Erzincan Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
2022 15(1), 46-55
ISSN: 1307-9085, e-ISSN: 2149-4584
Araştırma Makalesi

Erzincan University
Journal of Science and Technology
2022 15(1), 46-55
DOI: 10.18185/erzifbed.911472
Research Article

Quantum Codes from $(1-2w-2uv)$-Constacyclic Codes over the $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$

Ceremnur TETIK[1*], Abdullah DERTLI[1]

[1]Department of Mathematics, Ondokuz Mayıs University, Samsun, Turkey

Geliş / Received: 07/04/2021, Kabul / Accepted: 21/12/2021

Abstract

In this paper, we give construction of quantum codes over $\mathbb{F}_q$ from $(1-2w-2uv)$ - constacyclic codes over the $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = wu = vw = wv = 0$, $q = p^m$, m is a positive integer and p is an odd prime. We determine the parameters of quantum error correcting codes which constructed from $(1-2w-2uv)$ - constacyclic codes over the $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$.

Keywords: quantum code, constacyclic code, Gray map

$\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$ Halkası Üzerindeki $(1-2w-2uv)$ –Sabit Devirli Kodlardan Elde Edilen Kuantum Kodlar

Öz

Bu çalışmada, $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = wu = vw = wv = 0$, $q = p^m$, m pozitif tam sayı ve p tek asal sayı olmak üzere $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$ halkası üzerindeki $(1-2w-2uv)$-sabit devirli kodlardan $\mathbb{F}_q$ üzerindeki kuantum kodların inşası verilmiştir. Ayrıca, $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$ halkası üzerindeki $(1-2w-2uv)$ –sabit devirli kodlardan elde edilen hata düzeltici kuantum kodların parametreleri belirlenmiştir.

Anahtar Kelimeler: kuantum kod, sabit devirli kod, Gray dönüşümü

1. Introduction

At the beginning of the twentieth century, people believed that Newton and Maxwell's laws of physics were true. By the 1930's, however, it had become apparent that these classical theories faced serious problems in trying to account for the observed results of certain experiments. As a result, a new mathematical framework for physics called quantum mechanics was formulated, and new theories of physics called quantum physics were developed in this framework (Kaye et al., 2006).

*Corresponding Author: ceremnurtetik@gmail.com

Quantum information processing is the result of using the physical reality that quantum theory tells us about for the purposes of performing tasks that were previously thought impossible or infeasible. Devices that perform quantum information processing are known as quantum computers (Kaye et al., 2006). Quantum computers have a great deal of potential, but to realize that potential, they need some sort of protection from noise. Classical computers do not use error correction. One reason for this is that classical computers use a large number of electrons, so when one goes wrong, it is not too serious. A single qubit in a quantum computer will probably be just one or a small number of particles, which already creates a need for some sort of correction. Classical information can not travel faster than light, while quantum information appears to in some circumstances. Classical information can be duplicated, while quantum information can not. Also, quantum computers use probabilities, unlike classical computers. These probabilities enable more complex structures to be resolved with faster processing power. This fast processing power is provided by performing many operations at the same time. Quantum computers need subatomic particles to perform many operations simultaneously. Quantum error correcting codes provide an efficent way to overcome decoherence. Therefore, quantum information is more convenient than classical information.

The first quantum error correcting code was found by (Shor, 1995). Calderbank et al. (1998), gave a method to construct quantum error correcting codes from classical error correcting codes. The name given to this method is CSS construction. From then on, the construction of quantum error correcting codes from different types of classical codes has studied.

Many quantum error correcting codes have been constructed by constacyclic codes over many finite rings (Li et al., 2018; Gao and Wang, 2018; Islam and Parakash, 2020).

In this paper, motivated by the previous works (Gao and Wang, 2018), (Li et al., 2018), (Islam and Prakash, 2020), (Mohan and Durairajan, 2020), we study the quantum codes which are obtained from $(1-2w-2uv)$-constacyclic codes over the finite ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+w\mathbb{F}_q+uv\mathbb{F}_q$.

