ORIGINAL PAPER

QUANTUM CODES FROM CYCLIC CODES OVER THE $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$

CEREMNUR TETİK[1], ABDULLAH DERTLİ[1]

Manuscript received: 14.12.2020. Accepted paper: 08.09.2021;
Published online: 30.09.2021.

Abstract: *In this paper, we give construction of quantum codes over* $\mathbb{F}_q$ *from cyclic codes over the* $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$, *where* $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = wu = vw = wv = 0$, $q = p^m$ *and* p *is an odd prime. We determine the parameters of quantum error correcting codes which constructed from cyclic codes over the* $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q$. *Finally, we give some examples of quantum codes.*

Keywords: *quantum codes; cyclic codes; gray map.*
Mathematics Subject Classification: *94B05, 94B15, 81P70.*

1. INTRODUCTION

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 cannot travel faster than light, while quantum information appears to in some circumstances. Classical information can be duplicated, while quantum information cannot. Quantum error correcting codes provide an efficient way to overcome decoherence. Therefore, quantum information is more convenient than classical information.

The first quantum error correcting code was found by Shor [1] in 1995. In 1998, Calderbank, Rains, Shor and Sloane [2] 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 classical cyclic codes and their generalizations over the finite field $\mathbb{F}_q$ has developed. Many quantum error correcting codes have been constructed by using classical error correcting codes over many finite rings, in [3-6]. In this paper, motivated by the previous works we study the quantum codes which are obtained from cyclic 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. PRELIMINARIES

In [7], 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, $q = p^m$ and p is an odd prime. The other results have appeared in [7].

[1]Ondokuz Mayıs University, Mathematics Department, 55270 Samsun, Turkey.
E-mail: ceremnurtetik@gmail.com; abdullah.dertli@gmail.com.

Let $\varepsilon_1 = u - uv, \varepsilon_2 = 1 - u - v - w + uv, \varepsilon_3 = v - uv, \varepsilon_4 = uv$ and $\varepsilon_5 = w$ 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 $i \neq j$. We have $R = \varepsilon_1 R \oplus \varepsilon_2 R \oplus \varepsilon_3 R \oplus \varepsilon_4 R \oplus \varepsilon_5 R$. By calculation, we can easily obtain 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 $i = 1,2,3,4,5$, in [7].

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.

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 is denoted by

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

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

A linear code C over R is called cyclic if every $c = (c_0, c_1, \dots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$. A subset C of R^n is a linear cyclic code of length n if and only if it is polynomial representation is an ideal of $R[x]/\langle x^n - 1 \rangle$.

Let $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ be any two elements of R^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 $C^\perp$ of C is defined as

$$C^\perp = \{x \in R^n | x \cdot y = 0, for\ all\ y \in C\}.$$

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 in [7] as follows:

$$\delta : R \longrightarrow \mathbb{F}_q^5$$
$$\delta(\varepsilon_1 a_1 + \varepsilon_2 a_2 + \varepsilon_3 a_3 + \varepsilon_4 a_4 + \varepsilon_5 a_5) = (a_1, a_2, a_3, a_4, a_5)$$

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

Equivalently, if $r = a_1' + u a_2' + v a_3' + w a_4' + uv a_5' \in R$, 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 $r = \varepsilon_1 a_1 + \varepsilon_2 a_2 + \varepsilon_3 a_3 + \varepsilon_4 a_4 + \varepsilon_5 a_5 \in R$, 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 distinct pairs of codewords of a code C is called the minimum distance of C and denoted by $d_L(C)$ or shortly d_L.

Lemma 1. [7] 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.

Lemma 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 parameters $(5n, M, d)$.

Proof: From Lemma 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, we have that $\delta(C)$ 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. ∎

Let A_i be codes over R, $i = 1, 2, 3, 4, 5$. We denote

$$A_1 \otimes A_2 \otimes A_3 \otimes A_4 \otimes A_5 = \{(a_1, a_2, a_3, a_4, a_5) | a_i \in A_i, i = 1, 2, 3, 4, 5\}$$

and

$$A_1 \oplus A_2 \oplus A_3 \oplus A_4 \oplus A_5 = \{a_1 + a_2 + a_3 + a_4 + a_5 | a_i \in A_i, i = 1, 2, 3, 4, 5\}.$$

