Received September 2, 2020, accepted October 14, 2020, date of publication October 19, 2020, date of current version October 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3032078

A Study of $\mathbb{F}_q R$-Cyclic Codes and Their Applications in Constructing Quantum Codes

HAI Q. DINH[1,4], SACHIN PATHAK[2], TUSHAR BAG[2], ASHISH KUMAR UPADHYAY[2], AND WARATTAYA CHINNAKUM[3]

[1]Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[2]Department of Mathematics, Indian Institute of Technology Patna, Patna 801103, India
[3]Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Chiang Mai 50200, Thailand
[4]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam

Corresponding author: Sachin Pathak (sachin.pma16@iitp.ac.in)

The work of Hai Q. Dinh and Warattaya Chinnakum was supported in part by the Centre of Excellence in Econometrics, Chiang Mai University, Thailand. The work of Sachin Pathak and Tushar Bag was supported by the University Grant Commission (UGC), Government of India. This work was supported in part by the Research Administration Centre, Chiang Mai University, Thailand.

ABSTRACT Let $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, with $u^2 = u, v^2 = v, uv = vu$, where $q = p^m$ for a positive integer m and an odd prime p. We study the algebraic structure of $\mathbb{F}_q R$-cyclic codes of block length (r, s). These codes can be viewed as $R[x]$-submodules of $\mathbb{F}_q[x]/\langle x^r - 1\rangle \times R[x]/\langle x^s - 1\rangle$. For this family of codes we discuss the generator polynomials and minimal generating sets. We study the algebraic structure of separable codes. Further, we discuss the duality of this family of codes and determine their generator polynomials. We obtain several optimal and near-optimal codes from this study. As applications, we discuss a construction of quantum error-correcting codes (QECCs) from $\mathbb{F}_q R$-cyclic codes and construct some good QECCs.

INDEX TERMS $\mathbb{F}_q R$-cyclic codes, generator polynomials, minimal generating sets, QECCs.

I. INTRODUCTION

One of the important class of linear codes is that of cyclic codes. These codes have a significant role in the algebraic coding theory. Since the early 1990's, following the work of Hammons *et al.* [30], linear codes have been studied over finite rings. The authors in [30] have shown that some classes of binary non-linear codes can be obtained through so-called Gray images of linear codes over the ring $\mathbb{Z}_4$. Cyclic codes are among the many classes of codes that are studied the most. During the last thirty years, researchers have studied the algebraic properties of cyclic codes and one of their generalization, constacyclic codes over finite rings.

RifÃ and Pujol [39] introduced the codes over mixed alphabets for the first time in 1997. After that, in 1998, Brouwer *et al.* [16] considered the mixed alphabets $\mathbb{Z}_2$ and $\mathbb{Z}_3$ and obtained bounds for the maximum possible size of error-correcting codes over mixed alphabets. Since then, several scholars have focused extensively on mixed alphabets. In 2009, Borges *et al.* [14] continued to explore codes over mixed alphabets, and they studied $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. The coordinate set was divided into two parts to study these codes, the first corresponding to the coordinates over $\mathbb{Z}_2$ and the second to the coordinates over $\mathbb{Z}_4$. These codes were defined as subgroups of the group $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Further, they determined the standard forms of the generator matrices and parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and obtained fundamental parameters for these codes. In 2013, the work of Borges *et al.* [14] was extended by Aydogdu and Siap [9], and they introduced the algebraic structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes. A few years later, Aydogdu *et al.* [5] generalized the discussion of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes to $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. In this generalization, the authors studied some basic properties of $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. They determined the standard forms of generator matrices and parity-check matrices for this family of codes. They also obtained a result which

The associate editor coordinating the review of this manuscript and approving it for publication was Xueqin Jiang.

TABLE 1. Some optimal and near-optimal codes constructed from cyclic codes C_s over R.

q	s	$g_1(x)$	$g_2(x)$	$g_3(x)$	$g_4(x)$	ψ_1-Gray images
3	2	12	12	12	11	$[8,4,4]^*$
5	2	11	11	11	14	$[8,4,4]^*$
5	3	14	111	1004	1004	$[12,3,8]^*$
5	3	14	111	111	111	$[12,5,6]^*$
7	3	13	15	16	1006	$[12,6,6]^*$
7	3	13	15	16	111	$[12,7,5]^*$
3	4	11	1111	1111	10002	$[16,5,8]^{**}$
5	4	11	1111	1243	1342	$[16,6,8]^*$
3	4	11	11	12	1212	$[16,10,4]^*$
3	5	12	11111	11111	11111	$[20,7,8]^{**}$
5	5	14	131	14	14	$[20,15,3]^{**}$
5	6	11	1221	1221	141414	$[24,12,8]^{**}$
5	6	11	14	14	1324	$[24,18,4]^{**}$
3	8	11	11012	102212	110011	$[32,17,8]^{**}$
3	8	11	1011	11012	122	$[32,21,6]^*$
5	18	12	12021	12	11	$[72,65,3]^{**}$
5	20	13	11	13	114	$[80,75,3]^*$

establishes a relationship between the weight enumerator of $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. In 2014, Abualrub *et al.* [1] addressed $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and described their generator polynomials and minimal generating sets. Further, they constructed several optimal and MDS codes from their study. In 2017, Aydogdu *et al.* [6] studied $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacylic codes. They examined the generators and minimal generating sets of this family of codes. Further, they determined the generators of their duals as well.

Using the theory of mixed alphabets, Borges *et al.* [13] introduced double cyclic codes over $\mathbb{Z}_2$ and determined their generator polynomials and spanning sets. The relationship between generator polynomials of double cyclic codes over $\mathbb{Z}_2$ and their duals was established. They also constructed many optimal binary codes from their study. Analogously, Gao *et al.* [24] discussed double cyclic codes over $\mathbb{Z}_4$ and studied their generator polynomials as well as minimal generating sets. They also studied the generator polynomials of duals of double cyclic codes over $\mathbb{Z}_4$ and obtained some optimal codes from their study. Mostafanasab [38] extended the structure of double cyclic codes over $\mathbb{Z}_2$ to triple cyclic codes over $\mathbb{Z}_2$ and determined their generator polynomials along with their duals. After that, Wu *et al.* [45] studied triple cyclic codes over $\mathbb{Z}_4$ and obtained some new optimal linear codes over $\mathbb{Z}_4$ form their study. In this line, recently, Dinh *et al.* [23] discussed cyclic codes over mixed alphabets and studied their applications in constructing new quantum codes and LCD codes. Some other studies related to cyclic codes over mixed alphabets can be seen in [7], [8], [15], [46].

In 2015, Ashraf and Mohammad [2] discussed cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and constructed several new quantum codes from their discussion. In 2016, Ashraf and Mohammad [3] extended this work and studied the construction of quantum codes from cyclic codes over $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. Motivated by the study of cyclic codes over mixed alphabets, we look at the structure of $\mathbb{F}_q R$-cyclic codes and their application in constructing quantum error-correcting codes (QECCs, in short).

Compared to traditional computers, quantum computers are more effective in solving complex issues. The appositeness of QECCs is one of the reasons for its performance. Research on QECCs has grown enormously since the discovery that there are QECCs that protect quantum information as traditional error-correcting codes protect classical information. Such codes provide an essential way of preventing decoherence. Sequentially placed, Shor [43] discovered the maiden QECC. After that, in 1998, Calderbank *et al.* [17] studied a construction of QECCs from classical linear codes and the complete proof of their existence. Using Calderbank *et al.* [17] concept, several QECCs have been constructed from cyclic codes and their generalizations over finite rings and finite fields [2]–[4], [11], [22].

As an application, we provide several optimal and near-optimal codes in Tables 1 and 2. Further, several new QECCs from $\mathbb{F}_q R$-cyclic codes are also obtained. This paper is structured as follows: In Section 2, we present basic definitions and define $\mathbb{F}_q R$-cyclic codes of block length (r, s). In Section 3, we discuss the structure of linear codes over R and an extended Gray map from $\mathbb{F}_q^r \times R^s$ to $\mathbb{F}_q^{r+4s}$ is defined. In Section 4, we study the structure of $\mathbb{F}_q R$-cyclic codes. Further, their generator polynomials and the structure of separable codes are also discussed. Moreover, we discuss the minimal generating sets of this family of codes. In Section 5, we study the duality of $\mathbb{F}_q R$-cyclic codes and determine their generator polynomials. In Section 6, we look at the application to QECCs of our study on cyclic codes over mixed alphabets. We provide some new QECCs from $\mathbb{F}_q R$-cyclic codes in Examples 40 and 41 and several new QECCs are given in Table 3. In Section 7, we conclude this paper.

II. PRELIMINARIES

Let $\mathbb{F}_q$ be a finite field, where $q = p^m$ for a positive integer m and an odd prime p. Then $\mathbb{F}_q^r$ forms a vector space of dimension r over $\mathbb{F}_q$ under the usual operation. Suppose C_r is a non-empty subset of $\mathbb{F}_q^r$. If C_r forms a subspace of $\mathbb{F}_q^r$, then C_r is said to be a linear code of length r over $\mathbb{F}_q$. The elements

TABLE 2. Some optimal and near-optimal codes constructed from $\mathbb{F}_qR$-cyclic codes.

q	(r,s)	$f(x)$	$\ell(x)$	$g_1(x)$	$g_2(x)$	$g_3(x)$	$g_4(x)$	Ψ_1-Gray images
3	$(3,1)$	1002	111	1	1	12	12	$[7,2,4]^{**}$
3	$(3,1)$	111	12	1	1	1	1	$[7,5,2]^{*}$
3	$(4,1)$	1212	101	1	1	12	12	$[8,3,4]^{**}$
3	$(4,1)$	102	11	1	1	1	1	$[8,6,2]^{*}$
7	$(1,3)$	16	1	13	15	16	1006	$[13,6,6]^{**}$
7	$(1,3)$	16	1	13	15	16	111	$[13,7,5]^{**}$
5	$(3,3)$	1004	131	14	111	1004	1004	$[15,3,10]^{**}$
3	$(3,3)$	111	12	1	1	1	1	$[15,13,2]^{*}$
5	$(1,4)$	14	1	11	1111	1243	1342	$[17,6,8]^{**}$
5	$(6,3)$	141414	13013	1	111	111	111	$[18,7,6]^{**}$
3	$(2,4)$	102	12	12	1	1	1	$[18,15,2]^{*}$
3	$(4,4)$	1212	112	1	12	12	12	$[20,14,4]^{*}$

TABLE 3. New quantum codes from cyclic codes C_s over R.

s	$g_1(x)$	$g_2(x)$	$g_3(x)$	$g_4(x)$	New QECC	Existing QECC
5	14	131	14	14	$[[20,10,3]]_5$	$[[25,9,3]]_5$ (ref. [23])
10	121	14	11	11	$[[40,30,3]]_5$	$[[40,28,3]]_5$ (ref. [23])
15	13	15	13	12412	$[[60,46,3]]_7$	$[[60,36,2]]_7$ (ref. [22])
18	12	12021	12	11	$[[72,58,3]]_3$	$[[72,48,2]]_3$ (ref. [4])
20	13	11	13	114	$[[80,70,3]]_5$	$[[80,56,3]]_5$ (ref. [23])
24	15	152	14	12	$[[96,86,3]]_7$	$[[96,78,3]]_7$ (ref. [12])
30	11	11	111	121	$[[120,108,3]]_5$	$[[120,96,3]]_5$ (ref. [22])
36	11	11	101	11011	$[[144,128,3]]_3$	$[[144,36,3]]_3$ (ref. [29])
45	14	12321	14014014	1001001	$[[180,144,3]]_5$	$[[180,108,3]]_5$ (ref. [29])
78	13	14	1191	11	$[[312,300,4]]_{13}$	$[[312,288,3]]_{13}$ (ref. [22])
90	14056	12	141456411	13026064	$[[360,320,4]]_7$	$[[360,288,2]]_7$ (ref. [29])

of C_r are called codewords. If $a = (a_0, a_1, \ldots, a_{r-1}) \in C_r$, then the number of non-zero components of a is called the Hamming weight of a, denoted by $w_H(a)$. We define the Hamming distance between two codewords $a, a' \in C$ as $d_H(a, a') = w_H(a - a')$. The minimum Hamming distance of C is defined as $d_H(C) = \min\{d_H(a, a') \mid a \neq a'; \forall\, a, a' \in C\}$. The Euclidean inner product of $\mathbf{a} = (a_0, a_1, \ldots, a_{r-1})$ and $\mathbf{a}' = (a'_0, a'_1, \ldots, a'_{r-1})$ in $\mathbb{F}_q^r$ is defined as usual $\mathbf{a} \cdot \mathbf{a}' = a_0a'_0 + a_1a'_1 + \cdots + a_{r-1}a'_{r-1}$. Further, the dual of C_r is defined as $C_r^{\perp} = \{\mathbf{a}' \in \mathbb{F}_q^r \mid \mathbf{a} \cdot \mathbf{a}' = 0,\ \forall\, \mathbf{a} \in C_r\}$.

A linear code C_r of length r over $\mathbb{F}_q$ is said to be a cyclic code if for any $\mathbf{a} = (a_0, a_1, \ldots, a_{r-1}) \in C_r$, its cyclic shift $\tau(\mathbf{a}) := (a_{r-1}, a_0, \ldots, a_{r-2}) \in C_r$. We can associate each codeword $\mathbf{a} = (a_0, a_1, \ldots, a_{r-1}) \in C_r$ with a polynomial $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{r-1} \in \frac{\mathbb{F}_q[x]}{\langle x^r - 1\rangle}$. From this polynomial identification, we get that the code C_r is a cyclic code if and only if its corresponding polynomial identification forms an ideal of the ring $\frac{\mathbb{F}_q[x]}{\langle x^r - 1\rangle}$. Note that, $\frac{\mathbb{F}_q[x]}{\langle x^r - 1\rangle}$ is a principal ideal ring, so there is a monic polynomial $f(x) \in \frac{\mathbb{F}_q[x]}{\langle x^r - 1\rangle}$ of smallest degree in C_r such that $C_r = \langle f(x)\rangle$ with $f(x) \mid (x^r - 1)$. If the polynomial $f(x)$ has degree $n - k$, then the set $\{f(x), xf(x), \cdots, x^{k-1}f(x)\}$ forms a basis of C_r with dimension k.

The concept of cyclic codes and their properties can also be extended over finite commutative rings. Suppose R is a finite commutative ring, then a linear code C_s of length s over R is an R-submodule of R^s. Now we extend this study of cyclic codes from single alphabets to mixed alphabets.

