axioms

IMPACT FACTOR 1.824

CITESCORE 2.6

Article

On the Construction of Quantum and LCD Codes from Cyclic Codes over the Finite Commutative Rings

Shakir Ali, Amal S. Alali, Mohammad Jeelani, Muhammet Kurulay, Elif Segah Öztas and Pushpendra Sharma

Special Issue
Mathematical Modelling and Applications

Edited by
Dr. Chihhsiong Shih

MDPI

https://doi.org/10.3390/axioms12040367

axioms

MDPI

Article

On the Construction of Quantum and LCD Codes from Cyclic Codes over the Finite Commutative Rings

Shakir Ali [1,*], Amal S. Alali [2], Mohammad Jeelani [3], Muhammet Kurulay [4], Elif Segah Öztas [5] and Pushpendra Sharma [1]

[1] Department of Mathematics, Faculty of Science, Aligarh Muslim University, Aligarh 202002, India
[2] Department of Mathematical Sciences, College of Science, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; asalali@pnu.edu.sa
[3] Department of Computer Application, Faculty of Science, Integral University, Lucknow 226001, India
[4] Department of Mathematics, Yildiz Technical University, Istanbul 34000, Turkey
[5] Department of Mathematics, Karamanoglu Mehmetbey University, Karaman 70100, Turkey
* Correspondence: shakir.ali.mm@amu.ac.in

Abstract: Let $\mathbb{F}_q$ be a field of order q, where q is a power of an odd prime p, and α and β are two non-zero elements of $\mathbb{F}_q$. The primary goal of this article is to study the structural properties of cyclic codes over a finite ring $R = \mathbb{F}_q[u_1, u_2]/\langle {u_1}^2 - \alpha^2,\ u_2^2 - \beta^2,\ u_1u_2 - u_2u_1\rangle$. We decompose the ring R by using orthogonal idempotents $\Delta_1, \Delta_2, \Delta_3$, and Δ_4 as $R = \Delta_1 R \oplus \Delta_2 R \oplus \Delta_3 R \oplus \Delta_4 R$, and to construct quantum-error-correcting (QEC) codes over R. As an application, we construct some optimal LCD codes.

Keywords: cyclic code; Gray map; quantum code; LCD code

MSC: 94B05; 94B15; 94B60

Citation: Ali, S.; Alali, A.S.; Jeelani, M.; Kurulay, M.; Öztas, E.S.; Sharma, P. On the Construction of Quantum and LCD Codes from Cyclic Codes over the Finite Commutative Rings. *Axioms* **2023**, *12*, 367. https://doi.org/10.3390/axioms12040367

Academic Editor: Chihhsiong Shih

Received: 2 February 2023
Revised: 22 February 2023
Accepted: 4 April 2023
Published: 10 April 2023

1. Introduction

Throughout this paper, unless indicated otherwise, $\mathbb{F}_q$ (where q is an odd prime power) denotes the field of order q, and α and β are non-zero elements of $\mathbb{F}_q$. Next, let us consider the finite ring $R = \mathbb{F}_q[u_1, u_2]/\langle u_1^2 - \alpha^2,\ u_2^2 - \beta^2,\ u_1u_2 - u_2u_1\rangle$. It is straightforward to check that R is a non-chain semi-local ring of order q^4. Cyclic codes are very useful for the construction of quantum-error-correcting (QEC) codes. QEC codes are different from classical-error-correcting (CEC) codes. A significant breakthrough happened in 1998, when Calderbank et al. [1] solved the problem of obtaining QEC codes with the help of CEC codes over GF (4). Calderbank et al. [1] also introduced a method to construct QEC codes from CEC codes. Over finite fields, cyclic codes have been extensively investigated (see, for example, [2–5] 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. [6] constructed new quantum codes over $\mathbb{F}_q$. Afterwards, Ozen et al. [7] 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. [8] 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 [8–13] (and references therein).

In this paper, our main aim is to study the structural properties of cyclic codes over the finite ring R, and to construct quantum-error-correcting (QEC) codes over R. Moreover, we also study LCD codes. The major contributions of this paper are as follows:

1. This paper provides superior quantum codes to those presented in recent references [8–13], see Table 1.

2. This paper provides some new quantum codes, see Table 2.
3. This paper investigates some optimal LCD codes over the ring R, see Table 3.

Table 1. Quantum codes from cyclic codes over R.

