Filomat 37:15 (2023), 5137–5147
https://doi.org/10.2298/FIL2315137C

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Cyclic codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ and binary quantum codes

Fatma Çalışkan[a], **Refia Aksoy**[b]

[a] *Department of Mathematics, Faculty of Sciences, Istanbul University, Istanbul, Türkiye*
[b] *Department of Computer Engineering, Faculty of Engineering, Istanbul Gedik University, Istanbul, Türkiye*

Abstract. In the present study, we define cyclic codes over the commutative principal ideal ring $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ with $v^2 = v$ and obtain some results on cyclic codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$. We also investigate the dual of a cyclic code over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ depending on two inner products. We determine a generator polynomial of cyclic codes and give the calculation of the number of cyclic codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$. Furthermore, we show that the Gray images of a cyclic code over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ of length n are binary quasi-cyclic codes of length $3n$ and of index 3. We find numerous binary codes as Gray images of cyclic codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ and tabulate the optimal ones. Moreover, we show that it is possible to obtain binary quantum error-correcting codes (QECCs) from cyclic codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$.

1. Introduction

Cyclic codes (C-codes) have been studied by coding theorists because of their algebraic structure. Since C-codes can be described as polynomials or vectors, they present a different perspective in coding theory and provide ease of use in application.

Codes over rings have gained attention after the seminal paper by Hammons et al. [1]. Hammons et al. show in the paper that numerous good non-linear binary codes correspond to the Gray images of linear codes (L-codes) over $\mathbb{Z}_4$. In light of this paper, codes over rings have been investigated by many researchers [2–6]. For example, Zhu et al. [6] study on C-codes over $\mathbb{F}_2 + v\mathbb{F}_2$ of order 4 with $v^2 = v$. Later, by using non-trivial ring automorphism on $\mathbb{F}_2 + v\mathbb{F}_2$, Abualrub et al. [2] consider θ-C-codes over $\mathbb{F}_2 + v\mathbb{F}_2$. They give the definition of θ-C-codes and characterize the generators of these codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$.

Recently, many researchers have focused on codes over mixed alphabets [4, 7–11]. In most studies, for two positive integers r and s, codes are considered as $\mathfrak{B}$-submodules of $\mathfrak{A}^r \times \mathfrak{B}^s$, where $\mathfrak{A}$ and $\mathfrak{B}$ are two rings [7, 9, 10]. Besides, Çalışkan and Aksoy [8] consider codes as $\mathfrak{A} \times \mathfrak{B}$-submodules of $(\mathfrak{A} \times \mathfrak{B})^n$, where $\mathfrak{A} = \mathbb{F}_2$, $\mathfrak{B} = \mathbb{F}_2 + v\mathbb{F}_2$ with $v^2 = v$ and n is a positive integer. They study the L-codes over the product ring $\mathfrak{A} \times \mathfrak{B}$ and give the weight enumerators of these codes. Later, Aksoy and Çalışkan [11] investigate self-dual codes over $\mathfrak{A} \times \mathfrak{B}$.

QECCs play a pivotal role in protecting quantum information. The first examples of QECCs were given by Shor [12] and Steane [13]. In the notable paper by Calderbank et al. [14], it is shown that QECCs can be constructed from error-correcting codes over GF(4). Hence, researchers have sought to determine good

2020 *Mathematics Subject Classification*. Primary 94B15; Secondary 11T71, 94B60.
Keywords. Cyclic code; Generator polynomial; Dual code; Quantum code.
Received: 08 September 2022; Accepted: 09 January 2023
Communicated by Paola Bonacini
Email addresses: fatmac@istanbul.edu.tr (Fatma Çalışkan), refia.aksoy@gedik.edu.tr (Refia Aksoy)

QECCs from C-codes over finite fields. Later, a lot of research on the theory of QECCs has been directed to finite rings. We refer the reader to [15–18] for more details.

We focus in the present study on C-codes over the commutative Frobenius ring $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ of order 8 with $v^2 = v$. We show that a C-code over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ is principally generated. Moreover, we determine the generator polynomial of a C-code and find the number of C-codes depending on their length. We obtain some optimal binary codes by using C-codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$. We tabulate the optimal binary codes as Gray images of C-codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$. Therefore, we show that C-codes over the ring $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ can be used to construct optimal binary L-codes. Finally, as an application, we establish QECCs from Euclidean dual containing C-codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$.

The organization of this paper is as follows. In Section 2, we mention some basic properties of the ring $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ and recall the L-codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$, which are presented in [8]. We give the definition of a C-code over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ in Section 3. Also, we describe the form of the generator polynomial and the parity-check polynomial of a C-code over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$. We show that the binary image of a C-code over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ with respect to two Gray maps is a quasi-C-code of index 3. Moreover, we obtain a number of optimal codes as binary images of C-codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$. We construct QECCs from dual-containing C-codes over $\mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ in Section 4. We use Magma software [19] in all calculations.

2. Preliminaries

The finite commutative ring $\mathfrak{H} := \mathbb{F}_2 \times (\mathbb{F}_2 + v\mathbb{F}_2)$ was introduced by Çalışkan and Aksoy [8], where $\mathbb{F}_2$ is the binary field and $\mathbb{F}_2 + v\mathbb{F}_2$ is the finite commutative ring with $v^2 = v$. They also studied the L-codes over $\mathfrak{H}$ in [8]. In this section of the paper, we mention the properties of the ring $\mathfrak{H}$ and L-codes over $\mathfrak{H}$.

The ring $\mathfrak{H}$ is a Frobenius ring of characteristic 2. It can also be obtained that $\mathfrak{H}$ is a Boolean and principal ideal ring. Moreover, the ring is not a local ring.

Let $h = (h_1, h_2 + vh_3)$ and $a = (\kappa, \xi + v\tau)$ be two elements in $\mathfrak{H}$. The multiplication on $\mathfrak{H}$ given as $ha = (h_1\kappa, h_2\xi + v(h_3\xi + (h_2 + h_3)\tau))$ can be extended to $\mathfrak{H}^n$ as

$$h\,\boldsymbol{\alpha} = ((h_1\kappa_1, h_2\xi_1 + v(h_3\xi_1 + (h_2 + h_3)\tau_1)), \ldots, (h_1\kappa_n, h_2\xi_n + v(h_3\xi_n + (h_2 + h_3)\tau_n))),$$

where $\boldsymbol{\alpha} = (a_1, \ldots, a_n) \in \mathfrak{H}^n$ such that $a_i = (\kappa_i, \xi_i + v\tau_i) \in \mathfrak{H}$ for $1 \leq i \leq n$. $\mathfrak{H}^n$ is an $\mathfrak{H}$-module with this multiplication. A L-code $\mathfrak{C}$ over $\mathfrak{H}$ of length n is an $\mathfrak{H}$-submodule of $\mathfrak{H}^n$.

Two Gray maps over $\mathfrak{H}$ are defined in [8]. The first Gray map $\Phi_1 : \mathfrak{H} \to \mathbb{F}_2^3$ defined as $\Phi_1((\kappa, \xi + v\tau)) = (\kappa, \xi, \xi + \tau)$ is a ring isomorphism. Its extension to $\mathfrak{H}^n$ is

$$\phi_1((\boldsymbol{\kappa}, \boldsymbol{\xi} + v\boldsymbol{\tau})) = (\boldsymbol{\kappa}, \boldsymbol{\xi}, \boldsymbol{\xi} + \boldsymbol{\tau})$$

for any $\boldsymbol{\kappa}, \boldsymbol{\xi}, \boldsymbol{\tau} \in \mathbb{F}_2^n$. Let $w_H(\kappa)$ be the Hamming weight of $\kappa \in \mathbb{F}_2$ and $w_L^*(\xi + v\tau)$ be the Lee weight of $\xi + v\tau \in \mathbb{F}_2 + v\mathbb{F}_2$. The Lee weight of $(\kappa, \xi + v\tau) \in \mathfrak{H}$ is $w_L((\kappa, \xi + v\tau)) = w_H(\kappa) + w_L^*(\xi + v\tau)$. The second Gray map $\Phi_2 : \mathfrak{H} \to \mathbb{F}_2^3$ defined as $\Phi_2((\kappa, \xi + v\tau)) = (\kappa + \xi, \kappa + \tau, \kappa + \xi + \tau)$ is extended to $\mathfrak{H}^n$ as

