ISSN: 0304-9787

The Aligarh Bulletin of Mathematics
Volume 41, Number 2 (2022), 47-61

Some structural properties of cyclic codes over the semi-local ring

Shakir Ali[1], Turki Alsuraiheed[2], Kholood Alnefaie[3]
Pushpendra Sharma[1*] and Mohammad Jeelani[4]
[1]Department of Mathematics, Aligarh Muslim University
Aligarh - 202002, India
Department of Mathematics, College of Science
King Saud University, Riyadh, KSA
Department of Mathematics, College of Science & Arts, Alula
Taibah University, Madina, KSA
Department of Computer Application, Faculty of Science
Integral University Lucknow, India
Email: shakir.ali.mm@amu.ac.in, talsuraiheed@ksu.edu.sa
alnefaie@taibahu.edu.sa, sharmapushpendra52@gmail.com

(Received: October 31, 2022 Accepted: December 31, 2022)

Abstract

Let α be non-zero element of $\mathbb{F}_q$, where $\mathbb{F}_q$ is a field of order q and q is a power of an odd prime p. The main goal of this paper is to study structural properties of cyclic codes over the finite ring $R = \mathbb{F}_q[u_1, u_2]/\langle {u_1}^2 - \alpha^2,\ u_2^2 - 1,\ u_1u_2 - u_2u_1\rangle$. Moreover, as an application, we construct quantum-error-correcting (QEC) codes.

1 Introduction

Unless otherwise stated, the field of order q is denoted by $\mathbb{F}_q$, where q is an odd prime power, and α is the non-zero element of $\mathbb{F}_q$. Next, let us consider

Keywords and phrases: Cyclic code, Quantum code, Gray map, Dual code
2020 AMS Subject Classification: 94B05, 94B15, 94B60
*Corresponding Author

the finite ring $R = \mathbb{F}_q[u_1, u_2]/\langle u_1^2 - \alpha^2,\ u_2^2 - 1,\ u_1u_2 - u_2u_1\rangle$. It is simple to verify that R is an order q^4 non-chain semi-local ring. For the construction of quantum-error-correcting (QEC) codes, cyclic codes are immensely useful. Compared to classical-error-correcting (CEC) codes, QEC codes are different. A significant breakthrough happened in 1998, when Calderbank et al. [9] solved the problem of obtaining QEC codes with the help of CEC codes over GF(4). Calderbank et al. [9] also introduced a concept to construct QEC codes from CEC codes. Over finite fields, cyclic codes have been extensively investigated (see, for example [13], [17], [18], and [20], and references therein). In 2015, from the cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$ (where $q = p^m$, p is a prime such that $3|(p-1)$, $v^4 = v$, and m is a positive integer), Gao et al. [11] constructed new quantum codes over $\mathbb{F}_q$. Afterwards, Ozen et al. [19] constructed many ternary quantum codes from cyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$. In 2021, Ashraf et al. [2] found better quantum and LCD codes over the ring $\mathbb{F}_{p^m} + v\mathbb{F}_{p^m}$ with $v^2 = 1$, where m is a positive integer. In this article, we discuss the structural properties of cyclic codes over the ring R. On this ring R, we construct a Gray map that provides better parameters and contributes to the finding of better quantum codes over R than presented in [1], [2], [3], [4], [6], [10], and [16].

Our primary goals in this article are to construct quantum-error-correcting (QEC) codes over the finite ring R, and to study the structural properties of cyclic codes over R. Paper's main contribution is that it provides better quantum codes to those presented in recent references ([1], [2], [3], [4], [6], [10], [16] and references therein).

2 Some preliminaries

This section deals with some preliminary studies and describe the Gray map over the ring R. Additionally, we establish certain important results that are required for the subsequent discussions. If a code $\mathcal{C}$ is an R-submodule of R^n (where n is a positive integer), then $\mathcal{C}$ is linear. The components of $\mathcal{C}$ are referred to as codewords. The total number of codewords in $\mathcal{C}$, denoted by $|\mathcal{C}|$, is referred to as the size of $\mathcal{C}$.

An element z of R is of the form $z = z_1 + z_2u_1 + z_3u_2 + z_4u_1u_2$, where $z_i \in \mathbb{F}_q$ and $1 \le i \le 4$. With the help of a set of orthogonal idempotents, every element of this ring can be represented:

$$\Delta_1 = \frac{(\alpha+u_1)(1+u_2)}{4\alpha},$$

$$\Delta_2 = \frac{(\alpha+u_1)(1-u_2)}{4\alpha},$$

$$\Delta_3 = \frac{(\alpha-u_1)(1+u_2)}{4\alpha}$$

and

$$\Delta_4 = \frac{(\alpha-u_1)(1-u_2)}{4\alpha}.$$

It is easy to show that $\Delta_i^2 = \Delta_i,\ 0 = \Delta_i\Delta_j$, and $\Delta_1+\Delta_2+\Delta_3+\Delta_4 = 1$, where $1 \le i, j \le 4$, and $i \ne j$. In view of Chinese Remainder, we obtain $R = \Delta_1 R \oplus \Delta_2 R \oplus \Delta_3 R \oplus \Delta_4 R \cong \Delta_1\mathbb{F}_q \oplus \Delta_2\mathbb{F}_q \oplus \Delta_3\mathbb{F}_q \oplus \Delta_4\mathbb{F}_q$.

We can express every element z of R as $z = \Delta_1 z_1+\Delta_2 z_2+\Delta_3 z_3+\Delta_4 z_4$, where $z_i \in \mathbb{F}_q$ and $1 \le i \le 4$.