Throughout this paper, we denote $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ with $u^2 = u$, $v^2 = v$, $uv = vu$, where q is power of an odd prime number. We define

$$R_{r,s} = \frac{\mathbb{F}_q[x]}{\langle x^r - 1\rangle} \times \frac{R[x]}{\langle x^s - 1\rangle}$$

and

$$\mathbb{F}_qR = \{(d_1, d_2) \mid d_1 \in \mathbb{F}_q,\ d_2 \in R\}.$$

Under the usual addition and multiplication, the set $\mathbb{F}_qR$ forms a ring. Consider an element $e = a + ub + vc + uvd \in R$, we define $\eta : R \longrightarrow \mathbb{F}_q$ such that $\eta(e) = a$. We can see that η is a ring homomorphism. For any $e \in R$, the R-scalar multiplication on $\mathbb{F}_qR$ is defined as follows

$$\cdot : R \times \mathbb{F}_qR \longrightarrow \mathbb{F}_qR \text{ such that } e \cdot (d_1, d_2) = (\eta(e)d_1, d_2).$$

This multiplication can be extended componentwise to $\mathbb{F}_q^r \times R^s$ as $\cdot : R \times (\mathbb{F}_q^r \times R^s) \longrightarrow \mathbb{F}_q^r \times R^s$ such that

$$e \cdot \mathbf{c} = (\eta(e)a_0, \eta(e)a_1, \ldots, \eta(e)a_{r-1}, eb_0, eb_1, \ldots, eb_{s-1}),$$

for any $e \in R$ and $\mathbf{c} = (a_0, a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1}) \in \mathbb{F}_q^r \times R^s$. We see that $\mathbb{F}_q^r \times R^s$ forms an R-module from this multiplication.

Now we provide the definition of linear codes and cyclic codes over mixed alphabets.

Definition 1: A non-empty subset C of $\mathbb{F}_q^r \times R^s$ is said to be a $\mathbb{F}_qR$-linear code of block length (r, s) if C is an R-submodule of $\mathbb{F}_q^r \times R^s$.

Definition 2: Let C be a $\mathbb{F}_qR$-linear code of block length (r, s). Then C is said to be a $\mathbb{F}_qR$-cyclic code, if for any $\mathbf{c} = (a_0, a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1}) \in C$, its cyclic shift $\rho(\mathbf{c}) := (a_{r-1}, a_0, a_1, \ldots, a_{r-2}, b_{s-1}, b_0, b_1, \ldots, b_{s-2}) \in C$.

We can identify any element $c' = (a'_0, a'_1, \ldots, a'_{r-1}, b'_0, b'_1, \ldots, b'_{s-1}) \in \mathbb{F}_q^r \times R^s$ with an element of $c'(x) \in R_{r,s}$, where

$$c'(x) = (a'_0 + a'_1x + \cdots + a'_{r-1}x^{r-1}, \quad b'_0 + b'_1x + \cdots + b'_{s-1}x^{s-1}).$$

For ease of the notation, we denote $c'(x) = (a'(x), b'(x))$. With this identification, we get a one-to-one correspondence between the elements of $\mathbb{F}_q^r \times R^s$ and $R_{r,s}$. We define a multiplication of any element $t(x) = t_0 + t_1x + \cdots + t_{\delta-1}x^{\delta-1} \in R[x]$ with the element $c'(x) = (a'(x), b'(x)) \in R_{r,s}$ as follows.

$$t(x) \star (a'(x), b'(x)) = (\eta(t(x))a'(x), t(x)b'(x)),$$

where $\eta(t(x)) = \eta(t_0) + \eta(t_1)x + \cdots + \eta(t_{\delta-1})x^{\delta-1}$. We can see that $R_{r,s}$ forms an $R[x]$-module under the usual addition and multiplication $\star$.

Suppose $c'(x) = (a'_0 + a'_1x + \cdots + a'_{r-1}x^{r-1}, b'_0 + b'_1x + \cdots + b'_{s-1}x^{s-1}) \in R_{r,s}$, then

$$x \star c'(x) = (a'_{r-1} + a'_0x + \cdots + a'_{r-2}x^{r-1}, b'_{s-1} + b'_0x + \cdots + b'_{s-2}x^{s-1}),$$

corresponds to the element $(a'_{r-1}, a'_0, \ldots, a'_{r-2}, b'_{s-1}, b'_0, \ldots, b'_{s-2}) \in \mathbb{F}_q^r \times R^s$, which is a cyclic shift of $\mathbf{c}' = (a'_0, a'_1, \ldots, a'_{r-1}, b'_0, b'_1, \ldots, b'_{s-1})$ the corresponding element of $c'(x)$. The next result is obtained from this argument.

Theorem 3: A linear code C is a $\mathbb{F}_qR$-cyclic code of block length (r, s) if and only if C is an $R[x]$-submodule of $R_{r,s}$.

III. LINEAR CODES OVER R AND GRAY MAP ON $\mathbb{F}_qR$

In this section, we present the orthogonal idempotent decomposition of the ring R and then the structure of linear codes from this decomposition is discussed. A Gray map on R is defined and some properties of this map are discussed. Further, we extend this map on $\mathbb{F}_qR$.

Let A_1, A_2, A_3, A_4 be codes. Then we denote

$$A_1 \oplus A_2 \oplus A_3 \oplus A_4 = \{\sum_{i=1}^{4} a_i \mid a_i \in A_i, \ i = 1, 2, 3, 4\}.$$

Consider any element $e = a + ub + vc + uvd \in R$. This element can be uniquely expressed as $e = \xi_1\hat{a} + \xi_2\hat{b} + \xi_3\hat{c} + \xi_4\hat{d}$, where $a, \hat{a}, b, \hat{b}, c, \hat{c}, d, \hat{d} \in \mathbb{F}_q$ such that $\hat{a} = a$, $\hat{b} = a + b$, $\hat{c} = a + c$, $\hat{d} = a + b + c + d$ and

$$\xi_1 = 1 - u - v + uv, \quad \xi_2 = u - uv, \quad \xi_3 = v - uv,$$
$$\xi_4 = uv.$$

It can be easily seen that $\xi_i^2 = \xi_i$, $\xi_i\xi_j = 0$ for $i, j = 1, 2, 3, 4;$ $i \neq j$ and $\sum_{i=1}^{4} \xi_i = 1$. Hence, we get $R = \xi_1R \oplus \xi_2R \oplus \xi_3R \oplus \xi_4R$ and we can see that any element $e \in R$ can be written uniquely as $e = \xi_1e_1 + \xi_2e_2 + \xi e_3 + \xi e_4$, where $e_1, e_2, e_3, e_4 \in \mathbb{F}_q$.

Let $M_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$. Now a Gray map on R such that $\psi_1 : R \to \mathbb{F}_q^4$ is defined as

$$\psi_1(e) = (e_1, e_2, e_3, e_4)M_1.$$

For convenience, we denote $(e_1, e_2, e_3, e_4)M_1$ by eM_1, where $e = \xi_1e_1 + \xi_2e_2 + \xi e_3 + \xi e_4$. This map can be extended componentwise from R^s to $\mathbb{F}_q^{4s}$ as follows.

$$\psi_1 : R^s \longrightarrow \mathbb{F}_q^{4s}$$

given by

$$(e'_0, e'_1, \ldots, e'_{s-1}) \longmapsto (e'_0M_1, e'_1M_1, \ldots, e'_{s-1}M_1) = \mathbf{e}M_1,$$

where $\mathbf{e} = (e'_0, e'_1, \ldots, e'_{s-1}) \in R^s$ and $e'_i = \xi_1e_{i,1} + \xi_2\, e_{i,2} + \xi_3e_{i,3} + \xi_4\, e_{i,4}$ for $i = 0, 1, \ldots, s-1$. The Lee weight of any element $e'_i = \xi_1e_{i,1} + \xi_2\, e_{i,2} + \xi_3e_{i,3} + \xi_4\, e_{i,4} \in R$ is defined as $w_L(e'_i) = w_H(\psi_1(e'_i)) = w_H(e'_iM_1)$, where w_H denotes the Hamming weight over $\mathbb{F}_q$. Further, we define the Lee distance between any two elements $\mathbf{e} = (e'_0, e'_1, \ldots, e'_{s-1})$ and $\mathbf{e}' = (e''_0, e''_1, \ldots, e''_{s-1}) \in R^s$ as $d_L(\mathbf{e}, \mathbf{e}') = w_L(\mathbf{e} - \mathbf{e}') = w_H(\psi_1(\mathbf{e} - \mathbf{e}'))$.

Suppose we have a linear code C_s of length s over R. Then we define

$$\begin{aligned} C_{s,1} &= \{\mathbf{e_1} \in \mathbb{F}_q^s \mid \xi_1\mathbf{e_1} + \xi_2\mathbf{e_2} + \xi_3\mathbf{e_3} + \xi_4\mathbf{e_4} \in C_s \\ &\quad \text{for some } \mathbf{e_2}, \mathbf{e_3}, \mathbf{e_4} \in \mathbb{F}_q^s\}, \\ C_{s,2} &= \{\mathbf{e_2} \in \mathbb{F}_q^s \mid \xi_1\mathbf{e_1} + \xi_2\mathbf{e_2} + \xi_3\mathbf{e_3} + \xi_4\mathbf{e_4} \in C_s \\ &\quad \text{for some } \mathbf{e_1}, \mathbf{e_3}, \mathbf{e_4} \in \mathbb{F}_q^s\}, \\ C_{s,3} &= \{\mathbf{e_3} \in \mathbb{F}_q^s \mid \xi_1\mathbf{e_1} + \xi_2\mathbf{e_2} + \xi_3\mathbf{e_3} + \xi_4\mathbf{e_4} \in C_s \\ &\quad \text{for some } \mathbf{e_1}, \mathbf{e_2}, \mathbf{e_4} \in \mathbb{F}_q^s\}, \\ C_{s,4} &= \{\mathbf{e_4} \in \mathbb{F}_q^s \mid \xi_1\mathbf{e_1} + \xi_2\mathbf{e_2} + \xi_3\mathbf{e_3} + \xi_4\mathbf{e_4} \in C_s \\ &\quad \text{for some } \mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3} \in \mathbb{F}_q^s\}. \end{aligned}$$

Therefore, $C_{s,i}$ are linear codes of length s over $\mathbb{F}_q$, for $i = 1, 2, 3, 4$. Further, we get that C_s can be uniquely written as $C_s = \xi_1\, C_{s,1} \oplus \xi_2\, C_{s,2} \oplus \xi_3\, C_{s,3} \oplus \xi_4\, C_{s,4}$.

Some properties of the Gray map ψ_1 are discussed in the next result.

Proposition 4: Let ψ_1 be the Gray map defined above.

1) *Then ψ_1 is a $\mathbb{F}_q$-linear map which preserves distance from R^s (Lee distance) to $\mathbb{F}_q^{4s}$ (Hamming distance).*
2) *If C_s is a $[s, q^{k_1}, d_L]$ linear code over R, then $\psi_1(C_s)$ is a $[4s, k_1, d_H]$ linear code over $\mathbb{F}_q$, where $d_L = d_H$.*

Proof: (1.) Suppose $\mathbf{e} = (e'_0, e'_1, \ldots, e'_{s-1})$ and $\mathbf{e}' = (e''_0, e''_1, \ldots, e''_{s-1}) \in R^s$, where $e'_i = \xi_1e_{i,1} + \xi_2\, e_{i,2} + \xi_3e_{i,3} + \xi_4\, e_{i,4}$ and $e''_i = \xi_1e''_{i,1} + \xi_2\, e''_{i,2} + \xi_3e''_{i,3} + \xi_4\, e''_{i,4}$ for $i = 0, 1, \ldots, s-1$. Then we have

$$\begin{aligned} \psi_1(\mathbf{e} + \mathbf{e}') &= ((e'_0 + e''_0)M_1, (e'_1 + e''_1)M_1, \ldots, (e'_{s-1} + e''_{s-1})M_1) \\ &= (e'_0M_1, e'_1M_1, \ldots, e'_{s-1}M_1) + (e''_0M_1, e''_1M_1, \ldots, e''_{s-1}M_1) \\ &= \psi_1(\mathbf{e}) + \psi_1(\mathbf{e}'), \end{aligned}$$

and for any $\delta \in \mathbb{F}_q$, $\mathbf{e} = (e'_0, e'_1, \ldots, e'_{s-1}) \in R^s$, we get

$$\psi_1(\delta\mathbf{e}) = (\delta e'_0 M_1, \delta e'_1 M_1, \ldots, \delta e'_{s-1} M_1) = \delta\psi_1(\mathbf{e}).$$

Thus, ψ_1 is a $\mathbb{F}_q$-linear map. Further, we have $d_L(\mathbf{e}, \mathbf{e}') = w_L(\mathbf{e} - \mathbf{e}') = w_H(\psi_1(\mathbf{e} - \mathbf{e}')) = w_H(\psi_1(\mathbf{e}) - \psi_1(\mathbf{e}')) = d_H(\psi_1(\mathbf{e}), \psi_1(\mathbf{e}'))$. Hence, ψ_1 is a $\mathbb{F}_q$-linear map which preserves distance.

(2.) Since ψ_1 is a distance preserving $\mathbb{F}_q$-linear and bijective map, then we can conclude that $\psi_1(C_s)$ is a $[4s, k_1, d_H]$ linear code over $\mathbb{F}_q$. □

Next we extend this Gray map on $\mathbb{F}_qR$ and discuss some of its properties.

Any element $(m, e) \in \mathbb{F}_qR$ can be written as $(m, e) = (m, \xi_1 e_1 + \xi_2 e_2 + \xi_3 e_3 + \xi_4 e_4)$. Define a Gray map from $\mathbb{F}_qR$ to $\mathbb{F}_q^5$ as

$$\Psi_1 : \mathbb{F}_qR \to \mathbb{F}_q^5$$

given by

$$\Psi_1(m, e) = (m, \psi_1(e)) = (m, eM_1).$$

As above, this Gray map can also be extended on $\mathbb{F}_q^r \times R^s$ as follows.

$$\Psi_1 : \mathbb{F}_q^r \times R^s \longrightarrow \mathbb{F}_q^{r+4s}$$

given by

$$(m_0, m_1, \ldots, m_{r-1}, e'_0, e'_1, \ldots, e'_{s-1}) \longmapsto (m_0, m_1, \ldots, m_{r-1}, e'_0 M_1, e'_1 M_1, \ldots, e'_{s-1} M_1),$$

where $(m_0, m_1, \ldots, m_{r-1}) \in \mathbb{F}_q^r$, $(e'_0, e'_1, \ldots, e'_{s-1}) \in R^s$, and $e'_i = \xi_1 e_{i,1} + \xi_2 e_{i,2} + \xi_3 e_{i,3} + \xi_4 e_{i,4} \in R$ for $i = 0, 1, \ldots, s-1$.

Similar to [46], we define the Lee weight of any element $(\mathbf{m}, \mathbf{e}) \in \mathbb{F}_q^r \times R^s$ as $w_L(\mathbf{m}, \mathbf{e}) = w_H(\mathbf{m}) + w_L(\mathbf{e})$, where w_H denotes the Hamming weight over $\mathbb{F}_q$ and w_L denotes the Lee weight. Further, we define the Lee distance between any two elements $\mathbf{t}_1, \mathbf{t}_2$ of $\mathbb{F}_q^r \times R^s$ as $d_L(\mathbf{t}_1, \mathbf{t}_2) = w_L(\mathbf{t}_1 - \mathbf{t}_2) = w_H(\Psi_1(\mathbf{t}_1 - \mathbf{t}_2)) = d_H(\Psi_1(\mathbf{t}_1), \Psi_1(\mathbf{t}_2))$.

Proposition 5: Let Ψ_1 be the Gray map defined above.

