Araştırma Makalesi / *Research Article* **Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 10(1): 556-562, 2020**
Matematik / Mathematics ***Journal of the Institute of Science and Technology,* 10(1): 556-562, 2020**

DOI: 10.21597/jist.569915 **ISSN: 2146-0574, eISSN: 2536-4618**

Kuantum Kodlar

Abdullah DERTLİ[1*], Yasemin ÇENGELLENMİŞ[1]

ÖZET: Bu çalışmada, $u^2=1, v^3=v, uv=vu, q=p^m$ ve p tek asal sayı olmak üzere $R=F_q+uF_q+vF_q+uvF_q+v^2F_q+uv^2F_q$ halkası üzerindeki devirli kodlar kullanılarak F_q üzerindeki kuantum kodlar elde edildi. Ayrıca F_q üzerindeki kuantum kodların parametreleri belirlendi. Bazı örnekler verildi.

Anahtar kelimeler: Kuantum kodlar, devirli kodlar, Gray dönüşümü.

Quantum Codes

ABSTRACT: In the present paper, the quantum codes over F_q which are obtained from cyclic codes over the finite ring $R=F_q+uF_q+vF_q+uvF_q+v^2F_q+uv^2F_q$ with $u^2=1, v^3=v, uv=vu,$ where $q=p^m$ and p is an odd prime. Moreover the parameters of quantum codes over F_q are determined. Some examples are given.

Keywords: Quantum codes, cyclic codes, Gray map.

[1] Abdullah DERTLİ (**Orcid ID:** 0000-0001-8687-032X), Ondokuz Mayıs Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Samsun, Türkiye
[2] Yasemin ÇENGELLENMİŞ (**Orcid ID:** 0000-0002-8133-9836), Trakya Üniversitesi, Fen Fakültesi, Matematik Bölümü, Edirne, Türkiye

*Sorumlu Yazar/Corresponding Author: Abdullah DERTLİ, e-mail: abdullah.dertli@gmail.com

Geliş tarihi / *Received:* 24-05-2019
Kabul tarihi / *Accepted:* 08-10-2019

GİRİŞ

Kuantum hesaplama ve kuantum iletişimde kullanılan kuantum kodlar, kuantum bilginin taşınması sırasında oluşabilecek hataların tespiti ve düzeltilmesi için kullanılır.

Kuantum hata düzeltici kodlar ilk olarak Shor ve Steane tarafından birbirinden bağımsız olarak elde edilmiştir (Shor, 1995; Steane, 1996).

Klasik kodlama teorisi, kuantum teorisinden farklı olmasına rağmen Calderbank ve ark. bu iki teori arasındaki geçişi bulmuşlardır (Calderbank ve ark., 1998). Bu makalede sonlu cisimler üzerindeki kodlardan kuantum kodlar elde edilmiştir.

J. Qian ve ark. $F_2+uF_2,u^2=0$ sonlu halkası üzerindeki devirli kodlardan kuantum hata düzeltici kodları elde etmişlerdir (Qian ve ark., 2009). X. Kai, S. Zhu, $F_4+uF_4,u^2=0$ halkası üzerinde (Kai ve Zhu, 2011), X. Yin ve W. Ma, $F_2+uF_2+u^2F_2,u^3=0$ halkası üzerinde (Yin ve Ma, 2011), devirli kodları kullanarak kuantum kodların parametrelerini oluşturmuşlardır. J. Qian, $F_2+vF_2,v^2=v$ halkası üzerinde keyfi uzunlukta devirli kodlardan kuantum kodları bulmuştur (Qian, 2013). (Ashraf ve Mohammed, 2014; Ashraf ve Mohammed, 2015; Ashraf ve Mohammed, 2016), M. Ashraf ve G. Mohammed $F_3+vF_3,v^2=1$, $F_p+vF_p,v^2=v$ ve $F_q+uF_q+vF_q+uvF_q,u^2=u,v^2=v,uv=vu$ halkaları üzerinde devirli kodlardan kuantum kodların parametrelerini elde etmişlerdir. A. Dertli ve ark. sonlu halkaları kullanarak kuantum kodların parametrelerini devirli kodlardan elde etmişlerdir (Dertli ve ark., 2015a; Dertli ve ark., 2015b; Dertli ve ark., 2015c; Dertli ve ark., 2016b). Ayrıca A. Dertli ve ark. R_3, R_p halkalarını kullarak negacyclic kodlardan kuantum kodları oluşturmuşlardır (Dertli ve ark., 2015d; Dertli ve ark., 2016a).

