Quantum Codes Constructed from Cyclic Codes over a Finite Non-chain Ring

Djoko Suprijanto*, *Member, IAENG* and Hopein Christofen Tang

Abstract—**In this article, we investigate the properties of cyclic codes over a finite non-chain ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q + v^4\mathbb{F}_q$, where $q = p^r$, r is a positive integer, p is an odd prime, $4 \mid (p-1)$, and $v^5 = v$. We construct quantum error-correcting codes over the finite field $\mathbb{F}_q$ from cyclic codes over R using a specific Gray map.**

Index Terms—**Non-chain ring, Gray map, cyclic codes, quantum codes.**

I. Introduction

The fact that quantum physics is superior to classical mechanics in some ways motivates the study of quantum communication and quantum computing. Instead of classical bits, we use qubits (quantum bits) in quantum computing. Qubits can theoretically store more information due to their superposition state, allowing them to perform certain computations much faster than in the classical case. According to Sari and Siap [15], "while qubits have some superiorities than classical bits, one of the main problems for qubits is the decoherence that destroys the information in a superposition of qubits." Fortunately, quantum error-correcting codes (QECC) can handle this problem.

In 1995, Shor [18] introduced the first quantum error-correcting code that encoded one qubit into a highly entangled state of nine qubits. In 1996, Calderbank, Shor [5], and Steane [19] introduced a method for constructing quantum error-correcting codes from classical error-correcting codes. Their method is known as Calderbank-Shor-Steane construction, or CSS construction, for short. Later, Steane [20] proposed a generalization of the CSS construction, allowing him to obtain many new quantum codes that were unknown to exist before.

Although quantum error-correcting codes were originally studied over a binary field, they were later generalized to non-binary fields "with the goal to relate the later codes to the former ones" (see [6] for the earliest study, cf. [1]). Many others later constructed quantum error-correcting codes from cyclic codes over various rings (see, e.g., [7], [13], [15], [16], to name a few). Qian, Ma, and Guo [13] constructed quantum error-correcting codes starting from cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, with $u^2 = 0$. Gao [7] constructed quantum error-correcting codes from cyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, where $v^4 = v$. Gao's work [7] can be seen as a certain generalization of Sari and Siap's work [15], in which they constructed quantum codes from cyclic codes over the ring $\mathbb{F}_p + v\mathbb{F}_p + \cdots + v^{p-1}\mathbb{F}_p$, where $v^p = v$, and p is a prime number. Sari and Siap [16] have also considered binary quantum error-correcting codes constructed from the cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{s-1}\mathbb{F}_2$, where $u^s = 0$.

In this paper, we continue Gao's investigation [7] by studying the structural aspects of cyclic codes over the ring $R := \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q + v^4\mathbb{F}_q$, where $q = p^r$, r is a positive integer, p is an odd prime, $4 \mid (p-1)$, and $v^5 = v$. As an application, we construct quantum error-correcting codes over $\mathbb{F}_q$ from cyclic codes over the ring R.

This paper is organized as follows. In Section 2, we consider the structure of linear and cyclic codes over the ring R. We also define a Gray map from R^n to $\mathbb{F}_q^{5n}$ and derive some related properties. The construction of quantum error-correcting codes over $\mathbb{F}_q$ from cyclic codes over R is given in Section 3. To illustrate the results, we give several concrete examples at the end of Section 3.

II. Linear codes over R and the Gray map

Let $\mathbb{F}_q$ be the finite field of order q, where $q = p^r$, r is a positive integer, p is an odd prime, and $4 \mid (p-1)$. Let R denote the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q + v^4\mathbb{F}_q$, where $v^5 = v$. It is clear that R is isomorphic to the ring $\mathbb{F}_q[v]/\langle v^5 - v\rangle$. It is also well-known (see, e.g., [12]) that $v^{p-1} - 1$ has a unique factorization into linear factors over $\mathbb{F}_q$. Moreover, since $4 \mid (p-1)$, we have $(v^4 - 1) \mid (v^{p-1} - 1)$, which implies $v^5 - v = v(v^4 - 1) = v(v-1)(v+1)(v-a_1)(v-a_2) = v(v-1)(v+1)(v-a)(v+a)$, where $a, a_1, a_2 \in \mathbb{F}_q$ with $a^2 = -1$.

Let $f_1 = v$, $f_2 = v - 1$, $f_3 = v + 1$, $f_4 = v - a$, $f_5 = v + a$; and for $i \in [1,5]_{\mathbb{Z}}$, let $\widehat{f_i} = \frac{v^5 - v}{f_i}$. Then there exist $\alpha_i, \beta_i \in \mathbb{F}_q[v]$ such that $\alpha_i f_i + \beta_i \widehat{f_i} = 1$. Now, for $i \in [1,5]_{\mathbb{Z}}$, let $\eta_i = \beta_i \widehat{f_i}$. Then we have

(i) $\eta_1, \eta_2, \eta_3, \eta_4, \eta_5 \in R$ are nonzero idempotents orthogonal in R.

(ii) $\eta_1 + \eta_2 + \eta_3 + \eta_4 + \eta_5 = 1$ in R.

It implies that, by the Chinese Remainder Theorem, the ring R can be decomposed as follows:

$$\begin{aligned} R &= R\eta_1 \oplus R\eta_2 \oplus R\eta_3 \oplus R\eta_4 \oplus R\eta_5 \\ &= \mathbb{F}_q\eta_1 \oplus \mathbb{F}_q\eta_2 \oplus \mathbb{F}_q\eta_3 \oplus \mathbb{F}_q\eta_4 \oplus \mathbb{F}_q\eta_5. \end{aligned} \tag{1}$$

Example II.1. For $q = p = 13$, the five roots of $(v^5 - v)$ are $v_1 = 0$, $v_2 = 1$, $v_3 = 12 = -1$, $v_4 = 5$, and $v_5 = 8 = -5$.