1) *Then Ψ_1 is a $\mathbb{F}_q$-linear map which preserves distance from $\mathbb{F}_q^r \times R^s$ (Lee distance) to $\mathbb{F}_q^{r+4s}$ (Hamming distance).*
2) *If C is a $\mathbb{F}_qR$-linear code of block length (r, s) with $|C| = q^k$, then $\Psi_1(C)$ is a $[r + 4s, k, d_H]$ linear code over $\mathbb{F}_q$, where $d_L = d_H$.*

Proof: (1.) Let $\mathbf{t}_1 = (\mathbf{m}, \mathbf{e})$, $\mathbf{t}_2 = (\mathbf{m}', \mathbf{e}') \in \mathbb{F}_q^r \times R^s$, where

$$\mathbf{m} = (m_0, m_1, \ldots, m_{r-1}),\ \mathbf{m}' = (m'_0, m'_1, \ldots, m'_{r-1}) \in \mathbb{F}_q^r,$$
$$\mathbf{e} = (e'_0, e'_1, \ldots, e'_{s-1}),\ \mathbf{e}' = (e''_0, e''_1, \ldots, e''_{s-1}) \in R^s.$$

Then we have

$$\begin{aligned}\Psi_1(\mathbf{t}_1 + \mathbf{t}_2) &= (\mathbf{m} + \mathbf{m}', (e'_0 + e''_0)M_1, (e'_1 + e''_1)M_1, \ldots, (e'_{s-1} + e''_{s-1})M_1)\\ &= (\mathbf{m}, e'_0 M_1, e'_1 M_1, \ldots, e'_{s-1} M_1)\\ &\quad + (\mathbf{m}', e''_0 M_1, e''_1 M_1, \ldots, e''_{s-1} M_1)\\ &= \Psi_1(\mathbf{t}_1) + \Psi_1(\mathbf{t}_2),\end{aligned}$$

and $\Psi_1(r_1\mathbf{t}_1) = (r_1\mathbf{m}, r_1\, e'_0 M_1, r_1\, e'_1 M_1, \ldots, r_1\, e'_{s-1} M_1) = r_1\Psi_1(\mathbf{t}_1)$, where $r_1 \in \mathbb{F}_q$. Thus, Ψ_1 is a $\mathbb{F}_q$-linear map.

As Ψ_1 is a $\mathbb{F}_q$-linear map, we get $d_L(\mathbf{t}_1, \mathbf{t}_2) = w_L(\mathbf{t}_1 - \mathbf{t}_2) = w_H(\Psi_1(\mathbf{t}_1 - \mathbf{t}_2)) = d_H(\Psi_1(\mathbf{t}_1), \Psi_1(\mathbf{t}_2))$. Hence, Ψ_1 is a $\mathbb{F}_q$-linear map which preserves distance.

(2.) Since Ψ_1 is a distance preserving $\mathbb{F}_q$-linear and bijective map, then we can infer that $\Psi_1(C)$ is a $[r + 4s, k, d_H]$ linear code over $\mathbb{F}_q$. □

IV. THE STRUCTURE OF $\mathbb{F}_qR$-CYCLIC CODES

This section is dedicated to the discussion of the algebraic structure of $\mathbb{F}_qR$-cyclic codes of block length (r, s). We determine their generator polynomials as well as minimal generating sets.

Before determining the generators of $\mathbb{F}_qR$-cyclic codes, we first present the structure of cyclic codes over R discussed by Ashraf *et al.* [3] as follows.

Lemma 6 [3, Lemma 3.3]: Let $C_s = \xi_1 C_{s,1} \oplus \xi_2 C_{s,2} \oplus \xi_3 C_{s,3} \oplus \xi_4 C_{s,4}$ be a linear code of length s over R. Then C_s is a cyclic code if and only if $C_{s,i}$ are cyclic codes of length s over $\mathbb{F}_q$, for $i = 1, 2, 3, 4$.

The generators of a cyclic code C_s are given in the next result.

Theorem 7 [3, Lemma 3.5]: Let $C_s = \xi_1 C_{s,1} \oplus \xi_2 C_{s,2} \oplus \xi_3 C_{s,3} \oplus \xi_4 C_{s,4}$ be a cyclic code of length s over R and $C_{s,i} = \langle g_i(x)\rangle$ for $i = 1, 2, 3, 4$. Then $C_s = \langle g(x)\rangle$ and $g(x) \mid (x^s - 1)$, where $g(x) = \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)$ with $g_i(x) \mid (x^s - 1)$. Moreover, $|C_s| = q^{4s - \sum_{i=1}^4 \deg(g_i(x))}$.

Now by using the results studied in above discussion, we present the algebraic structure and generator polynomials of $\mathbb{F}_qR$-cyclic codes.

As we have $\sum_{i=1}^4 \xi_i = 1$, then for any $\mathbf{t}_1 = (\mathbf{m}, \mathbf{e}) \in \mathbb{F}_q^r \times R^s$, we get $\mathbf{t}_1 = (\sum_{i=1}^4 \xi_i \mathbf{m}, \mathbf{e}) \in \mathbb{F}_q^r \times R^s$, where $\mathbf{m} \in \mathbb{F}_q^r$ and $\mathbf{e} = \xi_1\mathbf{e}_1 + \xi_2\mathbf{e}_2 + \xi_3\mathbf{e}_3 + \xi_4\mathbf{e}_4 \in R^s$. We define

$$\begin{aligned} C_1 &= \{(\mathbf{m}, \mathbf{e}_1) \in \mathbb{F}_q^r \times \mathbb{F}_q^s \mid \mathbf{m} \in \mathbb{F}_q^r,\ \mathbf{e}_1 \in C_{s,1}\},\\ C_2 &= \{(\mathbf{m}, \mathbf{e}_2) \in \mathbb{F}_q^r \times \mathbb{F}_q^s \mid \mathbf{m} \in \mathbb{F}_q^r,\ \mathbf{e}_2 \in C_{s,2}\},\\ C_3 &= \{(\mathbf{m}, \mathbf{e}_3) \in \mathbb{F}_q^r \times \mathbb{F}_q^s \mid \mathbf{m} \in \mathbb{F}_q^r,\ \mathbf{e}_3 \in C_{s,3}\},\\ C_4 &= \{(\mathbf{m}, \mathbf{e}_4) \in \mathbb{F}_q^r \times \mathbb{F}_q^s \mid \mathbf{m} \in \mathbb{F}_q^r,\ \mathbf{e}_4 \in C_{s,4}\}.\end{aligned}$$

Therefore, C_i are linear codes of block length (r, s) over $\mathbb{F}_q$, for $i = 1, 2, 3, 4$. Hence, any $\mathbb{F}_qR$-linear code C of block length (r, s) can be uniquely written as $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3 \oplus \xi_4 C_4$.

The next result is obtained from the above discussion.

Theorem 8: Let $C = \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3 \oplus \xi_4 C_4$ be a $\mathbb{F}_qR$-linear code of block length (r, s). Then C is a $\mathbb{F}_qR$-cyclic code if and only if C_i are cyclic codes of block length (r, s) over $\mathbb{F}_q$, for $i = 1, 2, 3, 4$.

Proof: Let $\mathbf{t}_1 = (m_0, m_1, \ldots, m_{r-1}, e'_0, e'_1, \ldots, e'_{s-1}) \in C$, where $e'_i = \xi_1\, e_{i,1} + \xi_2 e_{i,2} + \xi_3\, e_{i,3} + \xi_4 e_{i,4} \in R$ for $i = 0, 1, \ldots, s-1$. Then

$$\begin{aligned}&(m_0, m_1, \ldots, m_{r-1}, e_{0,1}, e_{1,1}, \ldots, e_{s-1,1}) \in C_1,\\ &(m_0, m_1, \ldots, m_{r-1}, e_{0,2}, e_{1,2}, \ldots, e_{s-1,2}) \in C_2,\\ &(m_0, m_1, \ldots, m_{r-1}, e_{0,3}, e_{1,3}, \ldots, e_{s-1,3}) \in C_3,\\ &(m_0, m_1, \ldots, m_{r-1}, e_{0,4}, e_{1,4}, \ldots, e_{s-1,4}) \in C_4.\end{aligned}$$

Now suppose C is a $\mathbb{F}_qR$-cyclic code of block length (r, s), then by definition we get $\rho(\mathbf{t}_1) = (m_{r-1}, m_0, m_1, \ldots, m_{r-2}, e'_{s-1}, e'_0, e'_1, \ldots, e'_{s-2}) \in C$.

Therefore,

$$(m_{r-1}, m_0, \ldots, m_{r-2}, e_{s-1,1}, e_{0,1}, \ldots, e_{s-2,1}) \in C_1,$$
$$(m_{r-1}, m_0, \ldots, m_{r-2}, e_{s-1,2}, e_{0,2}, \ldots, e_{s-2,2}) \in C_2,$$
$$(m_{r-1}, m_0, \ldots, m_{r-2}, e_{s-1,3}, e_{0,3}, \ldots, e_{s-2,3}) \in C_3,$$
$$(m_{r-1}, m_0, \ldots, m_{r-2}, e_{s-1,4}, e_{0,4}, \ldots, e_{s-2,4}) \in C_4.$$

Hence, we get C_i are cyclic codes of block length (r, s) over $\mathbb{F}_q$, for $i = 1, 2, 3, 4$.

Conversely, by following the similar steps as above we get the result. □

In the next result, the generator polynomials of $\mathbb{F}_qR$-cyclic codes are determined. Using such polynomials, we will study the minimum generating sets as well as the size of this family of codes. Now onward, we consider that the block length of $\mathbb{F}_qR$-cyclic codes is (r, s).

Theorem 9: Suppose C is a $\mathbb{F}_qR$-cyclic code of block length (r, s). Then

$$C = \langle (f(x), 0), (\ell(x), g(x)) \rangle,$$

where $f(x), \ell(x) \in \mathbb{F}_q[x]/\langle x^r - 1\rangle$, $f(x) \mid (x^r - 1)$, $g(x) = \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)$, $g(x) \mid (x^s - 1)$ and $g_i(x) \in \mathbb{F}_q[x]$ with $g_i(x) \mid (x^s - 1)$, for $i = 1, 2, 3, 4$.

Proof: Note that both C and $\frac{R[x]}{\langle x^s-1\rangle}$ are $R[x]$-submodules of $R_{r,s}$. Consider a map Θ as follows

$$\Theta : C \longrightarrow \frac{R[x]}{\langle x^s - 1\rangle}$$

given as

$$\Theta(p(x), q(x)) = q(x).$$

We can see that Θ is an $R[x]$-module homomorphism and $\Theta(C)$ forms an ideal of the ring $\frac{R[x]}{\langle x^s-1\rangle}$. Then by Theorem 7, we get $\Theta(C) = \langle g(x)\rangle$. Also $Ker(\Theta) = \{(p(x), 0) \in R_{r,s} \mid (p(x), q(x)) \in C\}$. Define a set I as

$$I = \{p(x) \in \mathbb{F}_q[x]/\langle x^r - 1\rangle \mid (p(x), 0) \in Ker(\Theta)\}.$$

In the ring $\mathbb{F}_q[x]/\langle x^r - 1\rangle$, I is simply an ideal, and thus $I = \langle f(x)\rangle$ with $f(x) \mid (x^r - 1)$. Now, for any element $(p(x), 0) \in Ker(\Theta)$, we get $p(x) = \langle f(x)\rangle$, which implies $p(x) = \lambda(x)f(x)$ for some $\lambda(x) \in \mathbb{F}_q[x]/\langle x^r - 1\rangle$. Thus, $(p(x), 0) = \lambda(x) \star (f(x), 0)$. So we get $Ker(\Theta)$ is a submodule of C, and generated by $(f(x), 0)$. Now, by the first isomorphism theorem, we get

$$\frac{C}{Ker(\Theta)} \cong \langle g(x)\rangle.$$

Suppose $(\ell(x), g(x)) \in C$, then

$$\Theta(\ell(x), g(x)) = g(x).$$

Thus, $(f(x), 0)$ and $(\ell(x), g(x))$ generate any $\mathbb{F}_qR$-cyclic code as an $R[x]$-submodule of $R_{r,s}$. In other words, we can say that $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$, where $\ell(x) \in \mathbb{F}_q[x]/\langle x^r - 1\rangle$. □

Lemma 10: Suppose $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$ is a $\mathbb{F}_qR$-cyclic code of block length (r, s). Then $\deg(\ell(x))$ *can be reduced so that* $\deg \ell(x) < \deg(f(x))$.

Proof: Let $\deg(\ell(x)) \geq \deg(f(x))$ and suppose $\deg(\ell(x)) - \deg(f(x)) = i$. Now consider

$$C' = \langle (f(x), 0), (\ell(x) - x^i f(x), g(x))\rangle.$$

Note that

$$(\ell(x) - x^i f(x), g(x)) = (\ell(x), g(x)) - x^i \star (f(x), 0),$$

this implies $C' \subseteq C$.

On the other hand, we have

$$(\ell(x), g(x)) = (\ell(x) - x^i f(x), g(x)) + x^i \star (f(x), 0),$$

this implies $C \subseteq C'$. So we have $C = C'$. Thus, the degree of $\ell(x)$ can be reduced. Hence, the result follows. □

Hereafter, by Lemma 10, for any code $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$, we will assume without loss of generality that $\deg(\ell(x)) < \deg(f(x))$.

In Theorem 9, we have $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$, where $f(x), \ell(x) \in \mathbb{F}_q[x]$, $g(x) = \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)$ with $g_i(x)h_i(x) = x^s - 1$, for some $h_i(x) \in \mathbb{F}_q[x]$, $i = 1, 2, 3, 4$. From these conditions, the next useful result is obtained.

Lemma 11: Suppose $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$ is a $\mathbb{F}_qR$-cyclic code of block length (r, s). Then $f(x) | h_1(x)\ell(x)$.

Proof: From Theorem 7, we get

$$\begin{aligned}(\xi_1 h_1(x) + \xi_2 h_2(x) + \xi_3 h_3(x) + \xi_4 h_4(x)) \star (\ell(x), \xi_1 g_1(x)\\ + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x))\\ = (h_1(x)\ell(x), 0).\end{aligned}$$

Then $(h_1(x)\ell(x), 0) \in Ker(\Theta)$, this implies $f(x)|h_1(x)\ell(x)$. □

The next corollary is obtained from Lemma 11.

Corollary 12: Suppose $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$ is a $\mathbb{F}_qR$-cyclic code of block length (r, s). Then $f(x)|h_1(x) \gcd(f(x), \ell(x))$.

The generator polynomials of $\mathbb{F}_qR$-cyclic codes have been obtained in our above discussion. Now we study separable codes and determine their generator polynomials.

Suppose C is a $\mathbb{F}_qR$-cyclic code of block length (r, s), consider C_r and C_s are the projections of C on first r coordinates and last s coordinates, respectively. Then clearly C_r is a linear code of length r over $\mathbb{F}_q$ and C_s is a linear codes of length s over R. If C is the direct product of C_r and C_s, i.e., $C = C_r \times C_s$, then C is called a separable code.

Using the result obtained in Theorem 9, we now discuss the algebraic structure of separable codes.