The Gray map $\eta : R \longrightarrow \mathbb{F}_q^4$ is defined by

$$\eta(\Delta_1 z_1 + \Delta_2 z_2 + \Delta_3 z_3 + \Delta_4 z_4) = (z_1,\ z_2,\ z_3,\ z_4)A, \tag{2.1}$$

where $A \in GL_4(\mathbb{F}_q)$ is a fixed matrix and $GL_4(\mathbb{F}_q)$ is the linear group of all 4×4 invertible matrices over the field $\mathbb{F}_q$ such that $AA^T = \epsilon I_{4\times 4}$, where A^T is the transpose of A and $\epsilon \in \mathbb{F}_q \backslash \{0\}$.

The aforementioned Gray map is linear, and we can also extend it componentwise from R^n to $\mathbb{F}_q^{4n}$, where n is a positive integer. The Hamming weight $w_H(\mathcal{C})$ is the number of non-zero components in any codeword $c = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C}$. Consider $c = (c_0,\ c_1, c_2,\ \ldots, c_{n-1}), d = (d_0,\ d_1, d_2,\ \ldots, d_{n-1}) \in R^n$, the Hamming distance is denoted by $d_H(c,d) = \{i \mid c_i \ne d_i\}$ for the codewords c and d. $d_H(\mathcal{C}) = \min\{d_H(c,d) \mid c \ne d\}$, or in short d_H, is the Hamming distance of the code $\mathcal{C}$. For any element $z = \Delta_1 z_1 + \Delta_2 z_2 + \Delta_3 z_3 + \Delta_4 z_4 \in R$, the Lee weight of z is defined as $w_L(z) = w_H(\eta(z))$, where w_H represents the Hamming weight over $\mathbb{F}_q$. We begin our discussion with the first result of the above-described Gray map.

Proposition 2.1. *The map $\eta : R \longrightarrow \mathbb{F}_q^4$ defined in (2.1) is an $\mathbb{F}_q$-linear and distance-preserving map from (R^n, d_L) to $(\mathbb{F}_q^{4n}, d_H)$, where $d_L = d_H$.*

Define $\Theta_1 \otimes \Theta_2 \otimes \Theta_3 \otimes \Theta_4 = \{(\theta_1,\ \theta_2,\ \theta_3,\ \theta_4) \mid \theta_i \in \Theta_i :\ 1 \leq i \leq 4\}$ and $\Theta_1 \oplus \Theta_2 \oplus \Theta_3 \oplus \Theta_4 = \{(\theta_1 + \theta_2 + \theta_3 + \theta_4) \mid \theta_i \in \Theta_i :\ 1 \leq i \leq 4\}$. Let C be a linear code of length n over R. We assume that

$$\mathcal{C}_1 = \{z_1 \in \mathbb{F}_q^n \mid \Delta_1 z_1 + \Delta_2 z_2 + \Delta_3 z_3 + \Delta_4 z_4 \in \mathcal{C},\ \textit{where}\ z_2,\ z_3,\ z_4 \in \mathbb{F}_q^n\},$$

$$\mathcal{C}_2 = \{z_2 \in \mathbb{F}_q^n \mid \Delta_1 z_1 + \Delta_2 z_2 + \Delta_3 z_3 + \Delta_4 z_4 \in \mathcal{C},\ \textit{where}\ z_1,\ z_3,\ z_4 \in \mathbb{F}_q^n\},$$

$$\mathcal{C}_3 = \{z_3 \in \mathbb{F}_q^n \mid \Delta_1 z_1 + \Delta_2 z_2 + \Delta_3 z_3 + \Delta_4 z_4 \in \mathcal{C},\ \textit{where}\ z_1,\ z_2,\ z_4 \in \mathbb{F}_q^n\}$$

and

$$\mathcal{C}_4 = \{z_4 \in \mathbb{F}_q^n \mid \Delta_1 z_1 + \Delta_2 z_2 + \Delta_3 z_3 + \Delta_4 z_4 \in \mathcal{C},\ \textit{where}\ z_1,\ z_2,\ z_3 \in \mathbb{F}_q^n\}.$$

Now, each $\mathcal{C}_i$ is a linear code of length n over $\mathbb{F}_q$, for $1 \leq i \leq 4$. Hence, any linear code of length n can be represented as $\mathcal{C} = \Delta_1\mathcal{C}_1 \oplus \Delta_2\mathcal{C}_2 \oplus \Delta_3\mathcal{C}_3 \oplus \Delta_4\mathcal{C}_4$ such that $|\mathcal{C}| = |\mathcal{C}_1||\mathcal{C}_2||\mathcal{C}_3||\mathcal{C}_4|$ over R. A matrix is called a generator matrix of $\mathcal{C}$ if the rows of the matrix generate $\mathcal{C}$. If M_i are the generator matrices of the linear code $\mathcal{C}_i$, for $i = 1, 2, 3, 4$, respectively, then a generator matrix of $\mathcal{C}$ is

$$M = \begin{pmatrix} \Delta_1 M_1 \\ \Delta_2 M_2 \\ \Delta_3 M_3 \\ \Delta_4 M_4 \end{pmatrix}$$

and a generator matrix of $\eta(\mathcal{C})$ is

$$\eta(M) = \begin{pmatrix} \eta(\Delta_1 M_1) \\ \eta(\Delta_2 M_2) \\ \eta(\Delta_3 M_3) \\ \eta(\Delta_4 M_4) \end{pmatrix}.$$

Proposition 2.2. *Let* $\mathcal{C} = \Delta_1\mathcal{C}_1 \oplus \Delta_2\mathcal{C}_2 \oplus \Delta_3\mathcal{C}_3 \oplus \Delta_4\mathcal{C}_4$ *be a linear code of length* n *over* R*. Then,* $\eta(\mathcal{C})$ *is a* $[4n,\ \sum_{i=1}^{4} k_i,\ d]$ *linear code over* $\mathbb{F}_q$ *for* $1 \leq i \leq 4$*, where each* $\mathcal{C}_i$ *is* $[n,\ k_i,\ d]$*.*

Proof. The proof is obvious with the help of the Gray map.

