ISSN: 2307-7743
www.scienceasia.asia

Asian J. Math. Appl. (2026) 2026:6

An Application of Ω-Cyclic Codes

Yasemin Cengellenmis[1], Abdullah Dertli[2]

[1]Department of Mathematics, Trakya University, Edirne, Turkey
[2]Department of Mathematics, Ondokuz Mayıs University, Samsun, Turkey
Email(s): ycengellenmis@gmail.com, abdullah.dertli@gmail.com

Correspondence should be addressed to Yasemin Cengellenmis: ycengellenmis@gmail.com

Abstract
In this paper, the Ω-cyclic codes of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$ are studied, where $\Omega = R_{000}R_{100}R_{110}R_{111}$ and $I = \{(0,0,0), (1,0,0), (1,1,0), (1,1,1)\}$. By defining a Gray map, we obtain the Gray images of Ω-cyclic codes. Their generator polynomials are given. The necessary and sufficient conditions of Ω-cyclic codes to be separable are determined. We obtain quantum error correcting codes from Ω-cyclic codes.

Keywords: Cyclic code, Ω-cyclic code, Gray map, separable code, quantum error correcting code.

1 Introduction

Cyclic codes are error correcting codes and they have algebraic properties that are suitable for efficient error correction and detection. In addition to studying some features of cyclic codes, studying the application areas of these codes attracted the attention of researchers. One of the application areas of cyclic codes is quantum error correcting codes. Some researchers studied cyclic codes over a finite ring or a family of finite rings in order to obtain QECC(quantum error correcting code) [5],[4], respectively. Recently, researchers begin to study on cyclic code over mix alphabet in order to obtain QECC [2, 3]. Motivated by the work [2] and [3], we decide to study on $\Omega = R_{000}R_{100}R_{110}R_{111}$-cyclic codes in order to construct quantum codes, where $R_{000} = F_q$ are finite fields with $q = p^e$ elements, p is an odd prime $e \geq 1$ is a positive integer and $R_{100} = F_q[u]/< u^2 - 1 >$, $R_{110} = F_q[u,v]/< u^2 - 1, v^2 - v, uv - vu >$,$R_{111} = F_q[u,v,w]/< u^2 - 1, v^2 - v, w^2 - \alpha w, uv - vu, uw - wu, vw - wv >$, where $\alpha \in {R_{000}}^*$ are finite commutative rings. The aim of this paper is that we hope to finds optimal quantum codes that would not to be found in literature.

The paper is organized as follows. In the section 2, some basic knowledges are given. The sets R_{ijk} are introduced for $(i,j,k) \in I$, where I is lexicographic ordered set and it is equal to $\{(0,0,0), (1,0,0), (1,1,0), (1,1,1)\}$. The structures of the linear codes over R_{ijk}, for $(i,j,k) \in I'$, where $I' = \{(1,0,0), (1,1,0), (1,1,1)\}$ and the Gray maps are given. The structures of the cyclic codes over R_{ijk} are obtained, for $(i,j,k) \in I'$. In the section 3, Ω- linear codes are investigated. The Gray map is given, in the section 4. The Gray images of them are obtained. In the section 5, the structures of Ω- cyclic codes are discussed. The necessary and sufficient conditions of the Ω- cyclic to be separable are determined. In the section 6, it is obtained the quantum error correcting codes, by using a map and Ω- cyclic codes and CSS construction.

Received: 2026-07-07

2 Preliminaries

Let F_q denote finite fields of characteristic p with q elements. A k dimensional subspace C of ${F_q}^n$ is called a linear code over F_q of length n. Each element $\mathbf{c} \in C$ is called a codeword. A linear code C over F_q with length n is cyclic code if $\mathbf{c} = (c_0, ..., c_{n-1}) \in C$, then its cyclic shift $\sigma(\mathbf{c}) = (c_{n-1}, c_0, ..., c_{n-2}) \in C$. The Hamming weight of $\mathbf{c}$ is defined as the number of its nonzero components, it is denoted by $w_H(\mathbf{c})$. The Hamming weigth of a code C is defined as the smallest Hamming weight among all its non zero codewords, it is denoted by $w_H(C)$. The Hamming distance between $\mathbf{c}$ and $\mathbf{e}$ is defined $d_H(\mathbf{c}, \mathbf{e}) = w_H(\mathbf{c} - \mathbf{e})$. The Hamming distance of a code C is defined as $d_H(C) = min\{d_H(\mathbf{c}, \mathbf{e}) | \mathbf{c} \neq \mathbf{e}, \forall \mathbf{c}, \mathbf{e} \in C\}$. The dual of C is defined $C^{\perp} = \{\hat{\mathbf{c}} = (\hat{c}_0, ..., \hat{c}_{n-1}) \in {F_q}^n | c_0\hat{c}_0 + ... + c_{n-1}\hat{c}_{n-1} = 0$, all $\mathbf{c} = (c_0, ..., c_{n-1}) \in C\}$. A code C is called self orthogonal if $C \subset C^{\perp}$.

Let R denote any finite commutative ring. A non empty subset D of R^n is called linear code of length n over R if D forms an R-submodule of R^n. A linear code D over R with length n is cyclic code if $\mathbf{d} = (d_0, ..., d_{n-1}) \in D$, then its cyclic shift $\sigma(\mathbf{d}) = (d_{n-1}, d_0, ..., d_{n-2}) \in D$. By identifiying each codeword $\mathbf{d} = (d_0, ..., d_{n-1})$ to a polynomial $d(x) = d_0 + d_1x + ... + d_{n-1}x^{n-1}$ in $R[x]/< x^n - 1 >$, a linear code D is a cyclic code if and only if it is an ideal of the ring $R[x]/< x^n - 1 >$.

Let

$$R_{ijk} = \{\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1} u^i v^j w^k a_{ijk} | a_{ijk} \in R_{000}, u^2 = 1, v^2 = v, w^2 = \alpha w, \alpha \in {R_{000}}^*\}$$

be commutative rings, where $(i, j, k) \in I' = \{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ and $R_{000} = F_q$ are finite fields with $q = p^e$ elements, p is an odd prime $e \geq 1$ is a positive integer. For $(i, j, k) = (1, 0, 0)$, then the finite ring $R_{100} = F_q[u]/< u^2 - 1 >$. For $(i, j, k) = (1, 1, 0)$, then the finite ring $R_{110} = F_q[u, v]/< u^2 - 1, v^2 - v, uv - vu >$. For $(i, j, k) = (1, 1, 1)$, then the finite ring $R_{111} = F_q[u, v, w]/< u^2 - 1, v^2 - v, w^2 - \alpha w, uv - vu, uw - wu, vw - wv >$, where $\alpha \in {R_{000}}^*$. They have q^2, q^4, q^8 elements, respectively.

