we can represent the dual code $\mathfrak{C}^{\perp}$ by

$$\mathfrak{C}^{\perp} = ((\phi_1^*(\varepsilon), \phi_2^*(\varepsilon) + v\phi_3^*(\varepsilon) + v^2\phi_4^*(\varepsilon))).$$

It result that $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$. Then, by Theorem 4, it is possible to construct a QECC parameterized by $[2^8, 2^4.3.5, 2]$ over $\mathbb{F}_5 \times (\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5)$.

7 Discussion

We used PARI GP and Magma to create some new QECC compared with pre-existing research. Table 1 (Appendix 8), Table 2 (Appendix 8), Table 3 (Appendix 8), Table 4 (Appendix 8), Table 5 (Appendix 8), Table 6 (Appendix 8), and Table 7 (Appendix 8), indicate our results of constructing QECC from cyclic codes over $\mathbb{F}_p \times (\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)$ for $3 \leq p \leq 19$, respectively. We varied i from 4 to 40 and we took $deg(\chi_j) = 2$ for $j = 1, 2, 3, 4$. As a result, we obtained QECC over $\mathbb{F}_p \times (\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)$ which its dimensions $2k$–$4n$ is divided by p and 2^4. The first column 2^i represents the length of cyclic code $\mathfrak{C}$ over $\mathbb{F}_p \times (\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)$, The parameters of the $\Gamma(\mathfrak{C})$ are denoted in the second column and the third column stands for the characteristics of the QECC over $\mathbb{F}_p \times (\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)$.

8 Conclusion

In this study, we use the Calderbank, Shor, and Steane (CSS) building to create QECC from cyclic codes over the finite nonlocal ring $\mathcal{R}$. In addition, we organize and provide several interesting examples. The results ensure that cyclic codes over finite nonlocal rings are an excellent resource for building QECC. This study is extremely important for quantum communication. We will build better QECC in the future using cyclic codes over-generalized finite nonlocal rings.

Acknowledgment:
The authors show their appreciation to the anonymous reviewers and the editor for sharing their informative comments.

References:

[1] S. T. Dougherty, *Algebraic Coding Theory Over Finite Commutative Rings*, Springer, 2017. DOI10.1007/978-3-319-59806-2

[2] S. Roman, *Coding and Information Theory*, Springer-Verlag, New York, 1992.

[3] M. Grassl and T. Beth, *On optimal quantum codes*, Int. J. Quantum Inform., Vol. 2, pp.55-64, 2004. https://doi.org/10.1142/S0219749904000079

[4] P.W Shor, *Scheme for reducing decoherence in quantum memory*, Phys. Rev.A., Vol. 52, pp.2493-2496, 1995. https://doi.org/10.1103/PhysRevA.52.R2493

[5] A.M. Steane, *Simple quantum error-correcting codes*, Phys. Rev. A., Vol. 54, pp.4741-4751, 1996. https://doi.org/10.1103/PhysRevA.54.4741

[6] A.R. Calderbank, E.M. Rains, P.M. Shor and N.J.A. Sloane, *Quantum error-correction via codes over GF(4)*, IEEE Trans. Inf. Theory, Vol. 44, pp.1369-1387, 1998. https://doi.org/10.48550/arXiv.quant-ph/9608006

[7] S.A. Aly, A. Klappenecker and P.K. Sarvepalli *On quantum and classical BCH codes*, IEEE Trans. Inf. Theory, Vol. 53, pp.1183-1188 , 2007. DOI:10.1109/TIT.2006.890730

[8] K. Feng, S. Ling and C. Xing *Asymtotic bounds on quantum codes from algebraic geometry codes*, IEEE Trans. Inform. Theory, Vol. 52, pp.986-991 , 2006. 10.1109/TIT.2005.862086

[9] R. Li and Z. Xu, *Construction of* $[n, n-4, 3]_q$ *quantum codes for odd prime power q*, Phys. Rev. A., Vol. 82, pp.1-4 , 2010. https://doi.org/10.1103/PhysRevA.82.052316

[10] J. Qian and L. Zhang, *Improved constructions for nonbinary quantum BCH codes*, Int. J. Theor. Phys. 56(4), 1355-1363 , 2017. DOI:10.1007/s10773-017-3277-y

[11] A. Thangaraaj and S.W. MacLaughlin, *Quantum codes from cyclic codes over* $GF(4^m)$, IEEE Trans. Inf. Theory 47(3), 1176-1178 , 2001. DOI:10.1109/18.915675

[12] C. Bechoc, *Applications of Coding Theory to the Construction of Modular Lattices*, journal of combinatorial theory, Series A 78, 92-119 , 1997. https://doi.org/10.1006/jcta.1996.2763