2. Materials and Methods

The commutative ring $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+w\mathbb{F}_q+uv\mathbb{F}_q$ with $u^2=u, v^2=v, w^2=w, uv=vu, uw=wu=vw=wv=0$ introduced, where $\mathbb{F}_q$ is a finite field with q elements, $q=p^m$, m is a positive integer and p is an odd prime (Mohan and Durairajan, 2020). Please see (Mohan and Durairajan, 2020) for more details on this ring.

Let

$$\varepsilon_1=u-uv,$$

$$\varepsilon_2=1-u-v-w+uv,$$

$$\varepsilon_3=v-uv,$$

$$\varepsilon_4=uv,$$

$$\varepsilon_5 = w$$

are elements in R. It can be easily seen that $(\varepsilon_i)^2 = \varepsilon_i, \varepsilon_i.\varepsilon_j = 0$ and $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 = 1$, where $i, j = 1,2,3,4,5$ and $i \neq j$. They had $R = \varepsilon_1 R \oplus \varepsilon_2 R \oplus \varepsilon_3 R \oplus \varepsilon_4 R \oplus \varepsilon_5 R$. By calculation, they obtained that $\varepsilon_i R \cong \varepsilon_i \mathbb{F}_q$, $i = 1,2,3,4,5$. Therefore, for any $r \in R$, r can be expressed uniquely as $r = \sum_{i=1}^{5} \varepsilon_i a_i$, where $a_i \in \mathbb{F}_q$ for $i = 1,2,3,4,5$ (Mohan and Durairajan, 2020).

A non-empty subset C of R^n ($\mathbb{F}_q^n$) is called a linear code of length n over R ($\mathbb{F}_q$) if C is an R-submodule of R^n (a subspace of $\mathbb{F}_q^n$). An element of C is called a codeword. Let σ, γ, τ be maps from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ given by

$$\sigma(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, \dots, c_{n-2}),$$

$$\gamma(c_0, c_1, \dots, c_{n-1}) = (-c_{n-1}, c_0, \dots, c_{n-2})$$

and

$$\tau(c_0, c_1, \dots, c_{n-1}) = \big((1-2w-2uv)c_{n-1}, c_0, \dots, c_{n-2}\big),$$

respectively. Then C is called to be cyclic if $\sigma(C) = C$, negacyclic if $\gamma(C) = C$ and $(1-2w-2uv)$-constacyclic if $\tau(C) = C$.

The Hamming weight $w_H(x)$ of a codeword $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ is the number of nonzero components. The minimum weight $w_H(C)$ of a code C is the smallest weight among all its nonzero codewords. For $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_q^n$, $d_H(x,y) = |\{i : x_i \neq y_i\}|$ is called the Hamming distance between x and y. Moreover,

$$d_H(x,y) = w_H(x-y).$$

The minimum Hamming distance between different codewords of a code C is called the minimum distance of C and denoted by $d_H(C)$ or shortly d_H.

Let $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ be any two elements of $\mathbb{F}_q^n$. Then the Euclidean inner product of x and y is defined as

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

The dual code of C is defined as

$$C^{\perp} = \{x \in \mathbb{F}_q^n : x \cdot y = 0, for\ all\ y \in C\}.$$

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

Now, recall the definition of the Gray map which was defined by Mohan and Durairajan (2020) as follows:

$$\delta: R \longrightarrow \mathbb{F}_q^5$$

$$\delta(a_1\varepsilon_1 + a_2\varepsilon_2 + a_3\varepsilon_3 + a_4\varepsilon_4 + a_5\varepsilon_5) = (a_1, a_2, a_3, a_4, a_5),$$

where $a_1, a_2, a_3, a_4, a_5 \in \mathbb{F}_q$.