For $(i, j, k) \in I'$, an arbitrary element $r_{ijk} = \sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1} u^i v^j w^k a_{ijk} \in R_{ijk}$ can be uniquely

$$\sum_{(y,s,t)\in T} \eta_{yst} b_{\alpha_{i+j+k},yst}$$

where $b_{\alpha_{i+j+k},yst} \in R_{000}$ and the set T is lexicographic ordered on the cartesian product $A \times B \times C$. Since $A = \{0, 1\}, B = \{0\}, C = \{0\}$, for R_{100}, then $T = \{(0, 0, 0), (1, 0, 0)\}$. Since $A = \{0, 1\}, B = \{0, 1\}, C = \{0\}$, for R_{110}, then $T = \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 0)\}$. Since $A = \{0, 1\}, B = \{0, 1\}, C = \{0, 1\}$, for R_{111}, then $T = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$.

Moreover, η_{yst} are idempotent generators, where $(y, s, t) \in T$, for $(i, j, k) \in I'$. That is, $\sum_{(y,s,t)\in T} \eta_{yst} = 1$, $\eta_{yst}^2 = \eta_{yst}$ and $\eta_{yst}\eta_{lmn} = 0$, where $\eta_{yst} \neq \eta_{lmn}$, all $(y, s, t), (l, m, n) \in T$, for $(i, j, k) \in I'$.

For the finite ring R_{100}, then

$$\eta_{000} = (u + 1)/2, \eta_{100} = (1 - u)/2$$

.

For the finite ring R_{110}, then

$$\eta_{000} = (uv + v)/2, \eta_{010} = (1 + u - v - uv)/2,$$

$$\eta_{100} = (v - uv)/2, \eta_{110} = (1 - u - v + uv)/2$$

.

For the finite ring R_{111}, then

$$\eta_{000} = (wuv + wv)/2\alpha, \eta_{001} = (v\alpha - wv + \alpha uv - uvw)/2\alpha,$$

$$\eta_{010} = (w - wv + uw - uvw)/2\alpha, \eta_{011} = (\alpha - w - v\alpha + vw + u\alpha + wu - uv\alpha + uvw)/2\alpha,$$
$$\eta_{100} = (vw - uvw)/2\alpha, \eta_{101} = (\alpha v - vw - \alpha uv + uvw)/2\alpha,$$
$$\eta_{110} = (w - wv - uw + uvw)/2\alpha, \eta_{111} = (\alpha - w - \alpha v + vw - u\alpha + uw + \alpha uv - uvw)/2\alpha$$

.

The Gray map is defined as follows;

$$\begin{array}{rcl} \psi_{ijk} & : & R_{ijk} \longrightarrow R_{000}^{2^{i+j+k}} \\ \sum\limits_{(y,s,t)\in T} \eta_{yst} b_{\alpha_{i+j+k},yst} & \longmapsto & (f_l)_{l\in U} \end{array}$$

where $f_l = b_{\alpha_{i+j+k},yst}$, for $(y, s, t) \in T$ and $U = \{1, 2, 3, ..., 2^{i+j+k}\}$ for $(i, j, k) \in I'$. For example;

$$\begin{array}{rcl} \psi_{110} & : & R_{110} \longrightarrow R_{000}^4 \\ r_{110} & \longmapsto & (b_{\alpha_2,000}, b_{\alpha_2,010}, b_{\alpha_2,100}, b_{\alpha_2,110}) \end{array}$$

We define the Lee weight of $r_{ijk} \in R_{ijk}$ as ;

$$w_L(r_{ijk}) = w_H(\psi_{ijk}(r_{ijk}))$$

where $(i, j, k) \in I'$ and w_H denotes the Hamming weight over R_{000}.

This map can be extended from $R_{ijk}^{\alpha_{i+j+k}}$ to $R_{000}^{\alpha_{i+j+k}2^{i+j+k}}$ as follows,

$$\begin{array}{rcl} \psi_{ijk} & : & R_{ijk}^{\alpha_{i+j+k}} \longrightarrow R_{000}^{\alpha_{i+j+k}2^{i+j+k}} \\ \mathbf{r_{ijk}} = (r_{ijk}^a)_{a\in M} & \longmapsto & (b^a_{\alpha_{i+j+k},rst})_{(r,s,t)\in T, a\in M} \end{array}$$

where $(i, j, k) \in I'$. The elements $\mathbf{r_{ijk}} = (r_{ijk}^a)_{a\in M} \in R_{ijk}^{\alpha_{i+j+k}}$ denotes $\mathbf{r_{ijk}} = (r_{ijk}^0, ..., r_{ijk}^{\alpha_{i+j+k}-1})$. The Lee weight of $\mathbf{r_{ijk}} = (r_{ijk}^a)_{a\in M} \in R_{ijk}^{\alpha_{i+j+k}}$ where $M = \{0, 1, ..., \alpha_{i+j+k} - 1\}$ for $(i, j, k) \in I'$ is $w_L(\mathbf{r_{ijk}}) = \sum_{a=0}^{\alpha_{i+j+k}-1} w_L(r_{ijk}^a)$. The Lee distance between any two elements $\mathbf{r_{ijk}} = (r_{ijk}^a)_{a\in M}$,$\hat{\mathbf{r}}_{\mathbf{ijk}} = (\hat{r}_{ijk}^a)_{a\in M} \in R_{ijk}^{\alpha_{i+j+k}}$, where $M = \{0, 1, 2, ..., \alpha_{i+j+k} - 1\}$ for $(i, j, k) \in I'$ is defined as

$$d_L(\mathbf{r_{ijk}}, \hat{\mathbf{r}}_{\mathbf{ijk}}) = w_H(\psi_{ijk}(\mathbf{r_{ijk}} - \hat{\mathbf{r}}_{\mathbf{ijk}}))$$

It is easily seen that the Gray map ψ_{ijk} is an R_{000}-linear and distance preserving map from $R_{ijk}^{\alpha_{i+j+k}}$(Lee distance) to $R_{000}^{\alpha_{i+j+k}2^{i+j+k}}$(Hamming Distance), where $(i, j, k) \in I'$.

Let $C_{\alpha_{i+j+k}}$ be a linear code of length α_{i+j+k} over R_{ijk} for $(i, j, k) \in I'$. We define $C_{\alpha_{i+j+k},olm} = \{\mathbf{b}_{\alpha_{i+j+k},olm} = (b^a_{\alpha_{i+j+k},olm})_{a\in M} \in R_{000}^{\alpha_{i+j+k}} | \sum_{(y,s,t)\in T} \eta_{yst}\mathbf{b}_{\alpha_{i+j+k},yst} \in C_{\alpha_{i+j+k}}$ for some $\mathbf{b}_{\alpha_{i+j+k},yst} \neq \mathbf{b}_{\alpha_{i+j+k},olm}\}$ where $(o, l, m) \in T$ for $(i, j, k) \in I'$. Then $C_{\alpha_{i+j+k},olm}$ are linear codes of length α_{i+j+k} over R_{000}, where $(o, l, m) \in T$, for $(i, j, k) \in I'$ and $C_{\alpha_{i+j+k}}$ can be uniquely written as ;

$$C_{\alpha_{i+j+k}} = \oplus_{(o,l,m)\in T} \eta_{olm} C_{\alpha_{i+j+k},olm}$$

for $(i, j, k) \in I'$. Then $|C_{\alpha_{i+j+k}}| = \Pi_{(o,l,m)\in T} |C_{\alpha_{i+j+k},olm}|$, for $(i, j, k) \in I'$.

