International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 5, No. 2, 12-22

Constacyclic Codes Over $\mathbb{F}_q[u]/\langle u^3 = 0\rangle$ and Their Application of Constructing Quantum Codes

Zineb Hebbache

School of Built and Ground Works Engineering NSBGWE (ENSTP)
Laboratory of Algebra and number theory, Faculty of Mathematics, U.S.T.H.B.
BP32, 16111 El-Alia, Algiers, Algeria.
z.hebbache@enstp.edu.dz

Abstract. Let $R = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q, u^3 = 0$ be a finite chain ring. In this paper, we give the structure of constacyclic codes over R and obtain self-orthogonal codes over $\mathbb{F}_q$ by using the Gray map from R^n to $\mathbb{F}_q^{3n}$. As an application, we present a construction of quantum codes from the codes obtained from this class.

Keywords: Constacyclic Codes · Gray Map · Euclidean Selforthogonal · Quantum Codes.

1 Introduction

Classical computers work by manipulating bits that exist in one of two states, namely, 0 or 1. Quantum computers are not just limited to these two states, they are encoded with quantum data in the two conditions of 0 and 1 as quantum bits, or qubits, which can exist in superposition. That means, the qubits are both 0 and 1 and all points in between, which are processed at the same time, giving quantum computers the ability of performing many calculations at once. Qubits represent atoms, ions, photons or electrons and their respective control devices that are working together to act as computer memory and a processor. Since quantum computers can contain these multiple states simultaneously, they have the potential to be millions of times more powerful than the most powerful classical supercomputers. Quantum computers will make use of qubits to encode quantum data and figure complex scientific issues utilizing the resources unique to quantum computers, such as direct access to superposition and entanglement. Using quantum computing, one can harness the magnificent powers superposition and entanglement to tackle complicated issues that classical computer systems cannot practically do. The two properties of superposition and entanglement together will empower qubits to process huge amounts of information at the same time and take care of complex issues. While traditional classical computer systems would need to arrange and figure out each conceivable arrangement, which may take a huge amount of time on a massive scale problem, quantum computers can locate every single imaginable variation simultaneously utilizing superposition and entanglement and move through a lot of information in an altogether limited quantity of time. As a quantum computer has the potential to simulate things that a classical computer could not, quantum computers outrun the classical computers in their ability to solve complex problems, and the application of error-correcting codes in quantum computers can be labelled as one of the pivotal reasons for this efficiency. Consequently, it has become evident that quantum error-correcting codes can protect quantum information investigations, and researches concerning quantum error-correcting codes have seen a tremendous headway. During the last few years, research on error-correcting codes has increased in both the public and private sectors. For instance, in October 2019, Google AI, in partnership with the U.S. National Aeronautics and Space Administration (NASA), claimed to be able to perform a quantum computation that is infeasible on any classical computer.

Quantum error-correcting codes (QECCs) are based on the classical information theory and quantum mechanics. They play an important role in quantum computation and quantum secret communications, such as quantum signature schemes [15], quantum identities authentication schemes [4] and quantum key distribution protocol [14]. Recently, it has become a hot topic of constructing quantum error-correcting codes ([7], [10]) and quantum error-avoiding codes [13]. The first quantum code was discovered by Shor [11]. Later, a construction method called CSS construction of quantum codes from classical error-correcting codes was given by Claderbank *et al.* [3]. Afterwards, many good quantum codes have been constructed from classical error-correcting codes.

The error-correcting codes over finite rings have richer algebraic structures than those over finite fields. Therefore, the quantum coding theory over the finite rings has received a lot of attention, recently. Many coding scholars have constructed new quantum codes with Euclidean and Hermitian orthogonality from cyclic and constacyclic codes over finite rings such as ([5],[8],[6],[12]). Recently, the structural properties of cyclic, constacyclic over the ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$ have been studied. Ashraf *et al.* [2] constructed quantum codes over $\mathbb{F}_5$ from cyclic codes over $\mathbb{F}_5+u\mathbb{F}_5+v\mathbb{F}_5+uv\mathbb{F}_5$. Zheng *et al.* [18] studied some properties of Euclidean dual codes of constacyclic codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$. Ma *et al.* [9] constructed some non-binary quantum codes from constacyclic codes over $\mathbb{F}_p[u,v]/\langle u^2-1, v^2-v, uv-vu\rangle$. But many of these studies are on the non-chain rings. Motivated by that, in this paper, we study constacyclic codes over the finite chain ring R and their application of quantum codes. The paper is organized in the following way. The second section presents some basic definitions and theorems used in this study. In Sec. 3, we present the structure of linear codes over R. In Sec. 4, we study algebraic structure of constacyclic codes over R. Finally, as an application, we construct quantum codes via these codes having Euclidean dual containing property.