Lemma 13: Suppose $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$ is a $\mathbb{F}_qR$-cyclic code of block length (r, s). Then

$$C_r = \langle \gcd(f(x), \ell(x))\rangle, \ C_s = \langle g(x)\rangle.$$

Proof: Consider $p_1(x) \in C_r$, then for some polynomial $p_2(x) \in R[x]/\langle x^s - 1\rangle$ we have $(p_1(x), p_2(x)) \in C$. It follows that there exist two polynomials $\lambda_1(x), \lambda_2(x) \in R[x]$ such that

$$(p_1(x), p_2(x)) = \lambda_1(x) \star (f(x), 0) + \lambda_2(x) \star (\ell(x), g(x)).$$

This implies $p_1(x) = \eta(\lambda_1(x))f(x) + \eta(\lambda_2(x))\ell(x)$, and therefore, $\gcd(f(x), \ell(x)) \mid p_1(x)$. Hence, $p_1(x) \in \langle \gcd(f(x), \ell(x))\rangle$, this implies $C_r \subseteq \langle \gcd(f(x), \ell(x))\rangle$.

On the other hand, for some polynomials $\lambda_1'(x), \lambda_2'(x) \in \mathbb{F}_q[x]$, we get

$$\gcd(f(x), \ell(x)) = \lambda_1'(x)f(x) + \lambda_2'(x)\ell(x).$$

Then

$$(\gcd(f(x), \ell(x)), \lambda_2'(x)g(x)) = \lambda_1'(x) \star (f(x), 0) + \lambda_2'(x) \star (\ell(x), g(x)) \subseteq C,$$

this implies $\langle \gcd(f(x), \ell(x))\rangle \subseteq C_r$. Therefore, we get $C_r = \langle \gcd(f(x), \ell(x))\rangle$. Other part can be proved in a similar manner. □

Lemma 14: Suppose $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$ is a $\mathbb{F}_qR$-cyclic code of block length (r, s). Then $f(x) \mid \ell(x)$ if and only if $\ell(x) = 0$.

Proof: If $\ell(x) = 0$, then its obvious that $f(x) \mid \ell(x)$.

Conversely, let us consider that $f(x) \mid \ell(x)$, then $\ell(x) = \lambda_1(x)f(x)$ for some polynomial $\lambda_1(x) \in \mathbb{F}_q[x]$. Suppose

$$C' = \langle (f(x), 0), (0, g(x))\rangle.$$

On the one hand, we get

$$(0, g(x)) = (\ell(x), g(x)) - \lambda_1(x) \star (f(x), 0) \in C,$$

this implies, $C' \subseteq C$. On the other hand,

$$(\ell(x), g(x)) = \lambda_1(x) \star (f(x), 0) + (0, g(x)) \in C',$$

this implies, $C \subseteq C'$. Thus, we get $C = C'$. Therefore, we conclude that $\ell(x) = 0$. □

We obtain the following result from Lemmas 13 and 14 for a $\mathbb{F}_qR$-cyclic code to be a separable code.

Theorem 15: Suppose $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$ is a $\mathbb{F}_qR$-cyclic code of block length (r, s). Then the following affirmations are equivalent:

1) *C is a separable code;*
2) *$f(x) \mid \ell(x)$;*
3) *$C_r = \langle f(x)\rangle$, $C_s = \langle g(x)\rangle$;*
4) *$C = \langle (f(x), 0), (0, g(x))\rangle$.*

Proof: From Lemmas 13 and 14, the proof follows immediately. □

From above discussion about separable codes, We get the result below.

Theorem 16: Let C be a $\mathbb{F}_qR$-linear code of block length (r, s). Then C is a separable $\mathbb{F}_qR$-cyclic code if and only if C_r and C_s are cyclic codes of length r and s over $\mathbb{F}_q$ and R, respectively.

Proof: Suppose C is a separable $\mathbb{F}_qR$-cyclic code and $(m_0, m_1, \ldots, m_{r-1}, e_0', e_1', \ldots, e_{s-1}') \in C$, where $(m_0, m_1, \ldots, m_{r-1}) \in C_r$, $(e_0', e_1', \ldots, e_{s-1}') \in C_s$. As C is a $\mathbb{F}_qR$-cyclic code, then we have

$$(m_{r-1}, m_0, m_1, \ldots, m_{r-2}, e_{s-1}', e_0', e_1', \ldots, e_{s-2}') \in C,$$

which implies $(m_{r-1}, m_0, m_1, \ldots, m_{r-2}) \in C_r$ and $(e_{s-1}', e_0', e_1', \ldots, e_{s-2}') \in C_s$. Therefore, C_r and C_s are cyclic codes of length r and s over $\mathbb{F}_q$ and R, respectively.

On the other hand, suppose C_r and C_s are cyclic codes of length r and s over $\mathbb{F}_q$ and R, respectively. Let $(m_0', m_1', \ldots, m_{r-1}') \in C_r$, $(e_0'', e_1'', \ldots, e_{s-1}'') \in C_s$, then $(m_{r-1}', m_0', \ldots, m_{r-2}') \in C_r$, $(e_{s-1}'', e_0'', \ldots, e_{s-2}'') \in C_s$. Therefore,

$$(m_{r-1}', m_0', \ldots, m_{r-2}', e_{s-1}'', e_0'', \ldots, e_{s-2}'') \in C_r \times C_s = C.$$

Thus, C is a separable $\mathbb{F}_qR$-cyclic code. □

In our above discussion, we have studied the algebraic structure of $\mathbb{F}_qR$-cyclic codes. We have determined their generator polynomials and studied the structure of separable codes also. Now, by using the result obtained in Theorem 9, we study minimal generating sets of $\mathbb{F}_qR$-cyclic codes.

From the ring homomorphism η, defined in Section 2, we have $\eta(\xi_1) = 1, \eta(\xi_2) = \eta(\xi_3) = \eta(\xi_4) = 0$. We will use these facts in the proof of the following result.

Theorem 17: Let $C = \langle (f(x), 0), (\ell(x), g(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code, where $f(x)k(x) = x^r - 1$, $g(x) = \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)$ with $g_i(x)h_i(x) = x^s - 1$ for some $h_i(x) \in \mathbb{F}_q[x]$, $i = 1, 2, 3, 4$.

Let

$$S_1 = \bigcup_{i=0}^{\deg(k(x))-1} \{x^i \star (f(x), 0)\},$$

$$S_2 = \bigcup_{i=0}^{\deg(h_1(x))-1} \{x^i \star (\ell(x), \xi_1 g_1(x))\},$$

$$S_3 = \bigcup_{i=0}^{\deg(h_2(x))-1} \{x^i \star (0, \xi_2 g_2(x))\},$$

$$S_4 = \bigcup_{i=0}^{\deg(h_3(x))-1} \{x^i \star (0, \xi_3 g_3(x))\},$$

$$S_5 = \bigcup_{i=0}^{\deg(h_4(x))-1} \{x^i \star (0, \xi_4 g_4(x))\}.$$

Then $S = \bigcup_{i=1}^{5} S_i$ forms a minimal generating set of C. Furthermore, C has q^k codewords, where $k = \deg(k(x)) + \sum_{i=1}^{4} \deg(h_i(x))$.

Proof: Let $c''(x) \in C$. Then for some polynomials $m_1(x), m_2(x) \in R[x]$ we have

$$c''(x) = m_1(x) \star (f(x), 0) + m_2(x) \star (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)).$$

Let $m_1(x) = t_0 + t_1 x + \cdots + t_\alpha x^\alpha$, where $t_i = \xi_1 a_i + \xi_2 b_i + \xi_3 c_i + \xi_4 d_i$, $i = 0, 1, \cdots, \alpha$. Then we have

$$\begin{aligned} m_1(x) &= \xi_1(a_0 + a_1 x + \cdots + a_\alpha x^\alpha) + \xi_2(b_0 + b_1 x + \cdots \\ &\quad + b_\alpha x^\alpha) + \xi_3(c_0 + c_1 x + \cdots + c_\alpha x^\alpha) \\ &\quad + \xi_4(d_0 + d_1 x + \cdots + d_\alpha x^\alpha) \\ &= \xi_1 a(x) + \xi_2 b(x) + \xi_3 c(x) + \xi_4 d(x). \end{aligned}$$

Now,

$$\begin{aligned}m_1(x) \star (f(x), 0) &= (\xi_1 a(x) + \xi_2 b(x) + \xi_3 c(x) + \xi_4 d(x)) \star (f(x), 0) \\ &= a(x) \star (\eta(\xi_1) f(x), 0) \\ &= a(x) \star (f(x), 0).\end{aligned}$$

If $\deg(a(x)) < \deg(k(x))$, then $a(x) \star (f(x), 0) \in \mathrm{Span}(S_1)$. Otherwise, by division algorithm, we have $a(x) = k(x)q_0(x) + r_0(x)$ for some polynomials $q_0(x), r_0(x) \in \mathbb{F}_q[x]$ with $r_0(x) = 0$ or $\deg(r_0(x)) < \deg(k(x))$. Therefore,

$$\begin{aligned}a(x) \star (f(x), 0) &= (k(x)q_0(x) + r_0(x)) \star (f(x), 0) \\ &= k(x)q_0(x) \star (f(x), 0) + r_0(x) \star (f(x), 0) \\ &= 0 + r_0(x) \star (f(x), 0).\end{aligned}$$

Thus, we get $r_0(x) \star (f(x), 0) \in \mathrm{Span}(S_1)$. Hence, we have $a(x) \star (f(x), 0) \in \mathrm{Span}(S_1)$. Now we only need to prove that

$$m_2(x) \star (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)) \in \mathrm{Span}(S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5).$$

Let $m_2(x) = t'_0 + t'_1 x + \cdots + t'_\beta x^\beta$, where $t'_i = \xi_1 a'_i + \xi_2 b'_i + \xi_3 c'_i + \xi_4 d'_i$, $i = 0, 1, \cdots, \beta$. Then we have

$$\begin{aligned}m_2(x) &= \xi_1(a'_0 + a'_1 x + \cdots + a'_\beta x^\beta) + \xi_2(b'_0 + b'_1 x + \cdots \\ &\quad + b'_\beta x^\beta) + \xi_3(c'_0 + c'_1 x + \cdots + c'_\beta x^\beta) \\ &\quad + \xi_4(d'_0 + d'_1 x + \cdots + d'_\beta x^\beta) \\ &= \xi_1 a'(x) + \xi_2 b'(x) + \xi_3 c'(x) + \xi_4 d'(x).\end{aligned}$$

Now,

$$\begin{aligned}&m_2(x) \star (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)) \\ &= (\xi_1 a'(x) + \xi_2 b'(x) + \xi_3 c'(x) + \xi_4 d'(x)) \\ &\quad \star (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)) \\ &= a'(x) \star (\ell(x), \xi_1 g_1(x)) + b'(x) \star (0, \xi_2 g_2(x)) \\ &\quad + c'(x) \star (0, \xi_3 g_3(x)) + d'(x) \star (0, \xi_4 g_4(x)).\end{aligned}$$

If $\deg(b'(x)) < \deg(h_2(x))$, then $b'(x) \star (0, \xi_2 g_2(x)) \in \mathrm{Span}(S_3)$. Otherwise, by division algorithm, we have $b'(x) = h_2(x)q_1(x) + r_1(x)$ for some polynomials $q_1(x), r_1(x) \in R[x]$ with $r_1(x) = 0$ or $\deg(r_1(x)) < \deg(h_2(x))$. Therefore,

$$\begin{aligned}b'(x) \star (0, \xi_2 g_2(x)) &= v(h_2(x)q_1(x) + r_1(x)) \star (0, \xi_2 g_2(x)) \\ &= h_2(x)q_1(x) \star (0, \xi_2 g_2(x)) \\ &\quad + r_1(x) \star (0, \xi_2 g_2(x)) \\ &= 0 + r_1(x) \star (0, \xi_2 g_2(x)).\end{aligned}$$

Thus, we get $r_1(x) \star (0, \xi_2\, g_2(x)) \in \mathrm{Span}(S_3)$. Hence, we have $b'(x) \star (0, \xi_2 g_2(x)) \in \mathrm{Span}(S_3)$. Similarly, we can get $c'(x) \star (0, \xi_3 g_3(x)) \in \mathrm{Span}(S_4)$ and $d'(x) \star (0, \xi_4 g_4(x)) \in \mathrm{Span}(S_5)$.

Now, consider $a'(x) \star (\ell(x), \xi_1 g_1(x))$. If $\deg(a'(x)) < \deg(h_1(x))$, then $a'(x) \star (\ell(x), \xi_1 g_1(x)) \in \mathrm{Span}(S_2)$. Otherwise, by division algorithm, we have $a'(x) = h_1(x)q_2(x) + r_2(x)$ for some polynomials $q_2(x), r_2(x) \in R[x]$ with $r_2(x) = 0$ or $\deg(r_2(x)) < \deg(h_1(x))$. Therefore,

$$\begin{aligned}&a'(x) \star (\ell(x), \xi_1 g_1(x)) \\ &= (h_1(x)q_2(x) + r_2(x)) \star (\ell(x), \xi_1 g_1(x)) \\ &= h_1(x)q_2(x) \star (\ell(x), \xi_1 g_1(x)) + r_2(x) \star (\ell(x), \xi_1 g_1(x)) \\ &= q_2(x) \star (h_1(x)\ell(x), 0) + r_2(x) \star (\ell(x), \xi_1 g_1(x)).\end{aligned}$$

Clearly, we get $r_2(x)) \star (\ell(x), \xi_1 g_1(x)) \in \mathrm{Span}(S_2)$. From Lemma 11, we have $f(x) \mid h_1(x)\ell(x)$ which implies $q_2(x) \star (h_1(x)\ell(x), 0) \in \mathrm{Span}(S_1)$. Thus, we get $a'(x) \star (\ell(x), \xi_1 g_1(x)) \in \mathrm{Span}(S_1 \cup S_2)$. Hence, we infer that $c''(x) \in \mathrm{Span}(S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5)$. Clearly, the elements in $\mathrm{Span}(S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5)$ are R-linearly independent. Thus, we conclude that $S = \bigcup_{i=1}^{5} S_i$ forms a minimal generating set of C as an R-submodule and C has q^k codewords, where $k = \deg(k(x)) + \sum_{i=1}^{4} \deg(h_i(x))$. □

To illustrate our results discussed above, we now present an example.

Example 18: Let $q = 5$, $r = 3$ and $s = 3$. Suppose $C = \langle (f(x), 0), (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)) \rangle$ is a $\mathbb{F}_5R$-cyclic code of block length $(3, 3)$, where

$$\begin{aligned}f(x) &= 1 + x + x^2, \\ g_1(x) &= g_2(x) = x + 4, \\ g_3(x) &= g_4(x) = 1 + x + x^2, \\ \ell(x) &= 1.\end{aligned}$$

Furthermore, we can determine the polynomials $h_i(x)$ for $i = 1, 2, 3, 4$ as follows.

$$\begin{aligned}g_1(x)h_1(x) &= g_2(x)h_2(x) = x^3 - 1 \\ &\implies h_1(x) = h_2(x) = 1 + x + x^2, \\ g_3(x)h_3(x) &= g_4(x)h_4(x) = x^3 - 1 \\ &\implies h_3(x) = h_4(x) = x + 4.\end{aligned}$$

By Theorem 17, C has the following generator matrix G.