$$\phi_2((\boldsymbol{\kappa}, \boldsymbol{\xi} + v\boldsymbol{\tau})) = (\boldsymbol{\kappa} + \boldsymbol{\xi}, \boldsymbol{\kappa} + \boldsymbol{\tau}, \boldsymbol{\kappa} + \boldsymbol{\xi} + \boldsymbol{\tau})$$

for any $\boldsymbol{\kappa}, \boldsymbol{\xi}, \boldsymbol{\tau} \in \mathbb{F}_2^n$. The Gray weight of $a \in \mathfrak{H}$ is $w_G(a) = 0$ if $a = (0, 0)$, $w_G(a) = 1$ if $a = (1, 1), (1, v), (1, 1 + v)$, $w_G(a) = 2$ if $a = (0, 1), (0, v), (0, 1 + v)$ and $w_G(a) = 3$ if $a = (1, 0)$. The Lee weight (or the Gray weight) of an element in $\mathfrak{H}^n$ is the sum of the Lee weights (or Gray weights) of its components. We note that the Gray map ϕ_1 is distance-preserving from ($\mathfrak{H}^n$, Lee distance-d_L) to ($\mathbb{F}_2^{3n}$, Hamming distance-d_H) and the Gray map ϕ_2 is distance preserving from ($\mathfrak{H}^n$, Gray distance-d_G) to ($\mathbb{F}_2^{3n}$, Hamming distance-d_H).

Let $\boldsymbol{x} = (x_1, x_2, ..., x_n)$, $\boldsymbol{y} = (y_1, y_2, ..., y_n) \in (\mathbb{F}_2 + v\mathbb{F}_2)^n$. We recall that the Euclidean inner product and the Hermitian inner product of $\boldsymbol{x}$ and $\boldsymbol{y}$ are defined as $\langle \boldsymbol{x}, \boldsymbol{y} \rangle_E = \sum\limits_{i=1}^{n} x_i y_i$ and $[\mathbf{x}, \boldsymbol{y}]_H = \sum\limits_{i=1}^{n} x_i \overline{y_i}$, respectively, where $\overline{y_i} = \overline{y_i' + vy_i''} = (y_i' + y_i'') + vy_i''$ for all $y_i', y_i'' \in \mathbb{F}_2$. Let $\boldsymbol{\alpha} = (a_1, \ldots, a_n)$, $\boldsymbol{\beta} = (b_1, \ldots, b_n) \in \mathfrak{H}^n$ and $\boldsymbol{\kappa}, \boldsymbol{\xi}, \boldsymbol{\tau}, \boldsymbol{\zeta}, \boldsymbol{\eta}, \boldsymbol{\lambda} \in \mathbb{F}_2^n$. The Euclidean inner product of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ is given as $\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle = \sum\limits_{i=1}^{n} a_i b_i$ and can be defined as

$$\langle\, (\boldsymbol{\kappa}, \boldsymbol{\xi} + v\boldsymbol{\tau}), (\boldsymbol{\zeta}, \boldsymbol{\eta} + v\boldsymbol{\lambda})\, \rangle = (\boldsymbol{\kappa} \cdot \boldsymbol{\zeta}, \langle\, \boldsymbol{\xi} + v\boldsymbol{\tau},\ \boldsymbol{\eta} + v\boldsymbol{\lambda}\, \rangle_E),$$

where '$\cdot$' denotes the dot product in $\mathbb{F}_2^n$. Also, the Hermitian inner product of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ is given as $[\boldsymbol{\alpha},\boldsymbol{\beta}] = \sum_{i=1}^{n} a_i\overline{b_i}$, where $\overline{b_i} = \overline{(\zeta_i, \eta_i + v\lambda_i)} = (\zeta_i, \eta_i + \lambda_i + v\lambda_i)$ for all $\zeta_i, \eta_i, \lambda_i \in \mathbb{F}_2$, and can be defined as

$$[(\boldsymbol{\kappa}, \boldsymbol{\xi} + v\boldsymbol{\tau}), (\boldsymbol{\zeta}, \boldsymbol{\eta} + v\boldsymbol{\lambda})] = (\boldsymbol{\kappa} \cdot \boldsymbol{\zeta}, [\, \boldsymbol{\xi} + v\boldsymbol{\tau},\ \boldsymbol{\eta} + v\boldsymbol{\lambda}\,]_H).$$

Let $\mathbb{C}$ be a code over $\mathfrak{H}^n$. The Euclidean dual $\mathbb{C}^{\perp_E}$ of $\mathbb{C}$ is defined as $\mathbb{C}^{\perp_E} = \{\boldsymbol{\beta} \in \mathfrak{H}^n | \langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle = (0,0),\ \forall \boldsymbol{\alpha} \in \mathfrak{H}^n\}$ and the Hermitian dual $\mathbb{C}^{\perp_H}$ of $\mathbb{C}$ is defined as $\mathbb{C}^{\perp_H} = \{\boldsymbol{\beta} \in \mathfrak{H}^n | [\boldsymbol{\alpha}, \boldsymbol{\beta}] = (0,0),\ \forall \boldsymbol{\alpha} \in \mathfrak{H}^n\}$.

One can obtain equivalent codes by permuting the coordinates of any code and interchanging the elements v and $1+v$ of all coordinates in necessary cases. Now, let us remind the following properties about L-codes over $\mathfrak{H}$.

Remark 2.1. *[8] A L-code $\mathbb{C}$ over $\mathfrak{H}$ of length n is permutation equivalent to $\mathbb{C}_1 \times \mathbb{C}_2$ where $\mathbb{C}_1$ is a binary L-code of length n and $\mathbb{C}_2$ is a L-code over $\mathbb{F}_2 + v\mathbb{F}_2$ of length n, which is denoted as $\mathbb{C} = (\mathbb{C}_1, \mathbb{C}_2)$.*

Lemma 2.2. *[8] Let $\mathbb{C}^{\perp_E}$ be the Euclidean dual of a L-code $\mathbb{C}$. Then $\phi_1(\mathbb{C}^{\perp_E}) = (\phi_1(\mathbb{C}))^{\perp_E}$, where $(\phi_1(\mathbb{C}))^{\perp_E}$ is the Euclidean dual of $\phi_1(\mathbb{C})$ as a binary code.*

3. C-codes over $\mathfrak{H}$

We study on C-codes over the ring $\mathfrak{H}$ in this section. We find that both the Euclidean dual and the Hermitian dual of C-codes over $\mathfrak{H}$ are also cyclic. Also, we seek the Gray images of C-codes over $\mathfrak{H}$ based on the Gray map ϕ_1 and the Gray map ϕ_2. Then, we obtain that the Gray images of any C-code over $\mathfrak{H}$ of length n are binary quasi-C-codes of length $3n$ and index 3. Therefore, the benefit of working on C-codes over $\mathfrak{H}$ of length n is that it is easier than working on binary L-codes of length $3n$ in application.

Definition 3.1. *Let $\rho(\mathfrak{c}) = (\mathfrak{c}_{n-1}, \mathfrak{c}_0, \ldots, \mathfrak{c}_{n-2})$ be the cyclic shift of any element $\mathfrak{c} = (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ in a code $\mathbb{C}$ over $\mathfrak{H}$. $\mathbb{C}$ is called a C-code over $\mathfrak{H}$ if $\mathbb{C}$ is a L-code over $\mathfrak{H}$ and $\rho(\mathbb{C}) = \mathbb{C}$.*

Let k be an integer and $\mathfrak{c} = (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ be an element in $\mathbb{C}$. Then the k-th cyclic shift of $\mathfrak{c}$ is defined as $\rho^k(\mathfrak{c}) = (\mathfrak{c}_{0-k}, \mathfrak{c}_{1-k}, \ldots, \mathfrak{c}_{n-1-k})$ where all the subscripts are computed modulo n. We note that $\rho^1(\mathfrak{c}) = \rho(\mathfrak{c})$ and $\rho^{-1}(\mathfrak{c}) = \rho^{n-1}(\mathfrak{c})$.