Equivalently, if $r = a_1' + ua_2' + va_3' + wa_4' + uva_5' \in R$, then

$$\delta(r) = (a_1' + a_2', a_1', a_1' + a_3', a_1' + a_2' + a_3' + a_5', a_1' + a_4').$$

This map can be extended naturally to the case over R^n.

For any element $r = a_1\varepsilon_1 + a_2\varepsilon_2 + a_3\varepsilon_3 + a_4\varepsilon_4 + a_5\varepsilon_5 \in R$, define the Lee weight of r as $w_L(r) = w_H(a_1, a_2, a_3, a_4, a_5)$, where w_H denotes the ordinary Hamming weight for codes over $\mathbb{F}_q$.

The Lee distance between $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in R^n$ is defined by

$$d_L(x, y) = w_L(x - y) = \sum_{i=1}^{n} w_L(x_i - y_i).$$

The minimum Lee distance between different codewords of a code C is called the minimum distance of C and denoted by $d_L(C)$ or shortly d_L.

Theorem 2.1.The Gray map δ is a distance-preserving map or isometry from R^n (Lee distance) to $\mathbb{F}_q^{5n}$ (Hamming distance) and it is also $\mathbb{F}_q$-linear (Mohan and Durairajan, 2020).

Theorem 2.2. Let C be a linear code of length n over R with $|C| = M$ and Lee distance $d_L(C) = d$. Then $\delta(C)$ is a q-ary linear code with parameter $(5n, M, d)$.

Proof. From Theorem 2.1, we see that $\delta(C)$ is $\mathbb{F}_q$-linear, which implies that $\delta(C)$ is $\mathbb{F}_q$-linear code. By definition of the Gray map δ, $\delta(C)$ is of length $5n$. Moreover one can check that δ is bijective map from R^n to $\mathbb{F}_q^{5n}$, which implies that $|C| = |\delta(C)|$. Finally, the property of preserving distance of δ leads to $\delta(C)$ having the minimum Hamming distance d.

■

3. Results and Disscussion

$(1-2w-2uv)$-Constacyclic Codes over R

Let

$$A_1 \otimes \cdots \otimes A_5 = \{(a_1, a_2, a_3, a_4, a_5) : a_i \in A_i, i = 1, 2, 3, 4, 5\}$$

and

$$A_1 \oplus \cdots \oplus A_5 = \{a_1 + a_2 + a_3 + a_4 + a_5 : a_i \in A_i, i = 1,2,3,4,5\}.$$

For a linear code C of length n over R, define

$$C_1 = \left\{ \begin{array}{c} a_1 \in \mathbb{F}_q^n : \sum_{i=1}^{n} a_i\varepsilon_i \in C, \\ for\ some\ a_2, a_3, a_4, a_5 \in \mathbb{F}_q^n \end{array} \right\}$$

$$C_2 = \left\{ \begin{array}{c} a_2 \in \mathbb{F}_q^n : \sum_{i=1}^{n} a_i\varepsilon_i \in C, \\ for\ some\ a_1, a_3, a_4, a_5 \in \mathbb{F}_q^n \end{array} \right\}$$

$$C_3 = \left\{ \begin{array}{c} a_3 \in \mathbb{F}_q^n : \sum_{i=1}^{n} a_i\varepsilon_i \in C, \\ for\ some\ a_1, a_2, a_4, a_5 \in \mathbb{F}_q^n \end{array} \right\}$$

$$C_4 = \left\{ \begin{array}{c} a_4 \in \mathbb{F}_q^n : \sum_{i=1}^{n} a_i\varepsilon_i \in C, \\ for\ some\ a_1, a_2, a_3, a_5 \in \mathbb{F}_q^n \end{array} \right\}$$

$$C_5 = \left\{ \begin{array}{c} a_5 \in \mathbb{F}_q^n : \sum_{i=1}^{n} a_i\varepsilon_i \in C, \\ for\ some\ a_1, a_2, a_3, a_4 \in \mathbb{F}_q^n \end{array} \right\}$$