Manuscript received November 29, 2021; revised May 19, 2022. This research was supported by the Institut Teknologi Bandung (ITB) and the Ministry of Research, Technology and Higher Education (*Kementerian Riset dan Teknologi/ Badan Riset dan Inovasi Nasional (Kemenristek/ BRIN)*), Republic of Indonesia.

D. Suprijanto is an associate professor in the Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jl. Ganesha 10, Bandung, 40132, INDONESIA. (Corresponding author, email: djoko.suprijanto@itb.ac.id)

H.C. Tang is a postgraduate student in the Department of Mathematics, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jl. Ganesha 10, Bandung, 40132, INDONESIA. (email: hopeinct@students.itb.ac.id)

The five idempotents are

$$\begin{aligned}\eta_1 &= 12v^4 + 1,\\ \eta_2 &= 10v^4 + 10v^3 + 10v^2 + 10v,\\ \eta_3 &= 10v^4 + 3v^3 + 10v^2 + 3v,\\ \eta_4 &= 10v^4 + 2v^3 + 3v^2 + 11v,\\ \eta_5 &= 10v^4 + 11v^3 + 3v^2 + 2v.\end{aligned}$$

$\diamondsuit$

From Equation (1), we know that for any $r \in R$ there exist $b_1, b_2, b_3, b_4, b_5 \in \mathbb{F}_q$ such that $r = b_1\eta_1 + b_2\eta_2 + b_3\eta_3 + b_4\eta_4 + b_5\eta_5$. Let us define a Gray map ϕ from R to $\mathbb{F}_q^5$ by

$$r \longmapsto (b_1, b_2, b_3, b_4, b_5)\begin{pmatrix} 6 & 2 & 3 & -6 & 6\\ 6 & 6 & 2 & 3 & -6\\ -6 & 6 & 6 & 2 & 3\\ 3 & -6 & 6 & 6 & 2\\ 2 & 3 & -6 & 6 & 6 \end{pmatrix},$$

where $6 = 1 + 1 + 1 + 1 + 1 + 1$.

Next, we define the Gray map Φ from R^n to $\mathbb{F}_q^{5n}$ as an extension of a Gray map ϕ by

$$\mathbf{r} \longmapsto (\phi(r_0), \phi(r_1), \dots, \phi(r_{n-1})),$$

where $\mathbf{r} = (r_0, r_1, \dots, r_{n-1}) \in R^n$.

The Hamming weight of a vector $\mathbf{x} \in \mathbb{F}_q^m$, denoted by $w_H(\mathbf{x})$, is defined as a number of nonzero components of $\mathbf{x}$. The Lee weight of the element $r = b_1\eta_1 + b_2\eta_2 + b_3\eta_3 + b_4\eta_4 + b_5\eta_5 \in R$, denoted by $w_L(r)$, is defined by

$$w_L(r) = w_H(\phi(r)).$$

We also define the Lee weight of a vector $\mathbf{r} = (r_0, r_1, \dots, r_{n-1}) \in R^n$, naturally, to be the rational sum of Lee weights of its components, i.e. $w_L(\mathbf{r}) = \sum_{i=0}^{n-1} w_L(r_i)$. For any vectors $\mathbf{x}_1$ and $\mathbf{x}_2$ in R^n, the Lee distance between $\mathbf{x}_1$ and $\mathbf{x}_2$ is given by $d(\mathbf{x}_1, \mathbf{x}_2) = w_L(\mathbf{x}_1 - \mathbf{x}_2)$.

A code C of length n over R is defined as a nonempty subset of R^n. Any element of a code C is called a codeword. A code C is called linear if and only if C is an R-submodule of R^n. The minimum Lee distance of C is the smallest nonzero Lee distance between all pairs of distinct codewords. The minimum Lee weight of C is the smallest nonzero Lee weight among all codewords. It is easy to see that if C is linear, then the minimum Lee distance of the code C is the same as its minimum Lee weight. In this paper, we always assume that C is a linear code over R. Note that the Hamming distance $d_H(\mathbf{x}_1, \mathbf{x}_2)$ is defined similarly.

Since the map ϕ satisfies $\phi(r + \alpha s) = \phi(r) + \alpha\phi(s)$ for every $\alpha \in \mathbb{F}_q$ and $r, s \in R$, then Φ is $\mathbb{F}_q$-linear. Now, let $\mathbf{x}, \mathbf{y} \in R^n$. Then $d_L(\mathbf{x}, \mathbf{y}) = w_L(\mathbf{x} - \mathbf{y}) = w_H(\Phi(\mathbf{x} - \mathbf{y})) = w_H(\Phi(\mathbf{x}) - \Phi(\mathbf{y})) = d_H(\Phi(\mathbf{x}), \Phi(\mathbf{y}))$. Hence, we have proven the lemma below.

Lemma II.2. *The Gray map Φ is an isometry, namely a distance-preserving map, from $(R^n,\ d_L)$ to $(\mathbb{F}_q^{5n}, d_H)$. Moreover, it is also $\mathbb{F}_q$-linear.*

Moreover, if C is a linear code over the ring R, then the Gray image of C is a linear code over $\mathbb{F}_q$.

Lemma II.3. *Let C be a $[n, A, d_L]$ linear code over R, where n, A, and d_L are the code length, the number of codewords, and the minimum Lee distance of C, respectively. Then $\Phi(C)$ is a $[5n, \log_q A, d_L]$ linear code over $\mathbb{F}_q$.*

Proof: From Lemma II.2, we see that $\Phi(C)$ is a linear code over $\mathbb{F}_q$. By definition of the Gray map Φ, we have that $\Phi(C)$ is of length $5n$. Moreover, since Φ is a bijection, which is easy to verify, we have that $\Phi(C)$ has dimension $\log_q A$. Finally, since Φ is an isometry, $\Phi(C)$ has the minimum Hamming distance d_L. ■

Let $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \dots, y_{n-1})$ be two vectors in R^n. Then the inner product of $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$\mathbf{x} \cdot \mathbf{y} := \sum_{i=0}^{n-1} x_i y_i.$$

The dual of a code C over R, denoted by $C^\perp$, is defined by

$$C^\perp := \{\mathbf{x} \in R^n :\ \mathbf{x} \cdot \mathbf{y} = 0,\ \text{for all } \mathbf{y} \in C\}.$$

If $C \subseteq C^\perp$, then C is said to be a self-orthogonal code.