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & \xi_1 & 4\xi_1 & 0 \\ 0 & 1 & 0 & 0 & \xi_1 & 4\xi_1 \\ 0 & 0 & 0 & \xi_2 & 4\xi_2 & 0 \\ 0 & 0 & 0 & 0 & \xi_2 & 4\xi_2 \\ 0 & 0 & 0 & \xi_3 & \xi_3 & \xi_3 \\ 0 & 0 & 0 & \xi_4 & \xi_4 & \xi_4 \end{pmatrix},$$

Moreover, $|C| = 5^7$. □

V. DUALITY OF $\mathbb{F}_qR$-CYCLIC CODES

This section is dedicated to the discussion of structural properties of dual of $\mathbb{F}_qR$-cyclic codes. We determine the relationship between the generators of $\mathbb{F}_qR$-cyclic codes and their duals. Recall, throughout the paper, we suppose the block length of $\mathbb{F}_qR$-cyclic codes is (r, s).

Let $\mathbf{c} = (a_0, a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1})$ and $\mathbf{c}' = (a'_0, a'_1, \ldots, a'_{r-1}, b'_0, b'_1, \ldots, b'_{s-1}) \in \mathbb{F}_q^r \times R^s$. Then the inner product is defined as follows.

$$\mathbf{c} \cdot \mathbf{c}' = \xi_1 \sum_{i=0}^{r-1} a_i a'_i + \sum_{j=0}^{s-1} b_j b'_j \in R.$$

Definition 19: If C is a $\mathbb{F}_qR$-linear code, then its dual code $C^{\perp}$ is defined as

$$C^{\perp} = \{\mathbf{c}' \in \mathbb{F}_q^r \times R^s \mid \mathbf{c} \cdot \mathbf{c}' = 0, \forall\, \mathbf{c} \in C\}.$$

C is called self-dual if $C^{\perp} = C$ and self-orthogonal if $C \subseteq C^{\perp}$.

In the next result, we present a relationship between $\mathbb{F}_qR$-cyclic codes and their duals.

Lemma 20: If C is any $\mathbb{F}_qR$-cyclic code of block length (r, s), then $C^{\perp}$ is also a $\mathbb{F}_qR$-cyclic code of same block length.

Proof: Let C be a $\mathbb{F}_qR$-cyclic code and $\mathbf{c} = (a_0, a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1}) \in C^{\perp}$. We need to show that $\rho(\mathbf{c}) = (a_{r-1}, a_0, \ldots, a_{r-2}, b_{s-1}, b_0, \ldots, b_{s-2}) \in C^{\perp}$. Since $\mathbf{c} \in C^{\perp}$, for any $\mathbf{c}' = (a'_0, a'_1, \ldots, a'_{r-1}, b'_0, b'_1, \ldots, b'_{s-1}) \in C$, we get $\mathbf{c} \cdot \mathbf{c}' = 0$. Now, let $\mathfrak{m} = \operatorname{lcm}(r, s)$ and $\rho^{\mathfrak{m}-1}(\mathbf{c}') = (a'_1, a'_2, \ldots, a'_{r-1}, a'_0, b'_1, b'_2, \ldots, b'_{s-1}, b'_0) = \mathbf{d}$. Then $\rho^{\mathfrak{m}}(\mathbf{c}') = \mathbf{c}'$. Since the code C is a $\mathbb{F}_qR$-cyclic code, then $\mathbf{d} \in C$. Therefore,

$$\begin{aligned} 0 = \mathbf{c} \cdot \mathbf{d} &= \xi_1(a_0 a'_1 + a_1 a'_2 + \cdots + a_{r-1} a'_0) \\ &\quad + (b_0 b'_1 + b_1 b'_2 + \cdots + b_{s-1} b'_0) \\ &= \xi_1(a_{r-1} a'_0 + a_0 a'_1 + \cdots + a_{r-2} a'_{r-1}) \\ &\quad + (b_{s-1} b'_0 + b_0 b'_1 + \cdots + b_{s-2} b'_{s-1}) \\ &= \rho(\mathbf{c}) \cdot \mathbf{c}'. \end{aligned}$$

Thus, we have $\rho(\mathbf{c}) \in C^{\perp}$. Hence, $C^{\perp}$ is also a $\mathbb{F}_qR$-cyclic code of same block length. □

In the above result, we have seen that the dual of a $\mathbb{F}_qR$-cyclic code C is also a $\mathbb{F}_qR$-cyclic code, then we denote

$$\begin{aligned} C^{\perp} = \langle(\widehat{f}(x), 0), (\widehat{\ell}(x), \xi_1\widehat{g_1}(x) + \xi_2\widehat{g_2}(x) \\ + \xi_3\widehat{g_3}(x) + \xi_4\widehat{g_4}(x))\rangle \end{aligned}$$

where $\widehat{g_i}(x)\widehat{h_i}(x) = x^s - 1$ in $R[x]$ for $i = 1, 2, 3, 4$, $\widehat{f}(x), \widehat{\ell}(x) \in \mathbb{F}_q[x]/(x^r - 1)$ with $\widehat{f}(x) \mid (x^r - 1)$, $\deg(\widehat{\ell}(x)) < \deg(\widehat{f}(x))$ and $\widehat{f}(x) \mid \widehat{h_1}(x)\widehat{\ell}(x)$.

Throughout the paper, we consider $\mathfrak{m} = \operatorname{lcm}(r, s)$, and the reciprocal of a polynomial $p(x)$ is denoted by $p^*(x) = x^{\deg(p(x))} p(x^{-1})$.

Definition 21: Let $t_1(x) = (m(x), e(x))$ and $t_2(x) = (m'(x), e'(x))$ be two elements of $R_{r,s}$. Define a map

$$\bullet : R_{r,s} \times R_{r,s} \to R[x]/(x^{\mathfrak{m}} - 1)$$

such that

$$\begin{aligned} &\bullet(t_1(x), t_2(x)) \\ &= \xi_1 m(x) m'^*(x) x^{\mathfrak{m}-\deg(m'(x))-1} \frac{x^{\mathfrak{m}} - 1}{x^r - 1} \\ &\quad + e(x) e'^*(x) x^{\mathfrak{m}-\deg(e'(x))-1} \frac{x^{\mathfrak{m}} - 1}{x^s - 1} \pmod{x^{\mathfrak{m}} - 1}. \end{aligned}$$

The map $\bullet$ is a bilinear map between $R[x]$-modules. For more details about the Definition 21 one can see [13, Definition 3]. Now onward, for convenience, we denote $\bullet(t_1(x), t_2(x))$ by $t_1(x) \bullet t_2(x)$.

Proposition 22: Let $\mathbf{t}_1$ and $\mathbf{t}_2 \in \mathbb{F}_q^r \times R^s$ be two vectors and let $t_1(x) = (m(x), e(x))$ and $t_2(x) = (m'(x), e'(x))$ be their associated polynomials. Then, $\mathbf{t}_1$ is orthogonal to $\mathbf{t}_2$ and all its shifts if and only if

$$t_1(x) \bullet t_2(x) = 0.$$

Proof: Let $\mathbf{t}_1 = (m_0, m_1, \ldots, m_{r-1}, e'_0, e'_1, \ldots, e'_{s-1})$ and $\mathbf{t}_2 = (m'_0, m'_1, \ldots, m'_{r-1}, e''_0, e''_1, \ldots, e''_{s-1})$. Assume that $\mathbf{t}_2^{(i)} = (m'_{0-i}, m'_{1-i}, \ldots, m'_{r-1-i}, e''_{0-i}, e''_{1-i}, \ldots, e''_{s-1-i})$ is the i^{th} cyclic shift of $\mathbf{t}_2$, where $i = 0, 1, 2, \ldots, \mathfrak{m} - 1$. Then $\mathbf{t}_1 \cdot \mathbf{t}_2^{(i)} = 0$ if and only if

$$\xi_1 \sum_{\alpha=0}^{r-1} m_\alpha m'_{\alpha-i} + \sum_{\beta=0}^{s-1} e'_\beta e''_{\beta-i} = 0.$$

Let $B_i = \xi_1 \sum_{\alpha=0}^{r-1} m_\alpha m'_{\alpha-i} + \sum_{\beta=0}^{s-1} e'_\beta e''_{\beta-i}$. Then we get

$$\begin{aligned} t_1(x) \bullet t_2(x) &= \xi_1 \left(\frac{x^{\mathfrak{m}} - 1}{x^r - 1}\right) \sum_{a=0}^{r-1} \sum_{\alpha=0}^{r-1} m_\alpha m'_{\alpha-a} x^{\mathfrak{m}-1-a} \\ &\quad + \left(\frac{x^{\mathfrak{m}} - 1}{x^s - 1}\right) \sum_{b=0}^{s-1} \sum_{\beta=0}^{s-1} e'_\beta e''_{\beta-b} x^{\mathfrak{m}-1-b} \\ &= \sum_{i=0}^{\mathfrak{m}-1} B_i x^{\mathfrak{m}-1-i} \pmod{x^{\mathfrak{m}} - 1}. \end{aligned}$$

Hence, $t_1(x) \bullet t_2(x) = 0$ if and only if $B_i = 0$, for $i = 0, 1, \ldots, \mathfrak{m} - 1$. □

We get the next results from the above discussion, that will be used in determining the generator polynomials of dual codes.

Lemma 23: Let $t_1(x) = (m(x), e(x))$, $t_2(x) = (m'(x), e'(x)) \in R_{r,s}$ such that $t_1(x) \bullet t_2(x) = 0$. If $e(x) = 0$ or $e'(x) = 0$, then $m(x)m'^*(x) \equiv 0 \pmod{x^r - 1}$ over $\mathbb{F}_q$. Respectively, if $m(x) = 0$ or $m'(x) = 0$, then $e(x)e'^*(x) \equiv 0 \pmod{x^s - 1}$ over R.

Proof: Let $e(x) = 0$ or $e'(x) = 0$. Then

$$\begin{aligned} t_1(x) \bullet t_2(x) &= \xi_1 \left(\frac{x^{\mathfrak{m}} - 1}{x^r - 1}\right) m(x) m'^*(x) x^{\mathfrak{m}-\deg(m'(x))-1} \\ &\equiv 0 \pmod{x^{\mathfrak{m}} - 1}. \end{aligned}$$

This implies that there is a polynomial $\mu(x) \in \mathbb{F}_q[x]$ such that

$$\xi_1 \left(\frac{x^{\mathfrak{m}} - 1}{x^r - 1}\right) m(x) m'^*(x) x^{\mathfrak{m}-\deg(m'(x))-1} = \xi_1 \mu(x)(x^{\mathfrak{m}} - 1).$$

Consider $\mu'(x) = \mu(x) x^{\deg(m'(x))+1}$. Then we get $m(x)m'^*(x)x^{\mathfrak{m}} = \mu'(x)(x^r - 1)$. Thus, $m(x)m'^*(x) \equiv 0 \pmod{x^r - 1}$. Using similar argument we can prove other case. □

Proposition 24: Let $C = \langle(f(x), 0), (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code. Then

$$\begin{aligned} &|C_r| = q^{r-\deg(\gcd(f(x), \ell(x)))}, \ |C_s| = q^{4s-\sum_{i=1}^4 \deg(g_i(x))}, \\ &|(C_r)^{\perp}| = q^{\deg(\gcd(f(x), \ell(x)))}, \ |(C_s)^{\perp}| = q^{\sum_{i=1}^4 \deg(g_i(x))}, \\ &|(C^{\perp})_r| = q^{\deg(f(x))}, \\ &|(C^{\perp})_s| = q^{\sum_{i=1}^4 \deg(g_i(x)) + \deg(f(x)) - \deg(\gcd(f(x), \ell(x)))}, \end{aligned}$$

$$\begin{aligned}
|\xi_1\, C_s| &= q^{s-\deg(g_1(x))},\ |\xi_2\, C_s| = q^{s-\deg(g_2(x))},\\
|\xi_3\, C_s| &= q^{s-\deg(g_3(x))},\ |\xi_4\, C_s| = q^{s-\deg(g_4(x))},\\
|\xi_1(C_s)^\perp| &= q^{\deg(g_1(x))},\ |\xi_2(C_s)^\perp| = q^{\deg(g_2(x))},\\
|\xi_3(C_s)^\perp| &= q^{\deg(g_3(x))},\ |\xi_4(C_s)^\perp| = q^{\deg(g_4(x))},\\
|\xi_1(C^\perp)_s| &= q^{\deg(g_1(x))+\deg(f(x))-\deg(\gcd(f(x),\ell(x))},\\
|\xi_2(C^\perp)_s| &= q^{\deg(g_2(x))},\\
|\xi_3(C^\perp)_s| &= q^{\deg(g_3(x))},\ |\xi_4(C^\perp)_s| = q^{\deg(g_4(x))}.
\end{aligned}$$

Proof: From Lemma 13, we get $C_r = \langle \gcd(f(x), \ell(x))\rangle$ is a cyclic code of length r over $\mathbb{F}_q$ and $C_s = \langle \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)\rangle$ is a cyclic code of length s over R. Therefore, $|C_r| = q^{r-\gcd(f(x),\ell(x))}$ and $|C_s| = q^{4s-\sum_{i=1}^{4}\deg(g_i(x))}$. By the theory of cyclic codes and their duals, we can get the values of $|(C_r)^\perp|$, $|(C^\perp)_r|$, $|(C_s)^\perp|$ and $|(C^\perp)_s|$.

From minimal generating sets determined in Theorem 17, we have $\xi_i C_s = \langle \xi_i g_i(x)\rangle$, for $i = 1, 2, 3, 4$. Hence, we get $|\xi_i C_s| = q^{s-\deg(g_i(x))}$. Therefore, we can get the values of $|\xi_i(C_s)^\perp|$, $|\xi_i(C^\perp)_s|$, for $i = 1, 2, 3, 4$. □

From the above proposition, we get the following result, which calculates the degree of each generator polynomial of dual code.

Theorem 25: Let $C = \langle (f(x), 0), (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code, and $C^\perp = \langle (\widehat{f}(x), 0), (\widehat{\ell}(x), \xi_1\widehat{g_1}(x) + \xi_2\widehat{g_2}(x) + \xi_3\widehat{g_3}(x) + \xi_4\widehat{g_4}(x))\rangle$. Then

$$\begin{aligned}
\deg(\widehat{f}(x)) &= r - \deg(\gcd(f(x), \ell(x))),\\
\deg(\widehat{g_1}(x)) &= s - \deg(g_1(x)) - \deg(f(x))\\
&\quad + \deg(\gcd(f(x), \ell(x))),\\
\deg(\widehat{g_2}(x)) &= s - \deg(g_2(x)),\\
\deg(\widehat{g_3}(x)) &= s - \deg(g_3(x)),\\
\deg(\widehat{g_4}(x)) &= s - \deg(g_4(x)).
\end{aligned}$$

Proof: It can be seen that $(C_r)^\perp$ is a cyclic code generated by $\widehat{f}(x)$. So, $|(C_r)^\perp| = q^{r-\deg(\widehat{f}(x))}$. From Proposition 24, we get $|(C_r)^\perp| = p^{\deg(\gcd(f(x),\ell(x)))}$. Hence, $\deg(\widehat{f}(x)) = r - \deg(\gcd(f(x), \ell(x))$.