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

$$C_1 = \left\{a_1 \in \mathbb{F}_q^n \middle| \varepsilon_1 a_1 + \varepsilon_2 a_2 + \varepsilon_3 a_3 + \varepsilon_4 a_4 + \varepsilon_5 a_5 \in C, for\ some\ a_i \in \mathbb{F}_q^n (i \neq 1)\right\}$$

$$C_2 = \left\{a_2 \in \mathbb{F}_q^n \middle| \varepsilon_1 a_1 + \varepsilon_2 a_2 + \varepsilon_3 a_3 + \varepsilon_4 a_4 + \varepsilon_5 a_5 \in C, for\ some\ a_i \in \mathbb{F}_q^n (i \neq 2)\right\}$$

$$C_3 = \left\{a_3 \in \mathbb{F}_q^n \middle| \varepsilon_1 a_1 + \varepsilon_2 a_2 + \varepsilon_3 a_3 + \varepsilon_4 a_4 + \varepsilon_5 a_5 \in C, for\ some\ a_i \in \mathbb{F}_q^n (i \neq 3)\right\}$$

$$C_4 = \left\{a_4 \in \mathbb{F}_q^n \middle| \varepsilon_1 a_1 + \varepsilon_2 a_2 + \varepsilon_3 a_3 + \varepsilon_4 a_4 + \varepsilon_5 a_5 \in C, for\ some\ a_i \in \mathbb{F}_q^n (i \neq 4)\right\}$$

$$C_5 = \left\{a_5 \in \mathbb{F}_q^n \middle| \varepsilon_1 a_1 + \varepsilon_2 a_2 + \varepsilon_3 a_3 + \varepsilon_4 a_4 + \varepsilon_5 a_5 \in C, for\ some\ a_i \in \mathbb{F}_q^n (i \neq 5)\right\}$$

Then cyclic code C over R can be represented as $C = \varepsilon_1 C_1 \oplus \varepsilon_2 C_2 \oplus \varepsilon_3 C_3 \oplus \varepsilon_4 C_4 \oplus \varepsilon_5 C_5$, in [7].

Theorem 3. [7] Let C be a linear code of length n over R. Then $\delta(C) = \otimes_{i=1}^{5} C_i$, $|C| = \prod_{i=1}^{5} |C_i|$ and $d_L(C) = min\{d_H(C_i), i = 1, 2, 3, 4, 5\}$.

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

Theorem 4. [7] Let C be a linear code of length n over R. Then $\delta(C^\perp) = \left(\delta(C)\right)^\perp$.

Theorem 5. [7] Let C be a linear code of length n over R. Then C is self-orthogonal, so is $\delta(C)$.

Theorem 6. [7] 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 linear code of length n over R. Then C is a cyclic code if and only if $C_i, i = 1,2,3,4,5$, are cyclic codes over $\mathbb{F}_q$.

Theorem 7. 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 cyclic code of length n over R and suppose that $g_i(x)$ are the generator polynomials of $C_i, i = 1,2,3,4,5$, respectively. Then $C = \langle \varepsilon_1 g_1(x), \varepsilon_2 g_2(x), \varepsilon_3 g_3(x), \varepsilon_4 g_4(x), \varepsilon_5 g_5(x) \rangle$ and $|C| = q^{5n-\tau}$, where $\tau = deg(g_1(x)) + deg(g_2(x)) + deg(g_3(x)) + deg(g_4(x)) + deg(g_5(x))$.

Theorem 8. For any cyclic code C of length n over R, there is a unique polynomial $g(x)$ such that $C = \langle g(x) \rangle$ and $g(x)|x^n - 1$, where $g_i(x)$ are the generator polynomials of $C_i, i = 1,2,3,4,5$ and $g(x) = \varepsilon_1 g_1(x) + \varepsilon_2 g_2(x) + \varepsilon_3 g_3(x) + \varepsilon_4 g_4(x) + \varepsilon_5 g_5(x)$.

Theorem 9. Let C be a cyclic code of length n over R. Then $C^\perp = \varepsilon_1 C_1^\perp \oplus \varepsilon_2 C_2^\perp \oplus \varepsilon_3 C_3^\perp \oplus \varepsilon_4 C_4^\perp \oplus \varepsilon_5 C_5^\perp$. Moreover, C is a self-dual code over R if and only if $C_i, i = 1,2,3,4,5$, are self-dual codes over $\mathbb{F}_q$.