[13] J. Gao, *Some results on linear codes over* $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, J.Appl.Math. Comput. 47(1-2), 473-485, 2015. DOI10.1007/s12190-014-0786-1

[14] J. Gao, *Quantum codes from cyclic codes over* $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, Int. J. Quantum Inf. 13(8), 1550063(1-8), 2015. https://doi.org/10.1142/S021974991550063X

[15] A. Dertli, Y. Cengellenmis and S. Eren, *On quantum codes obtained from cyclic codes over* A_2, Int. J. Quantum Inform. 13(3), 1550031(1-9), 2015. https://doi.org/10.1142/S0219749915500318

[16] A. Dertli, Y. Cengellenmis and S. Eren, *Some results on the linear codes over the finite ring* $\mathbb{F}_2 + v_1\mathbb{F}_2 + \ldots + v_r\mathbb{F}_2$, International Journal of Quantum Information Vol. 14, No. 1 1650012 (1-12), 2016. https://doi.org/10.1142/S021974991650012X

[17] J. Qian, W. Ma and W. Gou, *Quantum codes from cyclic codes over finite ring*, Int. J. Quantum Inform., Vol. 7, pp.1277-1283, 2009.

[18] X. Kai, S. Zhu, *Quaternary construction of quantum codes from cyclic codes over* $\mathbb{F}_4 + u\mathbb{F}_4$, Int. J. Quantum Inform., Vol. 9, pp.689-700 , 2011. https://doi.org/10.1142/S0219749911007757

[19] J. Qian, *Quantum codes from cyclic codes over* $\mathbb{F}_2 + v\mathbb{F}_2$, J. Inform. Compt. Science, Vol. 10, pp.1715-1722, 2013. DOI:10.12733/jics20101705

[20] M. Ashraf, and G. Mohammad, *Quantum codes from cyclic codes over* $\mathbb{F}_3 + v\mathbb{F}_3$, Int. J. Quantum Inf. 12(6), 1450042(1-8), 2014. https://doi.org/10.1142/S0219749914500427

[21] M. Ashraf, and G. Mohammad, *Quantum codes from cyclic codes over* $\mathbb{F}_p + v\mathbb{F}_p$, Int. J. Information and Coding Theory, Vol. 3, No. 2, 137-144, 2015. https://doi.org/10.1504/IJICOT.2015.072627

[22] M. Ashraf, and G. Mohammad, *Quantum codes from cyclic codes over* $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, Quantum Inf. Process. 15(10), 4089-4098, 2016. https://doi.org/10.1007/s11128-016-1379-8

[23] Y. Tang, S. Zhu, X. Kai and J. Ding, *New quantum codes from dual-containing cyclic codes over finite rings*, Quantum Inf. process.

15(11), 4489-4500 , 2016.
DOI:10.1007/s11128-016-1426-5

[24] Y.Liu, R.Li, L. Lv and Y. Ma, *A class of constacyclic BCH codes and new quantum codes*, Quantum Inf. Process. , 2017. https://doi.org/10.1007/s11128-017-1533-y

[25] F. Ma, J. Gao and F.W. Fu *Constacyclic codes over the ring* $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ *and their application of constructing new non-binary quantum codes*, Quantum Inf Process 122 (1 - 19) , 2018. https://doi.org/10.1007/s11128-018-1898-6

[26] H.Q. Dinh, T. Bag, A. K. Upadhyay, R. Bandi, W. Chinnakum, *On the Structure of Cyclic Codes Over* $\mathbb{F}_q RS$ *and Applications in Quantum and LCD Codes Constructions*, IEEE Access 2020, 8, 18902-18914. https://doi.org/10.1109/ACCESS.2020.2966542

[27] M. Ashraf, N. Khan, G. Mohammad, *Quantum codes from cyclic codes over the mixed alphabet structure*. Quantum Inf. Process. 2022, 21, 1-25. https://doi.org/10.1007/s11128-022-03491-z

[28] F. Çalişkan, T. Yildirim and R. Aksoy, *Non-Binary Quantum Codes from Cyclic Codes over* $F_p \times (F_p + vF_p)$, International Journal of Theoretical Physics, 62:29, 2023. https://doi.org/10.1007/s10773-023-05294-z

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflicts of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Appendix

Table 1: QECC over $\mathbb{F}_3 \times (\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3)$