Since ψ_{ijk} is distance preserving map and $\psi_{ijk}(C_{\alpha_{i+j+k}}) = \otimes_{(o,l,m)\in T} C_{\alpha_{i+j+k},olm}$, for $(i, j, k) \in I'$, we get

$$d_L(C_{\alpha_{i+j+k}}) = min\{d_H(C_{\alpha_{i+j+k},olm})|(o, l, m) \in T\}$$

Example 1. If C is a linear code of length α_2 over R_{110}, then $C = \eta_{000}C_{\alpha_2,000} + \eta_{010}C_{\alpha_2,010} + \eta_{100}C_{\alpha_2,100} + \eta_{110}C_{\alpha_2,110}$ where

$C_{\alpha_2,000} = \{\mathbf{b}_{\alpha_2,000} \in R_{000}^{\alpha_2} | \eta_{000}\mathbf{b}_{\alpha_2,000} + \eta_{010}\mathbf{b}_{\alpha_2,010} + \eta_{100}\mathbf{b}_{\alpha_2,100} + \eta_{110}\mathbf{b}_{\alpha_2,110} \in C$ for some $\mathbf{b}_{\alpha_2,000} \neq \mathbf{b}_{\alpha_2,yst}\}$,

$C_{\alpha_2,010} = \{\mathbf{b}_{\alpha_2,010} \in R_{000}^{\alpha_2} | \eta_{000}\mathbf{b}_{\alpha_2,000} + \eta_{010}\mathbf{b}_{\alpha_2,010} + \eta_{100}\mathbf{b}_{\alpha_2,100} + \eta_{110}\mathbf{b}_{\alpha_2,110} \in C$ for some $\mathbf{b}_{\alpha_2,010} \neq \mathbf{b}_{\alpha_2,yst}\}$,

$C_{\alpha_2,100} = \{\mathbf{b}_{\alpha_2,100} \in R_{000}^{\alpha_2} | \eta_{000}\mathbf{b}_{\alpha_2,000} + \eta_{010}\mathbf{b}_{\alpha_2,010} + \eta_{100}\mathbf{b}_{\alpha_2,100} + \eta_{110}\mathbf{b}_{\alpha_2,110} \in C$ for some $\mathbf{b}_{\alpha_2,100} \neq \mathbf{b}_{\alpha_2,yst}\}$,

$C_{\alpha_2,110} = \{\mathbf{b}_{\alpha_2,110} \in R_{000}^{\alpha_2} | \eta_{000}\mathbf{b}_{\alpha_2,000} + \eta_{010}\mathbf{b}_{\alpha_2,010} + \eta_{100}\mathbf{b}_{\alpha_2,100} + \eta_{110}\mathbf{b}_{\alpha_2,110} \in C$ for some $\mathbf{b}_{\alpha_2,110} \neq \mathbf{b}_{\alpha_2,yst}\}$,

Theorem 2. Let $C_{\alpha_{i+j+k}} = \oplus_{(o,l,m)\in T}\eta_{olm}C_{\alpha_{i+j+k},olm}$ be a linear code of length α_{i+j+k} over R_{ijk}, for $(i,j,k) \in I'$. Then $C_{\alpha_{i+j+k}}$ is a cyclic code of length α_{i+j+k} if and only if $C_{\alpha_{i+j+k},olm}$ are cyclic codes of length α_{i+j+k} over R_{000}, where $(o,l,m) \in T$ for $(i,j,k) \in I'$.

Proof. Let $(b^a_{\alpha_{i+j+k},olm})_{a\in M} \in C_{\alpha_{i+j+k},olm}$, where $M = \{0, 1, 2, \ldots, \alpha_{i+j+k} - 1\}$ and $(o,l,m) \in T$ for $(i,j,k) \in I'$. Then $\mathbf{c} = (c_a)_{a\in M} \in C_{\alpha_{i+j+k}}$ where $M = \{0, 1, 2, \ldots, \alpha_{i+j+k} - 1\}$ and $c_d = \sum_{(o,l,m)\in T}\eta_{olm}b^d_{\alpha_{i+j+k},olm}$ where $d \in M$ for $(i,j,k) \in I'$. Suppose $C_{\alpha_{i+j+k}}$ is a cyclic code of length α_{i+j+k} over R_{ijk} for $(i,j,k) \in I'$, the $\sigma(\mathbf{c}) \in C_{\alpha_{i+j+k}}$, where $\sigma(\mathbf{c}) = \sum_{(o,l,m)\in T}\eta_{olm}\sigma(b^a_{\alpha_{i+j+k},olm})_{a\in M}$. Therefore $\sigma(b^a_{\alpha_{i+j+k},olm})_{a\in M} \in C_{\alpha_{i+j+k},olm}$, where $(o,l,m) \in T$ for $(i,j,k) \in I'$. Therefore $C_{\alpha_{i+j+k},olm}$ are cyclic codes over R_{000}, where $(o,l,m) \in T$ for $(i,j,k) \in I'$.

Conversely, let $\mathbf{s} = (s_a)_{a\in M} \in C_{\alpha_{i+j+k}}$, where $M = \{0, 1, 2, \ldots, \alpha_{i+j+k}-1\}$ such that $s_t = \sum_{(o,l,m)\in T}\eta_{olm}b^t_{\alpha_{i+j+k},olm}$, where $t \in M$. Then $(b^t_{\alpha_{i+j+k},olm})_{t\in M} \in C_{\alpha_{i+j+k},olm}$, where $(o,l,m) \in T$ for $(i,j,k) \in I'$. Suppose that $C_{\alpha_{i+j+k},olm}$ are cyclic codes of length α_{i+j+k} over R_{000}, where $(o,l,m) \in T$ for $(i,j,k) \in I'$. Then $\sigma(b^t_{\alpha_{i+j+k},olm})_{t\in M} \in C_{\alpha_{i+j+k},olm}$, where $(o,l,m) \in T$ for $(i,j,k) \in I'$. Since $\sum_{(o,l,m)\in T}\eta_{olm}\sigma(r^t_{\alpha_{i+j+k},olm})_{t\in M} = \sigma(\mathbf{s}) \in C_{\alpha_{i+j+k}}$, we get $C_{\alpha_{i+j+k}}$ is cyclic code. □

Corollary 3. Let $C_{\alpha_{i+j+k}} = \oplus_{(o,l,m)\in T}\eta_{olm}C_{\alpha_{i+j+k},olm}$ be a linear code of length α_{i+j+k} over R_{ijk}, for $(i,j,k) \in I'$. Then its dual $C^{\perp}_{\alpha_{i+j+k}} = \oplus_{(o,l,m)\in T}\eta_{olm}C^{\perp}_{\alpha_{i+j+k},olm}$ is also cyclic code of length α_{i+j+k} over R_{ijk} if and only if $C^{\perp}_{\alpha_{i+j+k},olm}$ are cyclic codes of length α_{i+j+k} over R_{000}, where $(o,l,m) \in T$ for $(i,j,k) \in I'$.