2 Preliminaries

Let $R=\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$, where p is a prime, $q=p^m$ and $u^3=0$. The ring R is isomorphic to the ring $R=\mathbb{Z}_q[u]/\langle u^3\rangle$ and $R=\{a+ub+u^2c \mid a,b,c\in\mathbb{F}_q\}$. It can easily be seen that the ideal $\langle u\rangle$ is the unique maximal ideal of R, and hence R is a finite chain ring. To know more about the ring R, we refer to Yao *et al.* [16].

We know that every element of R can be expressed as $a+ub+u^2c$, where $a,b,c\in\mathbb{F}_q$. Then we can extend the Gray map and the Lee weight given by Yao *et al.* [16] as follows.

$$\Phi\colon R^n \to \mathbb{F}_q^{3n}$$

$$\Phi(a+ub+u^2c)=(a+b,a+c,a+b+c), \tag{1}$$

where $a,b,c\in\mathbb{F}_q^n$. The Lee weight is defined as the Hamming weight of the Gray image

$$w_L(a+ub+u^2c)=w_H(a+b,a+c,a+b+c), \text{ for } a,b,c\in\mathbb{F}_q^n.$$

The Lee weight of $r=(x_1,x_2,\ldots,x_n)\in R^n$ is defined as the rational sum of the Lee weight of its components, i.e. $w_L(r)=\sum\limits_{i=1}^{n} w_L(x_i)$. It is easy to verify that Φ is a linear map and it is also a distance preserving map from R^n(Lee distance) to $\mathbb{F}_q^{3n}$ (Hamming distance), and $\Phi(C)$ is a linear code over $\mathbb{F}_q$ for C is a linear code over R.

A code of length n over R is a nonempty subset of R^n. A linear code C over R of length n is an R-submodule of R^n. In this paper, all codes are assumed to be linear, unless otherwise stated.

In this paper, we always assume that α is a unit of R. A linear code C of length n over R is said to be constacyclic, or specifically, α-constacyclic if C is closed under the α-constacyclic shift:

$$\rho_\alpha : R^n \to R^n$$

defined by

$$\rho_\alpha(a_0, a_1, \dots, a_{n-1}) = (\alpha a_{n-1}, a_0, \dots, a_{n-2}).$$

In particular, if $\alpha = 1$, (respectively $\alpha = -1$) then C is called a cyclic code (respectively a negacyclic code). Each codeword c $= (c_0, c_1, \dots, c_{n-1}) \in C$ is usually identified with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. In this way, $\alpha-$constacyclic code of length n over R can be viewed as an ideal of the quotient ring $R[x]/\langle x^n - \alpha\rangle$.

Let $x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in R^n$. The Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$\mathbf{x}.\mathbf{y} = x_0y_0 + x_1y_1, \dots, x_{n-1}y_{n-1}.$$

The Euclidean dual $C^\perp$ of C is defined as

$$C^\perp = \{\mathbf{x} \in R^n \mid \mathbf{x}.\mathbf{y} = 0, \text{ for all } \mathbf{y} \in C\}$$

A code C is called Euclidean dual-containing if $C^\perp \subseteq C$ and Euclidean self-orthogonal if $C \subseteq C^\perp$.

3 Linear codes over *R*

Let $R = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, where p is a prime, $q = p^m$ and $u^3 = 0$. The ring R is isomorphic to the ring $R = \mathbb{Z}_q[u]/\langle u^3\rangle$ and $R = \{a + ub + u^2c : a, b, c \in \mathbb{F}_q\}$. It can easily be seen that the ideal $\langle u\rangle$ is the unique maximal ideal of R, and hence R is a finite chain ring. To know more about the ring R, we refer to Yao *et al.* [16].

$$\begin{aligned} C_1 &= \{a + b \in \mathbb{F}_q^n \mid a + ub + u^2c \in C \text{ for some } c \in \mathbb{F}_q^n\} \\ C_2 &= \{a + c \in \mathbb{F}_q^n \mid a + ub + u^2c \in C \text{ for some } b, \in \mathbb{F}_q^n\} \\ C_3 &= \{a + b + c \in \mathbb{F}_q^n \mid a + ub + u^2c \in C\}. \end{aligned} \tag{2}$$

Then C_1, C_2 and C_3 are linear codes of length n over $\mathbb{F}_q$ and C can be uniquely expressed as $C = (1 - u^2)C_1 \oplus (1 - u)C_2 \oplus (u^2 + u - 1)C_3$.