We also define the Euclidean inner product in $\mathbb{F}_q^n$ as

$$[\mathbf{a}, \mathbf{b}] := \sum_{i=0}^{n-1} a_i b_i,$$

for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$. The dual of a linear code over $\mathbb{F}_q$ and the self-orthogonality of a linear code over $\mathbb{F}_q$ are defined similarly.

Theorem II.4. *Let C be a linear code over R. Then $\Phi(C^\perp) = \Phi(C)^\perp$. Moreover, if C is self-orthogonal over R, then $\Phi(C)$ is self-orthogonal over $\mathbb{F}_q$.*

Proof: Let $\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) \in C$ and $\mathbf{y} = (y_0, y_1, \dots, y_{n-1}) \in C^\perp$. For $i \in [0, n-1]_{\mathbb{Z}}$, let $x_i = x_{i1}\eta_1 + x_{i2}\eta_2 + x_{i3}\eta_3 + x_{i4}\eta_4 + x_{i,5}\eta_5$ and $y_i = y_{i1}\eta_1 + y_{i2}\eta_2 + y_{i3}\eta_3 + y_{i4}\eta_4 + y_{i5}\eta_5$. Then we have

$$\begin{aligned} 0 &= \mathbf{x} \cdot \mathbf{y}\\ &= \sum_{i=0}^{n-1} x_i y_i\\ &= \sum_{i=0}^{n-1} x_{i1}y_{i1}\eta_1 + x_{i2}y_{i2}\eta_2 + x_{i3}y_{i3}\eta_3\\ &\quad + x_{i4}y_{i4}\eta_4 + x_{i5}y_{i5}\eta_5. \end{aligned}$$

Hence, for all $j \in [1, 5]_{\mathbb{Z}}$, we have $\sum_{i=0}^{n-1} x_{ij}y_{ij} = 0$, which implies

$$\begin{aligned} &[\Phi(\mathbf{x}), \Phi(\mathbf{y})]\\ &= k\sum_{i=0}^{n-1} x_{i1}y_{i1} + x_{i2}y_{i2} + x_{i3}y_{i3} + x_{i4}y_{i4} + x_{i5}y_{i5} = 0, \end{aligned}$$

with $k = 6^2 + 6^2 + (-6)^2 + 3^2 + 2^2$. Therefore, $\Phi(C^\perp) \subseteq \Phi(C)^\perp$. By using the fact that Φ is a bijection, then $|\Phi(C)| = |C|$ and also $|\Phi(C^\perp)| = |C^\perp|$. Furthermore, since $|R^n| = |C||C^\perp|$ and $|\mathbb{F}_q^{5n}| = |\Phi(C)||\Phi(C)^\perp|$, we conclude that $|\Phi(C^\perp)| = |\Phi(C)^\perp|$, and hence $\Phi(C^\perp) = \Phi(C)^\perp$. Moreover, if C is self-orthogonal, then $\Phi(C) \subseteq \Phi(C^\perp) = \Phi(C)^\perp$, and hence $\Phi(C)$ is also self-orthogonal. ■

Now, for all $i \in [1,5]_{\mathbb{Z}}$, define a code $C_i \subseteq \mathbb{F}_q^n$ as follows:

$$C_1 := \{\mathbf{c}_1 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C\},$$

$$C_2 := \{\mathbf{c}_2 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C\},$$

$$C_3 := \{\mathbf{c}_3 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C\},$$

$$C_4 := \{\mathbf{c}_4 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C\},$$

$$C_5 := \{\mathbf{c}_5 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C\}.$$

It is not difficult to see that for all $i \in [1,5]_{\mathbb{Z}}$, the code C_i are linear over $\mathbb{F}_q$. Moreover, the linear code C over R can be uniquely expressed as

$$C = C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5. \qquad (2)$$

Let G be a generator matrix of a code C over R. Then, by Equation (2) we have

$$G = \begin{pmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \eta_3 G_3 \\ \eta_4 G_4 \\ \eta_5 G_5 \end{pmatrix},$$

where for $i \in [1,5]_{\mathbb{Z}}$, G_i is a generator matrix of C_i.

Lemma II.5. *Let $C = C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5$ be a linear code of length n over R. Then*

$$C^{\perp} = C_1^{\perp}\eta_1 \oplus C_2^{\perp}\eta_2 \oplus C_3^{\perp}\eta_3 \oplus C_4^{\perp}\eta_4 \oplus C_5^{\perp}\eta_5.$$

Moreover, C is a self-orthogonal code over R if and only if $C_1, C_2, C_3, C_4,$ and C_5 are all self-orthogonal codes over $\mathbb{F}_q$.