Theorem 10. 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 cyclic code over R with associated q-ary codes C_1, C_2, C_3, C_4 and C_5. Then $C^\perp = \langle \varepsilon_1 h_1^*(x) + \varepsilon_2 h_2^*(x) + \varepsilon_3 h_3^*(x) +$ *ε4h4∗x+ε5h5∗x* and *C⊥=qdegg1x+degg2x+degg3x+degg4x+degg5x*, where *hi∗x* are the reciprocal polynomials of $h_i(x)$, that is, $h_i(x) = x^n - 1/g_i(x)$, $h_i^*(x) = x^{deg(h_i(x))}.h_i(x^{-1})$ for $i = 1,2,3,4,5$.

3. QUANTUM CODES FROM CYCLIC 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 k over $\mathbb{F}_q$ is defined to be the Hilbert subspace of $H^{\otimes n}$. A quantum code with length n, dimension k and minimum distance d over $\mathbb{F}_q$ is denoted by $[[n,k,d]]_q$.

A fundamental link between linear codes and binary quantum stabilizer codes is given by the Calderbank-Shor-Steane (CSS) construction.

Theorem 11. [8] (CSS Construction) Let C and C' be two binary codes with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively. If $C^\perp \subset C'$, then an $[[n, k_1 + k_2 - n, min\{d_1, d_2\}]]$ quantum code can be constructed. Especially, if $C^\perp \subseteq C$, then there exists an $[[n, 2k_1 -$ *n, d1* quantum code.

Lemma 12. [2] A cyclic code C with generator polynomial $g(x)$ contains its dual code if and only if

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

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

Theorem 13. Let $C = \langle g(x) \rangle$ be a cyclic code of arbitrary 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 $C^\perp \subseteq C$ if and only if

$$x^n - 1 \equiv 0(mod g_i(x)g_i^*(x)),$$

where $g_i^*(x)$ are the reciprocal polynomials of $g_i(x)$, respectively, $i = 1,2,3,4,5$.

Proof: Let $x^n - 1 \equiv 0\big(mod g_i(x) g_i^*(x)\big)$ for $i = 1, 2, 3, 4, 5$. Then by Lemma 12, we have

$$C_i^{\perp} \subseteq C_i, \qquad i = 1, 2, 3, 4, 5.$$

This implies that

$$\varepsilon_i C_i^{\perp} \subseteq \varepsilon_i C_i, \qquad i = 1, 2, 3, 4, 5.$$

Therefore,

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

Hence,

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

that is, $C^{\perp} \subseteq C$.

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

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

Since C_i are the q-ary codes such that $\varepsilon_i C_i$ are equal to C mod ε_i, we find that $C_i^{\perp} \subseteq C_i$, $i = 1, 2, 3, 4, 5$. Therefore,

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

■

Corollary 14. 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 cyclic 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 15. 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 cyclic code of length n over R. If $C_i^{\perp} \subseteq C_i$, $i = 1, 2, 3, 4, 5$, then $C^{\perp} \subseteq C$ and there exists a quantum error-correcting code with parameters $\big[[5n, 2k - 5n, d_L]\big]$, where d_L is the minimum Lee weight of the code C and k is the dimension of the code $\delta(C)$.

Proof: Let $C_i^{\perp} \subseteq C_i$ for $i = 1, 2, 3, 4, 5$. Then by Corollary 14, $C^{\perp} \subseteq C$. Now let $c \in \delta(C^{\perp}) = \big(\delta(C)\big)^{\perp}$. Since δ is a bijection, so there exists $c' \in C^{\perp}$ such that $c = \delta(c')$, where $c' \cdot c'' = 0$ for all $c'' \in C$. As $C^{\perp} \subseteq C$ and $c' \in C^{\perp}$, so we get $c' \in C$. Hence, $c = \delta(c') \in \delta(C)$ implying that $\big(\delta(C)\big)^{\perp} \subseteq \delta(C)$. Also note that $\delta(C)$ is a $[5n, k, d_H]$ linear code over $\mathbb{F}_q$. Then by Theorem 11, there exists a quantum eror-correcting code with parameters $\big[[5n, 2k - 5n, d_L]\big]$.