Theorem 1. *If C is a linear code of length n over R, then $\Phi(C) = C_1 \otimes C_2 \otimes C_3$ and $|C| = |C_1||C_2||C_3|$.*

Proof. Since $C = (1 - u^2)C_1 \oplus (1 - u)C_2 \oplus (u^2 + u - 1)C_3$, where C_1, C_2, C_3 are as defined above, we have $|C| = |C_1||C_2||C_3|$. Let $x \in \Phi(C)$. Then there exists $(1 - u^2)C_1 \oplus (1 - u)C_2 \oplus (u^2 + u - 1)C_3 \in C$ such that $x = \Phi((1 - u^2)C_1 \oplus (1 - u)C_2 \oplus (u^2 + u - 1)C_3) = (a, b, c)$. Hence $x \in C_1 \otimes C_2 \otimes C_3$, and so $\Phi(C) \subseteq C_1 \otimes C_2 \otimes C_3$.

Conversely, let $(a, b, c) \in C_1 \otimes C_2 \otimes C_3$ then let $x = (1-u^2)C_1 \oplus (1-u)C_2 \oplus (u^2+u-1)C_3$. Note that $\Phi(x) = (a, b, c)$, which implies $(a, b, c) = \Phi(x) \in \Phi(C)$. Hence, $C_1 \otimes C_2 \otimes C_3 \subseteq \Phi(C)$, and $C_1 \otimes C_2 \otimes C_3 = \Phi(C)$. Also, $|\Phi(C)| = |C_1 \otimes C_2 \otimes C_3| = |C_1||C_2||C_3|$.

For the second part, since Φ is a linear map, so $\Phi(C)$ is also a linear code. $\Phi(C)$ is obviously a code of length $3n$.

Corollary 1. *If $\Phi(C) = C_1 \otimes C_2 \otimes C_3$, then $C = (1-u^2)C_1 \oplus (1-u)C_2 \oplus (u^2+u-1)C_3$. It is easy to see that,*

$$|C| = |C_1||C_2||C_3| = q^{3n-(\deg(g_1(x))+\deg(g_2(x))+\deg(g_3(x)))},$$

where $g_1(x), g_2(x), g_3(x)$ are generators of C_1, C_2 and C_3, respectively.

Corollary 2. *If G_1, G_2, G_3 are generator matrices of C_1, C_2 and C_3, respectively then C has the generator matrix*

$$\begin{bmatrix} (1-u^2)G_1 \\ (1-u)G_2 \\ (u^2+u-1)G_3 \end{bmatrix}$$

and $d_L(C) = \min\{d_H(C_1), d_H(C_2), d_H(C_2)\}$.

Proof. If G_1, G_1, G_1 are generator matrices of C_1, C_2, C_3, respectively, then $\Phi(C) = C_1 \otimes C_2 \otimes C_3$ has the generator matrix

$$\begin{bmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{bmatrix}.$$

Therefore, by Theorem 1, C has the generator matrix

$$\begin{bmatrix} (1-u^2)G_1 \\ (1-u)G_2 \\ (u^2+u-1)G_3 \end{bmatrix}.$$

Further, Φ being distance preserving, $d_L(C) = d_H(\Phi(C)) = d_H(C_1 \otimes C_2 \otimes C_3) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}$.

Corollary 3. *Suppose $C = (1-u^2)C_1 \oplus (1-u)C_2 \oplus (u^2+u-1)C_3$ is a linear code of length n over R where C_j is a $[n, k_j, d_H(C_j)]$ linear code over $\mathbb{F}_q$ for $j = 1, 2, 3$, then $\Phi(C)$ is a $[3n, k_1+k_2+k_3, \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}]$ linear code over $\mathbb{F}_q$.*

Proof. Follows from Theorem 1 and Corollary 2.

Proposition 1. *Let C be a code of length n over R. If C is self-orthogonal, so is $\Phi(C)$.*

Proof. Let $s = (s_0, s_2, \ldots, s_{n-1}) \in C$ and $r = (r_0, r_2, \ldots, r_{n-1}) \in C^{\perp}$, where $s_i = a_i + ub_i + u^2 c_i, r_i = e_i + uf_i + u^2 g_i \in R$, for $i = 0, 2, \ldots, n-1$. Now by Euclidean inner product of s and r, we have

$$s.r = \sum_{i=0}^{n-1} (a_i + ub_i + u^2 c_i)(e_i + uf_i + u^2 g_i),$$

that is, $ae + u(af + be + bf) + u^2(ce + ag + cg)$, since C is a self-orthogonal code, $C \subseteq C^{\perp}$ we find that $ae = 0, af + be + bf = 0$ and $ce + ag + cg = 0$.