Proof: Define

$$\widehat{C}_1 := \{\mathbf{c}_1 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C^{\perp}\},$$

$$\widehat{C}_2 := \{\mathbf{c}_2 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C^{\perp}\},$$

$$\widehat{C}_3 := \{\mathbf{c}_3 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C^{\perp}\},$$

$$\widehat{C}_4 := \{\mathbf{c}_4 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_5 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C^{\perp}\},$$

and

$$\widehat{C}_5 := \{\mathbf{c}_5 \in \mathbb{F}_q^n :\ \exists \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4 \in \mathbb{F}_q^n \text{ s.t. } \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C^{\perp}\}.$$

Then $C^{\perp} = \widehat{C}_1\eta_1 \oplus \widehat{C}_2\eta_2 \oplus \widehat{C}_3\eta_3 \oplus \widehat{C}_4\eta_4 \oplus \widehat{C}_5\eta_5$ and this expression is unique. It is easy to check that $\widehat{C}_1 \subseteq C_1^{\perp}$. Let $\mathbf{x} \in C_1^{\perp}$. For any $\mathbf{y} = \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C$, we have $\mathbf{x}\eta_1 \cdot \mathbf{y} = 0$ which implies $\mathbf{x}\eta_1 \in C^{\perp}$. By the unique expression of $C^{\perp}$, we have $\mathbf{x} \in \widehat{C}_1$ and hence $C_1^{\perp} = \widehat{C}_1$. Similarly, for all $i = 2, 3, 4, 5$ we have $C_i^{\perp} = \widehat{C}_i$, and hence we conclude that $C^{\perp} = C_1^{\perp}\eta_1 \oplus C_2^{\perp}\eta_2 \oplus C_3^{\perp}\eta_3 \oplus C_4^{\perp}\eta_4 \oplus C_5^{\perp}\eta_5$.

Moreover, it is clear that C is self-orthogonal over R if $C_1, C_2, C_3, C_4,$ and C_5 are all self-orthogonal over $\mathbb{F}_q$. Now let C self-orthogonal over R and $\mathbf{c} = \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5 \in C$, with $\mathbf{c}_1 \in C_1$, $\mathbf{c}_2 \in C_2$, $\mathbf{c}_3 \in C_3$, $\mathbf{c}_4 \in C_4$, and $\mathbf{c}_5 \in C_5$. Then for any $\mathbf{d} = \mathbf{d}_1\eta_1 + \mathbf{d}_2\eta_2 + \mathbf{d}_3\eta_3 + \mathbf{d}_4\eta_4 + \mathbf{d}_5\eta_5 \in C$, with $\mathbf{d}_1 \in C_1$, $\mathbf{d}_2 \in C_2$, $\mathbf{d}_3 \in C_3$, $\mathbf{d}_4 \in C_4$, and $\mathbf{d}_5 \in C_5$, we have $0 = \mathbf{c} \cdot \mathbf{d} = [\mathbf{c}_1, \mathbf{d}_1]\eta_1 + [\mathbf{c}_2, \mathbf{d}_2]\eta_2 + [\mathbf{c}_3, \mathbf{d}_3]\eta_3 + [\mathbf{c}_4, \mathbf{d}_4]\eta_4 + [\mathbf{c}_5, \mathbf{d}_5]\eta_5$. It implies $0 = [\mathbf{c}_1, \mathbf{d}_1] = [\mathbf{c}_2, \mathbf{d}_2] = [\mathbf{c}_3, \mathbf{d}_3] = [\mathbf{c}_4, \mathbf{d}_4] = [\mathbf{c}_5, \mathbf{d}_5]$, and hence for all $i \in [1,5]_{\mathbb{Z}}$ we have $\mathbf{c}_i \in C_i^{\perp}$. Therefore, C_1, C_2, C_3, C_4, and C_5 are all self-orthogonal over $\mathbb{F}_q$. ■

III. Quantum codes from cyclic codes over R

A quantum code of length n and dimension q over $\mathbb{F}_q$ is defined to be the subspace of the Hilbert space $(\mathbb{C}^q)^{\otimes n}$ of dimension q^k and we denote it by $[\![n, k, d]\!]_q$.

In the class of linear codes, cyclic codes play an important role in coding theory. Moreover, since we can obtain many quantum codes over $\mathbb{F}_q$ from cyclic codes over R, we will also provide some related results on cyclic codes over R.

A linear code $C \subseteq R^n$ over R is called cyclic if $T(C) = C$. Here, T is cyclic shift operator on R^n, namely for any $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in R^n$, we have $T(\mathbf{c}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$.

Define $R[x]/\langle x^n - 1\rangle := \{c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} + \langle x^n - 1\rangle :\ c_0, c_1, \ldots, c_{n-1} \in R\}$. Now, consider the following map

$$\lambda : R^n \longrightarrow R[x]/\langle x^n - 1\rangle,$$

defined by

$$\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \longmapsto c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1} + \langle x^n - 1\rangle.$$

For convenience, we omit the term $\langle x^n - 1\rangle$ when writing any element of $R[x]/\langle x^n - 1\rangle$. It is easy to prove that λ defines an R-module isomorphism. Hence, we can identify a cyclic code C over R as an ideal of the quotient ring $R[x]/\langle x^n - 1\rangle$.

Now, we recall a celebrated method to construct quantum error-correcting codes as introduced by Calderbank, Shor, and Steane. This well-known method is called Calderbank-Shor-Steane construction or CSS construction (see Theorem 9 and 12 in [6]).

Theorem III.1. *[6](CSS construction) Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ of parameter $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, such that $C_2 \subseteq C_1$. Then there exists a quantum error-correcting code with the parameters $[\![n, k_1 - k_2, min\{d_1, d_2^{\perp}\}]\!]_q$ where $d_2^{\perp}$ denotes the minimum Hamming distance of the dual code $C_2^{\perp}$ of C_2. Further, if $C_2 = C_1^{\perp}$, then there exists a quantum error-correcting code with the parameters $[\![n, 2k_1 - n, d_1]\!]_q$.*

The following two properties are easy to prove but important for our construction.