n	$h_1(z)$	$h_2(z)$	$h_3(z)$	$h_4(z)$	$\eta(\mathcal{C})$	$[[n, k, d]]_q$	$[[n', k', d']]_q$
10	$z+1$	$z+1$	$z+4$	$z+4$	$[40, 36, 2]$	$[[40, 32, 2]]_5$	$[[40, 24, 2]]_5$ [9]
20	$(z+2)^2$ $(z+4)$	$(z+2)^2$ $(z+4)$	$(z+2)^2$ $(z+4)$	$(z+2)^2$ $(z+4)$	$[80, 68, 3]$	$[[80, 56, 3]]_5$	$[[80, 54, 3]]_5$ [11]
22	$z+1$	$z+1$	$z+4$	$z+4$	$[88, 84, 2]$	$[[88, 80, 2]]_5$	$[[88, 48, 2]]_5$ [9]
28	$z+2$	$z+2$	$z+3$	$z+3$	$[112, 108, 2]$	$[[112, 104, 2]]_5$	$[[112, 64, 2]]_5$ [9]
30	$(z+1)^2$ (z^2+z+1)	$(z+1)^2$ (z^2+z+1)	$(z+1)^2$ (z^2+z+1)	$(z+1)^2$ (z^2+z+1)	$[120, 104, 3]$	$[[120, 88, 3]]_5$	$[[120, 32, 3]]_5$ [12]
31	$z+4$	$z+4$	$z+4$	(z^3+z^2+z+4) (z^3+z^2+3z+4)	$[124, 115, 4]$	$[[124, 106, 4]]_5$	$[[124, 100, 4]]_5$ [8]
35	$z+4$	$z+4$	$(z+4)^2$	$(z+4)$ $(z^6+z^5+z^4+$ $z^3+z^2+z+1)$	$[140, 129, 3]$	$[[140, 118, 3]]_5$	$[[140, 112, 2]]_5$ [9]
42	$(z+4)$ $(z^6+2z^4+$ $3z^3+2z^2+1)$	$(z+4)$ $(z^6+2z^4+$ $3z^3+2z^2+1)$	$(z+4)$ $(z^6+2z^4+$ $3z^3+2z^2+1)$	$(z+4)$ $(z^6+2z^4+$ $3z^3+2z^2+1)$	$[168, 140, 4]$	$[[168, 112, 4]]_5$	$[[168, 96, 2]]_5$ [10]
24	$z+3$	$z+3$	$z+3$	$(z+3)$ (z^2+z+4)	$[96, 90, 3]$	$[[96, 84, 3]]_7$	$[[96, 80, 3]]_7$ [8]
78	$(z+3)^2)$ $(z+12$	$(z+3)^2$ $(z+12)$	$(z+3)^2$ $(z+12)$	$(z+3)^2$ $(z+12)$	$[312, 300, 3]$	$[[312, 288, 3]]_{13}$	$[[312, 282, 3]]_{13}$ [13]
12	1	$z+1$	$z+1$	$(z+1)$ $(z^2+4z+16)$ (z^2+z+1)	$[48, 41, 4]$	$[[48, 34, 4]]_{17}$	$[[48, 32, 4]]_{17}$ [8]
19	$z+18$	$z+18$	$(z+18)^2$	$(z+18)^{14}$	$[76, 58, 4]$	$[[76, 40, 4]]_{19}$	...

Table 2. New quantum codes from cyclic codes over R.

n	$h_1(z)$	$h_2(z)$	$h_3(z)$	$h_4(z)$	$\eta(\mathcal{C})$	$[[n, k, d]]_q$	
9	$(z+2)^4$	$(z+2)^2$	$z+2$	1	$[36, 29, 3]$	$[[36, 22, 3]]_3$	*New quantum code*
25	$(z+4)^6$	$z+4$	$z+4$	1	$[100, 92, 3]$	$[[100, 84, 3]]_5$	*New quantum code*
15	$(z+4)^2(z^2+z+1)$	$z+4$	z^2+z+1	1	$[60, 53, 3]$	$[[60, 46, 3]]_5$	*New quantum code*
14	$(z+1)(z+6)^3$	$z+1$	$z+6$	1	$[56, 50, 4]$	$[[56, 44, 4]]_7$	*New quantum code*
11	$(z+10)^5$	$z+10$	$z+10$	1	$[44, 37, 4]$	$[[44, 30, 4]]_{11}$	*New quantum code*

Table 3. Gray images of LCD codes of length n over R.

n	$h_1(z)$	$h_2(z)$	$h_3(z)$	$h_4(z)$	$\eta(\mathcal{C})$	
4	1	$z+1$	$z+1$	$(z+1)(z^2+1)$	$[16, 11, 4]_3$	*Optimal*
22	$z+1$	$z+1$	$z+1$	$z+1$	$[88, 84, 2]_3$	*Optimal*
6	1	$z+1$	$z+1$	$(z+1)(z^2+z+1)$ (z^2+4z+1)	$[24, 17, 4]_5$	...
8	1	$z+1$	$z+1$	$(z+1)(z^2+4z+1)$	$[32, 27, 4]_7$	*Optimal*