Clearly, C_i is a linear code of length n over $\mathbb{F}_q$ for each $i = 1,2,3,4,5$. Moreover,

$$C = \varepsilon_1 C_1 \oplus \varepsilon_2 C_2 \oplus \varepsilon_3 C_3 \oplus \varepsilon_4 C_4 \oplus \varepsilon_5 C_5.$$

Theorem 3.1. Let C be a linear code of length n over R. Then $\delta(C) = \bigotimes_{i=1}^{5} C_i$, $|C| = \prod_{i=1}^{5} |C_i|$ and $d_L(C) = min\{d_H(C_i), i = 1,2,3,4,5\}$ (Mohan and Durairajan, 2020).

A generator matrix of C is a matrix whose rows generate C. Two codes are equivalent if one can be obtained from the other by permuting the coordinates. If G_i are the generator matrices of q-ary linear codes C_i, $i = 1,2,3,4,5$, respectively, then the generator matrix of C is

$$G = \begin{pmatrix} \varepsilon_1 G_1 \\ \varepsilon_2 G_2 \\ \varepsilon_3 G_3 \\ \varepsilon_4 G_4 \\ \varepsilon_5 G_5 \end{pmatrix}$$

and the generator matrix of $\delta(C)$ is

$$\delta(G)=\begin{pmatrix}\delta(\varepsilon_1G_1)\\ \delta(\varepsilon_2G_2)\\ \delta(\varepsilon_3G_3)\\ \delta(\varepsilon_4G_4)\\ \delta(\varepsilon_5G_5)\end{pmatrix}.$$

Theorem 3.2. Let C be a linear code of length n over R. Then $\delta(C^{\perp})=\big(\delta(C)\big)^{\perp}$ (Mohan and Durairajan, 2020).

Theorem 3.3. Let C be a linear code of length n over R. Then C is self-orthogonal, so is $\delta(C)$ (Mohan and Durairajan, 2020).

Theorem 3.4. Let $C=\varepsilon_1C_1\oplus\varepsilon_2C_2\oplus\varepsilon_3C_3\oplus\varepsilon_4C_4\oplus\varepsilon_5C_5$ be a linear code of length n over R. Then C is a $(1-2w-2uv)$-constacyclic code of length n over R if and only if C_1,C_2,C_3 are cyclic codes and C_4,C_5 are negacyclic codes of length n over $\mathbb{F}_q$.

Proof. Let $\alpha_i=\varepsilon_1a_i+\varepsilon_2b_i+\varepsilon_3c_i+\varepsilon_4d_i+\varepsilon_5e_i$, for any $a=(a_1,a_2,\dots,a_n)\in C_1,b=(b_1,b_2,\dots,b_n)\in C_2,c=(c_1,c_2,\dots,c_n)\in C_3,d=(d_1,d_2,\dots,d_n)\in C_4,e=(e_1,e_2,\dots,e_n)\in C_5,i=1,\dots,n$. Then $\alpha=(\alpha_1,\alpha_2,\dots,\alpha_n)\in C$. If C is a $(1-2w-2uv)$-constacyclic code over R, then

$$\tau(\alpha)=\big((1-2w-2uv)\alpha_n,\alpha_1,\dots,\alpha_{n-1}\big)$$

$$=\big((1-2w-2uv)(\varepsilon_1a_n+\varepsilon_2b_n+\varepsilon_3c_n+\varepsilon_4d_n+\varepsilon_5e_n),\varepsilon_1a_1+\varepsilon_2b_1+\varepsilon_3c_1+\varepsilon_4d_1+\varepsilon_5e_1,\dots,\varepsilon_1a_{n-1}+\varepsilon_2b_{n-1}+\varepsilon_3c_{n-1}+\varepsilon_4d_{n-1}+\varepsilon_5e_{n-1}\big)$$