We can see that $\xi_1(C^\perp)_s$ is a cyclic code generated by $\xi_1\widehat{g_1}(x)$. So, $|\xi_1(C^\perp)_s| = q^{s-\deg(\widehat{g_1}(x))}$. By Proposition 24, we get $|\xi_1(C^\perp)_s| = q^{\deg(g_1(x))+\deg(f(x))-\deg(\gcd(f(x),\ell(x)))}$. Hence, $\deg(\widehat{g_1}(x)) = s - \deg(g_1(x)) - \deg(f(x)) + \deg(\gcd(f(x), \ell(x))$.

We can see that $\xi_2(C^\perp)_s$ is a cyclic code generated by $\xi_2\widehat{g_2}(x)$. So, $|\xi_2(C^\perp)_s| = q^{s-\deg(\widehat{g_2}(x))}$. From Proposition 24, we get $|\xi_2(C^\perp)_s| = q^{\deg(g_2(x))}$. Hence, $\deg(\widehat{g_2}(x)) = s - \deg(g_2(x))$. Similarly, we can prove other parts. □

Now we discuss the generator polynomials of $C^\perp$ and establish the relationship between the generator polynomials of C and $C^\perp$.

Proposition 26: Let $C = \langle (f(x), 0), (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code, and $C^\perp = \langle (\widehat{f}(x), 0), (\widehat{\ell}(x), \xi_1\widehat{g_1}(x) + \xi_2\widehat{g_2}(x) + \xi_3\widehat{g_3}(x) + \xi_4\widehat{g_4}(x))\rangle$. Then

$$\widehat{f}(x) = \left(\frac{x^r - 1}{\gcd(f(x), \ell(x))}\right)^* \in \mathbb{F}_q[x].$$

Proof: Since $(\widehat{f}(x), 0) \in C^\perp$, then we get

$$\begin{aligned}
&(f(x), 0) \bullet (\widehat{f}(x), 0) = 0,\\
&(\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x)\\
&\qquad + \xi_4 g_4(x)) \bullet (\widehat{f}(x), 0)) = 0
\end{aligned}$$

Thus, from Lemma 23,

$$\begin{aligned}
f(x)\widehat{f}^*(x) &\equiv 0 \pmod{(x^r - 1)},\\
\ell(x)\widehat{f}^*(x) &\equiv 0 \pmod{(x^r - 1)},
\end{aligned}$$

over $\mathbb{F}_q$. Therefore, $\gcd(f(x), \ell(x))\widehat{f}^*(x) \equiv 0 \pmod{(x^r - 1)}$, and hence for some $\lambda(x) \in \mathbb{F}_q[x]$ we have $\gcd(f(x), \ell(x))\widehat{f}^*(x) = \lambda(x)(x^r - 1)$. Furthermore, as $\gcd(f(x), \ell(x)) \mid (x^r - 1)$ and $\widehat{f}^*(x) \mid (x^r - 1)$, then by Theorem 25, we get $\deg(\widehat{f}(x)) = r - \deg(\gcd(f(x), \ell(x)))$. So, $\lambda(x) = c_1$, for any $c_1 \in \mathbb{F}_q$. Then we could suppose $\lambda(x) = 1$. Hence, we get

$$\widehat{f}^*(x) = \frac{x^r - 1}{\gcd(f(x), \ell(x))} \in \mathbb{F}_q[x],$$

this implies

$$\widehat{f}(x) = \left(\frac{x^r - 1}{\gcd(f(x), \ell(x))}\right)^* \in \mathbb{F}_q[x].$$

□

Proposition 27: Let $C = \langle (f(x), 0), (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code, and $C^\perp = \langle (\widehat{f}(x), 0), (\widehat{\ell}(x), \xi_1\widehat{g_1}(x) + \xi_2\widehat{g_2}(x) + \xi_3\widehat{g_3}(x) + \xi_4\widehat{g_4}(x))\rangle$. Then

$$\widehat{g_1}(x) = \frac{(x^s - 1)\gcd(f(x), \ell(x))^*}{f^*(x) g_1^*(x)} \in R[x].$$

Proof: We have

$$\begin{aligned}
&\xi_1 \frac{f(x)}{\gcd(f(x), \ell(x))} \star (\ell(x), \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x)\\
&\quad + \xi_4 g_4(x)) - \frac{\ell(x)}{\gcd(f(x), \ell(x))} \star (f(x), 0)\\
&= (0, \xi_1 \frac{f(x)}{\gcd(f(x), \ell(x))} g_1(x)) \in C.
\end{aligned}$$

Further, $\xi_1 \star (\widehat{\ell}(x), \xi_1\widehat{g_1}(x) + \xi_2\widehat{g_2}(x) + \xi_3\widehat{g_3}(x) + \xi_4\widehat{g_4}(x)) = (\widehat{\ell}(x), \xi_1\widehat{g_1}(x)) \in C^\perp$. Therefore,

$$(\widehat{\ell}(x), \xi_1\widehat{g_1}(x)) \bullet \left(0, \xi_1 \frac{f(x)}{\gcd(f(x), \ell(x))} g_1(x)\right) = 0.$$

Thus, from Lemma 23,

$$\xi_1\widehat{g_1}(x)\left(\frac{f(x)}{\gcd(f(x), \ell(x))} g_1(x)\right)^* \equiv 0 \pmod{(x^s - 1)}.$$

Hence,

$$\xi_1\widehat{g_1}(x)\left(\frac{f(x)}{\gcd(f(x), \ell(x))} g_1(x)\right)^* = \xi_1\lambda_1(x)(x^s - 1)$$

for some $\lambda_1(x)$ in $R[x]$. This is equivalent to

$$\widehat{g_1}(x)\left(\frac{f(x)}{\gcd(f(x), \ell(x))} g_1(x)\right)^* = \lambda_1(x)(x^s - 1) \in R[x].$$

Since $\widehat{g_1}(x) \mid (x^s-1)$, then from Corollary 12, $\left(\frac{f(x)}{\gcd(f(x),\ell(x))}g_1(x)\right)^* \mid (x^s-1)$. Further, by Theorem 25, we get $\deg(\widehat{g_1}(x)) = s-\deg(g_1(x))-\deg(f(x))+\deg(\gcd(f(x),\ell(x))$. So, $\lambda_1(x)=c_2$, for any $c_2\in R$. Then we could suppose $\lambda_1(x)=1$. So, we have

$$\widehat{g_1}(x)=\frac{(x^s-1)\gcd(f(x),\ell(x))^*}{f^*(x)g_1^*(x)}\in R[x].$$

□

Proposition 28: Let $C = \langle (f(x),0),(\ell(x),\xi_1g_1(x)+\xi_2g_2(x)+\xi_3g_3(x)+\xi_4g_4(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code, and $C^\perp = \langle(\widehat{f}(x),0),(\widehat{\ell}(x),\xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x))\rangle$. Then

$$\widehat{g_2}(x)=\left(\frac{x^s-1}{g_2(x)}\right)^*\in R[x].$$

Proof: We have

$$\xi_2\star(\widehat{\ell}(x),\xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x)) = (0,\xi_2\widehat{g_2}(x))\in C^\perp.$$

Then

$$(\ell(x),\xi_1g_1(x)+\xi_2g_2(x)+\xi_3g_3(x) +\xi_4g_4(x))\bullet(0,\xi_2\widehat{g_2}(x))=0.$$

Thus, by Lemma 23, we get

$$\xi_2g_2(x)\widehat{g_2}^*(x)\equiv 0 \pmod{(x^s-1)}.$$

Hence, $\xi_2g_2(x)\widehat{g_2}^*(x)=\xi_2\lambda_2(x)(x^s-1)$, for some $\lambda_2(x)\in R[x]$. This is equivalent to $g_2(x)\widehat{g_2}^*(x)=\lambda_2(x)(x^s-1)\in R[x]$. Since $g_2(x)\mid(x^s-1)$ and $\widehat{g_2}^*(x)\mid(x^s-1)$, further by Theorem 25, we have $\deg(\widehat{g_2}(x))=s-\deg(g_2(x))$. Therefore, $\lambda_2(x)=c_3$, for any $c_3\in R$. Then we could suppose $\lambda_2(x)=1$. So, we have

$$\widehat{g_2}^*(x)=\frac{x^s-1}{g_2(x)}\in R[x],$$

this implies

$$\widehat{g_2}(x)=\left(\frac{x^s-1}{g_2(x)}\right)^*\in R[x].$$

□

Proposition 29: Let $C = \langle (f(x),0),(\ell(x),\xi_1g_1(x)+\xi_2g_2(x)+\xi_3g_3(x)+\xi_4g_4(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code, and $C^\perp = \langle(\widehat{f}(x),0),(\widehat{\ell}(x),\xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x))\rangle$. Then

$$\widehat{g_3}(x)=\left(\frac{x^s-1}{g_3(x)}\right)^*,\quad \widehat{g_4}(x)=\left(\frac{x^s-1}{g_4(x)}\right)^*\in R[x].$$

In the following, we determine a relation between the polynomials $\ell(x)$ and $\widehat{\ell}(x)$.

Proposition 30: Let $C = \langle (f(x),0),(\ell(x),\xi_1g_1(x)+\xi_2g_2(x)+\xi_3g_3(x)+\xi_4g_4(x))\rangle$ be a $\mathbb{F}_qR$-cyclic code, and $C^\perp = \langle(\widehat{f}(x),0),(\widehat{\ell}(x),\xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x))\rangle$. Then

$$\widehat{\ell}(x)=\frac{(x^r-1)}{f^*(x)}\mu(x)\in\mathbb{F}_q[x].$$

where

$$\mu(x)=-x^{\mathrm{m}-\deg(g_1(x))+\deg(\ell(x))}\left(\frac{\ell^*(x)}{\gcd(f(x),\ell(x))^*}\right)^{-1} \times\left(\bmod\left(\frac{f^*(x)}{\gcd(f(x),\ell(x))^*}\right)\right).$$

Proof: As $(\widehat{\ell}(x),\xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x))\in C^\perp$, then

$$(\widehat{\ell}(x),\xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x))\bullet(f(x),0)=0.$$

Thus, from Lemma 23, we have

$$\widehat{\ell}(x)f^*(x)\equiv 0 \pmod{(x^r-1)}.$$

Hence,

$$\widehat{\ell}(x)=\frac{x^r-1}{f^*(x)}\mu(x) \text{ for some } \mu(x)\in\mathbb{F}_q[x].$$

Since $\xi_1\star(\widehat{\ell}(x),\xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x)) = (\widehat{\ell}(x),\xi_1\widehat{g_1}(x))\in C^\perp$ and $\xi_1\star(\ell(x),\xi_1g_1(x)+\xi_2g_2(x)+\xi_3g_3(x)+\xi_4g_4(x))=(\ell(x),\xi_1g_1(x))\in C$, then

$$\begin{aligned}
&(\widehat{\ell}(x),\xi_1\widehat{g_1}(x))\bullet(\ell(x),\xi_1g_1(x))\\
&=\xi_1\frac{x^r-1}{f^*(x)}\mu(x)\ell^*(x)x^{\mathrm{m}-\deg(\ell(x))-1}\frac{x^{\mathrm{m}}-1}{x^r-1}\\
&\quad+\xi_1\frac{(x^s-1)\gcd(f(x),\ell(x))^*}{f^*(x)g_1^*(x)}g_1^*(x)x^{\mathrm{m}-\deg(g_1(x)-1}\frac{x^{\mathrm{m}}-1}{x^s-1}\\
&=\xi_1\frac{(x^{\mathrm{m}}-1)\gcd(f(x),\ell(x))^*}{f^*(x)}\\
&\quad\times\left(\mu(x)\frac{\ell^*(x)}{\gcd(f(x),\ell(x))^*}x^{\mathrm{m}-\deg(\ell(x))-1}+x^{\mathrm{m}-\deg(g_1(x))-1}\right)\\
&=0 \mod (x^{\mathrm{m}}-1).
\end{aligned}$$

Then, either

$$\left(\mu(x)\frac{\ell^*(x)}{\gcd(f(x),\ell(x))^*}x^{\mathrm{m}-\deg(\ell(x))-1}+x^{\mathrm{m}-\deg(g_1(x))-1}\right) \equiv 0 \pmod{(x^{\mathrm{m}}-1)}), \quad (1)$$

or

$$\left(\mu(x)\frac{\ell^*(x)}{\gcd(f(x),\ell(x))^*}x^{\mathrm{m}-\deg(\ell(x))-1}+x^{\mathrm{m}-\deg(g_1(x))-1}\right) \equiv 0\left(\bmod\left(\frac{f^*(x)}{\gcd(f(x),\ell(x))^*}\right)\right). \quad (2)$$

Since $\left(\frac{f^*(x)}{\gcd(f(x),\ell(x))^*}\right)\mid(x^{\mathrm{m}}-1)$, clearly (1) implies (2). Therefore,

$$\mu(x)\frac{\ell^*(x)}{\gcd(f(x),\ell(x))^*}x^{\mathrm{m}}=-x^{\mathrm{m}-\deg(g_1(x))+\deg(\ell(x))} \times\left(\bmod\left(\frac{f^*(x)}{\gcd(f(x),\ell(x))^*}\right)\right).$$

Further, we also know $x^{\mathrm{m}} \equiv 1 \pmod{(\frac{f^*(x)}{\gcd(f(x),\ell(x))^*})}$. Since $\gcd\left(\frac{f(x)}{\gcd(f(x),\ell(x))}, \frac{\ell(x)}{\gcd(f(x),\ell(x))}\right) = 1$, then there exists $\left(\frac{\ell^*(x)}{\gcd(f(x),\ell(x))^*}\right)^{-1} \pmod{(\frac{f^*(x)}{\gcd(f(x),\ell(x))^*})}$. Thus,

$$\mu(x) = -x^{\mathrm{m}-\deg(g_1(x))+\deg(\ell(x))}\left(\frac{\ell^*(x)}{\gcd(f(x),\ell(x))^*}\right)^{-1} \times \left(\mod \left(\frac{f^*(x)}{\gcd(f(x),\ell(x))^*}\right)\right).$$

□

In the next theorem, we summarize our above discussion.