Lemma III.2. *A linear code $C = C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5$ over R is cyclic if and only if $C_1, C_2, C_3, C_4,$ and C_5 are all cyclic over $\mathbb{F}_q$.*

Proof: ($\Longrightarrow$) For $i \in [1,5]_{\mathbb{Z}}$, let $(c_{i1}, c_{i2}, \dots, c_{in}) \in C_i$. Also, for $j \in [1,5]_{\mathbb{Z}}$, let $c_j = \eta_1 c_{1j} + \eta_2 c_{2j} + \eta_3 c_{3j} + \eta_4 c_{4j} + \eta_5 c_{5j}$. Then, we have $\mathbf{c} = (c_1, c_2, \dots, c_n) \in C$. Since C is cyclic over R, then it follows that $(c_n, c_1, c_2, \dots, c_{n-1}) \in C$. In addition, since $(c_n, c_1, c_2, \dots, c_{n-1}) = \sum_{j=1}^{5} \eta_j (c_{jn}, c_{j1}, c_{j2}, \dots, c_{jn-1})$, we have that $(c_{in}, c_{i1}, c_{i2}, \dots, c_{in-1}) \in C_i$, for $i \in [1,5]_{\mathbb{Z}}$. Thus, $C_1, C_2, C_3, C_4,$ and C_5 are all cyclic codes over $\mathbb{F}_q$.

($\Longleftarrow$) Suppose $C_1, C_2, C_3, C_4,$ and C_5 are all cyclic codes over $\mathbb{F}_q$. Let $\mathbf{c} = (c_1, c_2, \dots, c_n) \in C$, where $c_j = \eta_1 c_{1j} + \eta_2 c_{2j} + \eta_3 c_{3j} + \eta_4 c_{4j} + \eta_5 c_{5j}$, for $j \in [1,5]_{\mathbb{Z}}$. Then for $i \in [1,5]_{\mathbb{Z}}$, we have $(c_{i1}, c_{i2}, \dots, c_{in}) \in C_i$, which implies $(c_n, c_1, c_2, \dots, c_{n-1}) = \sum_{j=1}^{5} \eta_j (c_{jn}, c_{j1}, c_{j2}, \dots, c_{jn-1}) \in \oplus_{j=1}^{5} \eta_j C_j = C$. Hence, C is a cyclic code over R. ■

Lemma III.3. *Let $C = C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5$ be a cyclic code over R of length n. Then there exists a unique polynomial $g(x) \in R[x]/\langle x^n - 1\rangle$ such that*

$$C = \langle g(x) \rangle,$$

where $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x) + \eta_4 g_4(x) + \eta_5 g_5(x)$ and $g_1(x), g_2(x), g_3(x), g_4(x)$ and $g_5(x)$ are the generator polynomial of cyclic codes $C_1, C_2, C_3, C_4,$ and C_5 over $\mathbb{F}_q$, respectively. Moreover, $g(x)$ is a divisor of $x^n - 1$ over R.

Proof: Since $g(x) \in C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5 = C$, then $\langle g(x) \rangle \subseteq C$. For any $\mathbf{c} \in C$, there exists $\mathbf{c}_i \in C_i$ for $i \in [1,5]_{\mathbb{Z}}$ such that $\mathbf{c} = \mathbf{c}_1\eta_1 + \mathbf{c}_2\eta_2 + \mathbf{c}_3\eta_3 + \mathbf{c}_4\eta_4 + \mathbf{c}_5\eta_5$. We can identify $\mathbf{c}$ with the polynomial $c_1(x)\eta_1 + c_2(x)\eta_2 + c_3(x)\eta_3 + c_4(x)\eta_4 + c_5(x)\eta_5$, where $c_i(x) = a_i(x)g_i(x) \in \langle g_i(x) \rangle = C_i$ for $i \in [1,5]_{\mathbb{Z}}$. We have $c_1(x)\eta_1 + c_2(x)\eta_2 + c_3(x)\eta_3 + c_4(x)\eta_4 + c_5(x)\eta_5 = a_1(x)g_1(x)\eta_1 + a_2(x)g_2(x)\eta_2 + a_3(x)g_3(x)\eta_3 + a_4(x)g_4(x)\eta_4 + a_5(x)g_5(x)\eta_5 = a(x)g(x) \in \langle g(x) \rangle$, where $a(x) = a_1(x)\eta_1 + a_2(x)\eta_2 + a_3(x)\eta_3 + a_4(x)\eta_4 + a_5(x)\eta_5$. It implies $C \subseteq \langle g(x) \rangle$. Thus, $C = \langle g(x) \rangle$. The uniqueness of $g(x)$ follows immediately from the uniqueness of $g_1(x)$, $g_2(x)$, $g_3(x)$, $g_4(x)$, and $g_5(x)$.

Since for all $i \in [1,5]_{\mathbb{Z}}$, $g_i(x)$ is a divisor of $x^n - 1$, then there is $h_i(x) \in \mathbb{F}_q[x]$ such that $g_i(x)h_i(x) = x^n - 1$. It follows that $x^n - 1 = g(x)(\eta_1 h_1(x) + \eta_2 h_2(x) + \eta_3 h_3(x) + \eta_4 h_4(x) + \eta_5 h_5(x))$. Hence, we conclude that $g(x)$ is a divisor of $x^n - 1$ over R. ■

From the Lemma III.3, we conclude immediately that all ideals of the ring $R[x]/\langle x^n - 1\rangle$ are generated by only one element, and hence the ring is principal. Moreover, the cardinality of the cyclic code C can be easily calculated as follows:

$$\begin{aligned} |C| &= |C_1||C_2||C_3||C_4||C_5| \\ &= q^{n-\deg g_1(x)} q^{n-\deg g_2(x)} q^{n-\deg g_3(x)} \\ &\quad \cdot q^{n-\deg g_4(x)} q^{n-\deg g_5(x)}. \end{aligned}$$

Moreover, by applying Lemma II.5 and the well-known property regarding the dual code $C^{\perp}$ of a cyclic code C, we can obtain the generator polynomial of the dual code $C^{\perp}$. Hence, we deduce the following properties.