$$=\big((u-uv)a_n+(1-u-v-w+uv)b_n+(v-uv)c_n-uvd_n-we_n,(u-uv)a_1+(1-u-v-w+uv)b_1+(v-uv)c_1+uvd_1+we_1,\dots,(u-uv)a_{n-1}+(1-u-v-w+uv)b_{n-1}+(v-uv)c_{n-1}+uvd_{n-1}+we_{n-1}\big)$$

$$=(u-uv)\sigma(a)+(1-u-v-w+uv)\sigma(b)+(v-uv)\sigma(c)+uv\gamma(d)+w\gamma(e)\in C.$$

Therefore, C_1,C_2,C_3 are cyclic codes and C_4,C_5 are negacyclic codes of length n over $\mathbb{F}_q$.

On the other hand, let $a=(a_1,a_2,\dots,a_n),b=(b_1,b_2,\dots,b_n),c=(c_1,c_2,\dots,c_n),d=(d_1,d_2,\dots,d_n),e=(e_1,e_2,\dots,e_n)$, for any $\alpha=(\alpha_1,\alpha_2,\dots,\alpha_n)\in C$, where $\alpha_i=\varepsilon_1a_i+\varepsilon_2b_i+\varepsilon_3c_i+\varepsilon_4d_i+\varepsilon_5e_i$ and $a_i,b_i,c_i,d_i,e_i\in\mathbb{F}_q,i=1,\dots,n$. Then $a\in C_1,b\in C_2,c\in C_3,d\in C_4,e\in C_5$. If C_1,C_2,C_3 are cyclic codes and C_4,C_5 are negacyclic codes of length n over $\mathbb{F}_q$, then $\sigma(a)\in C_1,\sigma(b)\in C_2,\sigma(c)\in C_3,\gamma(d)\in C_4,\gamma(e)\in C_5$. Hence $(u-uv)\sigma(a)+(1-u-v-w+uv)\sigma(b)+(v-uv)\sigma(c)+uv\gamma(d)+w\gamma(e)\in C$. However, $\tau(\alpha)=(u-uv)\sigma(a)+(1-u-v-w+uv)\sigma(b)+(v-uv)\sigma(c)+uv\gamma(d)+w\gamma(e)\in C$, which implies that $\tau(\alpha)\in C$.

Therefore C is a $(1-2w-2uv)$-constacyclic code over R.

■

Theorem 3.5. Let C be a $(1-2w-2uv)$-constacyclic code of length n over R. Then $C=\langle \varepsilon_1 g_1(x), \varepsilon_2 g_2(x), \varepsilon_3 g_3(x), \varepsilon_4 g_4(x), \varepsilon_5 g_5(x)\rangle$, where $g_i(x)$ are the generator polynomials of $C_i, i=1,2,3,4,5$, respectively. Moreover, $C^{\perp}=\varepsilon_1 C_1^{\perp}\oplus \varepsilon_2 C_2^{\perp}\oplus \varepsilon_3 C_3^{\perp}\oplus \varepsilon_4 C_4^{\perp}\oplus \varepsilon_5 C_5^{\perp}$ is also a $(1-2w-2uv)$-constacyclic code over R and

$$C^{\perp}=\langle \sum_{i=1}^{5}\varepsilon_i h_i^*(x)\rangle,$$

where $h_i^*(x)$, $i=1,2,3,4,5$, are the reciprocal polynomials of $\frac{x^n-1}{g_1(x)}$, $\frac{x^n-1}{g_2(x)}$, $\frac{x^n-1}{g_3(x)}$, $\frac{x^n+1}{g_4(x)}$ and $\frac{x^n+1}{g_5(x)}$, respectively.