Theorem 4. Let $C_{\alpha_{i+j+k}} = \oplus_{(o,l,m)\in T}\eta_{olm}C_{\alpha_{i+j+k},olm}$ be a cyclic code of length α_{i+j+k} over R_{ijk}, for $(i,j,k) \in I'$, and $r_{\alpha_{i+j+k},olm}(x)$ be the generator monic polynomial of the cyclic code $C_{\alpha_{i+j+k},olm}$, where $(o,l,m) \in T$ for $(i,j,k) \in I'$. Then $C_{\alpha_{i+j+k}} = \{\sum_{(o,l,m)\in T}\eta_{olm}r_{\alpha_{i+j+k},olm}(x)s_{\alpha_{i+j+k},olm}(x) | s_{\alpha_{i+j+k},olm}(x) \in R_{ijk}[x]/< x^{\alpha_{i+j+k}} - 1 >\}$ for $(i,j,k) \in I'$. Moreover,

$$C_{\alpha_{i+j+k}} =< r_{\alpha_{i+j+k}}(x) >$$

where $r_{\alpha_{i+j+k}}(x) = \sum_{(o,l,m)\in T}\eta_{olm}r_{\alpha_{i+j+k},olm}(x)$, where $(o,l,m) \in T$ for $(i,j,k) \in I'$ such that $r_{\alpha_{i+j+k}}(x) | x^{\alpha_{i+j+k}} - 1$.

Proof. If $C_{\alpha_{i+j+k}}$ is a cyclic code of length α_{i+j+k} over R_{ijk}, then $C_{\alpha_{i+j+k},olm}$ is cyclic code of length α_{i+j+k} over R_{000}, where $(o,l,m) \in T$ for $(i,j,k) \in I'$. So $C_{\alpha_{i+j+k},olm} =< r_{\alpha_{i+j+k},olm}(x) > \subseteq R_{000}[x]/< x^{\alpha_{i+j+k}} - 1 >$, where $(o,l,m) \in T$ for $(i,j,k) \in I'$. Since $C_{\alpha_{i+j+k}} = \oplus_{(o,l,m)\in T}\eta_{olm}C_{\alpha_{i+j+k},olm}$, then $C_{\alpha_{i+j+k}} = \{r_{\alpha_{i+j+k}}(x) | r_{\alpha_{i+j+k}}(x) = \sum_{(o,l,m)\in T}\eta_{olm}r_{\alpha_{i+j+k},olm}(x)$ where $r_{\alpha_{i+j+k},olm}(x) \in R_{000}[x]/< x^{\alpha_{i+j+k}} - 1 >$. So $C_{\alpha_{i+j+k}} \subseteq \{\sum_{(o,l,m)\in T}\eta_{olm}r_{\alpha_{i+j+k},olm}(x)s_{\alpha_{i+j+k},olm}(x) | s_{\alpha_{i+j+k},olm}(x) \in R_{ijk}[x]/< x^{\alpha_{i+j+k}} - 1 >\}$,where $(o,l,m) \in T$ for $(i,j,k) \in I'$. The other part $\{\sum_{(o,l,m)}\eta_{olm}\, r_{\alpha_{i+j+k},olm}(x)s_{\alpha_{i+j+k},olm}(x) | s_{\alpha_{i+j+k},olm}(x) \in R_{ijk}[x]/< x^{\alpha_{i+j+k}} - 1 >\} \subseteq C_{\alpha_{i+j+k}}$ is seen easily. So

$C_{\alpha_{i+j+k}} = \{\sum_{(o,l,m)\in T}\eta_{olm}\, r_{\alpha_{i+j+k},olm}(x)s_{\alpha_{i+j+k},olm}(x) | s_{\alpha_{i+j+k},olm}(x) \in R_{ijk}[x]/< x^{\alpha_{i+j+k}} - 1 >\}$.

Let $r_{\alpha_{i+j+k},olm}(x)$ be the generator monic polynomial of the cyclic code $C_{\alpha_{i+j+k},olm}$ where $(o,l,m) \in T$ for $(i,j,k) \in I'$. We know that $C_{\alpha_{i+j+k}} = \{\sum_{(o,l,m)\in T}\eta_{olm}r_{\alpha_{i+j+k},olm}(x)s_{\alpha_{i+j+k},olm}(x) | s_{\alpha_{i+j+k},olm}(x) \in R_{ijk}[x]/<$

$x^{\alpha_{i+j+k}} - 1 >\}$ for $(i, j, k) \in I^{'}$. Let $C^{'} =< r_{\alpha_{i+j+k}}(x) >$ where $r_{\alpha_{i+j+k}}(x) = \sum_{(o,l,m)\in T} \eta_{olm} r_{\alpha_{i+j+k},olm}(x)$. Then $r_{\alpha_{i+j+k}}(x) \in C_{\alpha_{i+j+k}}$. Therefore $C^{'} \subseteq C_{\alpha_{i+j+k}}$. By multiplying with η_{abc}, we get $\eta_{abc}(\sum_{(o,l,m)\in T} \eta_{olm}\, r_{\alpha_{i+j+k},olm}(x) = \eta_{abc} r_{\alpha_{i+j+k},abc}(x)$, where $(a, b, c) \in T$ for $(i, j, k) \in I^{'}$. So $C_{\alpha_{i+j+k}} \subseteq C^{'}$. Therefore $C^{'} = C_{\alpha_{i+j+k}} =< r_{\alpha_{i+j+k}}(x) >$, where $r_{\alpha_{i+j+k}}(x) = \sum_{(o,l,m)\in T} \eta_{olm} r_{\alpha_{i+j+k},olm}(x)$, where $(o, l, m) \in T$ for $(i, j, k) \in I^{'}$. Since $r_{\alpha_{i+j+k},olm}(x)$ is the generator monic polynomial of the cyclic code $C_{\alpha_{i+j+k},olm}$ where $(o, l, m) \in T$ for $(i, j, k) \in I^{'}$, so there exists $f_{\alpha_{i+j+k},olm}(x) \in R_{000}[x]/ < x^{\alpha_{i+j+k}} - 1 >$ such that $x^{\alpha_{i+j+k}} - 1 = r_{\alpha_{i+j+k},olm}(x) f_{\alpha_{i+j+k},olm}(x)$, where $(o, l, m) \in T$ for $(i, j, k) \in I^{'}$. Thus $(\sum_{(o,l,m)\in T} \eta_{olm})(x^{\alpha_{i+j+k}} - 1) = \sum_{(o,l,m)\in T} \eta_{olm} r_{\alpha_{i+j+k},olm}(x) \sum_{(o,l,m)\in T} \eta_{olm} f_{\alpha_{i+j+k},olm}(x) = r_{\alpha_{i+j+k}}(x) f(x)$. So $r_{\alpha_{i+j+k}}(x) | x^{\alpha_{i+j+k}} - 1$. □