Theorem 31: Let $C = \langle (f(x), 0), (\ell(x), \xi_1 g_1(x)+\xi_2 g_2(x)+\xi_3 g_3(x) + \xi_4 g_4(x))\rangle$ *be a* $\mathbb{F}_qR$*-cyclic code, and* $C^\perp = \langle(\widehat{f}(x), 0), (\widehat{\ell}(x), \xi_1\widehat{g_1}(x)+\xi_2\widehat{g_2}(x)+\xi_3\widehat{g_3}(x)+\xi_4\widehat{g_4}(x))\rangle$. *Then*

1) $\widehat{f}(x) = \left(\frac{x^r-1}{\gcd(f(x),\ell(x))}\right)^* \in \mathbb{F}_q[x]$,
2) $\widehat{g_1}(x) = \frac{(x^s-1)\gcd(f(x),\ell(x))^*}{f^*(x)g_1^*(x)} \in R[x]$,
3) $\widehat{g_2}(x) = \left(\frac{x^s-1}{g_2(x)}\right)^*$, $\widehat{g_3}(x) = \left(\frac{x^s-1}{g_3(x)}\right)^*$, $\widehat{g_4}(x) = \left(\frac{x^s-1}{g_4(x)}\right)^* \in R[x]$,
4) $\widehat{\ell}(x) = \frac{(x^r-1)}{f^*(x)}\mu(x) \in \mathbb{F}_q[x]$, *where* $\mu(x)$ *as given in Proposition 30.*

Example 32: Let $C = \langle (f(x), 0), (\ell(x), \xi_1 g_1(x)+\xi_2 g_2(x)+\xi_3 g_3(x) + \xi_4 g_4(x))\rangle$ be a $\mathbb{F}_5R$-cyclic code with the generator polynomials given in Example 18. Then $C^\perp = \langle(\widehat{f}(x), 0), (\widehat{\ell}(x), \xi_1\widehat{g_1}(x) + \xi_2\widehat{g_2}(x) + \xi_3\widehat{g_3}(x) + \xi_4\widehat{g_4}(x))\rangle$. Hence, by Theorem 31, we have $\widehat{f}(x) = 4x^3+1$ and $\widehat{g_1}(x) = 4$, $\widehat{g_2}(x) = x^2+x+1$, $\widehat{g_3}(x) = \widehat{g_4}(x) = 4x+1$, $\widehat{\ell}(x) = 4x^2+1$. Moreover, $C^\perp$ has the following generator matrix H.

$$H = \begin{pmatrix} 1 & 0 & 4 & 4\xi_1 & 0 & 0 \\ 4 & 1 & 0 & 0 & 4\xi_1 & 0 \\ 0 & 4 & 1 & 0 & 0 & 4\xi_1 \\ 0 & 0 & 0 & \xi_2 & \xi_2 & \xi_2 \\ 0 & 0 & 0 & \xi_3 & 4\xi_3 & 0 \\ 0 & 0 & 0 & 0 & \xi_3 & 4\xi_3 \\ 0 & 0 & 0 & \xi_4 & 4\xi_4 & 0 \\ 0 & 0 & 0 & 0 & \xi_4 & 4\xi_4 \end{pmatrix}.$$

Further, $|C^\perp| = 5^8$. □

Next we present some optimal and near-optimal codes as Gray images of cyclic codes over R and $\mathbb{F}_qR$. In Table 1, we construct some optimal and near-optimal codes as ψ_1-Gray images of cyclic codes C_s over R. In Table 2, we construct some optimal and near-optimal codes as Ψ_1-Gray images of $\mathbb{F}_qR$-cyclic codes. We denote $[.]^*$ to indicate the optimal codes, and $[.]^{**}$ to indicate the near-optimal codes (codes with minimum distance one less than the codes given in [26]). The generator polynomial coefficients are written down in descending order, e.g. 11226 is corresponds to the polynomial $x^4 + x^3 + 2x^2 + 2x + 6$.

VI. QECCs FROM $\mathbb{F}_qR$-CYCLIC CODES

In the above sections, we have studied $\mathbb{F}_qR$-cyclic codes and separable codes. Now we discuss the application of $\mathbb{F}_qR$-cyclic codes in constructing quantum codes.

Shor [43] and Steane [42] first studied the QECCs individually. Calderbank *et al.* [17] subsequently studied the construction of this family of codes from classical codes, demonstrated their existence and methods of correction. In the last few years, a number of QECCs were discussed over finite fields using the theory of Calderbank *et al.* [17] (See [2], [3], [25], [27], [28], [32]–[37], [40], [41]).

To show a construction of QECCs from this study, we now define a Gray map on $\mathbb{F}_qR$. This map is just similar to the map defined in Section 3, but for our purpose here we consider a different matrix of order 4 than the previously considered matrix M_1.

Let us consider, $M_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \in GL_4(\mathbb{F}_q)$.

Since $\mathbb{F}_q$ is a field of odd characteristic, then by direct computation we can see that $M_2M_2^T = I_4$, where M_2^T denotes the transpose of matrix M_2 and I_4 denotes the identity matrix of order 4. A Gray map on R is defined as follows.

$$\psi_2 : R \longrightarrow \mathbb{F}_q^4 \quad \text{given by} \quad \psi_2(e) = (e_1, e_2, e_3, e_4)M_2.$$

We denote $(e_1, e_2, e_3, e_4)M_2$ by eM_2, where $e = \xi_1e_1+\xi_2e_2+\xi e_3 + \xi e_4$. As earlier, we can extend this map as follows.

$$\Psi_2 : \mathbb{F}_q^r \times R^s \longrightarrow \mathbb{F}_q^{r+4s}$$

given by

$$(m_0, m_1, \ldots, m_{r-1}, e'_0, e'_1, \ldots, e'_{s-1}) \longmapsto (m_0, m_1, \ldots, m_{r-1}, \psi_2(e'_0), \psi_2(e'_1), \ldots, \psi_2(e'_{s-1}))$$
$$(m_0, m_1, \ldots, m_{r-1}, e'_0, e'_1, \ldots, e'_{s-1}) \longmapsto (m_0, m_1, \ldots, m_{r-1}, e'_0M_2, e'_1M_2, \ldots, e'_{s-1}M_2),$$

where $(m_0, m_1, \ldots, m_{r-1}) \in \mathbb{F}_q^r$, $(e'_0, e'_1, \ldots, e'_{s-1}) \in R^s$ and $e'_i = \xi_1\, e_{i,1}+\xi_2e_{i,2}+\xi_3\, e_{i,3}+\xi_4e_{i,4} \in R$ for $i = 0, 1, \ldots, s-1$.

Similar to the Proposition 5, we can see that Ψ_2 is a $\mathbb{F}_q$-linear map and for a $\mathbb{F}_qR$-linear code C of block length (r, s) with $|C| = q^k$, $\Psi_2(C)$ is a $[r+4s, k, d_H]$ linear code over $\mathbb{F}_q$.

Proposition 33: Let C *be a* $\mathbb{F}_qR$*-linear code. Then* $\Psi_2(C^\perp) = \Psi_2(C)^\perp$. *Further, if* C *is self-dual then* $\Psi_2(C)$ *is also self-dual.*

Proof: Let $\mathbf{t}_1 = (m_0, m_1, \ldots, m_{r-1}, e'_0, e'_1, \ldots, e'_{s-1}) \in C$ and $\mathbf{t}_2 = (m'_0, m'_1, \ldots, m'_{r-1}, e''_0, e''_1, \ldots, e''_{s-1}) \in C^\perp$, where $e'_i = \xi_1e_{i,1} + \xi_2\, e_{i,2} + \xi_3e_{i,3} + \xi_4\, e_{i,4}$ and $e''_i = \xi_1e''_{i,1} + \xi_2\, e''_{i,2} + \xi_3e''_{i,3} + \xi_4\, e''_{i,4}$ for $i = 0, 1, \ldots, s-1$. Then by the definition of inner product, we have

$$\mathbf{t}_1 \cdot \mathbf{t}_2 = \xi_1\sum_{j=0}^{r-1} m_jm'_j + \sum_{i=0}^{s-1} e'_ie''_i = 0,$$

which implies

$$\xi_1\sum_{j=0}^{r-1} m_jm'_j + \sum_{i=0}^{s-1}(\xi_1e_{i,1} + \xi_2\, e_{i,2} + \xi_3e_{i,3} + \xi_4\, e_{i,4}) \times (\xi_1e''_{i,1} + \xi_2\, e''_{i,2} + \xi_3e''_{i,3} + \xi_4\, e''_{i,4}) = 0,$$

$$\xi_1 \sum_{j=0}^{r-1} m_j m'_j + \sum_{i=0}^{s-1} (\xi_1 e_{i,1} e''_{i,1} + \xi_2\, e_{i,2} e''_{i,2} + \xi_3 e_{i,3} e''_{i,3} + \xi_4\, e_{i,4} e''_{i,4}) = 0.$$

Now comparing the coefficients of ξ_1, ξ_2, ξ_3 and ξ_4 from both sides, we get

$$\sum_{j=0}^{r-1} m_j m'_j + \sum_{i=0}^{s-1} e_{i,1} e''_{i,1} = 0,$$
$$\sum_{i=0}^{s-1} e_{i,2} e''_{i,2} = 0,$$
$$\sum_{i=0}^{s-1} e_{i,3} e''_{i,3} = 0,$$

and

$$\sum_{i=0}^{s-1} e_{i,4} e''_{i,4} = 0.$$

Further, we have

$$\begin{aligned}\Psi_2(\mathbf{t}_1)\cdot\Psi_2(\mathbf{t}_2) &= \sum_{j=0}^{r-1} m_j m'_j + \sum_{i=0}^{s-1} e'_j M_2 M_2^T e''^T_j,\\ &= \sum_{j=0}^{r-1} m_j m'_j + \sum_{i=0}^{s-1} (e_{i,1} e''_{i,1} + e_{i,2} e''_{i,2} \\ &\quad + e_{i,3} e''_{i,3} + e_{i,4} e''_{i,4}).\end{aligned}$$

Then from the above equations, we get $\sum_{j=0}^{r-1} m_j m'_j + \sum_{i=0}^{s-1} (e_{i,1} e''_{i,1} + e_{i,2} e''_{i,2} + e_{i,3} e''_{i,3} + e_{i,4} e''_{i,4}) = 0$, i.e., $\Psi_2(\mathbf{t}_1)\cdot\Psi_2(\mathbf{t}_2) = 0$, which implies $\Psi_2(\mathbf{t}_2) \in \Psi_2(C)^\perp$ for $\Psi_2(\mathbf{t}_1) \in \Psi_2(C)$. Therefore, $\Psi_2(C^\perp) \subseteq \Psi_2(C)^\perp$. Since Ψ_2 is bijective, so $|\Psi_2(C^\perp)| = |(\Psi_2(C))^\perp|$. Hence, $\Psi_2(C^\perp) = (\Psi_2(C))^\perp$.

Now suppose that C is self-dual, i.e., $C = C^\perp$, then $\Psi_2(C) = \Psi_2(C^\perp) = (\Psi_2(C))^\perp$. Thus, $\Psi_2(C)$ is self-dual. □

Theorem 34 (CSS Construction [17]): Let $\mathcal{C}_1 = [n, k_1, d_1]$ and $\mathcal{C}_2 = [n, k_2, d_2]$ be two linear codes over $\mathbb{F}_q$ with $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1$. Then there exists a QECC with parameters $[[n, k_1 + k_2 - n, d]]_q$, where $d = \min\{d_1, d_2\}$. Moreover, if $\mathcal{C}_1^\perp \subseteq \mathcal{C}_1$, then a QECC having parameters $[[n, 2k_1 - n, d_1]]_q$ can be constructed.

Next we present following result for dual-containing cyclic codes over $\mathbb{F}_q$.

Theorem 35 [17, Theorem 13]: Let $C_r = \langle f(x)\rangle$ be a cyclic code of length r over $\mathbb{F}_q$. Then $C_r^\perp \subseteq C_r$ if and only if

$$x^r - 1 \equiv 0 \pmod{f(x)f^*(x)}.$$

Now extending Lemma 35 over R, we get the next result.

Theorem 36 [3, Theorem 4.2]: Let $C_s = \langle \xi_1 g(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)\rangle$ be a cyclic code of length s over R. Then $C_s^\perp \subseteq C_s$ if and only if

$$x^s - 1 \equiv 0 \pmod{g_i(x)g_i^*(x)}, \quad \text{for } i = 1, 2, 3, 4.$$

In the next result, we see the dual containing property on separable $\mathbb{F}_qR$-cyclic codes.

Theorem 37: Let $C = C_r \times C_s$ be a separable $\mathbb{F}_qR$-cyclic code. Then $C^\perp \subseteq C$ if and only if $C_r^\perp \subseteq C_r$ and $C_s^\perp \subseteq C_s$.

Proof: If $C^\perp \subseteq C = C_r \times C_s$ and $C^\perp = C_r^\perp \times C_s^\perp$, then $C_r^\perp \times C_s^\perp \subseteq C_r \times C_s$. Therefore, $C_r^\perp \subseteq C_r$ and $C_s^\perp \subseteq C_s$.

Converse part is straightforward. □

By Lemmas 35, 36 and Theorem 37, the next result is obtained.

Theorem 38: Let $C = C_r \times C_s$ be a separable $\mathbb{F}_qR$-cyclic code, where $C_r = \langle f(x)\rangle$ and $C_s = \langle \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)\rangle$. Then $C^\perp \subseteq C$ if and only if the following conditions holds

1) $x^r - 1 \equiv 0 \pmod{f(x)f^*(x)}$,
2) $x^s - 1 \equiv 0 \pmod{g_i(x)g_i^*(x))}$, *for* $i = 1, 2, 3, 4$.

The main result of constructing QECCs from this analysis is now presented.

Theorem 39: Let $C = C_r \times C_s$ be a separable $\mathbb{F}_qR$-cyclic code of block length (r, s). If $C_r^\perp \subseteq C_r$, $C_{s,i}^\perp \subseteq C_{s,i}$ for $i = 1, 2, 3, 4$, then there exists a QECC with parameters $[[r + 4s,\ 2k-(r+4s),\ d_H]]_q$, where d_H and k denote the Hamming distance and dimension of the code $\Psi_2(C)$, respectively.

Proof: Let $C_r^\perp \subseteq C_r$ and $C_{s,i}^\perp \subseteq C_{s,i}$, $i = 1, 2, 3, 4$. Then by Theorem 37, we have $C^\perp \subseteq C$. By Proposition 33, we have $\Psi_2(C^\perp) = \Psi_2(C)^\perp$, then we can easily see that $\Psi_2(C)^\perp \subseteq \Psi_2(C)$. Therefore, by Theorem 34, there exists a QECC with parameters $[[r + 4s,\ 2k - (r + 4s),\ d_H]]_q$. □

Now we present two detailed examples of constructing QECCs from mixed alphabets.

Example 40: Consider $r = 8$, $s = 20$ and $q = 5$. Denote $R = \mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ with $u^2 = u$, $v^2 = v$ and $uv = vu$.

$$x^8 - 1 = (x+4)(x+3)(x+2)(x+1) \times (x^2+3)(x^2+2) \in \mathbb{F}_5[x].$$

Let $f(x) = (x+2)(x^2+2)$. Then $C_r = \langle f(x)\rangle$ is a cyclic code over $\mathbb{F}_5$ with parameters $[8, 5, 3]$. Note that $f^*(x) = (x+3)(x^2+3)$. Thus, $x^8 - 1 \equiv 0 \pmod{f(x)f^*(x)}$, and by Lemma 35, we get $C_r^\perp \subseteq C_r$.

$$x^{20} - 1 = (x+4)^5(x+3)^5(x+2)^5(x+1)^5 \in \mathbb{F}_5[x].$$

Let $g_1(x) = (x+4)^2$, $g_2(x) = (x+3)$ and $g_i(x) = (x+2)$; $i = 3, 4$. Then $C_s = \langle \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)\rangle$ is a cyclic codes of length 20 over R, where $C_{s,j} = \langle g_j(x)\rangle$ are cyclic codes of length 20 over $\mathbb{F}_5$, for $j = 1, 2, 3, 4$. Then $\Psi_2(C)$ is a linear code over $\mathbb{F}_5$ with parameters $[88, 80, 3]$.