□

Proposition 2.3. *If $\mathcal{C}$ is a linear code of length n over R, then $\eta(\mathcal{C}) = \mathcal{C}_1 \otimes \mathcal{C}_2 \otimes \mathcal{C}_3 \otimes \mathcal{C}_4$.*

Proof. The proof is similar to the one in [7]. □

Theorem 2.1. *Let $\mathcal{C}$ be a self-orthogonal linear code of length n over R and A be a 4×4 non-singular matrix over $\mathbb{F}_q$ which has the property $AA^T = \epsilon I_4$, where I_4 is the identity matrix, $0 \neq \epsilon \in \mathbb{F}_q$, and A^T is the transpose of matrix A. Then, the Gray image $\eta(\mathcal{C})$ is a self-orthogonal linear code of length $4n$ over $\mathbb{F}_q$.*

3 Structural properties of cyclic codes over R

We will examine various structural properties of cyclic codes on a ring R and present some results. We start with the definition that follows:

Definition 3.1. *A linear code $\mathcal{C}$ of length n over R is said to be a cyclic code if every cyclic shift of a codeword in $\mathcal{C}$ is again a codeword in $\mathcal{C}$, i.e., $(c_0, c_1, c_2, \dots, c_{n-1}) \in \mathcal{C}$, its cyclic shift $(c_{n-1}, c_0, \dots, c_{n-2}) \in \mathcal{C}$.*

Theorem 3.1. *Let $\mathcal{C} = \Delta_1\mathcal{C}_1 \oplus \Delta_2\mathcal{C}_2 \oplus \Delta_3\mathcal{C}_3 \oplus \Delta_4\mathcal{C}_4$ be a linear code of length n over R. Then, $\mathcal{C}$ is a cyclic code over R if and only if each $\mathcal{C}_i$ is a cyclic code over $\mathbb{F}_q$, where $1 \leq i \leq 4$.*

Proof. Suppose s is any codeword in $\mathcal{C}$ such that $s = (s_0,\ s_1,\ \dots,\ s_{n-1})$. We can write its components as $s_i = \Delta_1 z_{1,i} + \Delta_2 z_{2,i} + \Delta_3 z_{3,i} + \Delta_4 z_{4,i}$, where $z_{1,i},\ z_{2,i},\ z_{3,i},\ z_{4,i} \in \mathbb{F}_q$ and $1 \leq i \leq n-1$. Let

$$
\begin{aligned}
z_1 &= (z_{0,1},\ z_{1,1},\ \dots,\ z_{n-1,1}),\\
z_2 &= (z_{0,2},\ z_{1,2},\ \dots,\ z_{n-1,2}),\\
z_3 &= (z_{0,3},\ z_{1,3},\ \dots,\ z_{n-1,3}),\\
z_4 &= (z_{0,4},\ z_{1,4},\ \dots,\ z_{n-1,4}),
\end{aligned}
$$

where $z_i \in \mathcal{C}_i$ and $1 \leq i \leq 4$. Now, let us assume that every $\mathcal{C}_i$ is a cyclic code over $\mathbb{F}_q$, where $1 \leq i \leq 4$. This implies that

$$\begin{aligned}\zeta(z_1) &= (z_{n-1,1},\ z_{0,1},\ \ldots,\ z_{n-2,1}) \in \mathcal{C}_1,\\ \zeta(z_2) &= (z_{n-1,2},\ z_{0,2},\ \ldots,\ z_{n-2,2}) \in \mathcal{C}_2,\\ \zeta(z_3) &= (z_{n-1,3},\ z_{0,3},\ \ldots,\ z_{n-2,3}) \in \mathcal{C}_3,\\ \zeta(z_4) &= (z_{n-1,4},\ z_{0,4},\ \ldots,\ z_{n-2,4}) \in \mathcal{C}_4,\end{aligned}$$

Thus, $\Delta_1\zeta(z_1) + \Delta_2\zeta(z_2) + \Delta_3\zeta(z_3) + \Delta_4\zeta(z_4) \in \mathcal{C}$. It can easily be seen that $\Delta_1\zeta(z_1) + \Delta_2\zeta(z_2) + \Delta_3\zeta(z_3) + \Delta_4\zeta(z_4) = \zeta(s)$. Hence, $\zeta(s) \in \mathcal{C}$. We can conclude that $\mathcal{C}$ is a cyclic code over R.

On the other hand, let us assume that $\mathcal{C}$ is a cyclic code over R. Next, let us consider $s_i = \Delta_1 z_{1,i} + \Delta_2 z_{2,i} + \Delta_3 z_{3,i} + \Delta_4 z_{4,i}$, where $z_1 = (z_{0,1},\ z_{1,1},\ \ldots,\ z_{n-1,1})$, $z_2 = (z_{0,2},\ z_{1,2},\ \ldots,\ z_{n-1,2})$, $z_3 = (z_{0,3},\ z_{1,3},\ \ldots,\ z_{n-1,3})$ and $z_4 = (z_{0,4},\ z_{1,4},\ \ldots,\ z_{n-1,4})$. Then, $z_1 \in \mathcal{C}_1,\ z_2 \in \mathcal{C}_2,\ z_3 \in \mathcal{C}_3,\ \textit{and}\ z_4 \in \mathcal{C}_4$. Again, $s = (s_0,\ s_1,\ \ldots,\ s_{n-1}) \in \mathcal{C}$, by the hypothesis $\zeta(s) \in \mathcal{C}$. We have $\Delta_1\zeta(z_1) + \Delta_2\zeta(z_2) + \Delta_3\zeta(z_3) + \Delta_4\zeta(z_4) \in \mathcal{C}$. Here, $\zeta(z_i) \in \mathcal{C}_i$, where $1 \leq i \leq 4$. Consequently, every $\mathcal{C}_i$ is a cyclic code of length n over $\mathbb{F}_q$, where $1 \leq i \leq 4$.