Table 3. *Cont.*

n	$h_1(z)$	$h_2(z)$	$h_3(z)$	$h_4(z)$	$\eta(\mathcal{C})$
37	z^6+5z^5 $+5z^4+$ $4z^3+5z^2$ $+5z+1$	z^6+5z^5 $+5z^4+$ $4z^3+5z^2$ $+5z+1$	z^6+4z^5 $+3z^4+$ $7z^3+3z^2$ $4z+1$	z^6+4z^5 $+3z^4+$ $7z^3+3z^2$ $4z+1$	$[148,124,5]11$
39	(z^2+z+1) $(z^{12}+z^{11}$ $+z^{10}+z^9$ $+z^8+z^7+$ $z^6+z^5+z^4$ $+z^3+z^2$ $+z+1)$	(z^2+z+1) $(z^{12}+z^{11}$ $+z^{10}+z^9$ $+z^8+z^7+$ $z^6+z^5+z^4$ $+z^3+z^2$ $+z+1)$	(z^2+z+1) $(z^{12}+z^{11}$ $+z^{10}+z^9$ $+z^8+z^7+$ $z^6+z^5+z^4$ $+z^3+z^2$ $+z+1)$	(z^2+z+1) $(z^{12}+z^{11}$ $+z^{10}+z^9$ $+z^8+z^7+$ $z^6+z^5+z^4$ $+z^3+z^2$ $+z+1)$	$[156,100,4]_{11}$
11	$z^{10}+z^9+z^8$ $+z^7+z^6+$ $z^5+z^4+z^3$ $+z^2+z+1$	$z^{10}+z^9+z^8$ $+z^7+z^6+$ $z^5+z^4+z^3$ $+z^2+z+1$	$z^{10}+z^9+z^8$ $+z^7+z^6+$ $z^5+z^4+z^3$ $+z^2+z+1$	$z^{10}+z^9+z^8$ $+z^7+z^6+$ $z^5+z^4+z^31$ $+z^2+z+1$	$[44,4,11]_{19}$
28	$(z+1)$ $(z^6+z^5+z^4+$ $z^3+z^2+z+1)$ $(z^6+11z^5+3z^4+$ $11z^3+3z^2$ $+11z+1)$	$(z+1)$ $(z^6+z^5+z^4+$ $z^3+z^2+z+1)$ $(z^6+11z^5+3z^4+$ $11z^3+3z^2$ $+11z+1)$	$(z+1)$ $(z^6+z^5+$ $z^4+)$ z^3+z^2+z+ $1)$ $(z^6+8z^5+$ $3z^4+$ $8z^3+3z^2$ $+8z+1)$	$(z+1)$ $(z^6+z^5+z^4+$ $z^3+z^2+z+1)$ $(z^6+8z^5+3z^4+$ $8z^3+3z^2$ $+8z+1)$	$[112,60,8]_{19}$
34	$(z+1)$ $(z^8+13z^7+15z^6+$ $16z^5+8z^4+16z^3$ $+15z^2+13z+1)$	$(z+1)$ $(z^8+13z^7+15z^6+$ $16z^5+8z^4+16z^3$ $+15z^2+13z+1)$	$(z+1)$ $(z^8+13z^7+$ $15z^6+$ $16z^5+8z^4+$ $16z^3$ $+15z^2+13z+$ $1)$	$(z+1)$ $(z^8+13z^7+15z^6+$ $16z^5+8z^4+16z^3$ $+15z^2+13z+1)$	$[136,100,4]_{19}$

2. Preliminary Results

In this section, we deal with the study of some preliminaries and describe the Gray map over the ring R. Moreover, we establish some important results which are needed in 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 elements of $\mathcal{C}$ are called codewords. The size of $\mathcal{C}$ refers to the total number of codewords in $\mathcal{C}$, which is indicated by $|\mathcal{C}|$. We recall some basic definitions as following:

(i) The Hamming distance between two vectors $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ and $\mathbf{y}=(y_1,y_2,\ldots,y_n)$ is the number of places where they differ, and is denoted by $d(\mathbf{x},\mathbf{y})$.
(ii) The Hamming weight of a vector $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ is the number of non-zero x_i and is denoted by $wt(\mathbf{x})$.
(iii) The Euclidean inner product of any two vectors $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ and $\mathbf{y}=(y_1,y_2,\ldots,y_n)$ is defined as $\mathbf{x}\cdot\mathbf{y}=x_0y_0+x_1y_1+\ldots+x_{n-1}y_{n-1}$ and the dual of linear code $\mathcal{C}$ is $\mathcal{C}^{\perp}=\{\mathbf{x}\in R^n\,|\mathbf{x}\cdot\mathbf{y}=0\;\forall\;\mathbf{y}\;\in\;\mathcal{C}\}$.
(iv) A code $\mathcal{C}$ is said to be self-dual if $\mathcal{C}=\mathcal{C}^{\perp}$, self-orthogonal if $\mathcal{C}\subseteq\mathcal{C}^{\perp}$, and dual containing if $\mathcal{C}^{\perp}\subseteq\mathcal{C}$.

Clearly, the ring R can be expressed as $R=\mathbb{F}_q+u_1\mathbb{F}_q+u_2\mathbb{F}_q+u_1u_2\mathbb{F}_q$ such that $u_1^2=\alpha^2$, $u_2^2=\beta^2$ and $u_1u_2=u_2u_1$; here $\mathbb{F}_q$ is the finite field of order q, where $q=p^m$ for odd prime p and $m\geq 1$. It is a commutative non-chain semi-local ring with four maximal ideals. An element z of R is of the form $z=a_1+a_2u_1+a_3u_2+a_4u_1u_2$, where $a_i\in\mathbb{F}_q$ and

$1 \leq i \leq 4$. With the help of a set of orthogonal idempotents, every element of this ring can be represented:

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

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

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

and

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

It is straightforward to show that $\Delta_i^2 = \Delta_i$, $0 = \Delta_i\Delta_j$, and $\Delta_1 + \Delta_2 + \Delta_3 + \Delta_4 = 1$, where $1 \leq i, j \leq 4$, and $i \neq j$. In view of the Chinese Remainder Theorem, we obtain $R = \Delta_1 R \oplus \Delta_2 R \oplus \Delta_3 R \oplus \Delta_4 R = \Delta_1\mathbb{F}_q \oplus \Delta_2\mathbb{F}_q \oplus \Delta_3\mathbb{F}_q \oplus \Delta_4\mathbb{F}_q$. Thus, we can express every element z of R as $z = a_1 + a_2u_1 + a_3u_2 + a_4u_1u_2 = \Delta_1z_1 + \Delta_2z_2 + \Delta_3z_3 + \Delta_4z_4$, where $a_i, z_i \in \mathbb{F}_q$ and $1 \leq i \leq 4$.

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

$$\eta(\Delta_1z_1 + \Delta_2z_2 + \Delta_3z_3 + \Delta_4z_4) = (z_1, z_2, z_3, z_4)A, \tag{1}$$

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 $AA^T = \epsilon I_{4\times4}$, where A^T is the transpose of A and $\epsilon \in \mathbb{F}_q\backslash\{0\}$.

The above Gray map is linear, and we can extend it component-wise from R^n to $\mathbb{F}_q^{4n}$, where n is a positive integer. For any element $z = \Delta_1z_1 + \Delta_2z_2 + \Delta_3z_3 + \Delta_4z_4 \in R$, 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 following result related to the Gray map (1):

Proposition 1. *The map $\eta : R \longrightarrow \mathbb{F}_q^4$ defined in (1) is an $\mathbb{F}_q$-linear and distance-preserving map from (R^n, d_L) to $(\mathbb{F}_q^{4n}, d_H)$, where $d_L = d_H$.*

Proof. Let $z, z' \in R^n$ such that

$$z = \Delta_1z_1 + \Delta_2z_2 + \Delta_3z_3 + \Delta_4z_4$$

$$z' = \Delta_1z_1' + \Delta_2z_2' + \Delta_3z_3' + \Delta_4z_4'$$

and $z_i, z_i' \in \mathbb{F}_q^n$ for $1 \leq i \leq 4$. Then, we have

$$\begin{aligned}
\eta(z + z') &= \eta(\Delta_1z_1 + \Delta_1z_1' + \Delta_2z_2 + \Delta_2z_2' + \Delta_3z_3 + \Delta_3z_3' + \Delta_4z_4 + \Delta_4z_4') \\
&= \eta(\Delta_1(z_1 + z_1') + \Delta_2(z_2 + z_2') + \Delta_3(z_3 + z_3') + \Delta_4(z_4 + z_4')) \\
&= (z_1 + z_1', z_2 + z_2', z_3 + z_3', z_4 + z_4')A \\
&= (z_1, z_2, z_3, z_4)A + (z_1', z_2', z_3', z_4')A \\
&= \eta(z) + \eta(z') \text{ for all } z, z' \in R^n.
\end{aligned}$$

Furthermore, for any $\alpha \in \mathbb{F}_q$, we have

$$\begin{aligned}
\eta(\alpha z) &= \eta(\Delta_1\alpha z_1 + \Delta_2\alpha z_2 + \Delta_3\alpha z_3 + \Delta_4\alpha z_4) \\
&= (\alpha z_1, \alpha z_2, \alpha z_3, \alpha z_4)A \\
&= \alpha(z_1, z_2, z_3, z_4)A \\
&= \alpha\eta(z) \text{ for all } z \in R^n.
\end{aligned}$$

Hence, η is an $\mathbb{F}_q$-linear. As for the second part, we know that

$$\begin{aligned} d_L(z, z') &= w_L(z - z') \\ &= w_H(\eta(z - z')) \\ &= w_H(\eta(z) - \eta(z')) \\ &= d_H(\eta(z), \eta(z')). \end{aligned}$$

Therefore, η is a distance-preserving map. □

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 define that

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

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

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

and

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

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 $\mathcal{C} = \Delta_1\mathcal{C}_1 \oplus \Delta_2\mathcal{C}_2 \oplus \Delta_3\mathcal{C}_3 \oplus \Delta_4\mathcal{C}_4$ and $|\mathcal{C}| = |\mathcal{C}_1||\mathcal{C}_2||\mathcal{C}_3||\mathcal{C}_4|$ 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. *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 an $[n, k_i, d]$ code.*

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

Proposition 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 [14]. □

Theorem 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 $\mathbb{F}_q$.*

Proof. Suppose $\mathcal{C}$ is a self-orthogonal linear code of length n over R, i.e., $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ and let $P, Q \in \eta(\mathcal{C})$ such that $P = \eta(p) = (p_0A, p_1A, \ldots, p_{n-1}A)$ and $Q = \eta(q) = (q_0A, q_1A,$