Note that $g_1^*(x) = (x+4)^2$, $g_2^*(x) = x+2$ and $g_i^*(x) = x+3$; $i = 3, 4$. Thus, $x^{20} - 1 \equiv 0 \pmod{g_j(x)g_j^*(x)}$; $j = 1, 2, 3, 4$, and by Lemma 36, we get $C_s^\perp \subseteq C_s$. Hence, by Theorem 39, there exists a QECC with parameters $[[88, 72, 3]]_5$, which is better than the constructed QECC $[[88, 48, 2]]_5$ given in [3]. □

Example 41: Consider $r = 24$, $s = 30$ and $q = 5$. Denote $R = \mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$, where $u^2 = u$, $v^2 = v$ and $uv = vu$.

$$x^{24} - 1 = (x+4)(x+3)(x+2)(x+1)(x^2+3)(x^2+2)$$

$$\times (x^2+x+2)(x^2+x+1)(x^2+2x+4) \times (x^2+2x+3)(x^2+4x+1)(x^2+4x+2) \times (x^2+3x+4)(x^2+3x+3) \in \mathbb{F}_5[x].$$

Let $f(x) = (x+2)(x^2+3x+3)$. Then $C_r = \langle f(x)\rangle$ is a cyclic code over $\mathbb{F}_5$ with parameters [24, 21, 3]. Note that $f^*(x) = (x+3)(x^2+x+2)$. Thus, $x^{24}-1 \equiv 0 \pmod{f(x)f^*(x)}$, and by Lemma 35, we get $C_r^{\perp} \subseteq C_r$.

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

Let $g_i(x) = x^2+x+1$, $g_2(x) = x+4$ and $g_3(x) = (x+1)^2$, where $i = 1, 4$. Then

$$C_s = \langle \xi_1 g_1(x) + \xi_2 g_2(x) + \xi_3 g_3(x) + \xi_4 g_4(x)\rangle$$

is a cyclic codes of length 30 over R, where $C_{s,j} = \langle g_j(x)\rangle$ are cyclic codes of length 30 over $\mathbb{F}_5$, for $j = 1, 2, 3, 4$. Then $\Psi_2(C)$ is a linear code over $\mathbb{F}_5$ with parameters [144, 134, 3].

Note that,

$$g_i^*(x) = x^2+x+1; \quad i = 1, 4,$$
$$g_2^*(x) = x+4, \quad \text{and } g_3^*(x) = (x+1)^2.$$

Thus, $x^{30}-1 \equiv 0 \pmod{g_j(x)g_j^*(x)}$; $j = 1, 2, 3, 4$, and by Lemma 36, we get $C_s^{\perp} \subseteq C_s$. Hence, from Theorem 39, there exists a QECC with parameters $[[144, 124, 3]]_5$, which is better than the constructed QECC $[[144, 120, 3]]_5$ given in [4]. □

In Table 3, we construct some QECCs which have better parameters then the previously known QECCs. The generator polynomial coefficients are written down in descending order, e.g. 1025 is corresponds to the polynomial x^3+2x+5.

VII. CONCLUSION

In this paper, we consider the ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ with $u^2 = u$, $v^2 = v$, $uv = vu$, where $q = p^m$ for an odd prime p and positive integer m. We study the $\mathbb{F}_qR$-cyclic codes of block length (r, s). We first present the orthogonal idempotent decomposition of the ring R and then discuss linear codes over R. A Gray map over $\mathbb{F}_q^r \times R^s$ is defined, and some of the properties of this map are examined. The algebraic structure and the generator polynomials of $\mathbb{F}_qR$-cyclic codes and separable codes are discussed. After that, the minimal generating sets and the size of this family of codes are determined. Further, we study the duality of $\mathbb{F}_qR$-cyclic codes, and we show that dual of a $\mathbb{F}_qR$-cyclic code is also a $\mathbb{F}_qR$-cyclic codes. The generators of dual codes are also described. Several optimal and near-optimal codes from this discussion are constructed in Tables 1 and 2. As an application of our study, we first define a Gray map on $\mathbb{F}_qR$, and then we discuss the dual containing property of separable codes. We present a construction of QECCs from separable $\mathbb{F}_qR$-cyclic codes. Finally, in Examples 40 and 41, we provide a detailed explanation of constructing QECCs from $\mathbb{F}_qR$-cyclic codes. Some new QECCs are given in Table 3. In the future, we will work on the construction of QECCs from non-separable codes. It is also interesting to study LCD codes and DNA codes over mixed alphabets.

ACKNOWLEDGMENT

The authors are grateful to the anonymous reviewers who has given helpful comments to improve the manuscript.

REFERENCES

[1] T. Abualrub, I. Siap, and N. Aydin, "$\mathbb{Z}_2\mathbb{Z}_4$-Additive cyclic and codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 3, pp. 1508–1514, Mar. 2014.
[2] M. Ashraf and G. Mohammad, "Construction of quantum codes from cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$," *Int. J. Inf. Coding Theory*, vol. 3, no. 2, pp. 137–144, 2015.
[3] M. Ashraf and G. Mohammad, "Quantum codes from cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$," *Quantum Inf. Process.*, vol. 15, no. 10, pp. 4089–4098, 2016.
[4] M. Ashraf and G. Mohammad, "Quantum codes over $\mathbb{F}_p$ from cyclic codes over $\mathbb{F}_p[u, v]/\langle u^2-1, v^3-v, uv-vu\rangle$," *Cryptogr. Commun.* vol. 11, no. 2, pp. 325–335, 2019.
[5] I. Aydogdu, T. Abualrub, and I. Siap, "On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes," *Int. J. Comput. Math.*, vol. 92, no. 9, pp. 1806–1814, 2015.
[6] I. Aydogdu, T. Abualrub, and I. Siap, "On $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 4883–4893, Nov. 2017.
[7] I. Aydogdu and F. Gursoy, "$\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-cyclic codes," *J. Appl. Math. Comput.*, vol. 60, pp. 327–341, 2019, doi: 10.1007/s12190-018-01216-z.
[8] I. Aydogdu, I. Siap, and R. T. Valls, "On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes," *Finite Fields Appl.*, vol. 48, pp. 241–260, Nov. 2017.
[9] I. Aydogdu and I. Siap, "The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes: Bounds on the minimum distance," *Appl. Math. Inf. Sci.*, vol. 7, no. 6, pp. 2271–2278, Nov. 2013.
[10] T. Bag, H. Q. Dinh, A. K. Upadhyay, R. Bandi, and W. Yamaka, "Quantum codes from classes of skew constacyclic codes over the ring $\mathbb{F}_q[u, v]/\langle u^2-1, v^2-1, uv-vu\rangle$," *Discrete Math.*, vol. 343, no. 3, Mar. 2020, Art. no. 111737, doi: 10.1016/j.disc.2019.111737.
[11] T. Bag, A. Dertli, Y. Cengellenmis, and A. K. Upadhyay, "Application of constacyclic codes over the semi local ring $F_p^m + vF_p^m$," *Indian J. Pure Appl. Math.*, vol. 51, no. 1, pp. 265–275, 2020.
[12] T. Bag, H. Q. Dinh, A. K. Upadhyay, and W. Yamaka, "New non-binary quantum codes from cyclic codes over product rings," *IEEE Commun. Lett.*, vol. 24, no. 3, pp. 486–490, Mar. 2020.
[13] J. Borges, C. F. Cordoba, and R. T. Valls, "$\mathbb{Z}_2$-double cyclic codes," *Des. Codes Cryptogr.* vol. 86, no. 3, pp. 463–479, 2018.
[14] J. Borges, C. F. Cordoba, J. Pujol, J. Rifa, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator matrices and duality," *Des. Codes Cryptogr.*, vol. 54, no. 2, pp. 167–179, 2009.
[15] J. Borges, C. F. Cordoba, and R. T. Valls, "$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6348–6354, Nov. 2016.
[16] A. E. Brouwer, H. O. Hamalainen, P. R. J. Ostergard, and N. J. A. Sloane, "Bounds on mixed binary/ternary codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 140–161, Jan. 1998.
[17] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[18] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257–397.
[19] A. Dertli, Y. Cengellenmis, and S. Eren, "Some results on the linear codes over the finite ring $\mathbb{F}_2 + v_1\mathbb{F}_2 + \cdots + v_r\mathbb{F}_2$," *Int. J. Quantum Inf.*, vol. 14, no. 1, Feb. 2016, Art. no. 1650012..
[20] A. Dertli, Y. Cengellenmis, and S. Eren, "On quantum codes obtained from cyclic codes over A_2," *Int. J. Quantum Inf.*, vol. 13, no. 3, 2015, Art. no. 1550031.
[21] L. Diao, J. Gao, and J. Lu, "Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes," *Adv. Math. Commun.*, vol. 14, no. 4, pp. 555–572, 2020, doi: 10.3934/amc.2020029.
[22] H. Q. Dinh, T. Bag, A. K. Upadhyay, M. Ashraf, G. Mohammad, and W. Chinnakum, "Quantum codes from a class of constacyclic codes over finite commutative rings," *J. Algebra Appl.*, vol. 19, no. 12, Dec. 2020, Art. no. 2150003.

[23] H. Q. Dinh, T. Bag, A. K. Upadhyay, R. Bandi, and W. Chinnakum, "On the structure of cyclic codes over $\mathbb{F}_q RS$ and applications in quantum and LCD codes constructions," *IEEE Access*, vol. 8, no. 1, pp. 18902–18914, 2020.

[24] J. Gao, M. J. Shi, T. Wu, and F. W. Fu, "On double cyclic codes over $\mathbb{Z}_4$," *Finite Fields Appl.*, vol. 39, pp. 233–250, Jan. 2016.

[25] G. G. La Guardia and R. Palazzo, Jr., "Constructions of new families of nonbinary CSS codes," *Discrete Math.*, vol. 310, no. 21, pp. 2935–2945, Nov. 2010.

[26] M. Grassl. *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Jul. 10, 2020. [Online]. Available: http://www.codetables.de

[27] M. Grassl and T. Beth, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 55–64, Mar. 2004.

[28] D. Gottesman, "An introduction to quantum error-correction," in *Proc. Symp. Appl. Math.*, vol. 58, pp. 221–236, 2002.

[29] K. Gowdhaman, C. Mohan, D. Chinnapillai, and J. Gao, "Construction of quantum codes from λ-constacyclic codes over the ring $\frac{\mathbb{F}_p[u,u]}{\langle u^3-u, v^3-v, uv-uv\rangle}$," *J. Appl. Math. Comput.*, 2020, doi: 10.1007/s12190-020-01407-7.

[30] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Slone, and P. Sole, "The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 301–319, Mar. 1994.

[31] R. Hill, *A First Course in Coding Theory*. Oxford, U.K.: Clarendon, Feb. 1986.

[32] X. Kai and S. Zhu, "Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$," *Int. J. Quantum Inf.*, vol. 9, pp. 689–700, Mar. 2011.

[33] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary quantum stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.

[34] J. Li, J. Gao, and Y. Wang, "Quantum codes from $(1-2v)$-constacyclic codes over the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$," *Discrete Math. Algorithms Appl.* vol. 10, no. 4, 2018, Art. no. 1850046, doi: 10.1142/S1793830918500465.

[35] R. Li, Z. Xu, and X. Li, "Binary construction of quantum codes of minimum distance three and four," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1331–1336, Jun. 2004.

[36] R. Li and Z. Xu, "Construction of $[[n, n-4, 3]]_q$ quantum codes for odd prime power q," *Phys. Rev. A, Gen. Phys.*, vol. 82, no. 5, pp. 1–4, 2010.

[37] F. Ma, J. Gao, and F. W. Fu, "Constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and their applications of constructing new non-binary quantum codes," *Quantum Inf. Process* vol. 17, no. 6, pp. 1–19, 2018.

[38] H. Mostafanasab, "Triple cyclic codes over $\mathbb{Z}_2$," *Palestine J. Math.*, vol. 6, no. 2, 123–134, 2017.

[39] J. RifÃ and J. Pujol, "Translation-invariant propelinear codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 590–598, Mar. 1997.

[40] J. Qian, W. Ma, and W. Guo, "Quantum codes from cyclic codes over finite ring," *Int. J. Quantum Inf.*, vol. 7, no. 6, pp. 1277–1283, Sep. 2009.

[41] M. Sari and I. Siap, "On quantum codes from cyclic codes over a class of nonchain rings," *Bull. Korean Math. Soc.*, vol. 53, no. 6, pp. 1617–1628, Nov. 2016.

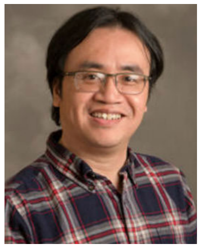
[42] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 6, pp. 4741–4751, Dec. 1996.

[43] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, pp. R2493–R2496, Oct. 1995.

[44] N. Sloane and J. Thompson, "Cyclic self-dual codes," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 364–366, May 1983.

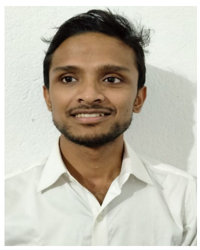
[45] T. Wu, J. Gao, and F. W. Fu, "Some results on triple cyclic codes over $\mathbb{Z}_4$," *IEICE Trans. Fundamnetals*, vol. 99, no. 5, pp. 998–1004, 2016.

[46] T. Wu, J. Gao, Y. Gao, and F. W. Fu, "$\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes," *Adv. Math. Commun.*, vol. 12, no. 4, pp. 641–657, 2018.



HAI Q. DINH received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from Ohio University, USA, in 1998, 2000, and 2003, respectively. He was a Visiting Professor with North Dakota State University, USA, for a period of one year. Since 2004, he has been with Kent State University, USA, as a tenure-Professor in mathematics, where he is currently a Professor in applied mathematics with the Department of Mathematical Sciences. Since 2004, he has been published more than 100 articles at high-level SCI(E) research journals, such as *Journal of Algebra*, *Journal of Pure and Applied Algebra*, the IEEE Transactions on Information Theory, the IEEE Communications Letters, *Finite Fields and Their Applications*, *Applicable Algebra in Engineering Communication and Computing*, and *Discrete Applied Mathematics*. He has been a well-known invited/keynote speaker at numerous international conferences and mathematics colloquium. He also gave many honorary tutorial lectures at international universities in China, Indonesia, Kuwait, Mexico, Singapore, Thailand, and Vietnam. His research interests include algebra and coding theory.

SACHIN PATHAK recieved the B.Sc. degree from Agra University, in 2012, and the M.Sc. degree in mathematics from IIT Kanpur, in 2015. He is currently a Research Scholar with the Department of Mathematics, Indian Institute of Technology Patna. His research interest includes algebraic coding theory.



TUSHAR BAG received the B.Sc. degree from the Ramakrishna Mission Vidyamandira, University of Calcutta, the M.Sc. degree from IIT Kanpur, India, and the Ph.D. degree from the Department of Mathematics, IIT Patna, in 2020. He has been publishing 14 articles. His main research interests include algebraic coding theory and codes over rings.

ASHISH KUMAR UPADHYAY received the B.Sc. and M.Sc. degrees in mathematics from the University of Allahabad, India, and the Ph.D. degree from the Indian Institute of Science, in 2005. He is currently an Associate Professor with the Department of Mathematics, Indian Institute of Technology Patna. His research interests include algebraic coding theory and algebraic topology.

WARATTAYA CHINNAKUM is currently an Assistant Professor with the Faculty of Economics, Chiang Mai University. She is also a member with the Centre of Excellence in Econometrics, Faculty of Economics. She works on macroeconomic theory, economic development, econometrics, and economic for public policy. Her research interests include wide range of topics, including economic development, financial econometrics, and tourism economics.