On the other hand

$$\Phi(s) = (a_1 + b_1, \ldots, a_n + b_n, a_1 + c_1, \ldots, a_n + c_n, c_1 + b_1 + a_1, \ldots, c_n + b_n + a_n),$$

$$\Phi(r) = (e_1 + f_1, \ldots, e_n + f_n, e_1 + g_1, \ldots, e_n + g_n, g_1 + f_1 + e_1, \ldots, g_n + f_n + e_n).$$

Then $\Phi(s).\Phi(r) = ae + (a+b)(e+f) + (a+c)(e+g) = 3ae + af + be + bf + ce + ag + cg = 0$. Therefore, $\Phi(C^{\perp}) \subseteq (\Phi(C))^{\perp}$. Hence, $\Phi(C)$ is self-orthogonal.

4 Constacyclic codes over *R*

In this section we discuss some structural properties of $(\alpha_1 + u\alpha_2 + u^2\alpha_3)-$constacyclic codes over R by the decomposition method.

Lemma 1. *An element $\alpha = \alpha_1 + u\alpha_2 + u^2\alpha_3 \in R$ where $\alpha_j \in \mathbb{F}_q$ for $j = 1, 2, 3$ is unit in R if and only if $\alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \alpha_1 + \alpha_2 + \alpha_3 \in \mathbb{F}_q$ are units in $\mathbb{F}_q$.*

Proof. Let $\alpha = \alpha_1 + u\alpha_2 + u^2\alpha_3 \in R$ be a unit in R. Then there exists an element $\beta = \beta_1 + u\beta_2 + u^2\beta_3 \in R$ such that $\alpha\beta = 1$. Therefore, $\alpha_1\beta_1 = 1, \alpha_1\beta_2 + \alpha_2\beta_1 = 0, \alpha_2\beta_2 + \alpha_3\beta_1 = 0$, which implies that $\alpha_1 + \alpha_2 \neq 0, \alpha_1 + \alpha_3 \neq 0, \alpha_1 + \alpha_2 + \alpha_3 \neq 0$. Conversely, let $\alpha_1 + \alpha_2 \neq 0, \alpha_1 + \alpha_3 \neq 0, \alpha_1 + \alpha_2 + \alpha_3 \neq 0$. Let $\alpha^{-1} = (1 - u^2)(\alpha_1 + \alpha_2)^{-1} + (1 - u)(\alpha_1 + \alpha_3)^{-1} + (u^2 + u - 1)(\alpha_1 + \alpha_2 + \alpha_3)^{-1}$. Then $\alpha\alpha^{-1} = 1$. Hence $\alpha = \alpha_1 + u\alpha_2 + u^2\alpha_3 \in R$ is a unit.

We now discuss the direct sum decomposition of a $(\alpha_1 + u\alpha_2 + u^2\alpha_3)-$constacyclic code over R using the relation between units of R and $\mathbb{F}_q$.

Theorem 2. *A linear code $C = (1 - u^2)C_1 \oplus (1 - u)C_2 \oplus (u^2 + u - 1)C_3$ is a $(\alpha_1 + u\alpha_2 + u^2\alpha_3)-$constacyclic code of length n over R if and only if C_1, C_2, C_3 are $(\alpha_1 + \alpha_2)-$constacyclic code, $(\alpha_1 + \alpha_3)-$constacyclic code and $(\alpha_1 + \alpha_2 + \alpha_3)-$constacyclic code of length n over $\mathbb{F}_q$, respectively.*

Proof. Let $s = (s_0, s_1, \ldots, s_{n-1}) \in C$ where $s_i = (1 - u^2)a_i + (1 - u)b_i + (u^2 + u - 1)c_i$ for $i = 0, 1, \ldots, n-1$. Consider $a = (a_0, a_1, \ldots, a_{n-1}), b = (b_0, b_1, \ldots, b_{n-1}), c = (c_0, c_1, \ldots, c_{n-1})$. Then $a \in C_1, b \in C_2, c \in C_3$. Suppose C_1, C_2 and C_3 are $(\alpha_1 + \alpha_2)-$constacyclic code, $(\alpha_1 + \alpha_3)-$constacyclic code and $(\alpha_1 + \alpha_2 + \alpha_3)-$constacyclic code of length n over $\mathbb{F}_q$ for $j = 1, 2, 3$. Then $\rho_{\alpha_1 + \alpha_2}(a) \in C_1, \rho_{\alpha_1 + \alpha_3}(b) \in C_2$ and $\rho_{\alpha_1 + \alpha_2 + \alpha_3}(a) \in C_3$. Now,

$$\rho_{\alpha_1+u\alpha_2+u^2\alpha_3}(s) = (1-u^2)\rho_{\alpha_1+\alpha_2}(a) + (1-u)\rho_{\alpha_1+\alpha_3}(b)$$
$$+(u^2+u-1)\rho_{\alpha_1+\alpha_2+\alpha_3}(c) \in (1-u^2)C_1 + (1-u)C_2 + (u^2+u-1)C_3 = C.$$