$\ldots, q_{n-1}A$). We have to show that $\eta(\mathcal{C})$ is self-orthogonal, that is, $P \cdot Q = 0$. Since $\mathcal{C}$ is self-orthogonal, $p \cdot q = \sum_{j=0}^{n-1} p_j.q_j = 0$. Therefore, $P \cdot Q = PQ^{\perp} = \sum_{j=0}^{n-1} p_j AA^T q_j^{\perp} = m\sum_{j=0}^{n-1} p_j.q_j = 0$. Suppose P and Q are arbitrary, then $\eta(\mathcal{C}) \subseteq \eta(\mathcal{C}^{\perp})$. Thus, $\eta(\mathcal{C})$ is a self-orthogonal linear code of length $4n$ over $\mathbb{F}_q$. □

3. Structural Properties of Cyclic Codes over R

On ring R, as described, we shall explore various structural properties of cyclic codes and prove some results. We begin with the following definition:

Definition 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 c in $\mathcal{C}$ is again a codeword in $\mathcal{C}$, i.e., if $c = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C}$, then its cyclic shift $\zeta(c) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$, where the operator ζ is known as cyclic shift.*

Theorem 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, $\mathcal{C}$ 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 $s = (s_0, s_1, \ldots, s_{n-1})$. 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

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

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, $z_1 \in \mathcal{C}_1$, $z_2 \in \mathcal{C}_2$, $z_3 \in \mathcal{C}_3$, *and* $z_4 \in \mathcal{C}_4$. Again, $s = (s_0, s_1, \ldots, s_{n-1}) \in \mathcal{C}$, and by this 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. *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 the 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 $c = \{c(z) \mid \Delta_1 h_1(z) + \Delta_2 h_2(z) + \Delta_3 h_3(z) + \Delta_4 h_4(z)$ 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 $t_4(z) \in R[z]/\langle z^n - 1\rangle$, 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

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

□

Theorem 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, 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, $\mathcal{C} = \langle \Delta_1 h_1(z),\ \Delta_2 h_2(z),\ \Delta_3 h_3(z),\ \Delta_4 h_4(z)\rangle$, 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 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. 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 $\sum_{i=1}^{4} t_i\Delta_i \in \mathcal{C}^\perp\}$, 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 1 ([1])**.** *Let $\mathcal{C} = \langle h(z)\rangle$ be a cyclic code of length n over $\mathbb{F}_q$; $h(z)$ be the generator polynomial of $\mathcal{C}$. Then $\mathcal{C}^\perp \subseteq \mathcal{C}$ 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 6. *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 $h_i(z)$ be 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 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 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 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 and LCD Codes

This section deals with the study of quantum and LCD codes over the ring R. We begin with the following definition: Let p be a prime and $q = p^m$ for a positive integer m. Let $H(\mathbb{C})$ be a q-dimensional Hilbert space 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 2 ([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 2 ([2]). *(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 7. *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 $[[4n,2k-4n,d_H]]_q$ over $\mathbb{F}_q$.*

Proof. Let us consider $\mathbf{x} = (x_0,x_1,\ldots,x_{n-1}) \in \mathcal{C}, \mathbf{y} = (y_0,y_1,\ldots,y_{n-1}) \in \mathcal{C}^{\perp}$, where $x_i = a_i + u_1b_i + u_2c_i + u_1u_2d_i$ and $y_i = a_i^{'} + u_1b_i^{'} + u_2c_i^{'} + u_1u_2d_i^{'}, a_i,b_i,c_i,d_i,a_i^{'},b_i^{'},c_i^{'},d_i^{'} \in \mathbb{F}_q$ for $0 \leq i \leq n-1$. Since $\mathbf{x} \cdot \mathbf{y} = 0$. This gives

$$\begin{aligned}
\sum_{i=0}^{n-1}(a_i + u_1b_i + u_2c_i + u_1u_2d_i)(a_i^{'} + u_1b_i^{'} + u_2c_i^{'} + u_1u_2d_i^{'}) &= 0 \\
\sum_{i=0}^{n-1}(a_ia_i^{'} + u_1a_ib_i^{'} + u_2a_ic_i^{'} + u_1u_2a_id_i^{'} + u_1b_ia_i^{'} + \alpha^2b_ib_i^{'} + u_1u_2b_ic_i^{'} + \alpha^2u_2b_id_i^{'} + u_2c_ia_i^{'} + & \\
u_1u_2c_ib_i^{'} + \beta^2c_ic_i^{'} + \beta^2u_1c_id_i^{'} + u_1u_2d_ia_i^{'} + \alpha^2u_2d_ib_i^{'} + \beta^2u_1d_ic_i^{'} + \alpha^2\beta^2d_id_i^{'}) &= 0 \\
\sum_{i=0}^{n-1}[(a_ia_i^{'} + \alpha^2b_ib_i^{'} + \beta^2c_ic_i^{'} + \alpha^2\beta^2d_id_i^{'}) + u_1(a_ib_i^{'} + b_ia_i^{'} + \beta^2c_id_i^{'} + \beta^2d_ic_i^{'}) + & \\
u_2(a_ic_i^{'} + \alpha^2b_id_i^{'} + c_ia_i^{'} + \alpha^2d_ib_i^{'}) + u_1u_2(a_id_i^{'} + b_ic_i^{'} + c_ib_i^{'} + d_ia_i^{'})] &= 0.
\end{aligned}$$