Quantum Codes from $(1-2w-2uv)$-Constacyclic Codes over R

Let H be a Hilbert space of q dimension over the complex numbers $\mathbb{C}$. Define $H^{\otimes n}$ to be n-fold tensor product of the Hilbert space H, that is, $H^{\otimes n}=H\otimes H\otimes\cdots\otimes H$ (n-times). Then $H^{\otimes n}$ is a Hilbert space of q^n dimension. A quantum code having the length n and the dimension t over $\mathbb{F}_q$ is defined to be the Hilbert subspace of $H^{\otimes n}$. A quantum code with length n, dimension t and minimum distance d over $\mathbb{F}_q$ is denoted by $\left[[n,t,d]\right]_q$.

Lemma 4.1. Let C be a cyclic or negacyclic code with the generator polynomial $g(x)$ over $\mathbb{F}_q$. Then C contains its dual code if and only if

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

where $\kappa=\pm 1$ (Li et al., 2018).

Theorem 4.2. Let $C=\langle \varepsilon_1 g_1(x)+\varepsilon_2 g_2(x)+\varepsilon_3 g_3(x)+\varepsilon_4 g_4(x)+\varepsilon_5 g_5(x)\rangle$ be a $(1-2w-2uv)$-constacyclic code of length n over R. Then $C^{\perp}\subseteq C$ if and only if

$$x^n-1\equiv 0\big(mod g_t(x)g_t^*(x)\big)$$

and

$$x^n+1\equiv 0\left(mod g_j(x)g_j^*(x)\right),$$

where $t=1,2,3$ and $j=4,5$.

Proof. Let $C=\langle g(x)\rangle$ be a $(1-2w-2uv)$-constacyclic code of length n over R, where $g(x)=\varepsilon_1 g_1(x)+\varepsilon_2 g_2(x)+\varepsilon_3 g_3(x)+\varepsilon_4 g_4(x)+\varepsilon_5 g_5(x)$. Then $C=\varepsilon_1 C_1\oplus \varepsilon_2 C_2\oplus \varepsilon_3 C_3\oplus \varepsilon_4 C_4\oplus \varepsilon_5 C_5$, where $C_i=\langle g_i(x)\rangle, i=1,2,3,4,5$. If

$$x^n-1\equiv 0\big(mod g_t(x)g_t^*(x)\big)$$

and

$$x^n+1\equiv 0\left(mod g_j(x)g_j^*(x)\right),$$

then $C_t^{\perp}\subseteq C_t$ and $C_j^{\perp}\subseteq C_j$, where $t=1,2,3$ and $j=4,5$. Therefore,

$$\varepsilon_t C_t^{\perp}\subseteq \varepsilon_t C_t$$

and

$$\varepsilon_j C_j^{\perp}\subseteq \varepsilon_j C_j,$$

which implies that

$$\varepsilon_1 C_1^{\perp}\oplus\varepsilon_2 C_2^{\perp}\oplus\varepsilon_3 C_3^{\perp}\oplus\varepsilon_4 C_4^{\perp}\oplus\varepsilon_5 C_5^{\perp}\subseteq \varepsilon_1 C_1\oplus\varepsilon_2 C_2\oplus\varepsilon_3 C_3\oplus\varepsilon_4 C_4\oplus\varepsilon_5 C_5.$$

Thus,

$$\langle\varepsilon_1 h_1^*+\varepsilon_2 h_2^*+\varepsilon_3 h_3^*+\varepsilon_4 h_4^*+\varepsilon_5 h_5^*\rangle\subseteq\langle\varepsilon_1 g_1+\varepsilon_2 g_2+\varepsilon_3 g_3+\varepsilon_4 g_4+\varepsilon_5 g_5\rangle.$$

Therefore, $C^{\perp}\subseteq C$.