Therefore, C is a $(\alpha_1+u\alpha_2+u^2\alpha_3)-$constacyclic code of length n over R. Conversely, let C be a $(\alpha_1+u\alpha_2+u^2\alpha_3)-$constacyclic code of length n over R. Let $a=(a_0,a_1,\ldots,a_{n-1}) \in C_1, b=(b_0,b_1,\ldots,b_{n-1}) \in C_2, c=(c_0,c_1,\ldots,c_{n-1}) \in C_3$. Take $s_i=(1-u^2)a_i+(1-u)b_i+(u^2+u-1)c_i$ for $i=0,1,\ldots,n-1$. Then $s=(s_0,s_1,\ldots,s_{n-1}) \in C$. Since C is a $(\alpha_1+u\alpha_2+u^2\alpha_3)-$constacyclic code over R, so $\rho_{\alpha_1+u\alpha_2+u^2\alpha_3}(s) \in C$, where $\rho_{\alpha_1+u\alpha_2+u^2\alpha_3}(s) = (1-u^2)\rho_{\alpha_1+\alpha_2}(a)+(1-u)\rho_{\alpha_1+\alpha_3}(b)+(u^2+u-1)\rho_{\alpha_1+\alpha_2+\alpha_3}(c)$. It follows that $\rho_{\alpha_1+\alpha_2}(a) \in C_1, \rho_{\alpha_1+\alpha_3}(b) \in C_2$ and $\rho_{\alpha_1+\alpha_2+\alpha_3}(a) \in C_3$. Consequently, C_1, C_2 and C_3 are $(\alpha_1+\alpha_2)-$constacyclic code, $(\alpha_1+\alpha_3)-$constacyclic code and $(\alpha_1+\alpha_2+\alpha_3)-$constacyclic code of length n over $\mathbb{F}_q$, respectively.

Theorem 3. *Let $C=(1-u^2)C_1+(1-u)C_2+(u^2+u-1)C_3$ be a $(\alpha_1+u\alpha_2+u^2\alpha_3)-$constacyclic code of length n over R. Then there exists a polynomial $g(x) \in R[x]$ with $g(x)|(x^n-(\alpha_1+u\alpha_2+u^2\alpha_3))$ such that $C=\langle g(x)\rangle$, where*

$$g(x) = (1-u^2)g_1(x) + (1-u)g_2(x) + (u^2+u-1)g_3(x)$$

and $g_1(x), g_2(x)$ and $g_3(x)$ are the generator polynomials of $(\alpha_1+\alpha_2)-$constacyclic code C_1, $(\alpha_1+\alpha_3)-$constacyclic code C_2 and $(\alpha_1+\alpha_2+\alpha_3)-$constacyclic code C_3, respectively.

Proof. Since C_1, C_2 and C_3 are $(\alpha_1+\alpha_2)-$constacyclic, $(\alpha_1+\alpha_3)-$constacyclic and $(\alpha_1+\alpha_2+\alpha_3)-$constacyclic codes of length n over $\mathbb{F}_q$ respectively, then we can assume that the generator polynomials of C_1, C_2 and C_3 are $g_1(x), g_2(x)$ and $g_3(x)$, respectively. Therefore,

$$(1-u^2)g_1(x) \in (1-u^2)C_1 \subseteq C,$$
$$(1-u)g_2(x) \in (1-u)C_2 \subseteq C \text{ and}$$
$$(u^2+u-1)g_3(x) \in (u^2+u-1)C_3 \subseteq C,$$