Theorem 3.2. $(\mathbb{C}_1, \mathbb{C}_2)$ *is a C-code over $\mathfrak{H}$ of length n if and only if $\mathbb{C}_1$ is a binary C-code of length n and $\mathbb{C}_2$ is a C-code over $\mathbb{F}_2 + v\mathbb{F}_2$ of length n.*

Proof. It is easy to see from Definition 3.1 and Remark 2.1. □

Proposition 3.3. *The Euclidean dual $\mathbb{C}^{\perp_E}$ of a C-code $\mathbb{C}$ over $\mathfrak{H}$ is also cyclic.*

Proof. Let $\mathfrak{c} = (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ be an element of a C-code $\mathbb{C}$ of length n over $\mathfrak{H}$. If $\mathfrak{u} = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{C}^{\perp_E}$, then we have

$$\langle \mathfrak{c}, \mathfrak{u} \rangle = \mathfrak{c}_0 u_0 + \mathfrak{c}_1 u_1 + \ldots + \mathfrak{c}_{n-1} u_{n-1} = 0.$$

Since $\mathbb{C}$ is cyclic, $\rho^k(\mathfrak{c}) \in \mathbb{C}$ for every integer k. Then $\langle \rho^k(\mathfrak{c}), \mathfrak{u} \rangle = 0$. Hence, for $k = n-1$, we have

$$\begin{aligned} 0 &= \langle \rho^{n-1}(\mathfrak{c}), \mathfrak{u} \rangle \\ &= \mathfrak{c}_1 u_0 + \mathfrak{c}_2 u_1 + \ldots + \mathfrak{c}_0 u_{n-1} \\ &= \mathfrak{c}_0 u_{n-1} + \mathfrak{c}_1 u_0 + \ldots + \mathfrak{c}_{n-1} u_{n-2} \\ &= \langle \mathfrak{c}, \rho(\mathfrak{u}) \rangle, \end{aligned}$$

which implies $\rho(\mathfrak{u}) \in \mathbb{C}^{\perp_E}$. Therefore, $\mathbb{C}^{\perp_E}$ is cyclic. □

Proposition 3.4. *The Hermitian dual $\mathfrak{C}^{\perp_H}$ of a C-code $\mathfrak{C}$ over $\mathfrak{H}$ is also cyclic.*

Proof. The proof can be done analogously as in the proof of Proposition 3.3. □

Let $p(\mathrm{t})$ be a polynomial in the ring $\mathfrak{H}[\mathrm{t}]$. It may be useful to consider $p(\mathrm{t})$ as

$$\begin{aligned} p(\mathrm{t}) &= p_0 + p_1\mathrm{t} + \ldots + p_{n-1}\mathrm{t}^{n-1} \\ &= (r_0, s_0 + vt_0) + (r_1, s_1 + vt_1)\mathrm{t} + \ldots + (r_{n-1}, s_{n-1} + vt_{n-1})\mathrm{t}^{n-1} \\ &= (r_0 + r_1\mathrm{t} + \ldots + r_{n-1}\mathrm{t}^{n-1}, s_0 + s_1\mathrm{t} + \ldots + s_{n-1}\mathrm{t}^{n-1} + v(t_0 + t_1\mathrm{t} + \ldots + t_{n-1}\mathrm{t}^{n-1})) \\ &= (r(\mathrm{t}), s(\mathrm{t}) + vt(\mathrm{t})), \end{aligned}$$

where $r(\mathrm{t}), s(\mathrm{t}), t(\mathrm{t}) \in \mathbb{F}_2[\mathrm{t}]$. Moreover, for two polynomials $k(\mathrm{t})$ and $l(\mathrm{t})$ in $\mathfrak{H}[\mathrm{t}]$, we note that

$$\begin{aligned} k(\mathrm{t})l(\mathrm{t}) &= (k_1(\mathrm{t}), k_2(\mathrm{t}) + vk_3(\mathrm{t}))(l_1(\mathrm{t}), l_2(\mathrm{t}) + vl_3(\mathrm{t})) \\ &= (k_1(\mathrm{t})l_1(\mathrm{t}), k_2(\mathrm{t})l_2(\mathrm{t}) + v(k_2(\mathrm{t})l_3(\mathrm{t}) + k_3(\mathrm{t})l_2(\mathrm{t}) + k_3(\mathrm{t})l_3(\mathrm{t}))), \end{aligned}$$

where $k_i(\mathrm{t}), l_i(\mathrm{t}) \in \mathbb{F}_2[\mathrm{t}]$ for $i = 1, 2, 3$.

Let $\mathfrak{H}_n = \mathfrak{H}[\mathrm{t}]/(\mathbf{1}\mathrm{t}^n - \mathbf{1})$, where $\mathbf{1} = (1, 1) \in \mathfrak{H}$. There is a one-to-one correspondence between the element $\mathfrak{c} = (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ in $\mathfrak{H}^n$ and the polynomial $c(\mathrm{t}) = \mathfrak{c}_0 + \mathfrak{c}_1\mathrm{t} + \ldots + \mathfrak{c}_{n-1}\mathrm{t}^{n-1}$ in $\mathfrak{H}_n$, where $\mathfrak{c}_i = (a_i, b_i + vd_i)$ for $a_i, b_i, d_i \in \mathbb{F}_2$ and $0 \leq i \leq n-1$. Note that we can denote a codeword of $\mathfrak{C}$ as an element $\mathfrak{c} = (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ in $\mathfrak{H}^n$ or as a polynomial $c(\mathrm{t}) = \mathfrak{c}_0 + \mathfrak{c}_1\mathrm{t} + \ldots + \mathfrak{c}_{n-1}\mathrm{t}^{n-1}$ in $\mathfrak{H}_n$ interchangeably.

Let $c(\mathrm{t}) = (a(\mathrm{t}), b(\mathrm{t}) + vd(\mathrm{t}))$ be a polynomial in $\mathfrak{H}_n$. If we operate on $c(\mathrm{t})$ with the polynomial $e(\mathrm{t}) = (\mathrm{t}, \mathrm{t})$, then we have

$$\begin{aligned} e(\mathrm{t})c(\mathrm{t}) &= (\mathrm{t}, \mathrm{t})(a(\mathrm{t}), b(\mathrm{t}) + vd(\mathrm{t})) \\ &= (\mathrm{t}, \mathrm{t})(a_0 + a_1\mathrm{t} + \ldots + a_{n-1}\mathrm{t}^{n-1}, b_0 + b_1\mathrm{t} + \ldots + b_{n-1}\mathrm{t}^{n-1} + v(d_0 + d_1\mathrm{t} + \ldots + d_{n-1}\mathrm{t}^{n-1})) \\ &= (a_0\mathrm{t} + a_1\mathrm{t}^2 + \ldots + a_{n-1}\mathrm{t}^n, b_0\mathrm{t} + b_1\mathrm{t}^2 + \ldots + b_{n-1}\mathrm{t}^n + v(d_0\mathrm{t} + d_1\mathrm{t}^2 + \ldots + d_{n-1}\mathrm{t}^n)) \\ &= (a_{n-1} + a_0\mathrm{t} + \ldots + a_{n-2}\mathrm{t}^{n-1}, b_{n-1} + b_0\mathrm{t} + \ldots + b_{n-2}\mathrm{t}^{n-1} + v(d_{n-1} + d_0\mathrm{t} + \ldots + d_{n-2}\mathrm{t}^{n-1})). \end{aligned}$$

Therefore, the product $e(\mathrm{t})c(\mathrm{t})$ in $\mathfrak{H}_n$ corresponds to the cyclic shift of $c(\mathrm{t})$. Since the codewords of a C-code $\mathfrak{C}$ over $\mathfrak{H}$ can be considered as polynomials in $\mathfrak{H}_n$, we have the following result.