2^i	$\Gamma(\mathfrak{C}) : [4n, k, d_L]$	**QECC:** $[n, 2k-4n, d_L]$
2^4	$[2^6, 2^3.7, 2]$	$[2^6, 2^4.3, 2]$
2^6	$[2^6, 2^3.31, 2]$	$[2^8, 2^4.3.5, 2]$
2^8	$[2^{10}, 2^3.127, 2]$	$[2^{10}, 2^4.3^2.7, 2]$
2^{10}	$[2^{12}, 2^3.7.73, 3]$	$[2^{12}, 2^4.3.5.17, 3]$
2^{12}	$[2^{14}, 2^3.23.89, 2]$	$[2^{12}, 2^4.3.11.31, 2]$
2^{14}	$[2^{16}, 2^3.8191, 4]$	$[2^{16}, 2^4.3^2.5.7.13, 4]$
2^{16}	$[2^{18}, 2^3.7.31.151, 2]$	$[2^{18}, 2^4.3.43.127, 2]$
2^{18}	$[2^{20}, 2^3.131071, 2]$	$[2^{20}, 2^4.3.5.17.257, 2]$
2^{20}	$[2^{22}, 2^3.524287, 2]$	$[2^{22}, 2^4.3^3.7.19.73, 2]$
2^{22}	$[2^{24}, 2^3.7^2.127.137, 2]$	$[2^{24}, 2^4.3.5^2.11.31.41, 2]$
2^{24}	$[2^{26}, 2^3.47.178481, 2]$	$[2^{26}, 2^4.3.23.89.683, 2]$
2^{26}	$[2^{28}, 2^3.31.601.1801, 2]$	$[2^{28}, 2^4.3^2.5.7.13.17.241, 2]$
2^{28}	$[2^{30}, 2^3.7.73.262657, 2]$	$[2^{30}, 2^4.3.2731.8191, 2]$
2^{30}	$[2^{32}, 2^3.233.1103.2089, 2]$	$[2^{32}, 2^4.3.5.29.43.113.127, 2]$
2^{32}	$[2^{34}, 2^3.2147483647, 2]$	$[2^{34}, 2^4.3^2.7.11.31.151.331, 2]$
2^{34}	$[2^{36}, 2^3.7.23.89.599479, 2]$	$[2^{36}, 2^4.3.5.17.257.65537, 2]$
2^{36}	$[2^{38}, 2^3.31.71.127.122921, 2]$	$[2^{38}, 2^4.3.43691.131071, 2]$
2^{38}	$[2^{40}, 2^3.223.616318177, 2]$	$[2^{40}, 2^4.3.174763.524287, 2]$
2^{40}	$[2^{42}, 2^3.7.79.8191.121369, 2]$	$[2^{42}, 2^4.3.174763.524287, 2]$

Table 2: QECC over $\mathbb{F}_5 \times (\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5)$

2^i	$\Gamma(\mathfrak{C}) : [4n, k, d_L]$	**QECC:** $[n, 2k-4n, d_L]$
2^6	$[2^8, 2^3.31, 2]$	$[2^8, 2^4.3.5, 2]$
2^{10}	$[2^{12}, 2^3.7.73, 2]$	$[2^{12}, 2^4.3.5.17, 2]$
2^{14}	$[2^{16}, 2^3.8191, 2]$	$[2^{16}, 2^4.3^2.5.7.13, 2]$
2^{18}	$[2^{20}, 2^3.131071, 3]$	$[2^{20}, 2^4.3.5.17.257, 3]$
2^{22}	$[2^{24}, 2^3.7^2.127.337, 2]$	$[2^{24}, 2^4.3.5^2.11.31.41, 2]$
2^{26}	$[2^{28}, 2^3.31.601.1801, 3]$	$[2^{28}, 2^4.3^2.5.7.13.17.241, 3]$
2^{30}	$[2^{32}, 2^3.233.1103.2089, 2]$	$[2^{32}, 2^4.3.5.29.43.113.127, 2]$
2^{34}	$[2^{36}, 2^3.7.23.89.599479, 2]$	$[2^{36}, 2^4.3.5.17.257.65537, 2]$
2^{38}	$[2^{40}, 2^3.223.616318177, 2]$	$[2^{40}, 2^4.3^3.5.7.13.19.37.73.109, 2]$

Table 3: QECC over $\mathbb{F}_7 \times (\mathbb{F}_7 + v\mathbb{F}_7 + v^2\mathbb{F}_7)$