Thus, $(1-u^2)g_1(x)+(1-u)g_2(x)+(u^2+u-1)g_3(x) \in C$. On the other hand, let $f(x) \in C$. Since, $C=(1-u^2)C_1+(1-u)C_2+(u^2+u-1)C_3$, then there exists $s(x)g_1(x) \in C_1, u(x)g_2(x) \in C_2$ and $t(x)g_3(x) \in C_3$ such that $f(x)=(1-u^2)s(x)g_1(x)+(1-u)u(x)g_2(x)+(u^2+u-1)t(x)g_3(x)$, where $s(x), u(x), t(x) \in \mathbb{F}_q[x]$. Therefore, $f(x) \in \langle(1-u^2)g_1(x)+(1-u)g_2(x)+(u^2+u-1)g_3(x)\rangle$. Thus, $C \subseteq \langle(1-u^2)g_1(x)+(1-u)g_2(x)+(u^2+u-1)g_3(x)\rangle$, which implies that $C=\langle(1-u^2)g_1(x)+(1-u)g_2(x)+(u^2+u-1)g_3(x)\rangle$. According to the theory of constacyclic codes over finite field, we know that $g_1(x)|(x^n-(\alpha_1+\alpha_2)), g_2(x)|(x^n-(\alpha_1+\alpha_3))$ and $g_3(x)|(x^n-(\alpha_1+\alpha_2+\alpha_3))$. Therefore, for $j=1,2,3$, there exist polynomials $h_j(x) \in \mathbb{F}_q[x]$ such that

$$x^n-(\alpha_1+\alpha_2) = h_1(x)g_1(x)$$
$$x^n-(\alpha_1+\alpha_3) = h_2(x)g_2(x)$$
$$x^n-(\alpha_1+\alpha_2+\alpha_3) = h_3(x)g_3(x),$$

which implies that $x^n-(\alpha_1+u\alpha_2+u^2\alpha_3) = (1-u^2)h_1(x)g_1(x)+(1-u)h_2(x)g_2(x)+(u^2+u-1)h_3(x)g_3(x) = [(1-u^2)h_1(x)+(1-u)h_2(x)+(u^2+u-1)h_3(x)]g(x)$ Therefore, $g(x)$ is a divisor of $x^n-(\alpha_1+u\alpha_2+u^2\alpha_3)$.

According to the above Theorem, it is easy to get the following corollary and omit the proof process here.

Corollary 4. *Let $C=(1-u^2)C_1\oplus(1-u)C_2(u^2+u-1)C_3$ be a $(\alpha_1+u\alpha_2+u^2\alpha_3)-$constacyclic code of length n over R and $g_1(x),g_2(x)$ and $g_3(x)$ be the generator polynomials of C_1,C_2 and C_3, respectively. Then*

$$|C|=q^{3n-(\deg(g_1(x))+\deg(g_2(x))+\deg(g_3(x)))}$$

Let $h_1(x)=\frac{x^n-(\alpha_1+\alpha_2)}{g_1(x)},h_2(x)=\frac{x^n-(\alpha_1+\alpha_3)}{g_2(x)}$ and $h_3(x)=\frac{x^n-(\alpha_1+\alpha_2+\alpha_3)}{g_3(x)}$. Let $h^*(x)=x^{\deg(h(x))}h(x^{-1})$ be the reciprocal polynomial of $h(x)$. We have the following result with regard to Euclidean inner.

Theorem 4. *Let $C=(1-u^2)C_1\oplus(1-u)C_2(u^2+u-1)C_3$ be a $(\alpha_1+u\alpha_2+u^2\alpha_3)-$constacyclic code of length n over R. Then dual $C^\perp=(1-u^2)C_1^\perp\oplus(1-u)C_2^\perp+(u^2+u-1)C_3^\perp$ is a $(\alpha_1+u\alpha_2+u^2\alpha_3)^{-1}-$constacyclic code over R, where C_1,C_2 and C_3 are $(\alpha_1+\alpha_2)^{-1}-$constacyclic, $(\alpha_1+\alpha_3)^{-1}-$constacyclic and $(\alpha_1+\alpha_2+\alpha_3)^{-1}-$constacyclic codes of length n over $\mathbb{F}_q$ respectively. Moreover,*

$$C^\perp=\langle(1-u^2)h_1^*(x)+(1-u)h_2^*(x)+(u^2+u-1)h_3^*(x)\rangle,$$

where, $h_j^*(x)$ is reciprocal polynomials of $h_j(x)$ for $j=1,2,3$.