Corollary 5. Let $C_{\alpha_{i+j+k}} = \oplus_{(o,l,m)\in T} \eta_{olm} C_{\alpha_{i+j+k},olm}$ be a linear code of length α_{i+j+k} over R_{ijk}, for $(i, j, k) \in I^{'}$. Suppose $r_{\alpha_{i+j+k},olm}(x)$ are the generator monic polynomial of the cyclic code $C_{\alpha_{i+j+k},olm}$ and $s^{*}_{\alpha_{i+j+k},olm}(x)$ are the reciprocal polynomial of $s_{\alpha_{i+j+k},olm}(x)$ such that $x^{\alpha_{i+j+k}} - 1 = r_{\alpha_{i+j+k},olm}(x) s_{\alpha_{i+j+k},olm}(x)$, where $(o, l, m) \in T$ for $(i, j, k) \in I^{'}$. Then $C^{\perp}_{\alpha_{i+j+k}} =< d_{\alpha_{i+j+k}}(x) >$, where $d_{\alpha_{i+j+k}}(x) = \oplus_{(o,l,m)\in T} \eta_{olm} s^{*}_{\alpha_{i+j+k},olm}(x)$, where $(o, l, m) \in T$ for $(i, j, k) \in I^{'}$.

3 Ω-Linear Codes

The set

$$\Omega = R_{000}R_{100}R_{110}R_{111} = \{(r_{ijk})_{(i,j,k)\in I} | r_{ijk} \in R_{ijk}\}$$

forms an R_{111} module under the componentwise addition and the following multiplication. For any elements $r = \sum_{i=0}^{1} \sum_{j=0}^{1} \sum_{k=0}^{1} u^i v^j w^k a_{ijk} \in R_{111}$ and $(r_{ijk})_{(i,j,k)\in I} \in \Omega$, the multiplication is defined as

$$\begin{aligned} . \quad &: \quad \Omega \longrightarrow \Omega \\ (r, (r_{ijk})_{(i,j,k)\in I}) \quad &\mapsto \quad (s_{ijk})_{(i,j,k)\in I} \end{aligned}$$

where $s_{ijk} = r.r_{ijk}$ for $(i, j, k) = (1, 1, 1)$ and $s_{ijk} = \pi_{ijk}(r) r_{ijk}$ where the maps

$$\begin{aligned} \pi_{ijk} \quad &: \quad R_{111} \longrightarrow R_{ijk} \\ r = \sum_{i=0}^{1} \sum_{j=0}^{1} \sum_{k=0}^{1} u^i v^j w^k a_{ijk} \quad &\mapsto \quad p_{ijk} \end{aligned}$$

are projection maps for $(i, j, k) \in I^{''} = \{(0, 0, 0), (1, 0, 0), (1, 1, 0)\}$. They are also ring homomorphisms. For the finite ring R_{000}, then $p_{ijk} = a_{000}$, for the finite ring R_{100}, then $p_{ijk} = \sum_{i=0}^{1} u^i a_{i00}$, for the finite ring R_{110}, then $p_{ijk} = \sum_{i=0}^{1} \sum_{j=0}^{1} u^i v^j a_{ij0}$.

This multiplication can be extended componentwise on $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3} = R_{000}^{\alpha_0} \times R_{100}^{\alpha_1} \times R_{110}^{\alpha_2} \times R_{111}^{\alpha_3}$ as follows for any $r \in R_{111}$ and $((r^a_{ijk})_{a\in M})_{(i,j,k)\in I} \in \Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$,

$$\begin{aligned} . \quad &: \quad R_{111} \times \Omega_{\alpha_0\alpha_1\alpha_2\alpha_3} \longrightarrow \Omega_{\alpha_0\alpha_1\alpha_2\alpha_3} \\ (r, ((r^a_{ijk})_{a\in M})_{(i,j,k)\in I}) \quad &\mapsto \quad (h_{ijk})_{(i,j,k)\in I} = (h_{000}, h_{100}, h_{110}, h_{111}) \end{aligned}$$

where $h_{ijk} = r(r^a_{ijk})_{a\in M}$ for $(i, j, k) = (1, 1, 1)$ and $h_{ijk} = \pi_{ijk}(r)(r^a_{ijk})_{a\in M}$ and $M = \{0, 1, 2, ..., \alpha_{i+j+k} - 1\}$ for $(i, j, k) \in I^{''}$. The element $(r^a_{ijk})_{a\in M})_{(i,j,k)\in I}$ denotes the element $(r^0_{000}, ..., r^{\alpha_0-1}_{000}, r^0_{100}, ..., r^{\alpha_1-1}_{100}, r^0_{110}, ..., r^{\alpha_2-1}_{110}, r^0_{111}, ..., r^{\alpha_3-1}_{111})$. So $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$ is an R_{111}-module.

Definition 6. A non empty subset $\mathbf{C}$ of $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$ is called Ω-linear code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$, if $\mathbf{C}$ is an R_{111}- submodule of $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$, where $I = \{(0, 0, 0), (1, 0, 0)\ (1, 1, 0), (1, 1, 1)\}$.

An inner product between $\mathbf{r} = ((r^a_{ijk})_{a\in M})_{(i,j,k)\in I} = (\mathbf{r}_{ijk})_{(i,j,k)\in I}$ and $\hat{\mathbf{r}} = ((\hat{r}^a_{ijk})_{a\in M})_{(i,j,k)\in I} = (\hat{\mathbf{r}}_{ijk})_{(i,j,k)\in I}$ is defined as

$$\mathbf{r}.\hat{\mathbf{r}} = \sum_{(i,j,k)\in I}(\sum_{s=0}^{\alpha_{i+j+k}-1} r^s_{ijk}\hat{r}^s_{ijk}) = \sum_{(i,j,k)\in I}\mathbf{r}_{ijk}\hat{\mathbf{r}}_{ijk}$$

where $M = \{0, 1, 2, ..., \alpha_{i+j+k} - 1\}$ If $\mathbf{C}$ is an Ω-linear code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$, then the dual code of $\mathbf{C}$ is defined as

$$\mathbf{C}^{\perp} = \{\mathbf{c}^{'} \in \Omega_{\alpha_0\alpha_1\alpha_2\alpha_3} | \mathbf{c}.\mathbf{c}^{'} = 0, \forall \mathbf{c} \in \mathbf{C}\}$$

Definition 7. An Ω-linear code $\mathbf{C}$ of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$ is said to be an Ω-cyclic code if its cyclic shift $\sigma(\mathbf{c}) = (\sigma(r^a_{ijk})_{a\in M})_{(i,j,k)\in I} = (r^{\alpha_0-1}_{000}, r^0_{000}, ..., r^{\alpha_0-2}_{000}, r^{\alpha_1-1}_{100}, r^0_{100}, ..., r^{\alpha_1-2}_{100}, r^{\alpha_2-1}_{110}, r^0_{110}, ..., r^{\alpha_2-2}_{110}, r^{\alpha_3-1}_{111}, r^0_{111}, ..., r^{\alpha_3-2}_{111}) \in \mathbf{C}$, for any $\mathbf{c} = ((r^a_{ijk})_{a\in M})_{(i,j,k)\in I} \in \mathbf{C}$,where $M = \{0, 1, 2, ..., \alpha_{i+j+k} - 1\}$.