2^i	$\Gamma(\mathfrak{C}) : [4n, k, d_L]$	**QECC:** $[n, 2k-4n, d_L]$
2^5	$[2^7, 2^3.3.5, 2]$	$[2^7, 2^4.7, 2]$
2^8	$[2^{10}, 2^3.127, 2]$	$[2^{10}, 2^4.3^2.7, 2]$
2^{11}	$[2^{13}, 2^3.3.11.31, 2]$	$[2^{13}, 2^4.7.73, 2]$
2^{14}	$[2^{16}, 2^3.8191, 2]$	$[2^{16}, 2^4.3^2.5.7.13, 2]$
2^{17}	$[2^{19}, 2^3.3.5.17.257, 2]$	$[2^{19}, 2^4.7.31.151, 2]$
2^{20}	$[2^{22}, 2^3.524287, 2]$	$[2^{22}, 2^4.3^3.7.19.73, 2]$
2^{23}	$[2^{25}, 2^3.3.23.89.683, 2]$	$[2^{25}, 2^4.7^2.127.337, 2]$
2^{26}	$[2^{28}, 2^3.31.601.1801, 2]$	$[2^{28}, 2^4.3^2.5.7.13.17.241, 2]$
2^{29}	$[2^{31}, 2^3.3.5.29.43.113.127, 2]$	$[2^{31}, 2^4.3^3.7.73.262657, 2]$
2^{32}	$[2^{34}, 2^3.2147483647, 2]$	$[2^{34}, 2^4.3^2.7.11.31.151.331, 2]$
2^{35}	$[2^{37}, 2^3.3.43691.131071, 2]$	$[2^{37}, 2^4.7.23.89.599479, 2]$
2^{38}	$[2^{40}, 2^3.223.616318177, 2]$	$[2^{40}, 2^4.3^3.5.7.13.19.37.73.109, 2]$

Table 4: QECC over $\mathbb{F}_{11} \times (\mathbb{F}_{11} + v\mathbb{F}_{11} + v^2\mathbb{F}_{11})$

2^i	$\Gamma(\mathfrak{C}) : [4n, k, d_L]$	**QECC:** $[n, 2k-4n, d_L]$
2^{12}	$[2^{14}, 2^3.23.89, 3]$	$[2^{14}, 2^4.3.11.31, 3]$
2^{22}	$[2^{24}, 2^3.7^2.127.337, 3]$	$[2^{24}, 2^4.3.5^2.11.31.41, 3]$
2^{32}	$[2^{34}, 2^3.2147483647, 3]$	$[2^{34}, 2^4.3^2.7.11.31.151.331, 3]$

Table 5: QECC over $\mathbb{F}_{13} \times (\mathbb{F}_{13} + v\mathbb{F}_{13} + v^2\mathbb{F}_{13})$

2^i	$\Gamma(\mathfrak{C}) : [4n, k, d_L]$	**QECC:** $[n, 2k-4n, d_L]$
2^{14}	$[2^{16}, 2^3.8191, 3]$	$[2^{16}, 2^4.3^2.5.7.13, 3]$
2^{26}	$[2^{28}, 2^3.31.601.1801, 3]$	$[2^{28}, 2^4.3^2.5.7.13.17.241, 3]$
2^{38}	$[2^{40}, 2^3.223.616318177, 3]$	$[2^{40}, 2^4.3^3.5.7.13.19.37.73.109, 3]$

Table 6: QECC over $\mathbb{F}_{17} \times (\mathbb{F}_{17} + v\mathbb{F}_{17} + v^2\mathbb{F}_{17})$

2^i	$\Gamma(\mathfrak{C}) : [4n, k, d_L]$	**QECC:** $[n, 2k-4n, d_L]$
2^{10}	$[2^{12}, 2^3.7.73, 2]$	$[2^{12}, 2^4.3.5.17, 2]$
2^{18}	$[2^{20}, 2^3.131071, 2]$	$[2^{20}, 2^4.3.5.17.257, 2]$
2^{26}	$[2^{28}, 2^3.31.601.1801, 2]$	$[2^{28}, 2^4.3^2.5.7.13.17.241, 2]$
2^{34}	$[2^{36}, 2^3.7.23.89.599479, 3]$	$[2^{36}, 2^4.3.5.17.257.65537, 3]$

Table 7: QECC over $\mathbb{F}_{19} \times (\mathbb{F}_{19} + v\mathbb{F}_{19} + v^2\mathbb{F}_{19})$

2^i	$\Gamma(\mathfrak{C}) : [4n, k, d_L]$	**QECC:** $[n, 2k-4n, d_L]$
2^{20}	$[2^{22}, 2^3.524287, 3]$	$[2^{22}, 2^4.3^3.7.19.73, 3]$
2^{38}	$[2^{40}, 2^3.223.616318177, 2]$	$[2^{40}, 2^4.3^3.5.7.13.19.37.73.109, 2]$