□

Theorem 3.2. *Let $\mathcal{C} = \Delta_1\mathcal{C}_1 \oplus \Delta_2\mathcal{C}_2 \oplus \Delta_3\mathcal{C}_3 \oplus \Delta_4\mathcal{C}_4$ be a cyclic code of length n over R and $h_i(z)$ be a standard generator polynomial of $\mathcal{C}_i$. Then, $\mathcal{C} = \langle h(z)\rangle$ and $|\mathcal{C}| = q^{4n-\sum_{i=0}^{4} h_i(z)}$, where $h(z) = \Delta_1 h_1(z) + \Delta_2 h_2(z) + \Delta_3 h_3(z) + \Delta_4 h_4(z)$ and $1 \leq i \leq 4$.*

Proof. Given $\mathcal{C}_i = \langle h_i(z)\rangle$, where $1 \leq i \leq 4$ and $\mathcal{C} = \Delta_1\mathcal{C}_1 \oplus \Delta_2\mathcal{C}_2 \oplus \Delta_3\mathcal{C}_3 \oplus \Delta_4\mathcal{C}_4$. Let $c \in \mathcal{C}$ be such that $c = \{c(z) \mid \Delta_1 h_1(z) + \Delta_2 h_2(z) + \Delta_3 h_3(z) + \Delta_4 h_4(z) \text{ for } h_i(z) \in \mathcal{C}_i\}$. Therefore, $\mathcal{C} \subseteq \langle \Delta_1 h_1(z),\ \Delta_2 h_2(z),\ \Delta_3 h_3(z),\ \Delta_4 h_4(z)\rangle \subseteq R[z]/\langle z^n - 1\rangle$. For any $\Delta_1 t_1(z) h_1(z) + \Delta_2 t_2(z) h_2(z) + \Delta_3 t_3(z) h_3(z) + \Delta_4 t_4(z) h_4(z) \in \langle \Delta_1 h_1(z) + \Delta_2 h_2(z) + \Delta_3 h_3(z) + \Delta_4 h_4(z)\rangle \subseteq R[z]/\langle z^n - 1\rangle$, where $t_1(z), t_2(z), t_3(z)$ and $t_4(z) \in R[z]/\langle z^n - 1\rangle$,
then there exist $s_1(z), s_2(z), s_3(z)$ and $s_4(z) \in \mathbb{F}_q[z]$ such that

$$\Delta_i t_i(z) = \Delta_i s_i(z),$$

where $1 \leq i \leq 4$. Hence, $\langle \Delta_1 h_1(z),\ \Delta_2 h_2(z),\ \Delta_3 h_3(z),\ \Delta_4 h_4(z) \rangle \subseteq \mathcal{C}$. This implies $\langle \Delta_1 h_1(z),\ \Delta_2 h_2(z),\ \Delta_3 h_3(z),\ \Delta_4 h_4(z) \rangle = \mathcal{C}$. Since $|\mathcal{C}| = |\mathcal{C}_1||\mathcal{C}_2||\mathcal{C}_3|$ $|\mathcal{C}_4|$, we have

$$|\mathcal{C}| = q^{4n - \sum\limits_{i=0}^{4} h_i(z)}.$$

□

Theorem 3.3. *Let $\mathcal{C} = \Delta_1 \mathcal{C}_1 \oplus \Delta_2 \mathcal{C}_2 \oplus \Delta_3 \mathcal{C}_3 \oplus \Delta_4 \mathcal{C}_4$ be a cyclic code of length n over R; there exists a unique monic polynomial $h(z) \in R[z]$ such that $\mathcal{C} = \langle h(z) \rangle$ and $h(z)$ divides $(z^n - 1)$. If $h_i(z)$ is the standard generator polynomial of $\mathcal{C}_i$, $1 \leq i \leq 4$, then $h(z) = \Delta_1 h_1(z) + \Delta_2 h_2(z) + \Delta_3 h_3(z) + \Delta_4 h_4(z)$.*

Proof. By Theorem 3.2, $\mathcal{C} = \langle \Delta_1 h_1(z),\ \Delta_2 h_2(z),\ \Delta_3 h_3(z),\ \Delta_4 h_4(z) \rangle$, where $h_i(z)$ is the generator polynomial of $\mathcal{C}_i$ and $1 \leq i \leq 4$. Let $h(z) = \Delta_1 h_1(z) + \Delta_2 h_2(z) + \Delta_3 h_3(z) + \Delta_4 h_4(z)$. From here, $\langle h(z) \rangle \subseteq \mathcal{C}$. Now, $\Delta_i h_i(z) = \Delta_i h(z)$ and $1 \leq i \leq 4$, so $\mathcal{C} \subseteq \langle h(z) \rangle$, hence $\mathcal{C} = \langle h(z) \rangle$. Since $h_i(z)$ is a monic right divisor of $(z^n - 1)$, there are $s_i(z) \in \mathbb{F}_q[z]/\langle z^n - 1 \rangle$, where $1 \leq i \leq 4$, such that $z^n - 1 = s_1(z)h_1(z) = s_2(z)h_2(z) = s_3(z)h_3(z)$ $= s_4(z)h_4(z)$. This shows that $z^n - 1 = [\Delta_1 s_1(z) + \Delta_2 s_2(z) + \Delta_3 s_3(z) + \Delta_4 s_4(z)]h(z)$, i.e., $h(z)|(z^n - 1)$. Here, each $h_i(z)$ is unique, and hence $h(z)$ is unique.