Theorem 3.5. *A code $\mathfrak{C}$ over $\mathfrak{H}$ of length n is a C-code if and only if $\mathfrak{C}$ is an ideal of $\mathfrak{H}_n$.*

We note that every binary C-code $\mathfrak{C}_1$ of length n corresponds to a principal ideal of the ring $\mathbb{F}_2[\mathrm{t}]/(\mathrm{t}^n - 1)$. A binary C-code $\mathfrak{C}_1$ can be generated by the unique monic polynomial $g_1(\mathrm{t})$ of minimal degree in $\mathfrak{C}_1$ such that $g_1(\mathrm{t}) \mid \mathrm{t}^n - 1$, and $|\mathfrak{C}_1| = 2^{n-\deg(g_1(\mathrm{t}))}$. Also every C-code $\mathfrak{C}_2$ over $\mathbb{F}_2 + v\mathbb{F}_2$ of length n is a principal ideal of $(\mathbb{F}_2 + v\mathbb{F}_2)[\mathrm{t}]/(\mathrm{t}^n - 1)$. A C-code $\mathfrak{C}_2$ can be generated by the unique polynomial $g(\mathrm{t})$ in $\mathfrak{C}_2$, where $g(\mathrm{t}) = (1 + v)g_2(\mathrm{t}) + vg_3(\mathrm{t})$ for $g_2(\mathrm{t}) \mid \mathrm{t}^n - 1$ and $g_3(\mathrm{t}) \mid \mathrm{t}^n - 1$. If $g_2(\mathrm{t}) = g_3(\mathrm{t})$, then $g(\mathrm{t}) = g_2(\mathrm{t})$. Also $|\mathfrak{C}_2| = 2^{2n-\deg(g_2(\mathrm{t}))-\deg(g_3(\mathrm{t}))}$. For more details, we refer the reader to [6].

Theorem 3.6. *There is a unique polynomial $f(\mathrm{t})$ for a C-code $\mathfrak{C}$ over $\mathfrak{H}$ of length n such that $\mathfrak{C} = \langle f(\mathrm{t}) \rangle$, where $f(\mathrm{t}) = (g_1(\mathrm{t}), (1 + v)g_2(\mathrm{t}) + vg_3(\mathrm{t}))$ and $g_i(\mathrm{t}) \mid \mathrm{t}^n - 1$ for $i = 1, 2, 3$. Moreover, $|\mathfrak{C}| = 2^{3n-\deg(g_1(\mathrm{t}))-\deg(g_2(\mathrm{t}))-\deg(g_3(\mathrm{t}))}$.*

Proof. In light of Remark 2.1 and Theorem 3.2, we observe that $\mathfrak{C} = \langle (g_1(\mathrm{t}), (1 + v)g_2(\mathrm{t}) + vg_3(\mathrm{t})) \rangle$, where $\mathfrak{C}_1 = \langle g_1(\mathrm{t}) \rangle$ and $\mathfrak{C}_2 = \langle (1 + v)g_2(\mathrm{t}) + vg_3(\mathrm{t}) \rangle$ such that $\mathfrak{C} = (\mathfrak{C}_1, \mathfrak{C}_2)$. We have $|\mathfrak{C}| = 2^{3n-deg(g_1(\mathrm{t}))-deg(g_2(\mathrm{t}))-deg(g_3(\mathrm{t}))}$ since $|\mathfrak{C}| = |\mathfrak{C}_1||\mathfrak{C}_2|$. □

From Theorem 3.5 and Theorem 3.6, the following corollary which provides to consider C-codes over $\mathfrak{H}$ as principal ideals can be obtained.

Corollary 3.7. *$\mathfrak{H}_n$ is a principal ideal ring.*

Now, we give the form of a parity-check polynomial of a C-code $\mathfrak{C}$ over $\mathfrak{H}$ of length n. We consider the polynomial $\mathfrak{h}_i(\mathrm{t}) = \frac{\mathrm{t}^n-1}{g_i(\mathrm{t})}$ $(i = 1, 2, 3)$. Let $\widetilde{\mathfrak{h}_i}(\mathrm{t}) = \mathrm{t}^{\deg(\mathfrak{h}_i(\mathrm{t}))}\mathfrak{h}_i(\mathrm{t}^{-1})$ be the reciprocal polynomial of $\mathfrak{h}_i(\mathrm{t})$ $(i = 1, 2, 3)$. In light of Theorem 3.6, we have the next results.

Corollary 3.8. *Let $\mathfrak{C}^{\perp_E}$ be the Euclidean dual of $\mathfrak{C}$ over $\mathfrak{H}$. We have $\mathfrak{C}^{\perp_E} = \langle(\widetilde{\mathfrak{h}_1}(\mathrm{t}), (1+v)\widetilde{\mathfrak{h}_2}(\mathrm{t}) + v\widetilde{\mathfrak{h}_3}(\mathrm{t}))\rangle$ and $|\mathfrak{C}^{\perp_E}| = 2^{deg(g_1(\mathrm{t}))+deg(g_2(\mathrm{t}))+deg(g_3(\mathrm{t}))}$.*

Corollary 3.9. *Let $\mathfrak{C}^{\perp_H}$ be the Hermitian dual of $\mathfrak{C}$ over $\mathfrak{H}$. We have $\mathfrak{C}^{\perp_H} = \langle(\widetilde{\mathfrak{h}_1}(\mathrm{t}), v\widetilde{\mathfrak{h}_2}(\mathrm{t}) + (1+v)\widetilde{\mathfrak{h}_3}(\mathrm{t}))\rangle$ and $|\mathfrak{C}^{\perp_H}| = 2^{deg(g_1(\mathrm{t}))+deg(g_2(\mathrm{t}))+deg(g_3(\mathrm{t}))}$.*

The number of C-codes over $\mathfrak{H}$ of length n can be obtained for a given n using the next result.

Theorem 3.10. *Let $\mathrm{t}^n - 1 = \prod_{k=1}^{s} p_k^{\alpha_k}(\mathrm{t})$ in $\mathbb{F}_2[\mathrm{t}]$, where $p_k(\mathrm{t})$ are pairwise relatively prime nonzero polynomials. The number of C-codes over the ring $\mathfrak{H}$ of length n is $\prod_{k=1}^{s}(\alpha_k + 1)^3$.*

Proof. The number of binary C-codes is $\prod_{k=1}^{s}(\alpha_k+1)$ and the number of C-codes over $\mathbb{F}_2+v\mathbb{F}_2$ is $\prod_{k=1}^{s}(\alpha_k+1)^2$ [6]. Thus, we obtain the result. □

Quasi-C-codes have been considered to obtain good L-codes in the literature. We recall the next concept before giving the definition of quasi-C-codes. For an integer k, let $\mathfrak{c}$ be an element of $\mathbb{F}_2^{kn}$. We can write

$$\begin{aligned}\boldsymbol{\mathfrak{c}} &= (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{kn-1}) \\ &= (\mathfrak{c}_{(0)}|\mathfrak{c}_{(1)}| \ldots |\mathfrak{c}_{(k-1)}),\end{aligned}$$

where $\mathfrak{c}_{(i)} \in \mathbb{F}_2^n$ for $i = 0, 1, \ldots, k-1$. Let us consider the map

$$\psi_k : \mathbb{F}_2^{kn} \to \mathbb{F}_2^{kn}, \quad \psi_k(\boldsymbol{\mathfrak{c}}) = (\rho(\mathfrak{c}_{(0)})|\, \rho(\mathfrak{c}_{(1)})| \ldots |\rho(\mathfrak{c}_{(k-1)})),$$

where ρ is the cyclic shift operator.