Conversely, if $C^{\perp}\subseteq C$, then

$$\varepsilon_1 C_1^{\perp}\oplus\varepsilon_2 C_2^{\perp}\oplus\varepsilon_3 C_3^{\perp}\oplus\varepsilon_4 C_4^{\perp}\oplus\varepsilon_5 C_5^{\perp}\subseteq \varepsilon_1 C_1\oplus\varepsilon_2 C_2\oplus\varepsilon_3 C_3\oplus\varepsilon_4 C_4\oplus\varepsilon_5 C_5,$$

which implies that $C_t^{\perp}\subseteq C_t$ and $C_j^{\perp}\subseteq C_j$, where $t=1,2,3$ and $j=4,5$. Therefore,

$$x^n-1\equiv 0\big(mod g_t(x)g_t^*(x)\big)$$

and

$$x^n+1\equiv 0\left(mod g_j(x)g_j^*(x)\right).$$

■

By Theorem 4.2, we have the following corollary directly.

Corollary 4.3. Let $C=\varepsilon_1 C_1\oplus\varepsilon_2 C_2\oplus\varepsilon_3 C_3\oplus\varepsilon_4 C_4\oplus\varepsilon_5 C_5$ be a $(1-2w-2uv)$-constacyclic code of length n over R. Then $C^{\perp}\subseteq C$ if and only if $C_i^{\perp}\subseteq C_i,\ i=1,2,3,4,5$.

Theorem 4.4. (CSS Construction) Let C be a linear code with parameters $[n,k,d]$ over $\mathbb{F}_q$. If $C^{\perp}\subset C$, then an $\big[[n,2k-n,\geq d]\big]$ quantum code can be obtained (Li et al., 2018).

By Corollary 4.3 and Theorem 4.4, the quantum codes can be constructed as follows.

Theorem 4.5. Let $C=\varepsilon_1C_1\oplus\varepsilon_2C_2\oplus\varepsilon_3C_3\oplus\varepsilon_4C_4\oplus\varepsilon_5C_5=\langle\varepsilon_1g_1(x)+\varepsilon_2g_2(x)+\varepsilon_3g_3(x)+\varepsilon_4g_4(x)+\varepsilon_5g_5(x)\rangle$ be a $(1-2w-2uv)$-constacyclic code of length n over R, where $g_i(x), i=1,2,3,4,5$, are the generator polynomials of C_i, respectively. If $C_i^{\perp}\subseteq C_i$, then $C^{\perp}\subseteq C$ and there exists a quantum error-correcting code with parameters $\left[[5n,2k-5n,\geq d_L]\right]$, where d_L is the minimum Lee distance of the code C and k is the dimension of the linear code $\delta(C)$.

Example 4.6. Let $R=\mathbb{F}_5+u\mathbb{F}_5+v\mathbb{F}_5+w\mathbb{F}_5+uv\mathbb{F}_5$ and $n=19$. We have

$$x^{19}-1=(x-4)(x^9+3x^7+2x^6+2x^5+2x^4+4x^3+2x^2+4x+4)(x^9+x^8+3x^7+x^6+3x^5+3x^4+3x^3+2x^2+4)\in\mathbb{F}_5[x]$$

and

$$x^{19}+1=(x+1)(x^9+3x^7+3x^6+2x^5+3x^4+4x^3+3x^2+4x+1)(x^9+4x^8+3x^7+4x^6+3x^5+2x^4+3x^3+3x^2+1)\in\mathbb{F}_5[x].$$

Let $g(x)=\varepsilon_1(x^9+3x^7+2x^6+2x^5+2x^4+4x^3+2x^2+4x+4)+\varepsilon_2(x^9+3x^7+2x^6+2x^5+2x^4+4x^3+2x^2+4x+4)+\varepsilon_3(x^9+3x^7+2x^6+2x^5+2x^4+4x^3+2x^2+4x+4)+\varepsilon_4(x^9+3x^7+3x^6+2x^5+3x^4+4x^3+3x^2+4x+1)+\varepsilon_5(x^9+3x^7+3x^6+2x^5+3x^4+4x^3+3x^2+4x+1)$ be the generator polynomial of C. Since $g_t(x)g_t^*(x)$ divides $x^{19}-1$ and $g_j(x)g_j^*(x)$ divides $x^{19}+1$, where $t=1,2,3$ and $j=4,5$, then by Theorem 4.2, we have $C^{\perp}\subseteq C$. Also, $\delta(C)$ is a linear code over $\mathbb{F}_5$ with parameters $[95,50,7]$. Now, using Theorem 4.5, we get a quantum code with parameters $\left[[95,5,\geq 7]\right]$.