Proof. From Proposition 6 of [1] we have $C^\perp$ is $(\alpha_1+u\alpha_2+u^2\alpha_3)^{-1}-$constacyclic code over R. Now, $\alpha_1+u\alpha_2+u^2\alpha_3=(1-u^2)(\alpha_1+\alpha_2)+(1-u)(\alpha_1+\alpha_3)+(u^2+u-1)(\alpha_1+\alpha_2+\alpha_3)$, it follow that, $(\alpha_1+u\alpha_2+u^2\alpha_3)^{-1}=(1-u^2)(\alpha_1+\alpha_2)^{-1}+(1-u)(\alpha_1+\alpha_3)^{-1}+(u^2+u-1)(\alpha_1+\alpha_2+\alpha_3)^{-1}$, Then , by Theorem 2, we have C_1,C_2 and C_3 are $(\alpha_1+\alpha_2)^{-1}-$constacyclic, $(\alpha_1+\alpha_3)^{-1}-$constacyclic and $(\alpha_1+\alpha_2+\alpha_3)^{-1}-$constacyclic codes of length n over $\mathbb{F}_q$ respectively.

5 Quantum from constacyclic codes over R

Quantum error-correction has an important role in quantum computing and quantum commutation. In stabilizer theory, quantum error-correction takes classical binary or quaternary codes as quantum error-correcting code satisfying the dual containing property. CSS codes are a special type of Stablizer codes constructed from classical codes with some conditions. This CSS construction is an important tool in quantum error-correction, named after Robert Calberbank, Peter Shor and Andrew Steane. The CSS construction gives us required tools to construct quantum error-correcting codes from linear codes.

In this section, we present the construction method quantum codes from $\alpha_1+u\alpha_2+u^2\alpha_3-$constacyclic codes over R bases on the following CSS construction.

Lemma 2. *[3] Let C be an $[n,k,d]$ linear code over $\mathbb{F}_q$. If $C^\perp\subseteq C$, then an $[[n,2k-n,\geq d]]_q$ quantum code can be obtained.*

Lemma 3. *[3] Let C be a $\kappa-$constacyclic code with generator polynomial $g(x)$ over $\mathbb{F}_q$. Then C contains its dual code if and only if*

$$x^n - \kappa \equiv 0(\mod g(x)g^*(x)),$$

where $g^*(x)$ is the reciprocal polynomial of $g(x)$ and $\kappa = \{-1, 1\}$.

According to the above results, we give a necessary and sufficient condition for the existence of Euclidean dual-containing constacyclic codes C of length n over R.

Theorem 5. *Let $C = \langle (1-u^2)g_1(x) + (1-u)g_2(x) + (u^2+u-1)g_3(x)\rangle$ be a $(\alpha_1 + u\alpha_2 + u^2\alpha_3)-$constacyclic code of length n over R, where $\lambda_j \in \{-1, 1\}$. Then $C^{\perp} \subseteq C$ if and only if*

$$x^n - \lambda_j = 0(\mod g_j(x)g_j^*(x)),$$

where $g_j^*(x)$ are the reciprocal polynomials of $g_j(x)$ respectively for $j = 1, 2, 3$.

Proof. Let $C = (1-u^2)C_1 + (1-u)C_2 + (u^2+u-1)C_3 = \langle (1-u^2)g_1(x) + (1-u)g_2(x) + (u^2+u-1)g_3(x)\rangle$ be a $(\alpha_1 + u\alpha_2 + u^2\alpha_3)-$constacyclic code of length n over R, where $C_1 = \langle g_1(x)\rangle, C_2 = \langle g_2(x)\rangle$ and $C_3 = \langle g_3(x)\rangle$. If

$$x^n - \alpha_j \equiv 0(\mod g_j(x)g_j^*(x)),$$

then $C_j^{\perp} \subseteq C_j$ for $j = 1, 2, 3$, which imply that $(1-u^2)C_1^{\perp} \subseteq (1-u^2)C_1, (1-u)C_2^{\perp} \subseteq (1-u)C_2$ and $(u^2+u-1)C_3^{\perp} \subseteq (u^2+u-1)C_3$ for $j = 1, 2, 3$. This implies $(1-u^2)C_1^{\perp} + (1-u)C_2^{\perp} + (u^2+u-1)C_3^{\perp} \subseteq (1-u^2)C_1 + (1-u)C_2 + (u^2+u-1)C_3$. Therefore, $C^{\perp} \subseteq C$.

Conversely, assume that $C^{\perp} \subseteq C$, then $(1-u^2)C_1^{\perp} + (1-u)C_2^{\perp} + (u^2+u-1)C_3^{\perp} \subseteq (1-u^2)C_1 + (1-u)C_2 + (u^2+u-1)C_3$. Therefore,

$$\langle (1-u^2)h_1^*(x) + (1-u)h_2^*(x) + (u^2+u-1)h_3^*(x)\rangle \subseteq \langle (1-u^2)g_1(x) + (1-u)g_2(x) + (u^2+u-1)g_3(x)\rangle.$$

By thinking $\mod (1-u^2)$, $\mod (1-u)$ and $\mod (u^2+u-1)$, respectively we find $C_j^{\perp} \subseteq C_j$ for $j = 1, 2, 3$. Therefore, $x^n - \lambda_j \equiv 0(\mod g_j(x)g_j^*(x)), j = 1, 2, 3$.