Definition 3.11. *A binary code $\mathfrak{C}$ of length nk is called a quasi-C-code of index k if $\psi_k(\mathfrak{C}) = \mathfrak{C}$. In particular, a quasi-C-code of index 1 is a C-code.*

Lemma 3.12. *Let ρ be the cyclic shift operator. We have $\phi_1\rho = \psi_3\phi_1$ and $\phi_2\rho = \psi_3\phi_2$.*

Proof. If $\boldsymbol{\kappa}, \boldsymbol{\xi}, \boldsymbol{\tau} \in \mathbb{F}_2^n$, then

$$(\phi_1\rho)((\boldsymbol{\kappa}, \boldsymbol{\xi} + v\boldsymbol{\tau})) = \phi_1(\rho(\boldsymbol{\kappa}), \rho(\boldsymbol{\xi}) + v\rho(\boldsymbol{\tau})) = (\rho(\boldsymbol{\kappa}), \rho(\boldsymbol{\xi}), \rho(\boldsymbol{\xi}) + \rho(\boldsymbol{\tau})).$$

On the other hand, we obtain

$$(\psi_3\phi_1)((\boldsymbol{\kappa}, \boldsymbol{\xi} + v\boldsymbol{\tau})) = \psi_3(\boldsymbol{\kappa}, \boldsymbol{\xi}, \boldsymbol{\xi} + \boldsymbol{\tau}) = (\rho(\boldsymbol{\kappa}), \rho(\boldsymbol{\xi}), \rho(\boldsymbol{\xi}) + \rho(\boldsymbol{\tau})).$$

Therefore, we have the desired equality. The second equality can also be obtained in the same way. □

We give the following theorem in order to characterize the images of C-codes over $\mathfrak{H}$ depending on the Gray maps ϕ_1 and ϕ_2.

Theorem 3.13. *Let $\mathfrak{C}$ be a C-code over $\mathfrak{H}$ of length n. The binary images $\phi_1(\mathfrak{C})$ and $\phi_2(\mathfrak{C})$ are binary quasi-C-codes of length $3n$ and of index 3.*

Proof. We know that $\rho(\mathbb{C}) = \mathbb{C}$ since $\mathbb{C}$ is a C-code over $\mathfrak{H}$. Therefore, we have

$$\phi_1(\rho(\mathbb{C})) = \phi_1(\mathbb{C}).$$

Hence, by using Lemma 3.12, we obtain

$$\psi_3(\phi_1(\mathbb{C})) = \phi_1(\mathbb{C}).$$

Likewise, we have that $\phi_2(\mathbb{C})$ is a binary quasi-C-code of length $3n$ and of index 3. □

Here we give some examples to exemplify the obtained results. We obtain C-codes over $\mathfrak{H}$ of lengths ≤ 15. However, we tabulate the generator polynomials of C-codes over $\mathfrak{H}$ for lengths 2, 3, 7 and 15 and the parameters of the corresponding Gray images of C-codes over $\mathfrak{H}$. Especially, we give generator matrices of C-codes over $\mathfrak{H}$ of length 2. We restrict our results to optimal binary codes for lengths 3, 7 and 15. These are the lengths that we obtained more optimal codes than the others. For the given length and dimension, by an optimal binary code, we mean a code which has the highest minimum distance over $\mathbb{F}_2$. We note that the notation $[n, k, d]$ in the tables means the parameters of a binary L-code of length n, dimension k and minimum distance d. In the tables, the column Number shows the number of codes of the same parameter and the column Generator polynomial indicates the generator polynomial of one of the codes with the same parameters.

Example 3.14. *The factorization of the polynomial* $\mathrm{t}^2 - 1$ *in* $\mathbb{F}_2$ *is*

$$\mathrm{t}^2 - 1 = (1 + \mathrm{t})^2.$$

The number of nonzero C-codes over $\mathfrak{H}$ *of length 2 is 26. In Table 1, we list all the nonzero C-codes with their generator matrices, generator polynomials and their binary images under the Gray maps* ϕ_1 *and* ϕ_2.

Example 3.15. *The factorization of the polynomial* $\mathrm{t}^3 - 1$ *in* $\mathbb{F}_2$ *is*

$$\mathrm{t}^3 - 1 = (1 + \mathrm{t})(1 + \mathrm{t} + \mathrm{t}^2).$$

The number of nonzero C-codes over $\mathfrak{H}$ *of length 3 is 63. In Table 2, we give the generator polynomials of C-codes whose Gray images under* ϕ_2 *are optimal binary codes. Here, we consider the Gray images under the map* ϕ_2 *rather than the map* ϕ_1 *since the Gray images under* ϕ_2 *have better minimum distance than the Gray images under* ϕ_1 *for the same length and dimension.*

Example 3.16. *The polynomial* $\mathrm{t}^7 - 1$ *in* $\mathbb{F}_2$ *can be factorized as*

$$\mathrm{t}^7 - 1 = (1 + \mathrm{t})(1 + \mathrm{t} + \mathrm{t}^3)(1 + \mathrm{t}^2 + \mathrm{t}^3).$$

The number of nonzero C-codes over $\mathfrak{H}$ *of length 7 is 511. In Table 3, we tabulate the generator polynomials of C-codes whose Gray images under the map* ϕ_2 *are optimal codes over* $\mathbb{F}_2$.

Example 3.17. *The polynomial* $\mathrm{t}^{15} - 1$ *can be uniquely expressed in* $\mathbb{F}_2$ *as*

$$\mathrm{t}^{15} - 1 = (1 + \mathrm{t})(1 + \mathrm{t} + \mathrm{t}^2)(1 + \mathrm{t} + \mathrm{t}^4)(1 + \mathrm{t}^3 + \mathrm{t}^4)(1 + \mathrm{t} + \mathrm{t}^2 + \mathrm{t}^3 + \mathrm{t}^4).$$

The number of nonzero C-codes over $\mathfrak{H}$ *of length 15 is 32767. In Table 4, we give the generator polynomials of C-codes whose Gray images under the map* ϕ_2 *are optimal binary codes.*

Table 1: C-codes over $\mathfrak{H}$ of Length 2

Generator matrix	Generator polynomial	Gray image (ϕ_1)	Gray image (ϕ_2)
$[\,(0,v)\ \ (0,v)\,]$	$(0,v)+(0,v)\mathrm{t}$	[6,1,2]	[6,1,4]
$[\,(0,1+v)\ \ (0,1+v)\,]$	$(0,1+v)+(0,1+v)\mathrm{t}$	[6,1,2]	[6,1,4]
$[\,(1,0)\ \ (1,0)\,]$	$(1,0)+(1,0)\mathrm{t}$	[6,1,2]	[6,1,6]
$[\,(1,v)\ \ (1,v)\,]$	$(1,v)+(1,v)\mathrm{t}$	[6,2,2]	[6,2,2]
$[\,(1,1+v)\ \ (1,1+v)\,]$	$(1,1+v)+(1,1+v)\mathrm{t}$	[6,2,2]	[6,2,2]
$\begin{bmatrix} (0,v) & (0,0) \\ (0,0) & (0,v) \end{bmatrix}$	$(0,v)$	[6,2,1]	[6,2,2]
$\begin{bmatrix} (0,1+v) & (0,0) \\ (0,0) & (0,1+v) \end{bmatrix}$	$(0,1+v)$	[6,2,1]	[6,2,2]
$\begin{bmatrix} (1,0) & (0,0) \\ (0,0) & (1,0) \end{bmatrix}$	$(1,0)$	[6,2,1]	[6,2,3]
$[\,(0,1)\ \ (0,1)\,]$	$(0,1)+(0,1)\mathrm{t}$	[6,2,2]	[6,2,4]
$[\,(1,1)\ \ (1,1)\,]$	$(1,1)+(1,1)\mathrm{t}$	[6,3,2]	[6,3,2]
$\begin{bmatrix} (0,1) & (0,1+v) \\ (0,1+v) & (0,1) \end{bmatrix}$	$(0,1)+(0,1+v)\mathrm{t}$	[6,3,1]	[6,3,2]
$\begin{bmatrix} (0,1) & (0,v) \\ (0,v) & (0,1) \end{bmatrix}$	$(0,1)+(0,v)\mathrm{t}$	[6,3,1]	[6,3,2]
$\begin{bmatrix} (1,v) & (1,0) \\ (1,1) & (1,v) \end{bmatrix}$	$(1,v)+(1,0)\mathrm{t}$	[6,3,1]	[6,3,2]
$\begin{bmatrix} (1,1+v) & (1,0) \\ (1,0) & (1,1+v) \end{bmatrix}$	$(1,1+v)+(1,0)\mathrm{t}$	[6,3,1]	[6,3,2]
$\begin{bmatrix} (1,v) & (0,v) \\ (0,v) & (1,v) \end{bmatrix}$	$(1,v)+(0,v)\mathrm{t}$	[6,3,1]	[6,3,2]
$\begin{bmatrix} (1,1+v) & (0,1+v) \\ (0,1+v) & (1,1+v) \end{bmatrix}$	$(1,1+v)+(0,1+v)\mathrm{t}$	[6,3,1]	[6,3,2]
$\begin{bmatrix} (1,v) & (0,0) \\ (0,0) & (1,v) \end{bmatrix}$	$(1,v)$	[6,4,1]	[6,4,1]
$\begin{bmatrix} (1,1+v) & (0,0) \\ (0,0) & (1,1+v) \end{bmatrix}$	$(1,1+v)$	[6,4,1]	[6,4,1]
$\begin{bmatrix} (0,1) & (0,0) \\ (0,0) & (0,1) \end{bmatrix}$	$(0,1)$	[6,4,1]	[6,4,2]
$\begin{bmatrix} (1,1) & (0,1) \\ (0,1) & (1,1) \end{bmatrix}$	$(1,1)+(0,1)\mathrm{t}$	[6,4,1]	[6,4,2]
$\begin{bmatrix} (1,1) & (1,1+v) \\ (1,1+v) & (1,1) \end{bmatrix}$	$(1,1)+(1,1+v)\mathrm{t}$	[6,4,1]	[6,4,2]
$\begin{bmatrix} (1,1) & (1,v) \\ (1,v) & (1,1) \end{bmatrix}$	$(1,1)+(1,v)\mathrm{t}$	[6,4,1]	[6,4,2]
$\begin{bmatrix} (1,1) & (0,1+v) \\ (0,1+v) & (1,1) \end{bmatrix}$	$(1,1)+(0,1+v)\mathrm{t}$	[6,5,1]	[6,5,1]
$\begin{bmatrix} (1,1) & (0,v) \\ (0,v) & (1,1) \end{bmatrix}$	$(1,1)+(0,v)\mathrm{t}$	[6,5,1]	[6,5,1]
$\begin{bmatrix} (1,1) & (1,0) \\ (1,0) & (1,1) \end{bmatrix}$	$(1,1)+(1,0)\mathrm{t}$	[6,5,1]	[6,5,2]
$\begin{bmatrix} (1,1) & (0,0) \\ (0,0) & (1,1) \end{bmatrix}$	$(1,1)$	[6,6,1]	[6,6,1]