The above relation yields

$$\begin{aligned}
\sum_{i=0}^{n-1}(a_i a_i^{'} + \alpha^2 b_i b_i^{'} + \beta^2 c_i c_i^{'} + \alpha^2\beta^2 d_i d_i^{'}) &= 0\\
\sum_{i=0}^{n-1}(a_i b_i^{'} + b_i a_i^{'} + \beta^2 c_i d_i^{'} + \beta^2 d_i c_i^{'}) &= 0\\
\sum_{i=0}^{n-1}(a_i c_i^{'} + \alpha^2 b_i d_i^{'} + c_i a_i^{'} + \alpha^2 d_i b_i^{'}) &= 0\\
\sum_{i=0}^{n-1}(a_i d_i^{'} + b_i c_i^{'} + c_i b_i^{'} + d_i a_i^{'}) &= 0.
\end{aligned}$$

Additionally, $\eta(\mathbf{x}) \cdot \eta(\mathbf{y}) = 0$. Therefore, $\eta(\mathcal{C}^{\perp}) \subseteq \eta(\mathcal{C})^{\perp}$. Since η is bijective, $|\eta(\mathcal{C}^{\perp})| = |\eta(\mathcal{C})^{\perp}|$. Hence, $\eta(\mathcal{C}^{\perp}) = \eta(\mathcal{C})^{\perp}$. Moreover, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ implies $\eta(\mathcal{C})^{\perp} \subseteq \eta(\mathcal{C})$. Hence, $\eta(\mathcal{C})$ is a dual-containing linear code with parameters $[4n, k, d_H]$. Thus by Lemma 2, there exists a quantum-error-correcting code with the parameters $[[4n, 2k - 4n, d_H]]_q$ over $\mathbb{F}_q$. □

Definition 3 ([16]). *A linear code $\mathcal{C}$ of length n over R is said to be linear complementary dual (LCD) if $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$.*

Lemma 3 ([17]). *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ generated by a polynomial $h(z)$ such that $n = p^{k_1}t$, where p and t are relatively prime and $k_1 \geq 0$. Then, $\mathcal{C}$ is an LCD code if, and only if, $h(z)$ is a self-reciprocal and all the monic irreducible factors of $h(z)$ have the same multiplicity in $h(z)$ and in $z^n - 1$.*

Definition 4. *A linear code $\mathcal{C}$ of length n over R is said to be reversible if $(c_{n-1}, c_{n-2}, \ldots, c_1, c_0) \in \mathcal{C}$, for all $(c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C}$.*

Lemma 4 ([17]). *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ such that $gcd(n, p) = 1$. Then, $\mathcal{C}$ is a reversible code if, and only if, $\mathcal{C}$ is an LCD code.*

The proofs of Theorems 8–10, Corollaries 2 and 3, and Lemma 5 are similar to those in [18].

Theorem 8. *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, $\mathcal{C}$ is an LCD code if, and only if, $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_4$ are LCD codes of length n over $\mathbb{F}_q$.*

Corollary 2. *Let $n = p^t m$ and $gcd(m, p) = 1$. 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, where $\mathcal{C}_i = \langle h_i(z)\rangle$ such that $h_i(z) \in \mathbb{F}_q$ and $h_i(z)|(z^n - 1)$ for $i = 1, 2, 3, 4$. Then, $\mathcal{C}$ is an LCD code if, and only if, $h_i(z)$ is self-reciprocal and each monic irreducible factor of $h_i(z)$ has the same multiplicity in $h_i(z)$ and in $z^n - 1$ for $i = 1, 2, 3, 4$.*

Theorem 9. *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 with $gcd(n, p) = 1$. Then, $\mathcal{C}$ is an LCD code if, and only if, $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_4$ are reversible codes of length n over $\mathbb{F}_q$.*

Corollary 3. *For $gcd(n, p) = 1$, 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, where $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_4$ are cyclic codes of length n over $\mathbb{F}_q$. Then, $\mathcal{C}$ is an LCD code if, and only if, $h_i(z)$ is a self-reciprocal polynomial in $\mathbb{F}_q$ for $i = 1, 2, 3, 4$.*

Lemma 5. *Let $\mathcal{C}$ be a linear code of length n over R. Then, $\eta(\mathcal{C} \cap \mathcal{C}^{\perp}) = \eta(\mathcal{C}) \cap \eta(\mathcal{C})^{\perp}$.*

Theorem 10. *Let $\mathcal{C}$ be a linear code of length n over R. Then, $\mathcal{C}$ is an LCD code if, and only if, its Gray image $\eta(\mathcal{C})$ is an LCD code of length $4n$ over $\mathbb{F}_q$.*

5. Applications

In this section, we present some applications of the results proven in the previous sections. Example 3 and Table 1 demonstrate that our results provide several quantum codes which are better than the existing quantum codes that have been reported [8–13]. Moreover, we obtained new quantum codes in Example 1 and in Table 2. All of the computations involved in these examples were accomplished by using the Magma computation system [19]. We begin our discussion with the following example:

Example 1. *Let* $R = \mathbb{F}_3[u_1, u_2]/\langle u_1^2 - 1,\ u_2^2 - 1,\ u_1u_2 - u_2u_1\rangle$ *be a finite commutative ring,* $n = 9$, *and* $\alpha = \beta = 1$. *Then,*

$$z^9 - 1 = (z+2)^9 \in \mathbb{F}_3[x].$$

Take

$$\begin{aligned} h_1(z) &= (z+2)^4 \\ h_2(z) &= (z+2)^2 \\ h_3(z) &= (z+2) \\ h_4(z) &= 1 \end{aligned}$$

and

$$A = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix}.$$

Here, matrix A *satisfies the condition* $AA^T = I_{4\times 4}$, *where* $A \in GL_4(\mathbb{F}_3)$ *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* 9 *over* R *and its Gray image is of length* 36, *dimension* 29, *and distance* 3 *over* $\mathbb{F}_3$, *i.e.,* $[36, 29, 3]_3$. *Moreover*

$$z^9 - 1 \equiv 0 \ (mod\ h_i(z)h_i^*(z)),$$

for $1 \le i \le 4$. *Thus,* $\mathcal{C}^\perp \subseteq \mathcal{C}$ *by Theorem 6. In view of Theorem 7, we conclude that there exists a quantum code* $[[36, 22, 3]]_3$. *This quantum code is a new quantum code (see [20] for details).*

Example 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* $\alpha = 2,\ \beta = 1$. *Then,*

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

Take

$$\begin{aligned} h_1(z) &= (z+18) \\ h_2(z) &= (z+18) \\ h_3(z) &= (z+18)^2 \\ h_4(z) &= (z+18)^{14} \end{aligned}$$

and

$$A = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix}.$$

Here, matrix A satisfies the condition $AA^T = 5I_{4\times4}$, *where* $A \in GL_4(\mathbb{F}_{19})$ *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* 19 *over R and its Gray image is of length* 76, *dimension* 58, *and distance* 4 *over* $\mathbb{F}_{19}$, *i.e.,* $[76, 58, 4]_{19}$. *Moreover*

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

for $1 \leq i \leq 4$. *Application of Theorem 6 yields* $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. *By Theorem 7, we conclude that there exists a quantum code* $[[76, 40, 4]]_{19}$.

Example 3. *Let* $R = \mathbb{F}_5[u_1, u_2]/\langle u_1^2 - 1,\ u_2^2 - 1,\ u_1u_2 - u_2u_1 \rangle$ *be a finite commutative ring,* $n = 30$, *and* $\alpha = \beta = 1$. *Then,*

$$z^{30} - 1 = (z+1)^5(z+4)^5(z^2+z+1)^5(z^2+4z+1)^5 \in \mathbb{F}_5[x].$$

Take

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

and

$$A = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix}.$$

Here, matrix A satisfies the condition $AA^T = 4I_{4\times4}$, *where* $A \in GL_4(\mathbb{F}_5)$ *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* 30 *over R and its Gray image is of length* 120, *dimension* 104, *and distance* 3 *over* $\mathbb{F}_5$, *i.e.,* $[120, 104, 3]_5$. *Moreover*

$$z^{30} - 1 \equiv 0 \ (mod\ h_i(z)h_i^*(z)),$$

for $1 \leq i \leq 4$. *This implies that* $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ *by Theorem 6. In view of Theorem 7, we conclude that there exists a quantum code* $[[120, 88, 3]]_5$, *which has the same minimum distance but a larger code rate than the best previously known quantum code* $[[120, 32, 3]]_5$ *(see [12] for details). Therefore, our quantum code* $[[120, 88, 3]]_5$ *is better than the best previously known quantum code* $[[120, 32, 3]]_5$ *reported in [12].*

Example 4. *Let* $R = \mathbb{F}_5[u_1, u_2]/\langle u_1^2 - 1,\ u_2^2 - 4,\ u_1u_2 - u_2u_1 \rangle$ *be a finite commutative ring,* $n = 6$, $\alpha = 1$, *and* $\beta = 2$. *Then,*

$$z^6 - 1 = (z+1)(z+4)(z^2+z+1)(z^2+4z+1) \in \mathbb{F}_5[x].$$

Take

$$\begin{aligned} h_1(z) &= 1 \\ h_2(z) &= (z+1) \\ h_3(z) &= (z+1) \\ h_4(z) &= (z+1)(z^2+z+1)(z^2+4z+1) \end{aligned}$$

and

$$A = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix}.$$

Matrix A satisfies the condition $AA^T = 4I_{4\times4}$, *where* $A \in GL_4(\mathbb{F}_5)$ *and* $I_{4\times4}$ *is an identity matrix. Here,* $h_1(z)$, $h_2(z)$, $h_3(z)$, *and* $h_4(z)$ *are self-reciprocal polynomials. By Corollary 3,*

$\mathcal{C} = \langle \sum_{i=0}^{4} \Delta_i h_i(z) \rangle$ *is an LCD code of length* 6 *over the ring* R. *Hence, by Theorem* 10, *its Gray image* $\eta(\mathcal{C})$ *is also an LCD code with the parameters* $[24, 17, 4]_5$ *over* $\mathbb{F}_5$.