Example 4.7. Let $R=\mathbb{F}_{11}+u\mathbb{F}_{11}+v\mathbb{F}_{11}+w\mathbb{F}_{11}+uv\mathbb{F}_{11}$ and $n=15$. We have

$$x^{15}-1=(x+2)(x+6)(x+7)(x+8)(x+10)(x^2+x+1)(x^2+3x+9)(x^2+4x+5)(x^2+5x+3)(x^2+9x+4)\in\mathbb{F}_{11}[x]$$

and

$$x^{15}+1=(x+1)(x+3)(x+4)(x+5)(x+9)(x^2+2x+4)(x^2+6x+3)(x^2+7x+5)(x^2+8x+9)(x^2+10x+1)\in\mathbb{F}_{11}[x].$$

Let $g(x)=\varepsilon_1(x^2+4x+5)+\varepsilon_2(x^2+9x+4)+\varepsilon_3(x^2+10x+5)+\varepsilon_4(x^2+7x+5)+\varepsilon_5(x^2+6x+3)$ be the generator polynomial of C. Since $g_t(x)g_t^*(x)$ divides $x^{15}-1$ and $g_j(x)g_j^*(x)$ divides $x^{15}+1$, where $t=1,2,3$ and $j=4,5$, then by Theorem 4.2, we have $C^{\perp}\subseteq C$. Also, $\delta(C)$ is a linear code over $\mathbb{F}_{11}$ with parameters $[75,65,3]$. Now, using Theorem 4.5, we get a quantum code with parameters $\left[[75,55,\geq 3]\right]$.

4. Conclusion:

In this paper, we have obtained quantum codes from $(1-2w-2uv)$ -constacyclic codes over $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+w\mathbb{F}_q+uv\mathbb{F}_q$, where $u^2=u, v^2=v, w^2=w, uv=vu, uw=wu=vw=wv=0$, $q=p^m$ and p is an odd prime. We have the parameters of quantum codes which are obtained from $(1-2w-2uv)$ -constacyclic codes over R.

Ethics in Publishing

There are no ethical issues regarding the publication of this study.

Acknowledgement: We would like to thank Y. Çengellenmiş for her many helpful suggestions.

References

Calderbank, A. R., Rains, E. M., Shor, P. M. and Sloane, N. J. 1998. "Quantum Error Correction via Codes over GF(4)", *IEEE Transactions on Information Theory*, 1369-1387.

Gao, J. and Wang, Y. 2018. "u-Constacyclic Codes over $\mathbb{F}_p+u\mathbb{F}_p$ and Their Applications of Constructing New Non-binary Quantum Codes", *Quantum Information Processing*, 17(1), 1-9.

Islam, H. and Prakash, O. 2020. "New Quantum Codes from Constacyclic and Additive Constacyclic Codes", *Quantum Information Processing*, 19(9), 1-17.

Kaye, P., Laflamme, R. and Mosca, M. (2006). "An Introducion to Quantum Computing", *OUP Oxford.*

Li, J., Gao J. and Wang Y. 2018. "Quantum Codes from $(1-2v)$-Constacyclic Codes over $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$", *Discrete Math.*, 10(4), 1850046.

Mohan, C. and Durairajan, C. 2020. "Skew-constacyclic codes over *R*", *Malaya Journal of Matematik*, 8(4), 1502-1508.

Shor, P. W. 1995. "Scheme for Reducing Decoherence in Quantum Memory", *Physical Review A*, 52, 2493-2496.