Table 2: Optimal Binary Codes Derived from C-codes over $\mathfrak{H}$ of Length 3

Number	Generator polynomial	Gray image (ϕ_2)
1	$(1,0) + (1,0)t + (1,0)t^2$	[9,1,9]
2	$(1,0) + (1,0)t$	[9,2,6]
6	$(1,1+v) + (1,1+v)t + (0,1+v)t^2$	[9,3,4]
2	$(1,1) + (1,1)t + (0,1)t^2$	[9,4,4]
2	$(1,1) + (0,1)t + (0,1)t^2$	[9,5,3]
8	$(1,1) + (1,v)t + (0,v)t^2$	[9,6,2]
4	$(1,1) + (1,1+v)t$	[9,7,2]
1	$(1,1) + (1,0)t$	[9,8,2]
1	$(1,1)$	[9,9,1]

Table 3: Optimal Binary Codes Derived from C-codes over $\mathfrak{H}$ of Length 7

Number	Generator polynomial	Gray image (ϕ_2)
1	$(1,0) + (1,0)t + (1,0)t^2 + (1,0)t^3 + (1,0)t^4 + (1,0)t^5 + (1,0)t^6$	[21,1,21]
1	$(0,1) + (0,1)t + (0,1)t^2 + (0,1)t^3 + (0,1)t^4 + (0,1)t^5 + (0,1)t^6$	[21,2,14]
2	$(1,0) + (1,0)t + (1,0)t^2 + (1,0)t^4$	[21,3,12]
4	$(1,v) + (1,v)t + (1,v)t^2 + (0,v)t^3 + (1,v)t^4 + (0,v)t^5 + (0,v)t^6$	[21,4,10]
2	$(1,1) + (1,1)t + (1,1)t^2 + (0,1)t^3 + (1,1)t^4 + (0,1)t^5 + (0,1)t^6$	[21,5,10]
8	$(1,1+v) + (1,0)t + (1,1+v)t^2 + (0,1+v)t^3 + (1,1+v)t^4$	[21,6,8]
6	$(1,1) + (1,1)t + (1,1)t^2 + (1,0)t^3 + (1,1)t^4 + (1,0)t^5 + (1,0)t^6$	[21,7,8]
2	$(1,1) + (0,1)t + (1,1)t^2 + (1,0)t^3 + (1,1)t^4$	[21,9,8]
2	$(1,1) + (1,1)t^2 + (1,1)t^3 + (1,0)t^4$	[21,11,6]
2	$(1,1) + (0,1)t + (1,0)t^2 + (1,1)t^3$	[21,12,5]
25	$(1,1) + (0,1)t + (1,0)t^2 + (1,v)t^3 + (1,0)t^4$	[21,13,4]
8	$(1,1) + (1,v)t + (0,1+v)t^2 + (0,1)t^3$	[21,14,4]
2	$(1,1) + (1,1)t + (1,0)t^2 + (1,0)t^4$	[21,15,4]
2	$(1,1) + (0,1)t + (1,0)t^2 + (1,0)t^3$	[21,16,3]
14	$(1,1) + (0,1+v)t + (0,v)t^2 + (0,v)t^3$	[21,17,2]
3	$(1,1) + (1,1)t$	[21,18,2]
3	$(1,1) + (1,v)t$	[21,19,2]
1	$(1,1) + (1,0)t$	[21,20,2]
1	$(1,1)$	[21,21,1]

Table 4: Optimal Binary Codes Derived from C-codes over $\mathfrak{S}$ of Length 15