Using Lemmas 2, 3 and Theorem 5, we can construct quantum codes as follows:

Theorem 6. *Let $C = (1-u^2)C_1 + (1-u)C_2 + (u^2+u-1)C_3$ be a $(\alpha_1 + u\alpha_2 + u^2\alpha_3)-$constacyclic code of length n over R. If $C^{\perp} \subseteq C$, then there exists a quantum error-correcting code with parameters $[[4n, 2k-3n \geq d_L]]_q$, where d_L is the minimum Lee weight of the code C and k is the dimension of the code $\Phi(C)$.*

6 Conclusion

In this paper, we have given the structure of constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, with $u^3 = 0$. To obtain quantum codes from constacyclic codes over this ring. We have established a method to obtain self-orthogonal codes over $\mathbb{F}_q$ as the Gray images of constacyclic codes over the ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$.

For further work, it would be interesting to construct quantum codes from constacyclic codes over the chain ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^k\mathbb{F}_q$ with $u^k = 0$ and obtain the good codes.

Acknowledgements

The authors are greatly indebted to the editor and reviewers for their remarks and advice which allowed us to improve the paper considerably.

References

1. S. Alabiad and Y. Alkhamees, Constacyclic codes over finite chain rings of characteristic p, Axioms , 10(2021).
2. M. Ashraf and G. Mohammad, Quantum codes over $\mathbb{F}_p$ from cyclic codes over $\mathbb{F}_p[u, v]/\langle u^2 - 1, v^2 - 1$, Cryptogr. Commun. , 11(2019), pp. 325–335.
3. A-R. Calderbank, E-M. Rains, P-M. Shor and N-J-A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory, 44(1998), pp. 1369–1387.
4. Z. Chen, K. Zhou and Q. Liao, Quantum identity authentication scheme of vehicular ad-hoc networks, Int. J. Theor. Phys. , 58(2019), pp. 40–57.
5. J. Gao, Quantum codes from cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, Int. J. Quantum Inf. , 8(2015), pp. 1550063(1-8).
6. 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., 17, 122 (2018).
7. Y. Gao, J. Gao and F-W. Fu, On Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$. Appl. Algebra Eng. Commun. Comput., 2(2019), pp. 161–174.
8. M. Guzeltepe and M. Sari, Quantum codes from codes over the ring $\mathbb{F}_q + \alpha\mathbb{F}_q$, Quantum Inf. Process., 12(2019), 365.
9. F. Ma, J. Gao and F-W. Fu, New non-binary quantum codes from constacyclic codes over $\mathbb{F}_q[u, v]/\langle u^2 - 1, v^2 - 1, uv = vu\rangle$, Adv. Math. Commun. 2(2019), pp. 421–434.
10. J. Mi, X. Cao, S. Xu and G. Luo, Quantum codes from Hermitian dual-containing cyclic codes, Int. J. Comput. Math., 3(2016).
11. P. Shor, Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A 4(1995), 2493–2496.
12. M. Özen, N. Özzaim and H. Ince, Quantum codes from cyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$, Int. Conf. Quantum Sci. Appl. J. Phys. Conf. Ser. 766(2016), pp. 012020-1–012020-6.
13. H. Xiao, Z. Zhang and A. Chronopoulos, New construction of quantum error avoiding codes via group representation of quantum stabilizer, codes. Eur. Phys. J. C 77(2017), pp. 667–680.

14. H. Xiao and Z. Zhang, Subcarrier multiplexing multiple-input multiple-output quantum key distribution with orthogonal quantum states, Quantum Inf. Process., 16(2017), pp.1–18 .
15. X. Xin, Q. He, Z. Wang, Q. Yang and F. Li, Efficient arbitrated quantum signature scheme without entangled states, Mod. Phys. Lett. A 34(2019), 1950166.
16. J. Gao , F.W. Fu, L. Xiao and R.K. Bandi, Double cyclic codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$, Discrete Math. Algorithms Appl., 7(2015), pp. 1550058.
17. W-C. Huffman and V. Pless, Fundamentals of Error Correcting Codes, The United states of America by Combridge. University Press, New york, 2003.
18. Zheng, X., Bo, K.: Cyclic codes and $\lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv-$constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$. Appl. Math. Comput. 306(2017), pp. 86-91 .