□

Theorem 3.4. *Let $\mathcal{C} = \Delta_1 \mathcal{C}_1 \oplus \Delta_2 \mathcal{C}_2 \oplus \Delta_3 \mathcal{C}_3 \oplus \Delta_4 \mathcal{C}_4$ be a cyclic code of length n over R. Then, $\mathcal{C}^\perp = \Delta_1 \mathcal{C}_1^\perp \oplus \Delta_2 \mathcal{C}_2^\perp \oplus \Delta_3 \mathcal{C}_3^\perp \oplus \Delta_4 \mathcal{C}_4^\perp$ is also a cyclic code of length n over R.*

Proof. $\mathcal{C}^\perp$ is a cyclic code of length n over R, since $\mathcal{C}$ is a cyclic code of length n over R. Now, we will show that $\mathcal{C}^\perp = \Delta_1 \mathcal{C}_1^\perp \oplus \Delta_2 \mathcal{C}_2^\perp \oplus \Delta_3 \mathcal{C}_3^\perp \oplus \Delta_4 \mathcal{C}_4^\perp$. Here, $\mathcal{C}$ is a cyclic code of of length n over R. This implies $\mathcal{C}$ is a linear code of length n over R. Let $T_1 = \{t_1 \in \mathbb{F}_q^n \mid \exists\ t_2,\ t_3,\ t_4$ such that $\sum\limits_{i=1}^{4} t_i \Delta_i \in \mathcal{C}^\perp\}$, for $1 \leq i \leq 4$. Hence, $\mathcal{C}^\perp$ is uniquely expressed as $\mathbb{C}^\perp = \oplus_{i=1}^4 \Delta_i T_i$. Therefore, $T_1 \subseteq \mathcal{C}_1^\perp$. Conversely, let $q \in \mathcal{C}_1^\perp$.

This implies $q \cdot s_1 = 0 \ \forall \ s_1 \in \mathcal{C}_1$. Consider $y = \sum_{i=1}^{4} \Delta_i s_i \in \mathcal{C}$. Now, $\Delta_1 q \cdot y = \Delta_1 s_1 \cdot q = 0$. This shows that $\Delta_1 q \in \mathcal{C}_1^{\perp}$. From the specific expression of $\mathcal{C}^{\perp}$, we obtain $q \in T_1$. From here, $\mathcal{C}^{\perp} \subseteq T_1$. Therefore, $\mathcal{C}_1^{\perp} = T_1$. In the same manner, $\mathcal{C}_i^{\perp} = T_i$ for $1 \leq i \leq 4$. Hence, $\mathcal{C}^{\perp} = \Delta_1 \mathcal{C}_1^{\perp} \oplus \Delta_2 \mathcal{C}_2^{\perp} \oplus \Delta_3 \mathcal{C}_3^{\perp} \oplus \Delta_4 \mathcal{C}_4^{\perp}$.

□

Lemma 3.1. *[9] Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ with a generator polynomial $h(z)$ that contains its dual if and only if*

$$z^n - 1 \equiv 0 \ (mod \ h(z)h^*(z)),$$

where the reciprocal polynomial of $h(z)$ is denoted by $h^*(z)$.

Theorem 3.5. *Let $\mathcal{C} = \Delta_1 \mathcal{C}_1 \oplus \Delta_2 \mathcal{C}_2 \oplus \Delta_3 \mathcal{C}_3 \oplus \Delta_4 \mathcal{C}_4$ be a cyclic code of length n over R and $\mathcal{C} = \langle h(z) \rangle = \langle \sum_{i=1}^{4} \Delta_i h_i(z) \rangle$, where $h_i(z)$ is the generator polynomial of $\mathcal{C}_i$. Then, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ if and only if*

$$z^n - 1 \equiv 0 \ (mod \ h_i(z)h_i^*(z)),$$

where the reciprocal polynomial of $h_i(z)$ is denoted by $h_i^*(z)$ and $1 \leq i \leq 4$.

Proof. Suppose $z^n - 1 \equiv 0 \ (mod \ h_i(z)h_i^*(z))$ for $1 \leq i \leq 4$. Hence, by Lemma 3.1, we have $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i$. From here, we can write $\Delta_i \mathcal{C}^{\perp} \subseteq \Delta_i \mathcal{C}_i$ for $1 \leq i \leq 4$. Similarly, $\mathcal{C}^{\perp} = \sum_{i=0}^{4} \Delta_i C_i^{\perp} \subseteq \sum_{i=0}^{4} \Delta_i \mathcal{C}_i = \mathcal{C}$. Conversely, assume $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ and $\sum_{i=0}^{4} \Delta_i \mathcal{C}_i^{\perp} \subseteq \sum_{i=0}^{4} \Delta_i \mathcal{C}_i$, but each $\mathcal{C}_i$ is a cyclic code over $\mathbb{F}_q$ such that $\Delta_i \mathcal{C}_i \equiv \mathcal{C}(mod \Delta_i)$. This implies that $\mathcal{C}_i^{\perp} \subseteq \mathcal{C}_i$, where $1 \leq i \leq 4$. By Lemma 3.1, we obtain

$$z^n - 1 \equiv 0 \ (mod \ h_i(z)h_i^*(z)),$$

where the reciprocal polynomial of $h_i(z)$ is denoted by $h_i^*(z)$ for $1 \leq i \leq 4$.