Number	Generator polynomial	Gray image (ϕ_2)
1	$(1,0)+(1,0)t+(1,0)t^2+(1,0)t^3+(1,0)t^4+(1,0)t^5+(1,0)t^6+(1,0)t^7+(1,0)t^8+(1,0)t^9+(1,0)t^{10}+(1,0)t^{11}+(1,0)t^{12}+(1,0)t^{13}+(1,0)t^{14}$	[45,1,45]
2	$(1,0)+(1,0)t+(1,0)t^3+(1,0)t^4+(1,0)t^6+(1,0)t^7+(1,0)t^9+(1,0)t^{10}+(1,0)t^{12}+(1,0)t^{13}$	[45,2,30]
2	$(1,0)+(1,0)t+(1,0)t^2+(1,0)t^3+(1,0)t^5+(1,0)t^7+(1,0)t^8+(1,0)t^{11}$	[45,4,24]
4	$(1,v)+(1,v)t+(1,v)t^2+(1,v)t^3+(0,v)t^4+(1,v)t^5+(0,v)t^6+(1,v)t^7+(1,v)t^8+(0,v)t^9+(0,v)t^{10}+(1,v)t^{11}+(0,v)t^{12}+(0,v)t^{13}+(0,v)t^{14}$	[45,5,22]
2	$(1,1)+(1,1)t+(1,1)t^2+(1,1)t^3+(0,1)t^4+(1,1)t^5+(0,1)t^6+(1,1)t^7+(1,1)t^8+(0,1)t^9+(0,1)t^{10}+(1,1)t^{11}+(0,1)t^{12}+(0,1)t^{13}+(0,1)t^{14}$	[45,6,22]
4	$(1,1)+(0,1)t+(0,v)t^2+(1,1)t^3+(1,1)t^4+(0,v)t^5+(1,1)t^6+(0,1)t^7+(1,v)t^8+(1,1)t^9+(1,1)t^{10}+(1,v)t^{11}+(0,1)t^{12}+(0,1)t^{13}+(0,v)t^{14}$	[45,7,20]
2	$(1,1)+(1,1)t+(1,0)t^2+(1,1)t^3+(0,1)t^4+(1,0)t^5+(0,1)t^6+(1,1)t^7+(1,0)t^8+(0,1)t^9+(0,1)t^{10}+(1,0)t^{11}+(0,1)t^{12}+(0,1)t^{13}$	[45,8,20]
8	$(1,1)+(1,1)t+(1,1+v)t^2+(0,1)t^3+(1,v)t^4+(1,1+v)t^5+(0,v)t^6+(0,1)t^7+(1,1+v)t^8+(0,v)t^9+(1,v)t^{10}+(0,1+v)t^{11}+(0,v)t^{12}+(0,v)t^{13}$	[45,11,16]
2	$(1,1)+(0,1)t+(0,1)t^2+(1,1)t^3+(1,0)t^4+(0,1)t^5+(1,0)t^6+(0,1)t^7+(1,1)t^8+(1,0)t^9+(1,0)t^{10}+(1,1)t^{11}$	[45,12,16]
2	$(1,1)+(1,0)t^2+(0,1)t^3+(0,1)t^4+(1,0)t^5+(1,1)t^6+(1,1)t^8+(1,1)t^9+(1,1)t^{10}+(0,1)t^{11}$	[45,13,16]
4	$(1,1)+(0,1)t+(1,1)t^2+(0,1)t^4+(1,1)t^5+(1,0)t^6+(1,1)t^8+(1,0)t^9+(1,1)t^{10}$	[45,15,14]
4	$(1,1)+(1,0)t+(1,0)t^2+(0,1)t^3+(1,1)t^4+(1,1)t^5+(1,1)t^8+(0,1)t^9+(1,0)t^{10}$	[45,17,12]
18	$(1,1)+(1,1+v)t^2+(0,1)t^3+(1,1)t^4+(1,v)t^5+(0,1+v)t^6+(0,v)t^8+(0,v)t^9$	[45,25,8]
10	$(1,1)+(1,v)t+(1,1+v)t^2+(0,v)t^3+(0,1+v)t^4+(1,1+v)t^5+(1,0)t^6+(1,v)t^7$	[45,26,8]
2	$(1,1)+(1,1)t+(1,0)t^2+(0,1)t^3+(1,1)t^5+(1,0)t^6+(1,0)t^7$	[45,28,8]
2	$(1,1)+(0,1)t+(1,0)t^2+(1,1)t^3+(1,0)t^4+(0,1)t^5+(1,0)t^6$	[45,29,7]
28	$(1,1)+(0,v)t+(1,v)t^2+(0,1)t^3+(1,1+v)t^4+(1,0)t^5+(0,v)t^6$	[45,30,6]
10	$(1,1)+(1,1+v)t+(0,v)t^2+(1,0)t^3+(0,1)t^4+(1,v)t^5$	[45,31,6]
2	$(1,1)+(1,1)t+(1,0)t^3+(0,1)t^4+(1,0)t^5$	[45,32,6]
56	$(1,1)+(1,v)t+(1,1+v)t^3+(0,1+v)t^4+(1,0)t^5$	[45,35,4]
18	$(1,1)+(0,1)t+(1,v)t^2+(1,0)t^3+(1,0)t^4+(1,0)t^6$	[45,36,4]
6	$(1,1)+(1,1)t+(0,v)t^2+(1,0)t^3+(1,0)t^5$	[45,37,4]
2	$(1,1)+(1,1)t+(1,0)t^3+(1,0)t^5$	[45,38,4]
2	$(1,1)+(0,1)t+(1,0)t^3+(1,0)t^4$	[45,39,3]
33	$(1,1)+(0,v)t+(0,v)t^2+(1,0)t^3$	[45,40,2]
15	$(1,1)+(0,v)t+(0,1+v)t^3$	[45,41,2]
8	$(1,1)+(1,v)t+(0,v)t^2$	[45,42,2]
4	$(1,1)+(1,0)t+(1,0)t^2$	[45,43,2]
1	$(1,1)+(1,0)t$	[45,44,2]
1	$(1,1)$	[45,45,1]

4. QECC from C-codes over $\mathfrak{H}$

A q-ary QECC of length n is defined to be a q^k dimensional subspace of the q^n dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$ and denoted by $[[n, k, d]]$, where q, $\otimes n$ and d are a prime power, the tensor product of vector spaces and the minimum Hamming distance of the QECC, respectively. There are some methods used to obtain QECC. One of them, the Calderbank-Shor-Steane (CSS) construction, is an important method given to construct QECCs from L-codes over finite fields. Now, let us give the CSS construction.

Theorem 4.1. *[14] Let $\mathcal{C}$ and $\mathcal{C}'$ be linear $[n, k_1, d_1]$ code and $[n, k_2, d_2]$ code over $GF(q)$. There exists an $[[n, k_1 + k_2 - n, min\{d_1, d_2\}]]$ QECC if $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}'$. Specially, there exists an $[[n, 2k_1 - n, d_1]]$ QECC if $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$.*

Next, we give dual-containing conditions both for C-codes over $\mathbb{F}_2$ and $\mathbb{F}_2 + v\mathbb{F}_2$, respectively.

Lemma 4.2. *[14] Let $\mathcal{C}$ be a binary C-code with the generating polynomial $f(\mathrm{t})$ and $\widetilde{f}(\mathrm{t})$ be the reciprocal polynomial of $f(\mathrm{t})$. The code $\mathcal{C}$ contains its dual if and only if $\mathrm{t}^n - 1 \equiv 0 \pmod{f(\mathrm{t})\widetilde{f}(\mathrm{t})}$.*

Lemma 4.3. *[20] Suppose $\mathcal{C} = \langle g(\mathrm{t})\rangle$ is a C-code of length n over $\mathbb{F}_2 + v\mathbb{F}_2$, where $g(\mathrm{t}) = (1 + v)g_1(\mathrm{t}) + vg_2(\mathrm{t})$. Then $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$ if and only if $\mathrm{t}^n - 1 \equiv 0 \pmod{g_i(\mathrm{t})\widetilde{g_i}(\mathrm{t})}$, where $\widetilde{g_i}(\mathrm{t})$ is the reciprocal polynomial of $g_i(\mathrm{t})$ for $i = 1, 2$.*

$\mathcal{C}$ is called a Euclidean dual-containing code if $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$. Now, we give a result about the Euclidean dual-containing C-codes over $\mathfrak{H}$.

Theorem 4.4. *Let $\mathcal{C} = \langle f(\mathrm{t})\rangle$ be a C-code of length n over $\mathfrak{H}$, where $f(\mathrm{t}) = (g_1(\mathrm{t}), (1+v)g_2(\mathrm{t})+vg_3(\mathrm{t}))$ and $g_i(\mathrm{t}) \mid \mathrm{t}^n - 1$ for $i = 1, 2, 3$. $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$ if and only if $\mathrm{t}^n - 1 \equiv 0 \pmod{g_i(\mathrm{t})\widetilde{g_i}(\mathrm{t})}$, where $\widetilde{g_i}(\mathrm{t})$ is the reciprocal polynomial of $g_i(\mathrm{t})$ for $i = 1, 2, 3$.*

Proof. In light of Theorem 3.2, the result can be obtained by using Lemma 4.2 and Lemma 4.3. □

The following result can be obtained as a consequence of Theorem 4.4.

Corollary 4.5. *Let $\mathcal{C} = (\mathcal{C}_1, \mathcal{C}_2)$ be a C-code of length n over $\mathfrak{H}$. $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$ if and only if $\mathcal{C}_1^{\perp_E} \subseteq \mathcal{C}_1$ and $\mathcal{C}_2^{\perp_E} \subseteq \mathcal{C}_2$.*

Next, we give a result to obtain QECCs from dual-containing C-codes over the ring $\mathfrak{H}$.