Corollary III.4. *The following three properties hold.*

1. *The quotient ring $R[x]/\langle x^n - 1\rangle$ is principal.*
2. *Let C be a cyclic code of length n over R as written in the Lemma III.3. Then*
$$|C| = q^{5n-\deg g_1(x)-\deg g_2(x)-\deg g_3(x)-\deg g_4(x)-\deg g_5(x)}.$$
3. *Let C be a cyclic code of length n over R as written in the Lemma III.3 and $g_1(x)h_1(x) = g_2(x)h_2(x) = g_3(x)h_3(x) = g_4(x)h_4(x) = g_5(x)h_5(x) = x^n - 1$. Then $C^{\perp} = \langle h(x) \rangle$, where $h(x) = \eta_1 h_1^*(x) + \eta_2 h_2^*(x) + \eta_3 h_3^*(x) + \eta_4 h_4^*(x) + \eta_5 h_5^*(x)$ and $h_i^*(x)$ is a reciprocal polynomial of $h_i(x)$, for $i \in [1,5]_{\mathbb{Z}}$.*

If C is a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x)$ and $g(x)h(x) = x^n - 1$, it is well-known that $C^{\perp} = \langle h^*(x) \rangle$. If $C^{\perp} \subseteq C = \langle g(x) \rangle$ then $h^*(x) = a(x)g(x)$ for some polynomial $a(x)$, so $x^n - 1 = -h^*(x)g^*(x) = -a(x)g(x)g^*(x)$. Conversely, if $x^n - 1 \equiv 0 \pmod{g(x)g^*(x)}$, then there exists $a(x)$ such that $-h^*(x)g^*(x) = x^n - 1 = a(x)g(x)g^*(x)$. We have $h^*(x) = -a(x)g(x)$, so $h^*(x) \in \langle g(x) \rangle$. Therefore, $C^{\perp} = \langle h^*(x) \rangle \subseteq \langle g(x) \rangle = C$. Hence, we have proven the property that give us a necessary and sufficient condition for a cyclic code over finite fields to contain its dual.

Lemma III.5. *A cyclic code C over $\mathbb{F}_q$ with generator polynomial $g(x)$ contains its dual if and only if*

$$x^n - 1 \equiv 0 \pmod{g(x)g^*(x)},$$

where $g^*(x)$ is the reciprocal polynomial of $g(x)$.

Similar to the lemma above, the theorem below gives us a necessary and sufficient condition for a cyclic code over R to contain its dual.

Theorem III.6. *Let $C = C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5$ be a cyclic code of length n over R, and let $C = \langle g(x) \rangle$. Then $C^{\perp} \subseteq C$ if and only if for all $i \in [1,5]_{\mathbb{Z}}$ we have*

$$x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)},$$

where $g_i(x)$ is the generator polynomial of the cyclic code C_i and $g_i^*(x)$ is the reciprocal polynomial of $g_i(x)$.

Proof: ($\Longrightarrow$) Let $C^{\perp} \subseteq C$. Then for any $i \in [1,5]_{\mathbb{Z}}$, we have

$$C_i^{\perp}\eta_i = C^{\perp}\eta_i \subseteq C\eta_i = C_i\eta_i.$$

Therefore, for any $i \in [1,5]_{\mathbb{Z}}$, we obtain $C_i^{\perp} \subseteq C_i$. Hence, by Lemma III.5, we have that for any $i \in [1,5]_{\mathbb{Z}}$,

$$x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}.$$

($\Longleftarrow$) For $i \in [1,5]_{\mathbb{Z}}$, let $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$. Then, by Lemma III.5, we have $C_i^{\perp} \subseteq C_i$, which implies $C_i^{\perp}\eta_i \subseteq C_i\eta_i$. Furthermore, by Lemma II.5, we obtain

$$\begin{aligned} C^{\perp} &= C_1^{\perp}\eta_1 \oplus C_2^{\perp}\eta_2 \oplus C_3^{\perp}\eta_3 \oplus C_4^{\perp}\eta_4 \oplus C_5^{\perp}\eta_5 \\ &\subseteq C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5 = C. \end{aligned}$$

■

By using Theorem III.1 (together with Theorem III.6) and Theorem II.4, we have the following theorem to construct quantum error-correcting codes directly.

Theorem III.7. *Let $C = C_1\eta_1 \oplus C_2\eta_2 \oplus C_3\eta_3 \oplus C_4\eta_4 \oplus C_5\eta_5$ be a cyclic code of length n over R and let $\Phi(C)$ be a linear code of parameters $[5n, k, d_L]$ over $\mathbb{F}_q$, where d_L is the minimum Lee distance of C. If $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, where $g_i(x)$ is the generator polynomial of the cyclic code C_i and $g_i^*(x)$ is the reciprocal polynomial of $g_i(x)$, then there exists a quantum error-correcting code of parameters $[\![5n, 2k - 5n, d_L]\!]$ over $\mathbb{F}_q$.*

Let us look at several concrete examples.

A. Examples

To illustrate the application of Theorem III.7 to construct quantum codes, we provide several examples of quantum error-correcting codes over $\mathbb{F}_5$, $\mathbb{F}_{13}$, $\mathbb{F}_{17}$, and $\mathbb{F}_{29}$.

Example III.8. Let $R = \mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5 + v^3\mathbb{F}_5 + v^4\mathbb{F}_5$ and $n = 5$. We have $x^5 - 1 = (x + 4)^5$ over $\mathbb{F}_5$. Let $g(x) = \eta_1 g_1(x)+\eta_2 g_2(x)+\eta_3 g_3(x)+\eta_4 g_4(x)+\eta_5 g_5(x)$ with $g_1(x) = (x + 4)^2, g_2(x) = g_3(x) = g_4(x) = g_5(x) = x + 4$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[25, 19, 3]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![25, 13, 3]\!]_5$. ♢

Example III.9. Let $R = \mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5 + v^3\mathbb{F}_5 + v^4\mathbb{F}_5$ and $n = 8$. We have $x^8 - 1 = (x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3)$ over $\mathbb{F}_5$. Let $g(x) = \eta_1 g_1(x)+\eta_2 g_2(x)+\eta_3 g_3(x)+\eta_4 g_4(x) + \eta_5 g_5(x)$ with $g_1(x) = g_2(x) = x + 2, g_3(x) = x + 3, g_4(x) = x^2 + 2, g_5(x) = x^2 + 3$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[40, 33, 4]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![40, 26, 4]\!]_5$. ♢