□

Corollary 3.1. *Let $\mathcal{C} = \Delta_1\mathcal{C}_1 \oplus \Delta_2\mathcal{C}_2 \oplus \Delta_3\mathcal{C}_3 \oplus \Delta_4\mathcal{C}_4$ be a cyclic code of length n over R. Then, $\mathcal{C}^\perp \subseteq \mathcal{C}$ if and only if $\mathcal{C}_i^\perp \subseteq \mathcal{C}_i$ and $1 \leq i \leq 4$.*

4 Quantum codes over R

The study of quantum codes over the ring R is the subject of this section. We start with the definition that follows: If m is a positive integer and p is a prime, then $q = p^m$. Let q-dimensional Hilbert space $H(\mathbb{C})$ over the complex field $\mathbb{C}$. Then, the set of n-folded tensor products $H(\mathbb{C})^n = \underbrace{H \otimes H \otimes \ldots \otimes H}_{n-times}$ is also a q^n-dimensional Hilbert space.

Definition 4.1. *[15] A quantum code represented by $[[n, k, d]]_q$ is defined as a subspace of $H(\mathbb{C})^n$ with dimension q^k and minimum distance d. Moreover, we consider $[[n, k, d]]_q$ to be better than $[[n^{'}, k^{'}, d^{'}]]_q$ if either or both of the following conditions hold:*
(i) $d > d^{'}$ whenever the code rate $\frac{k}{n} = \frac{k^{'}}{n^{'}}$ (larger distance).
(ii) $\frac{k}{n} > \frac{k^{'}}{n^{'}}$, whenever the distance $d = d^{'}$ (larger code rate).

Lemma 4.1. *([13], Theorem 3) (CSS Construction) Let $\mathcal{C}_1 = [n, k_1, d_1]_q$ and $\mathcal{C}_2 = [n, k_2, d_2]_q$ be two linear codes over GF(q) with $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1$. Furthermore, let $d = min\{wgt(v) : v \in (\mathcal{C}_1 \backslash \mathcal{C}_2^\perp) \cup (\mathcal{C}_2 \backslash \mathcal{C}_1^\perp)\} \geq min(d_1, d_2)$. Then, there exists a QEC code with the parameters $[[n, k_1 + k_2 - n, d]]_q$. In particular, if $\mathcal{C}_1^\perp \subseteq \mathcal{C}_1$, then there exists a QEC code with the parameters $[[n, 2k_1 - n, d_1]]_q$, where $d_1 = min\{wgt(v) : v \in (\mathcal{C}_1 \backslash \mathcal{C}_1^\perp)\}$.*

Theorem 4.1. *Let $\mathcal{C}$ be a cyclic code of length n over R and let the parameters of its Gray image be $[4n, k, d_H]$. If $\mathcal{C}^\perp \subseteq \mathcal{C}$, then there exists a QECC $[[4n, 2k - 4n, d_H]]$ over $\mathbb{F}_q$.*

5 Applications

In this section, we present some applications of the results proved in the previous sections. The Examples 5.1–5.3 and Table 1 demonstrate that our results provide several quantum codes better than the existing quantum codes that appeared in references ([1], [2], [3], [4], [6], [10], and [16]). All of the computations involved in these examples are accomplished by using the Magma computation system [8]. We begin our discussions with the following:

Example 5.1. *Let* $R = \mathbb{F}_7[u_1, u_2]/\langle u_1^2-1,\ u_2^2-1,\ u_1u_2-u_2u_1\rangle$ *be a finite commutative ring,* $n = 7$ *and* $\alpha = 1$*. Then,*

$$z^7 - 1 = (z+6)^7 \in \mathbb{F}_7[x].$$

Take

$$\begin{aligned} h_1(z) &= 1 \\ h_2(z) &= (z+6) \\ h_3(z) &= (z+6) \\ h_4(z) &= (z+6)^6 \end{aligned}$$

and

$$A = \begin{bmatrix} 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ 4 & 0 & 0 & 0 \end{bmatrix}.$$

Here, matrix A *satisfies the condition* $AA^T = 2I_{4\times4}$*, where* $A \in GL_4(\mathbb{F}_7)$ *and* $I_{4\times4}$ *is an identity matrix. The cyclic code* $\mathcal{C} = \langle \sum_{i=0}^{4} \Delta_i h_i(z)\rangle$ *is of length* 7 *over* R *and its Gray image is of length* 28*, dimension* 20*, and distance* 7 *over* $\mathbb{F}_7$*, i.e.,* $[28, 20, 7]_7$*. However,*

$$z^7 - 1 \equiv\ 0\ (mod\ h_i(z)h_i^*(z)),$$

for $1 \le i \le 4$*. Thus,* $\mathcal{C}^\perp \subseteq \mathcal{C}$ *by Theorem 3.5. In view of Theorem 4.1, we conclude that there exists a quantum code* $[[28, 12, 7]]_7$*. This quantum code is a new quantum code (see [5] for details).*

Example 5.2. *Let* $R = \mathbb{F}_{19}[u_1, u_2]/\langle u_1^2-4,\ u_2^2-1,\ u_1u_2-u_2u_1\rangle$ *be a finite commutative ring,* $n = 19$ *and* $\alpha = 2$*. Then,*

$$z^{19} - 1 = (z+18)^{19} \in \mathbb{F}_{19}[x].$$

Take

$$h_1(z) = (z+18)$$
$$h_2(z) = (z+18)^2$$
$$h_3(z) = (z+18)^3$$
$$h_4(z) = (z+18)^{14}$$

and

$$A = \begin{bmatrix} 0 & 9 & 0 & 0 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 9 \\ 9 & 0 & 0 & 0 \end{bmatrix}.$$

Here, matrix A satisfies the condition $AA^T = 5I_{4\times 4}$, where $A \in GL_4(\mathbb{F}_{19})$ and $I_{4\times 4}$ is an identity matrix. The cyclic code $\mathcal{C} = \langle \sum_{i=0}^{4} \Delta_i h_i(z) \rangle$ is of length 19 *over R and its Gray image is of length* 76*, dimension* 56*, and distance* 15 *over $\mathbb{F}_{19}$, i.e., $[76, 56, 15]_{19}$. However,*

$$z^{19} - 1 \equiv 0 \ (mod\ h_i(z)h_i^*(z)),$$

for $1 \leq i \leq 4$. Application of Theorem 3.5 yields $\mathcal{C}^\perp \subseteq \mathcal{C}$. By Theorem 4.1, we conclude that there exists a quantum code $[[76, 36, 15]]_{19}$ which has a larger code rate and larger minimum distance than the previous known quantum code $[[76, 22, 11]]_{19}$ (see [2] for details). Hence, our quantum code $[[76, 36, 15]]_{19}$ is better than the previous known quantum code $[[76, 22, 11]]_{19}$ appeared in [2]. $[[76, 36, 15]]_{19}$ is also a new quantum code.