Theorem 4.6. *Let $\mathcal{C}$ be a C-code over $\mathfrak{H}$ of length n with minimum Lee weight d_L. If $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$, then there exists a binary QECC with parameters $[[3n, 2k - 3n, d_L]]$, where k is the dimension of $\phi_1(\mathcal{C})$.*

Proof. Suppose $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$. We know that $\phi_1(\mathcal{C}^{\perp_E}) = \phi_1(\mathcal{C})^{\perp_E}$ from Lemma 2.2. Let $\mathfrak{c} \in \phi_1(\mathcal{C}^{\perp_E})$. There exists $\mathfrak{c}' \in \mathcal{C}^{\perp_E}$ such that $\mathfrak{c} = \phi_1(\mathfrak{c}')$, since ϕ_1 is a ring isomorphism. From $\mathfrak{c}' \in \mathcal{C}^{\perp_E}$ and $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$, we have $\mathfrak{c}' \in \mathcal{C}$. Then $\mathfrak{c} = \phi_1(\mathfrak{c}') \in \phi_1(\mathcal{C})$ which means $\phi_1(\mathcal{C})^{\perp_E} \subseteq \phi_1(\mathcal{C})$. Here $\phi_1(\mathcal{C})$ is a binary L-code $[3n, k, d_L]$. From Theorem 4.1, there exists a binary $[[3n, 2k - 3n, d_L]]$ QECC. □

Example 4.7. *The polynomial $\mathrm{t}^8 - 1$ has the factorization as*

$$\mathrm{t}^8 - 1 = (1 + \mathrm{t})^8 \ \textit{in} \ \mathbb{F}_2.$$

Let

$$g_1(\mathrm{t}) = 1 + \mathrm{t}, \quad g_2(\mathrm{t}) = 1 + \mathrm{t}^2 \ \textit{ and } \ g_3(\mathrm{t}) = 1 + \mathrm{t} + \mathrm{t}^2 + \mathrm{t}^3.$$

Then, $\mathcal{C} = \langle(1 + \mathrm{t}, 1 + v\mathrm{t} + \mathrm{t}^2 + v\mathrm{t}^3)\rangle$, which we can write as $\mathcal{C} = \langle(1, 1) + (1, v)\mathrm{t} + (0, 1)\mathrm{t}^2 + (0, v)\mathrm{t}^3\rangle$, is a C-code over $\mathfrak{H}$ of length 8 with minimum Lee weight 2. By Theorem 3.13, $\phi_1(\mathcal{C})$ is a binary quasi-C-code of index 3 with parameters $[24, 18, 2]$. We obtain that

$$\widetilde{g_1}(t) = 1 + \mathrm{t}, \quad \widetilde{g_2}(\mathrm{t}) = 1 + \mathrm{t}^2 \ \textit{ and } \ \widetilde{g_3}(\mathrm{t}) = 1 + \mathrm{t} + \mathrm{t}^2 + \mathrm{t}^3.$$

Thus, $g_i(\mathrm{t})\widetilde{g_i}(\mathrm{t}) \mid \mathrm{t}^8 - 1$ for $i = 1, 2, 3$. Therefore, by Theorem 4.4, we have $\mathcal{C}^{\perp_E} \subseteq \mathcal{C}$. Hence, there exists a binary QECC with parameters $[[24, 12, 2]]$ by Theorem 4.6.

In Table 5, we give binary QECCs obtained from the C-codes over $\mathfrak{H}$ of lengths ≤ 15. The first column denotes the lengths of the C-codes that we used to obtain binary QECCs. The second column consists of the generator polynomials of the C-codes. The third column shows the parameters of the Gray image of the C-code under the map ϕ_1. The last column indicates the parameters of the binary QECCs.

Table 5: Binary QECCs Derived from C-codes over $\mathfrak{H}$

Length	Generator polynomial	Gray image (ϕ_1)	$[[n,k,d]]$
2	$(1,1)+(1,1)\mathrm{t}$	[6,3,2]	[[6,0,2]]
3	$(1,1)$	[9,9,1]	[[9,9,1]]
4	$(1,1)+(1,1+v)\mathrm{t}+(0,v)\mathrm{t}^2$	[12,8,2]	[[12,4,2]]
5	$(1,1)$	[15,15,1]	[[15,15,1]]
6	$(1,1)+(1,1)\mathrm{t}+(1,v)\mathrm{t}^2$	[18,13,2]	[[18,8,2]]
7	$(1,1)+(1,v)\mathrm{t}+(0,1+v)\mathrm{t}^2+(1,1)\mathrm{t}^3$	[21,12,3]	[[21,3,3]]
8	$(1,1)+(0,1)\mathrm{t}+(1,v)\mathrm{t}^2+(0,v)\mathrm{t}^3$	[24,18,2]	[[24,12,2]]
9	$(1,1)$	[27,27,1]	[[27,27,1]]
10	$(1,1)+(1,v)\mathrm{t}+(0,1+v)\mathrm{t}^5$	[30,23,2]	[[30,16,2]]
11	$(1,1)$	[33,33,1]	[[33,33,1]]
12	$(1,1)+(1,1)\mathrm{t}+(0,v)\mathrm{t}^3+(0,v)\mathrm{t}^4$	[36,30,2]	[[36,24,2]]
13	$(1,1)$	[39,39,1]	[[39,39,1]]
14	$(1,1)+(0,v)\mathrm{t}+(1,1)\mathrm{t}^2+(0,v)\mathrm{t}^3+(1,1)\mathrm{t}^6+(0,v)\mathrm{t}^7$	[42,23,3]	[[42,4,3]]
15	$(1,1)+(1,v)\mathrm{t}+(0,1+v)\mathrm{t}^3+(1,1)\mathrm{t}^4$	[45,33,3]	[[45,21,3]]

Acknowledgement

The authors thank the anonymous reviewers and the editor for their valuable comments.

References

[1] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Transaction Information Theory 40 (1994) 301–319.

[2] T. Abualrub, N. Aydın, P. Seneviratne, On θ-cyclic codes over $\mathbb{F}_2+v\mathbb{F}_2$, Australasian Journal of Combinatorics 54 (2012) 115–126.

[3] A. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$, IEEE Transaction Information Theory 45(4) (1999) 1250–1255.

[4] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, $\mathbb{Z}_2$-double cyclic codes, Designs, Codes and Cryptography 86(3) (2018) 463–479.

[5] B. Yildiz, S. Karadeniz, Cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Designs, Codes and Cryptography 58 (2011) 221–234.

[6] S. Zhu, Y. Wang, M. Shi, Some results on cyclic codes over $\mathbb{F}_2+v\mathbb{F}_2$, IEEE Transaction Information Theory 56(4) (2010) 1680–1684.

[7] T. Abualrub, I. Siap, N. Aydın, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, IEEE Transaction Information Theory 60 (2014) 1508–1514.

[8] F. Çalışkan, R. Aksoy, Linear codes over $\mathbb{F}_2\times(\mathbb{F}_2+v\mathbb{F}_2)$ and the MacWilliams identities, Applicable Algebra in Engineering Communication and Computing 31 (2020) 135–147.

[9] I. Aydogdu, T. Abualrub, I. Siap, On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes, International Journal of Computational Mathematics 92 (2014) 1806–1814.

[10] I. Aydogdu, I. Siap, R. Ten-Valls, On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic code, Finite Fields and Their Applications 48 (2017) 241–260.

[11] R. Aksoy, F. Çalışkan, Self-dual codes over $\mathbb{F}_2\times(\mathbb{F}_2+v\mathbb{F}_2)$, Cryptography and Communications 13 (2020) 129–141.

[12] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, Physical Review A 52 (1995) 2493–2496.

[13] A. M. Steane, Simple quantum error-correcting codes, Physical Review A 54 (1996) 4741–4751.

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

[15] M. Ashraf, G. Mohammad, Construction of quantum codes from cyclic codes over $\mathbb{F}_p+v\mathbb{F}_p$, International Journal of Information and Coding Theory 3 (2015) 137–144.

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

[17] Y. Gao, J. Gao, F. W. Fu, Quantum codes from cyclic codes over the ring $\mathbb{F}_q+v_1\mathbb{F}_q+\cdots+v_r\mathbb{F}_q$, Applicable Algebra in Engineering Communication and Computing 30 (2019) 161–174.

[18] F. Ma, J. Gao, 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 Information Processing 17 (2018) 122.

[19] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, Journal of Symbolic Computation 24 (1997) 235–265.

[20] J. Qian, Quantum codes from cyclic codes over $\mathbb{F}_2+v\mathbb{F}_2$, Journal of Information and Computing Science 10 (2013) 1715–1722.