In Table 1 we present QEC codes obtained from 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 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. In Table 2, we obtain new quantum codes, and in Table 3 we construct LCD codes $\mathcal{C} = \langle \sum_{i=0}^{4} \Delta_i h_i(z) \rangle$ of length n over R, where $gcd(n, p) = 1$, $\mathcal{C}_i = \langle h_i(z) \rangle$, and $h_i(z)$ is the self-reciprocal divisor of $z^n - 1$ in $\mathbb{F}_q[z]$ for $i = 1, 2, 3, 4$.

6. Conclusions

In this article, we discuss some of the structural properties of cyclic codes over the ring $R = \mathbb{F}_q[u_1, u_2] / \langle u_1^2 - \alpha^2,\ u_2^2 - \beta^2,\ u_1 u_2 - u_2 u_1 \rangle$, where α and β are non-zero elements of $\mathbb{F}_q$. Furthermore, we obtain better quantum codes than presented in [8–13]. As an application, we obtain LCD codes over the ring R. This study can be generalized to a product of finite rings. We hope that this study will encourage readers to investigate these codes over other finite rings to explore new and better quantum codes in the future.

Author Contributions: All authors made equal contributions. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Princess Nourah bint Abdulrahman University grant number PNURSP2023R231.

Data Availability Statement: Data sharing is not applicable as no datasets were generated or analyzed during the current study.

Acknowledgments: The authors are very thankful to the anonymous referees for their valuable comments and suggestions which have improved the manuscript immensely. Moreover, the authors extend their appreciation to Princess Nourah bint Abdulrahman University (PNU), Riyadh, Saudi Arabia, for funding this research under the Researchers Supporting Project, No. PNURSP2023R231.

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. 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* **1998**, *44*, 1369–1387. [CrossRef]
2. Grassl, M.; Beth, T. On optimal quantum codes. *Int. J. Quantum Inf.* **2004**, *2*, 55–64. [CrossRef]
3. Qian, J.; Ma, W.; Gou, W. Quantum codes from cyclic codes over finite ring. *Int. J. Quantum Inf.* **2009**, *7*, 1277–1283. [CrossRef]
4. Kai, X.; Zhu, S. Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$. *Int. J. Quantum Inf.* **2011**, *9*, 689–700. [CrossRef]
5. Li, R.; Xu, Z.; Li, X. Binary construction of quantum codes of minimum distance three and four. *IEEE Trans. Inf. Theory* **2004**, *50*, 1331–1335. [CrossRef]
6. Gao, J. Quantum codes from cyclic codes over $F_q + vF_q + v^2F_q + v^3F_q$. *Int. J. Quantum Inf.* **2015**, *13*, 1550063. [CrossRef]
7. Özen, M.; Özzaim, N.T.; 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.* **2016**, *766*, 012020-1–012020-6.
8. Ashraf, M.; Khan, N.; Mohammad, G. New Quantum and LCD Codes Over the Finite Field of Odd Characteristic. *Int. J. Theor. Phys.* **2021**, *60*, 2322–2332. [CrossRef]
9. Ashraf, M.; Mohammad, G. Quantum codes from cyclic codes over $F_q + uF_q + vF_q + uvF_q$. *Quantum Inf. Process.* **2016**, *15*, 4089–4098. [CrossRef]
10. 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.* **2019**, *11*, 325–335. [CrossRef]
11. Bag, T.; Dinh, H.Q.; Upadhyay, A.K.; Yamaka, W. New non binary quantum codes from cyclic codes over product ring. *IEEE Commun. Lett.* **2019**, *24*, 486–490. [CrossRef]

12. 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.* **2019**, *60*, 625–635. [CrossRef]
13. Dinh, H.Q.; Bag, T.; Upadhyay, A.K.; Ashraf, M.; Mohammad, G.; Chinnakum, W. Quantum codes from a class of constacyclic codes over finite commutative rings. *J. Algebra Appl.* **2020**, *19*, 2150003. [CrossRef]
14. 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.* **2019**, *59*, 693–700. [CrossRef]
15. Islam, H.; Prakash, O. New quantum and LCD codes over the finite field of even characteristic. *Def. Sci. J.* **2020**, *71*, 656–661. [CrossRef]
16. Massey, J.L. Linear codes with complementary duals. *Discret. Math.* **1992**, *106*, 337–342. [CrossRef]
17. Yang, X.; Massey, J.L. The condition for a cyclic code to have a complementary dual. *Discret. Math.* **1994**, *126*, 391–393. [CrossRef]
18. Islam, H.; Prakash, O. Construction of LCD and new quantum codes from cyclic codes over a finite non chain ring. *Cryptogr. Commun.* **2022**, *14*, 59–73. [CrossRef]
19. Bosma, W.; Cannon, J. *Handbook of Magma Functions*; University of Sydney: Sydney, Australia, 1995.
20. Aydin, N.; Liu, P.; Yoshino, B. A Database of Quantum Codes. 2021. Available online: http://quantumcodes.info/ (accessed on 7 August 2021).