Example 5.3. *Let $R = \mathbb{F}_{13}[u_1, u_2]/\langle u_1^2 - 1,\ u_2^2 - 1,\ u_1u_2 - u_2u_1 \rangle$ be a finite commutative ring, $n = 78$ and $\alpha = 1$. Then,*

$$z^{78} - 1 = (z+1)^{13}(z+3)^{13}(z+4)^{13}(z+9)^{13}(z+10)^{13}(z+12)^{13} \in \mathbb{F}_{13}[x].$$

Take

$$h_1(z) = h_2(z) = (z+1)^2(z+4)$$
$$h_3(z) = h_4(z) = (z+1)^2(z+10)$$

and

$$A = \begin{bmatrix} 0 & 9 & 0 & 0 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 9 \\ 9 & 0 & 0 & 0 \end{bmatrix}.$$

Here, matrix A satisfies the condition $AA^T = 3I_{4\times 4}$, where $A \in GL_4(\mathbb{F}_{13})$ and $I_{4\times 4}$ is an identity matrix. The cyclic code $\mathcal{C} = \langle \sum_{i=0}^{4} \Delta_i h_i(z)\rangle$ is of length 78 *over R and its Gray image is of length* 312*, dimension* 300*, and distance* 3 *over $\mathbb{F}_{13}$, i.e., $[312, 300, 3]_{13}$. However,*

$$z^{78} - 1 \equiv 0 \ (mod\ h_i(z)h_i^*(z)),$$

for $1 \leq i \leq 4$. This implies that, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. In view of Theorem 4.1, we conclude that there exists a quantum code $[[312, 288, 3]]_{13}$, which has same minimum distance but larger code rate than the previous known quantum code $[[312, 282, 3]]_{13}$ (see [10] for details). Therefore, our quantum code $[[312, 288, 3]]_{13}$ is better than the previous known quantum code $[[312, 282, 3]]_{13}$ appeared in [10].

Table 1. Quantum codes from cyclic codes over R.

n	$h_1(z)$	$h_2(z)$	$h_3(z)$	$h_4(z)$	$\eta(C)$	$[[n,\ k,\ d]]_q$	$[[n',\ k',\ d']]_q$
15	$z+1$	$z+1$	$z+4$	$z+4$	$[60, 56, 2]$	$[[60, 52, 2]]_5$	$[[60, 48, 2]]_5$ [3]
20	$(z+1)^2$ $(z+3)$	$(z+1)^2$ $(z+3)$	$(z+1)$ $(z+3)^2$	$(z+1)$ $(z+3)^2$	$[80, 68, 3]$	$[[80, 56, 3]]_5$	$[[80, 54, 3]]_5$ [6]
30	$(z+4)$ $(z^2+4z+1)^2$	$(z+4)^2$ $(z^2+4z+1)^2$	$(z^2+z+1)^2$ $(z+1)$	$(z^2+z+1)^2$ $(z+1)$	$[120, 100, 3]$	$[[120, 80, 3]]_5$	$[[120, 32, 3]]_5$ [16]
31	1 (z^4+4z^2+3z+4)	$z+4$	$z+4$	(z^3+2z^2+z+4)	$[124, 115, 3]$	$[[124, 106, 3]]_5$	$[[124, 100, 4]]_5$ [2]
33	(z^2+z+1) $(z^5+4z^4+$ $4z^3+z^2+z+4)$	(z^2+z+1) $(z^5+4z^4+$ $4z^3+z^2+z+4)$	(z^2+z+1) $(z^5+4z^4+$ $4z^3+z^2+z+4)$	(z^2+z+1) $(z^5+4z^4+$ $4z^3+z^2+z+4)$	$[132, 104, 4]$	$[[132, 76, 4]]_5$	$[[132, 72, 2]]_5$ [4]
40	$z+3$	$z+3$	$z+4$	$z+4$	$[160, 156, 2]$	$[[160, 152, 2]]_[5]$	$[[160, 146, 2]]_5$ [1]
42	$(z+1)$ $(z^6+3z^4+$ $z^3+2z^2+4)$	$(z+1)$ $(z^6+3z^4+$ $z^3+2z^2+4)$	$(z+1)$ $(z^6+3z^4+$ $z^3+2z^2+4)$	$(z+1)$ $(z^6+3z^4+$ $z^3+2z^2+4)$	$[168, 140, 4]$	$[[168, 112, 4]]_5$	$[[168, 96, 2]]_5$ [4]
45	$z+4$	$z+4$	$z+4$	$z+4$	$[180, 176, 2]$	$[[180, 172, 2]]_5$	$[[180, 166, 2]]_5$ [1]
24	1	$z+2$	$z+2$	$(z+2)$ (z^2+2z+2)	$[96, 91, 3]$	$[[96, 86, 3]]_7$	$[[96, 80, 3]]_7$ [2]
78	$(z+1)^2)$ $(z+4$	$(z+1)^2$ $(z+4)$	$(z+1)^2$ $(z+10)$	$(z+1)^2$ $(z+10)$	$[312, 300, 3]$	$[[312, 288, 3]]_{13}$	$[[312, 282, 3]]_{13}$ [10]
19	$z+18$	$(z+18)^2$	$(z+18)^3$	$(z+18)^{14}$	$[76, 56, 15]$	$[[76, 36, 15]]_{19}$	$[[76, 22, 11]]_{19}$ [2]