■

Example 16. Let $R = \mathbb{F}_9 + u\mathbb{F}_9 + v\mathbb{F}_9 + w\mathbb{F}_9 + uv\mathbb{F}_9$ and $n = 20$. We have

$$x^{20} - 1 = (x+1)(x+2)(x^2+1)(x^4+x^3+2x+1)(x^4+x^3+x^2+x+1)(x^4+2x^3 + x + 1)(x^4+2x^3+x^2+2x+1) \in \mathbb{F}_9[x]$$

Let $g_1(x) = g_2(x) = g_3(x) = g_4(x) = g_5(x) = x^4 + x^3 + 2x + 1$. Then $C_i = \langle g_i(x) \rangle, i = 1, 2, 3, 4, 5$, are the cyclic codes over $\mathbb{F}_9$ having the same parameters $[20, 16, 4]$. Thus, from Theorem 7,

$$C = \langle \varepsilon_1 g_1(x), \varepsilon_2 g_2(x), \varepsilon_3 g_3(x), \varepsilon_4 g_4(x), \varepsilon_5 g_5(x) \rangle$$

is a cyclic code of length 20 over R. Since all $g_i(x) g_i^*(x)$ divide $x^{20} - 1$ for $i = 1, 2, 3, 4, 5$, by Theorem 13, $C^{\perp} \subseteq C$. Also, $\delta(C)$ is a linear code over $\mathbb{F}_9$ with parameters $[100, 80, 4]$.

Now, using Theorem 15, we get a quantum code with parameters $\big[[100, 60, 4]\big]$.

Example 17. Let $R=\mathbb{F}_5+u\mathbb{F}_5+v\mathbb{F}_5+w\mathbb{F}_5+uv\mathbb{F}_5$ and $n=31$. We have

$$x^{31}-1=(x+4)(x^3+x+4)(x^3+2x+4)(x^3+x^2+x+4)(x^3+x^2+3x+4)(x^3+2x^2+x+4)(x^3+2x^2+4x+4)(x^3+3x^2+4)(x^3+4x^2+4)(x^3+4x^2+3x+4)(x^3+4x^2+4x+4)\in\mathbb{F}_5[x]$$

Let $g_1(x)=g_2(x)=g_3(x)=g_4(x)=g_5(x)=x^3+x+4$. Then $C_i=\langle g_i(x)\rangle, i=1,2,3,4,5$, are the cyclic codes over $\mathbb{F}_5$ having the same parameters $[31,28,3]$. Thus, from Theorem 7,

$$C=\langle \varepsilon_1 g_1(x),\varepsilon_2 g_2(x),\varepsilon_3 g_3(x),\varepsilon_4 g_4(x),\varepsilon_5 g_5(x)\rangle$$

is a cyclic code of length 31 over R. Since all $g_i(x)g_i^*(x)$ divide $x^{31}-1$ for $i=1,2,3,4,5$, by Theorem 13, $C^\perp\subseteq C$. Also, $\delta(C)$ is a linear code over $\mathbb{F}_5$ with parameters $[155,140,3]$. Now, using Theorem 15, we get a quantum code with parameters $[[155,125,3]]$.

Let $g_1(x)=g_2(x)=g_3(x)=g_4(x)=g_5(x)=x^3+4x^2+3x+4$. Then $C_i=\langle g_i(x)\rangle, i=1,2,3,4,5$, are the cyclic codes over $\mathbb{F}_5$ having the same parameters $[31,28,4]$. Thus, from Theorem 7,

$$C=\langle \varepsilon_1 g_1(x),\varepsilon_2 g_2(x),\varepsilon_3 g_3(x),\varepsilon_4 g_4(x),\varepsilon_5 g_5(x)\rangle$$

is a cyclic code of length 31 over R. Since all $g_i(x)g_i^*(x)$ divide $x^{31}-1$ for $i=1,2,3,4,5$, by Theorem 13, $C^\perp\subseteq C$. Also, $\delta(C)$ is a linear code over $\mathbb{F}_5$ with parameters $[155,140,4]$. Now, using Theorem 15, we get a quantum code with parameters $[[155,125,4]]$.

4. CONCLUSION

In this paper, we have obtained quantum codes from cyclic 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 cyclic codes over R.

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

REFERENCES

[1] Shor, P.W., *Physical Review A*, **52**, 2493, 1995.
[2] Calderbank, A.R., Rains, E.M., Shor, P.M., Sloane, N.J., *IEEE Transactions on Information Theory*, **44**, 1369, 1998.
[3] Dertli, A., Cengellenmis, Y., Eren, S., *International Journal of Quantum Information*, **13**, 1550031, 2015.
[4] Gao, J., *International Journal of Quantum Information*, **13**, 1550063, 2015.
[5] Islam, H., Prakash, O., *Journal of Applied Mathematics and Computing*, **60**, 625, 2019.
[6] Ashraf, M., Mohammad, G., *Quantum Information Processing*, **15**, 4089, 2016.
[7] Mohan, C., Durairajan, C., *Malaya Journal of Matematik*, **8**, 1502, 2020.
[8] Qian, J., *Journal of Information and Computational Science*, **10**, 1715, 2013.