For the polynomial representation:

Let $r_{ijk}(x) = \sum_{t=0}^{\alpha_{i+j+k}-1} r^t_{ijk}x^t$ where $(i, j, k) \in I$. Then any element $\mathbf{c} = ((r^a_{ijk})_{a\in M})_{(i,j,k)\in I} = (r^0_{000}, ..., r^{\alpha_0-1}_{000}, r^0_{100}, ..., r^{\alpha_1-1}_{100}, r^0_{110}, ..., r^{\alpha_2-1}_{110}, r^0_{111}, ..., r^{\alpha_3-1}_{111}) \in \Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$, where $M = \{0, 1, 2, ..., \alpha_{i+j+k} - 1\}$ can be identified with

$$c(x) = (r_{ijk}(x))_{(i,j,k)\in I}$$

where $r_{ijk}(x) = r^0_{ijk} + r^1_{ijk}x + ... + r^{\alpha_{i+j+k}-1}_{ijk}x^{\alpha_{i+j+k}-1}$ for $(i, j, k) \in I$ Let $\Delta = \Pi_{(i,j,k)\in I}(R_{ijk}[x]/< x^{\alpha_{i+j+k}} - 1 >)$. There is a one to one correspondence between $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$ and Δ. The set Δ is an $R_{111}[x]$-module under the following multiplication. For any $r(x) = r_0 + r_1x + ...r_ex^e \in R_{111}[x]$ and $c(x) \in \Delta$

$$r(x)c(x) = (y_{ijk}(x))_{(i,j,k)\in I}$$

where $y_{ijk} = r(x)r_{ijk}(x)$ for $(i, j, k) = (1, 1, 1)$ and $y_{ijk} = \pi_{ijk}(r(x))r_{ijk}(x)$ where $\pi_{ijk}(r(x)) = \pi_{ijk}(r_0) + \pi_{ijk}(r_1)x + ... + \pi_{ijk}(r_e)x^e \in R_{ijk}[x]$ for $(i, j, k) \in I^{''}$.

Theorem 8. A code $\mathbf{C}$ is called Ω -cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$, if and only if $\mathbf{C}$ is an $R_{111}[x]$-submodule of Δ

Proof. Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$ for $(i, j, k) \in I$. Since every element $\mathbf{c} = ((r^a_{ijk})_{a\in M})_{(i,j,k)\in I} \in \mathbf{C}$ corresponds to the $c(x) = (r_{ijk}(x))_{(i,j,k)\in I}$, the polynomial $x.c(x)$ corresponds to the elements $\sigma(\mathbf{c})$. As $\mathbf{C}$ is a Ω-cyclic code, we have $\sigma(\mathbf{c}) \in \mathbf{C}$. By using the fact that $\mathbf{C}$ is a linear so the polynomial $f(x).c(x)$ corresponds to element $\hat{\mathbf{c}} = ((\hat{r}^a_{ijk})_{a\in M})_{(i,j,k)\in I} \in \mathbf{C}$, for every $f(x) \in R_{111}[x]$. So $\mathbf{C}$ is an $R_{111}[x]$-submodule of Δ. The other part is seen from definition. □

Theorem 9. Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then its dual $\mathbf{C}^{\perp}$ is also an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$.

Proof. For every $\mathbf{d} = ((d^a_{ijk})_{a\in M})_{(i,j,k)\in I} \in \mathbf{C}^{\perp}$, we will show that $\sigma(\mathbf{d}) \in \mathbf{C}^{\perp}$. Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Let $\mathbf{c} = ((c^a_{ijk})_{a\in M})_{(i,j,k)\in I} \in \mathbf{C}$, where $M = \{0, 1, ..., \alpha_{i+j+k}\}$ for $(i, j, k) \in I$. Take $lcm(\alpha_0, \alpha_1, \alpha_2, \alpha_3) = s$. As $\mathbf{C}$ is cyclic code, we have $\sigma^{s-1}(\mathbf{c}) \in \mathbf{C}$. So $\sigma^{s-1}(\mathbf{c})\mathbf{d} = 0$. Since $\sigma^{s-1}(\mathbf{c})\mathbf{d} = \mathbf{c}\sigma(\mathbf{d})$, we get $\mathbf{c}\sigma(\mathbf{d}) = 0$. Therefore $\mathbf{C}^{\perp}$ is cyclic code. □

4 The Gray map over Ω

For any element $(r_{ijk})_{(i,j,k)\in I}$, the Gray map defined also as follows

$$\begin{array}{ccc} \Psi & : & \Omega \longrightarrow R_{000}^{15} \\ (r_{ijk})_{(i,j,k)\in I} & \longmapsto & (r_{000}, (\psi_{ijk}(r_{ijk}))_{(i,j,k)\in I'}) \end{array}$$

This can be extended on $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$. It goes from $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$ to $R_{000}^{\sum_{(i,j,k)\in I}\alpha_{i+j+k}2^{i+j+k}}$. The Lee weight of any element $\mathbf{r} = ((r_{ijk}^a)_{a\in M})_{(i,j,k)\in I}$ is defined as

$$w_L(\mathbf{r}) = w_H((r_{000}^a)_{a\in M}) + \sum_{(i,j,k)\in I'}(\sum_{t=0}^{\alpha_{i+j+k}-1} w_L(r_{ijk}^t))$$

where w_H denotes the Hamming weight over R_{000}. The Lee distance between $\mathbf{r}$ and $\hat{\mathbf{r}} \in \Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$ is defined as $d_L(\mathbf{r}, \hat{\mathbf{r}}) = w_L(\mathbf{r} - \hat{\mathbf{r}}) = w_H(\Psi(\mathbf{r} - \hat{\mathbf{r}}))$.

Proposition 10. Ψ is an R_{000}- linear map which preserves distance from $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$ (Lee distance) to $R_{000}^{\sum_{(i,j,k)\in I}\alpha_{i+j+k}2^{i+j+k}}$ (Hamming distance). Moreover if $\mathbf{C}$ is Ω-linear code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$ with d_L, then $\Psi(\mathbf{C})$ is a linear code of length $\sum_{(i,j,k)\in I}\alpha_{i+j+k}2^{i+j+k}$ over R_{000} with d_H, where $d_L = d_H$.

Theorem 11. Let $\mathbf{C}$ be a Ω-linear code. Then $\Psi(\mathbf{C}^\perp) = \Psi(\mathbf{C})^\perp$. Moreover if $\mathbf{C}$ is self dual, then $\Psi(\mathbf{C})$ is olso self dual.