Example III.10. Let $R = \mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5 + v^3\mathbb{F}_5 + v^4\mathbb{F}_5$ and $n = 10$. We have $x^{10}-1 = (x+1)^5(x+4)^5$ over $\mathbb{F}_5$. Let $g(x) = \eta_1 g_1(x)+\eta_2 g_2(x)+\eta_3 g_3(x)+\eta_4 g_4(x)+\eta_5 g_5(x)$ with $g_1(x) = g_2(x) = x+1, g_3(x) = g_4(x) = x+4, g_5(x) = (x+4)^2$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[50, 44, 3]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![50, 38, 3]\!]_5$. ♢

Example III.11. Let $R = \mathbb{F}_{13}+v\mathbb{F}_{13}+v^2\mathbb{F}_{13}+v^3\mathbb{F}_{13}+v^4\mathbb{F}_{13}$ and $n = 3$. We have $x^3 - 1 = (x + 4)(x + 10)(x + 12)$ over $\mathbb{F}_{13}$. Let $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x) + \eta_4 g_4(x) + \eta_5 g_5(x)$ with $g_1(x) = g_2(x) = g_3(x) = x + 4$, $g_4(x) = g_5(x) = x + 10$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[15, 10, 3]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![15, 5, 3]\!]_{13}$. ♢

Example III.12. Let $R = \mathbb{F}_{13}+v\mathbb{F}_{13}+v^2\mathbb{F}_{13}+v^3\mathbb{F}_{13}+v^4\mathbb{F}_{13}$ and $n = 4$. We have $x^4 - 1 = (x + 1)(x + 5)(x + 8)(x + 12)$ over $\mathbb{F}_{13}$. Let $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x) + \eta_4 g_4(x) + \eta_5 g_5(x)$ with $g_1(x) = g_2(x) = g_3(x) = g_4(x) = g_5(x) = x + 8$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[20, 15, 2]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![20, 10, 2]\!]_{13}$. ♢

Example III.13. Let $R = \mathbb{F}_{13}+v\mathbb{F}_{13}+v^2\mathbb{F}_{13}+v^3\mathbb{F}_{13}+v^4\mathbb{F}_{13}$ and $n = 6$. We have $x^6 - 1 = (x + 1)(x + 3)(x + 4)(x + 9)(x+10)(x+12)$ over $\mathbb{F}_{13}$. Let $g(x) = \eta_1 g_1(x)+\eta_2 g_2(x)+\eta_3 g_3(x) + \eta_4 g_4(x) + \eta_5 g_5(x)$ with $g_1(x) = g_2(x) = x + 3, g_3(x) = x + 4, g_4(x) = x + 9, g_5(x) = x + 10$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[30, 25, 3]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![30, 20, 3]\!]_{13}$. ♢

Example III.14. Let $R = \mathbb{F}_{17} + v\mathbb{F}_{17} + v^2\mathbb{F}_{17} + v^3\mathbb{F}_{17} + v^4\mathbb{F}_{17}$ and $n = 4$. We have $x^4 - 1 = (x + 1)(x + 4)(x + 13)(x + 16)$ over $\mathbb{F}_{17}$. Let $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x) + \eta_4 g_4(x) + \eta_5 g_5(x)$ with $g_1(x) = x + 4, g_2(x) = g_3(x) = g_4(x) = g_5(x) = x + 13$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[20, 15, 2]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![20, 10, 2]\!]_{17}$. ♢

Example III.15. Let $R = \mathbb{F}_{17}+v\mathbb{F}_{17}+v^2\mathbb{F}_{17}+v^3\mathbb{F}_{17}+v^4\mathbb{F}_{17}$ and $n = 12$. We have $x^{12} - 1 = (x + 1)(x + 4)(x + 13)(x + 16)(x^2 + x + 1)(x^2 + 4x + 16)(x^2 + 13x + 16)(x^2 + 16x + 1)$ over $\mathbb{F}_{17}$. Let $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x) + \eta_4 g_4(x) + \eta_5 g_5(x)$ with $g_1(x) = x + 4, g_2(x) = x^2 + 4x + 16, g_3(x) = (x + 13)(x^2 + 13x + 16), g_4(x) = (x + 4)(x^2 + 16x+1), g_5(x) = (x+4)(x^2+13x+16)$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[60, 48, 2]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![60, 36, 2]\!]_{17}$. ♢

Example III.16. Let $R = \mathbb{F}_{29}+v\mathbb{F}_{29}+v^2\mathbb{F}_{29}+v^3\mathbb{F}_{29}+v^4\mathbb{F}_{29}$ and $n = 7$. We have $x^7-1 = (x+4)(x+5)(x+6)(x+9)(x+13)(x+22)(x+28)$ over $\mathbb{F}_{29}$. Let $g(x) = \eta_1 g_1(x)+\eta_2 g_2(x)+\eta_3 g_3(x) + \eta_4 g_4(x) + \eta_5 g_5(x)$ with $g_1(x) = x + 4, g_2(x) = x+5, g_3(x) = x+9, g_4(x) = x+13, g_5(x) = (x+4)(x+5)$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[35, 29, 5]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![35, 23, 5]\!]_{29}$. ♢