In Table 1, we present QEC codes by using cyclic codes $\mathcal{C} = \langle \sum_{i=0}^{4} \Delta_i h_i(z)\rangle$ of length n over R, where $\mathcal{C}_i = \langle h_i(z)\rangle$ such that $z^n - 1 \equiv 0\ (mod\ h_i(z)h_i^*(z))$, for $i = 1, 2, 3, 4$. It is noted that our obtained QEC codes $[[n, k, d]]_q$ are better than the existing quantum codes $[[n^{'}, k^{'}, d^{'}]]_q$ collected from the different references mentioned in this article.

6 Conclusion

In this article, we discuss some of the structural properties of cyclic codes over the ring $R = \mathbb{F}_q[u_1, u_2]/\langle u_1^2 - \alpha^2,\ u_2^2 - 1,\ u_1u_2 - u_2u_1\rangle$, where α is the non-zero element of $\mathbb{F}_q$. Furthermore, we obtain better quantum codes than presented in [1], [2], [3], [4], [6], [10], and [16].

Acknowledgements

The authors express their appreciation to the anonymous referee(s) whose feedback helped us to prepare a better final version of this paper.

References

[1] Alkenani, A. N., Ashraf, M., Mohammad, G.: Quantum codes from the constacyclic codes over the ring $F_q[u_1, u_2]/\langle u_1^2 - u_1, u_2^2 - u_2, u_1u_2 - u_2u_1\rangle$. Mathematics 8(5)(2020), 781. https://doi.org/10.3390/ math8050781.

[2] Ashraf, M., Khan, N., and Mohammad, G.: New Quantum and LCD Codes Over the Finite Field of Odd Characteristic. International Journal of Theoretical Physics, 60(6)(2021), 2322-2332.

[3] Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over $F_q + uF_q + vF_q + uvF_q$. Quantum Inf. Process. 15(10)(2016), 4089-4098.

[4] Ashraf, M., Mohammad, G.: Quantum codes over F_0p from cyclic codes over $F_p[u, v]/\langle u^2 - 1,\ v^3 - v,\ uv - vu\rangle$. Cryptogr. Commun. 11(2019), 325-335.

[5] Aydin, N., Liu, P., Yoshino, B.: A database of quantum codes. Online available at http://quantumcodes. info/ (2021). Accessed on 2021-08-07.

[6] Bag, T., Dinh, H. Q., Upadhyay, A. K., Yamaka, W.: New non binary quantum codes from cyclic codes over product ring. IEEE Commun. Lett., 24(3)(2019), 486-490.

[7] Bag, T., Upadhyay, A. K., Study on negacyclic codes over the ring $Z_p[u]/\langle u^{k+1} - u\rangle$. J. Appl. Math. Comput. 59(1)(2019), 693-700. https://doi.org/10.1007/s12190-018-1197-5.

[8] Bosma, W., Cannon, J.: Handbook of magma functions. University of Sydney (1995).

[9] Calderbank, A. R., Rains, E. M., Shor, P. M., Sloane, N. J. A.: Quantum error-correction via codes over GF(4). IEEE Trans. Inf Theory 44(1998), 1369-1387.

[10] Dinh, H. Q., Bag, T., Upadhyay, A. K., Ashraf, M., Mohammad, G., and Chinnakum, W. Quantum codes from a class of constacyclic codes over finite commutative rings. J. Algebra Appl., 19(12)(2020), 2150003.

[11] Gao, J.: Quantum codes from cyclic codes over $F_q + vF_q + v^2F_q + v^3F_q$. Int. J. Quantum Inf. 13(8)(2015), 1550063.

[12] Grassl, M.: Code Tables: Bounds on the parameters of various types of codes, avaiblable at http://www.codetables.de/accessed on 07/04/2020.

[13] Grassl, M. and Beth, T.: On optimal quantum codes. Int. J. Quantum Inf. 2(2004), 55-64.

[14] Islam, H., Prakash, O.: Construction of LCD and new quantum codes from cyclic codes over a finite non chain ring. Cryptogr. Commun. 14(2022), 59-73. https://doi.org/10.1007/s12095-021-00516-9.

[15] Islam, H., Prakash, O.: New quantum and LCD codes over the finite field of even characteristic. Defence Science Journal, 71(5)(2020), 656-661.

[16] Islam, H., Prakash, O.: Quantum codes from the cyclic codes over $F_p[u, v, w]/\langle u^2 - 1, v^2 - 1, w^2 - 1, uv - vu, vw - wv, wu - uw\rangle$. J. Appl. Math. Comput. 60(1-2)(2019), 625-635.

[17] Kai, X. and Zhu, S.: Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$. Int. J. Quantum Inf. 9(2011), 689-700.

[18] Li, R., Xu, Z. and Li, X.: Binary construction of quantum codes of minimum distance three and four. IEEE Trans. Inf. Theory 50(2004), 1331-1335.

[19] Özen, M., Özzaim, N. T. and Ince, H.: Quantum codes from cyclic codes over $F_3 + uF_3 + vF_3 + uvF_3$. Int. Conf. Quantum Sci. Appl. J. Phys. Conf. Ser. 766(2016), 012020-1-012020-6 .

[20] Qian, J., Ma, W. and Gou, W.: Quantum codes from cyclic codes over finite ring. Int. J. Quantum Inf. 7(2009), 1277-1283.