Proof. It is proven as proof of Proposition 33 in [2]. □

Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$, we define

$C_{\alpha_0} = \{(r_{000}^a)_{a\in M} \in R_{000}^{\alpha_0} | ((r_{000}^a)_{a\in M}, ((\sum_{(y,s,t)\in T}\eta_{yst}b^a_{\alpha_{i+j+k},yst})_{a\in M})_{(i,j,k)\in I'}) \in \mathbf{C}$ for some $(b^a_{\alpha_{i+j+k},yst})_{a\in M} \in R_{000}^{\alpha_{i+j+k}}\}$

$C_{\alpha_{i+j+k},olm} = \{(b^a_{olm})_{a\in M} \in R_{000}^{\alpha_{i+j+k}} | ((r_{000}^a)_{a\in M}, ((\sum_{(y,s,t)\in T}\eta_{yst}b^a_{yst})_{a\in M})_{(i,j,k)\in I'}) \in \mathbf{C},$ for some $(r_{000}^a)_{a\in M} \in R_{000}^{\alpha_0}$, $(b^a_{\alpha_{i+j+k},yst})_{a\in M} \in R_{000}^{\alpha_{i+j+k}}$, $(b^a_{\alpha_{i+j+k},yst})_{a\in M} \neq (b^a_{\alpha_{i+j+k},olm})_{a\in M}\}$
where $(o, l, m) \in T$ and $M = \{0, 1, ..., \alpha^{i+j+k} - 1\}$, for $(i, j, k) \in I'$.

Theorem 12. Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then

$$\Psi(\mathbf{C}) = C_{\alpha_0} \otimes_{(o,l,m)\in T} C_{\alpha_{i+j+k},olm}$$

for $(i, j, k) \in I'$. Moreover $|\Psi(\mathbf{C})| = |C_{\alpha_0}|\Pi_{(o,l,m)\in T,(i,j,k)\in I'}|C_{\alpha_{i+j+k},olm}|$.

Proof. It is follows from the definition of $\Psi(\mathbf{C})$ and $\otimes$. □

Theorem 13. Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then C_{α_0} and all $C_{\alpha_{i+j+k},olm}$ are cyclic codes over R_{000} with length α_{i+j+k}, where $(o, l, m) \in T$ for $(i, j, k) \in I'$.

Definition 14. Define

$$\kappa \quad : \quad F_q^{mn} \longrightarrow F_q^{mn}$$

by $\kappa(\mathbf{d_1}, ..., \mathbf{d_n}) = (\sigma(\mathbf{d_1}), ..., \sigma(\mathbf{d_n}))$, where $\mathbf{d} = (\mathbf{d_1}, ..., \mathbf{d_n}) \in F_q^{mn}$ and σ is the cyclic shift from F_q^m and F_q^m. Then a code C is called a quasi cyclic code of index n, if $\kappa(C) = C$.

Define

$$\kappa_g \quad : \quad F_q^{m_1} \times .. \times F_q^{m_n} \longrightarrow F_q^{m_1} \times .. \times F_q^{m_n}$$

by $\kappa_g(\hat{\mathbf{d_1}}, ..., \hat{\mathbf{d_n}}) = (\sigma(\hat{\mathbf{d_1}}), ..., \sigma(\hat{\mathbf{d_n}}))$, where $\hat{\mathbf{d}} = (\hat{\mathbf{d_1}}, ..., \hat{\mathbf{d_n}}) \in F_q^{m_1} \times .. \times F_q^{m_n}$ and σ is the cyclic shift from $F_q^{m_i}$ and $F_q^{m_i}$, for $i = 1, .., n$. Then a code C is called a generalized quasi cyclic code of index n, if $\kappa_g(C) = C$.

Proposition 15. If κ_g and Ψ are as above and σ is a cyclic shift over $\Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$, then we have $\Psi\sigma = \kappa_g\Psi$.

Proof. For every $\mathbf{c} = ((r^a_{ijk})_{a\in M})_{(i,j,k)\in I} \in \Omega_{\alpha_0\alpha_1\alpha_2\alpha_3}$, where $M = \{0, 1, \ldots, \alpha_{i+j+k} - 1\}$, it is easily seen that $\Psi(\sigma(\mathbf{c})) = \kappa_g(\Psi(\mathbf{c}))$. So $\Psi\sigma = \kappa_g\Psi$. □

Theorem 16. Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then the Gray image of Ω-cyclic code is a generalized quasi-cyclic code of index 15 over R_{000}. If $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3$, then the Gray image of Ω-cyclic code is a quasi-cyclic code of index 15 over R_{000}.

Proof. Let $\mathbf{C}$ be an Ω-cyclic code. So $\sigma(\mathbf{C}) = \mathbf{C}$. By applying Ψ, we have $\Psi(\sigma(\mathbf{C}) = \Psi(\mathbf{C})$. By using Proposition 15, we get So $\Psi\sigma(\mathbf{C}) = \kappa_g\Psi(\mathbf{C}) = \Psi(\mathbf{C})$. Therefore $\Psi(\mathbf{C})$ is a genaralized quasi-cyclic code. □

5 The Structures of Ω-Cyclic codes

Proposition 17. Let $\mathbf{C}$ be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then $\xi_{ijk}(\mathbf{C}) = C_{\alpha_{i+j+k}}$ is a cyclic code of length α_{i+j+k} over R_{ijk}, where

$$\begin{array}{rcl} \xi_{ijk} & : & \Delta \longrightarrow R_{ijk}[x]/ < x^{\alpha_{i+j+k}} - 1 > \\ c(x) = (r_{ijk}(x))_{(i,j,k)\in I} & \longmapsto & (r_{ijk})(x) \end{array}$$

for $(i, j, k) \in I$.

Theorem 18. Let C be an Ω-cyclic code of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then

$$\mathbf{C} =< (r_{\alpha_0}(x)|0|0|0), (0|r_{\alpha_1}(x)|0|0), (0|0|r_{\alpha_2}(x)|0), (f_0(x)|f_1(x)|f_2(x)|r_{\alpha_3}(x)) >$$

where $r_{\alpha_{i+j+k}}(x)|x^{\alpha_{i+j+k}} - 1$ for $(i, j, k) \in I$ and $f_{i+j+k}(x) \in R_{ijk}[x]/ < x^{\alpha_{i+j+k}} - 1 >$ where $(i, j, k) \in I''$.

Proof. From Proposition 17, we have $\xi_{ijk}(\mathbf{C}) = C_{\alpha_{i+j+k}}$ for $(i, j, k) \in I$. So $C_{\alpha_{i+j+k}} =< r_{\alpha_{i+j+k}}(x) >$ such that $r_{\alpha_{i+j+k}}(x)|x^{\alpha_{i+j+k}} - 1$ for $(i, j, k) \in I$. Therefore the proof follows from Theorem 3.1. of [6]. □

Definition 19. Let $\mathbf{C}$ be an Ω-cyclic codes of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$ and $C_{\alpha_{i+j+k}}$ be the canonical projection of $\mathbf{c}$ on the α_{i+j+k} coordinates. The code $\mathbf{C}$ is separable if $\mathbf{C}$ is the direct product of $C_{\alpha_{i+j+k}}$,where $(i, j, k) \in I$. i.e., $\mathbf{C} = \otimes_{(i,j,k)\in I} C_{\alpha_{i+j+k}}$.