Example III.17. Let $R = \mathbb{F}_{29}+v\mathbb{F}_{29}+v^2\mathbb{F}_{29}+v^3\mathbb{F}_{29}+v^4\mathbb{F}_{29}$ and $n = 8$. We have $x^8 - 1 = (x + 1)(x + 12)(x + 17)(x + 28)(x^2 + 12)(x^2 + 17)$ over $\mathbb{F}_{29}$. Let $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x)+\eta_3 g_3(x)+\eta_4 g_4(x)+\eta_5 g_5(x)$ with $g_1(x) = g_2(x) = g_3(x) = g_4(x) = x+17, g_5(x) = x^2+17$, and let $C = \langle g(x)\rangle$ be a cyclic code over R. Then $\Phi(C)$ is a linear code with parameters $[40, 34, 3]$. Since $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}$ for all $i \in [1, 5]_{\mathbb{Z}}$, then $C^\perp \subseteq C$ and $\Phi(C)^\perp \subseteq \Phi(C)$. Therefore, there exists a quantum error-correcting code of parameters $[\![40, 28, 3]\!]_{29}$. ♢

IV. Concluding remarks

We investigated the structures of cyclic codes over the finite non-chain ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q + v^4\mathbb{F}_q$ where $v^5 = v$. Several properties of cyclic codes over R are derived. As an application, we constructed several quantum error-correcting codes over $\mathbb{F}_q$ with certain parameters from cyclic codes over R using the Gray map Φ. All the examples obtained in this paper are new, and have not appeared in the database of quantum codes [2], [3].

The structures of cyclic codes over the more general non-chain ring, namely the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ where $v^m = v$, as well as its application in the construction of quantum error-correcting codes, are very interesting to investigate. Moreover, there are also many other finite non-chain rings with very nice structures, which have been explored in some publications. See, for examples, [8], [9], [10], and [11], where we defined and investigated the structures of the codes over the rings A_k and B_k, and also [4] and [14], where we recently investigated the structures of the codes over other rings. It is also very interesting to further explore the structures of skew-cyclic codes with derivation over those rings, together with their application in the construction of quantum error-correcting codes.

References

[1] A. Askhikhmin and E. Knill, ”Nonbinary quantum stabilizer codes,” *IEEE Trans. Inform. Theory* **47** (2000), 3065-3072.

[2] N. Aydin, P. Liu, and B. Yoshino, ”A database of quantum codes,” *preprint, 2021* (available at https://arxiv.org/abs/2108.03567).

[3] N. Aydin, P. Liu, and B. Yoshino, ”A Database of quantum codes” (available at http://quantumcodes.info/), accessed at February 11, 2022.

[4] Bustomi, A.P. Santika, and D. Suprijanto, ”Linear codes over the ring $\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4+w\mathbb{Z}_4+uv\mathbb{Z}_4+uw\mathbb{Z}_4+vw\mathbb{Z}_4+uvw\mathbb{Z}_4$,” *IAENG Int. J. Comput. Sci.* **48**(3) (2021), 686-696.

[5] A. R. Calderbank and P. W. Shor, ”Good quantum error-correcting codes exist,” *Phys. Rev.* A **54**(2) (1996), 1098–1105.

[6] A. R. Calderbank, M. Rains, P. W. Shor and N. J. A. Sloane, ”Quantum error correction via codes Over $GF(4)$,” *IEEE Trans. Inform. Theory* **44**(4) (1998), 1369-1387.

[7] 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) (2015), 15500063 (8 pages).

[8] Irwansyah, A. Barra, S.T. Dougherty, A. Muchlis, I. Muchtadi-Alamsyah, I., P. Solé, D. Suprijanto, D., and O. Yemen, ”Θ_S-Cyclic Codes over A_k,” *Int. J. Comput. Math. Comput. Syst. Theory* **1**(1) (2016), 14-31.

[9] Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis, and D. Suprijanto, ”Codes over infinite family of algebras,” *J. Algebra Comb. Discrete Struct. Appl.* **4**(2) (2016), 131-140.

[10] Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis, and D. Suprijanto, ”Skew-cyclic codes over B_k,” *J. Appl. Math. Comput.* **57**(1-2) (2018), 69-84.

[11] Irwansyah, and D. Suprijanto, ”Structure of linear codes over the ring B_k,” *J. Appl. Math. Comput.* **58**(1-2) (2018), 755-775.

[12] H. Niederreiter, ”Finite fields,” *Cambridge University Press,* (2009).

[13] J. Qian, W. Ma, and W. Guo, ”Quantum codes from cyclic codes over finite ring,” *Int. J. Quantum Inf.* **7**(6) (2009), 1277-1283.

[14] S. Rosdiana, M.I. Detiena, D. Suprijanto, and A. Barra, ”On linear codes over $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$,” *IAENG Int. J. App. Math.* **51**(1) (2021), 133-141.

[15] M. Sari and I. Siap, ”On quantum codes from cyclic codes over a class of nonchain rings,” *Bull. Korean Math. Soc.* **53**(6) (2016), 1617-1628.

[16] M. Sari and I. siap, ”Quantum codes over a class of finite chain rings,” *Quantum Inf. Comput.* **16**(1-2) (2016), 39-49.

[17] M. Shi, T. Yao, and P. Solé, ”Skew cyclic codes over a non-chain ring,” *Chin. J. Electron.* **26**(3) (2017), 544-548.

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

[19] A. M. Steane, ”Simple quantum error-correcting codes,” *Phys. Rev.* A **54**(6) (1996), 4741–4751.

[20] A. M. Steane, ”Enlargement of Calderbank-Shor-Steane quantum codes,” *IEEE Trans. Inform. Theory* **45**(7) (1999), 2492–2495.

Djoko Suprijanto received the M.Math. and PhD degrees in Mathematics from Graduate School of Mathematics, Kyushu University, Japan, in 2004 and 2007, respectively. His main research interests cover linear codes over finite rings, quantum error-correcting codes, algebraic combinatorics, and also algebraic graph theory.

Since 1998, he has been with the Department of Mathematics, Institut Teknologi Bandung, Bandung, Indonesia, where he is currently an Associate Professor.

Hopein Christofen Tang received the Bachelor degree in Mathematics from the Department of Mathematics, Institut Teknologi Bandung, Indonesia, in 2021. Currently, he is a postgraduate student in the Department of Mathematics, Institut Teknologi Bandung, Indonesia. His main research interest is algebraic coding theory.