Theorem 20. Let $C_{\alpha_{i+j+k}}$ be cyclic codes of length α_{i+j+k}, where $(i, j, k) \in I$, respectively. If $\mathbf{C}$ is separable, then

$$\mathbf{C} =< (r_{\alpha_0}(x)|0|0|0), (0|r_{\alpha_1}(x)|0|0), (0|0|r_{\alpha_2}(x)|0), (0|0|0|r_{\alpha_3}(x)) >$$

where $C_{\alpha_{i+j+k}} =< r_{\alpha_{i+j+k}}(x) >$ where $r_{\alpha_{i+j+k}}(x)|x^{\alpha_{i+j+k}} - 1$.

Theorem 21. Let $\mathbf{C} = \otimes_{(i,j,k)\in I} C_{\alpha_{i+j+k}}$ be an Ω-cyclic codes of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then $\mathbf{C}$ is separable Ω-cyclic codes if and only only if $C_{\alpha_{i+j+k}}$ are cyclic codes over R_{ijk} with length α_{i+j+k}, for $(i, j, k) \in I$, respectively.

6 Quantum Codes

Theorem 22. (CSS Construction) [1] Let $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ be linear codes over GF(q) with $C_2 \subseteq C_1$. Then there exists a quantum error-correcting code $C = [[n, k_1 - k_2, min\{d_1, d_2^{\perp}\}]]_q$, where $d_2^{\perp}$ denotes the minimum Hamming distance of the dual code $C_2^{\perp}$ of C_2. Further, if $C_1^{\perp} = C_2$, then there exists a quantum error-correcting code $C = [[n, 2k_1 - n, d_1]]$.

Lemma 23. [1] A cyclic code C over a finite field with generator polynomial $g(x)$ contains its dual code if and only if

$$x^n - 1 \equiv 0(mod \quad g(x)g^*(x))$$

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

Theorem 24. Let $C_{\alpha_{i+j+k}} =< \sum_{(o,l,m)\in T} \eta_{olm} r_{\alpha_{i+j+k},olm}(x) >$ be a cyclic code of length α_{i+j+k} over R_{ijk}. Then $C^{\perp}_{\alpha_{i+j+k}} \subset C_{\alpha_{i+j+k}}$ if and only if $x^{\alpha_{i+j+k}} - 1 \equiv 0(mod \quad r_{\alpha_{i+j+k},olm}(x) r^*_{\alpha_{i+j+k},olm}(x)$ where $(o, l, m) \in T$ for all $(i, j, k) \in I$.

Theorem 25. Let $\mathbf{C} = \otimes_{(i,j,k)\in I} C_{\alpha_{i+j+k}}$ be a separable Ω-cyclic codes of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. Then $C^{\perp}_{\alpha_{i+j+k}} \subset C_{\alpha_{i+j+k}}$, for all $(i, j, k) \in I$ if and only if $\mathbf{C}^{\perp} \subset \mathbf{C}$.

Theorem 26. Let $\mathbf{C} = \otimes_{(i,j,k)\in I} C_{\alpha_{i+j+k}}$ be a separable Ω-cyclic codes of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$, where $C_{\alpha_0} =< r_{\alpha_0}(x) >$ and $C_{\alpha_{i+j+k}} =< \sum_{(o,l,m)\in T} \eta_{plm} r_{\alpha_{i+j+k},olm}(x) >$ for all $(i, j, k) \in I'$. Then $\mathbf{C}^{\perp} \subset \mathbf{C}$ if and only if $x^{\alpha_0} - 1 \equiv 0(mod \quad r_{\alpha_0(x)} r_{\alpha_0^*}(x))$ and $x^{\alpha_{i+j+k}} - 1 \equiv 0(mod \quad r_{\alpha_{i+j+k},olm}(x) r^*_{\alpha_{i+j+k},olm}(x))$, where $(o, l, m) \in T$ for all $(i, j, k) \in I'$.

Theorem 27. Let $\mathbf{C} = \otimes_{(i,j,k)\in I} C_{\alpha_{i+j+k}}$ be a separable Ω-cyclic codes of block length $(\alpha_{i+j+k})_{(i,j,k)\in I}$. If $C^{\perp}_{\alpha_0} \subset C_{\alpha_0}$ and $C^{\perp}_{\alpha_{i+j+k},olm} \subset C_{\alpha_{i+j+k},olm}$, where $(o, l, m) \in T$ for all $(i, j, k) \in I'$, then there exists a QECC with parameters $[[\sum_{(i,j,k)\in I} \alpha_{i+j+k} 2^{i+j+k}, 2\mathbf{k} - \sum_{(i,j,k)\in I} \alpha_{i+j+k} 2^{i+j+k}, d_H]]_q$, where d_H denotes Hamming distance, $\mathbf{k}$ denotes dimension of the code $\Psi(\mathbf{C})$.

Proof. Let $C^{\perp}_{\alpha_0} \subset C_{\alpha_0}$, $C^{\perp}_{\alpha_{i+j+k},olm} \subset C_{\alpha_{i+j+k},olm}$, where $(o, l, m) \in T$ for all $(i, j, k) \in I'$. By using the Theorem 25, we have $\mathbf{C}^{\perp} \subset \mathbf{C}$. By using the fact that $\Psi(\mathbf{C}^{\perp}) = \Psi(\mathbf{C})^{\perp}$, it can be easily seen that $\Psi(\mathbf{C})^{\perp} \subset \Psi(\mathbf{C})$. So we can say that there exists a QECC with parameters $[[\sum_{(i,j,k)\in I} \alpha_{i+j+k} 2^{i+j+k}, 2\mathbf{k} - \sum_{(i,j,k)\in I} \alpha_{i+j+k} 2^{i+j+k}, d_H]]_q$, from Theorem 22. □

7 Conclusion

The structures of the Ω-cyclic codes are obtained. Their generator polynomials are constructed. A inner product is defined. It was shown that if $\mathbf{C}$ is an Ω-cyclic code, then $\mathbf{C}^{\perp}$ is an Ω-cyclic code. The necessary and sufficient conditions of the Ω-cyclic codes to be separable are determined. It is shown that quantum error correcting codes can be constructed from them.

References

[1] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory 44 (1998), no. 4, 1369–1387.

[2] H. Q. Dinh, S. Pathak, T. Bag, A. K. Upadhyay and W. Chinnakum, A study of F_qR-cyclic codes and their applications in constructing quantum codes, 2020.

[3] H. Q. Dinh, T. Bag, A. K. Upadhyay, R. Bandi and W. Chinnakum, On the structure of cyclic codes over F_qRS and applications in quantum and LCD constructions, IEEE Access (2020).

[4] Y. Gao, J. Gao and F. W. Fu, Quantum codes from cyclic codes over the ring $F_q + v_1F_q + \cdots + v_rF_q$, Appl. Algebra Engrg. Comm. Comput. 30 (2019), 161–174.

[5] J. Qian, Quantum codes from cyclic codes over $F_2 + vF_2$, J. Inform. Comput. Sci. 10 (2013), no. 6, 1715–1722.

[6] T. Wu, J. Gao, Y. Gao and F. W. Fu, $Z_2Z_4Z_8$ additive cyclic codes, Adv. Math. Commun. 12 (2018), no. 4, 641–657.