Liu Yan ve ark. $u^2=1,v^3=v,uv=vu$, $q=p^m$, p tek asal sayı olmak üzere $R=F_q+uF_q+vF_q+uvF_q+v^2F_q+uv^2F_q$ halkası üzerinde skew cyclic kodları çalışmışlardır (Liu ve ark., 2017). Biz ise bu çalışmada Liu Yan ve ark. makalesindeki R sonlu halkasını kullanarak devirli kodlardan kuantum kodlar elde ettik. Çalışmamızın 2. bölümünde halka ile ilgili temel bilgiler verildi. 3. bölümünde R halkası üzerindeki devirli kodların dualini içermesi için gerekli ve yeterli şart verildi. Son olarak bazı örnekler elde edildi.

MATERYAL VE YÖNTEM

İlk olarak Liu Yan ve ark.

$$\begin{aligned} R &= F_q+uF_q+vF_q+uvF_q+v^2F_q+uv^2F_q \\ &= \left\{a_1+ua_2+va_3+uva_4+v^2a_5+uv^2a_6 \ : \ a_j\in F_q, 1\le j\le 6\right\} \end{aligned}$$

sonlu halkasını incelediler. Ayrıca bu çalışmalarında $R_1=F_q+uF_q$, $u^2=1$ halkasını kullanarak $F_q[u,v]/<u^2-1,v^3-v,uv-vu>$ halkasını $R=R_1+vR_1+v^2R_1$ olarak gösterdiler (Liu ve ark., 2017).

Liu Yan ve ark. $a=a_1+ua_2+va_3+uva_4+v^2a_5+uv^2a_6, a_j\in F_q$, $j=1,2,...,6$, $a,b,c\in R_1$, $s,t\in F_q$ olmak üzere

$$\varphi: R\to R_1^3$$
$$a+vb+v^2c\mapsto (a,a+b+c,a-b+c)$$

$$\phi_1 : R_1 \to F_q^2$$
$$s + ut \mapsto (s,t)$$

Gray dönüşümlerini kullanarak aşağıdaki Φ Gray dönüşümünü tanımladılar.

$$\Phi : R \to F_q^6$$
$$a \mapsto (a_1, a_2, a_1 + a_3 + a_5, a_2 + a_4 + a_6, a_1 - a_3 + a_5, a_2 - a_4 + a_6)$$

F_q üzerinde x ve y vektörlerinin $d_H(x,y)$ Hamming uzaklığı $x-y$ vektörünün Hamming ağırlığına eşittir. $x = (x_0,...,x_{n-1}) \in R^n$ elemanının Lee ağırlığı $w_L(x)$, $w_L(x) = w_H(\Phi(x))$, herhangi bir $x, y \in R^n$ elemanlarının Lee uzaklığı $d_L(x,y)$, $d_L(x,y) = w_L(x-y)$ olarak tanımlanır.

Teorem 1: Gray dönüşümü Φ uzaklık koruyan bir dönüşümdür ve F_q -lineerdir (Liu ve ark., 2017).

R üzerinde n uzunluğa sahip bir C lineer kodu R^n nin bir R -altmodülüdür.

Lemma 2: C, R üzerinde n uzunluğa sahip, rankı k ve minimum Lee uzaklığı d olan bir lineer kod olsun. Bu durumda $\Phi(C)$, F_q üzerinde bir $[6n,k,d]$ lineer bir koddur (Liu ve ark., 2017).

Herhangi bir $x = (x_0,...,x_{n-1}), y = (y_0,...,y_{n-1})$ elemanlarının iç çarpımı aşağıdaki gibi tanımlanır

$$xy = \sum_{i=0}^{n-1} x_i y_i$$

Eğer $xy = 0$ ise x ve y elemanları ortogonaldir denir. C, R üzerinde n uzunluğa sahip bir lineer kod olmak üzere C kodunun duali

$$C^{\perp} = \{x : \forall y \in C, xy = 0\}$$

şeklindedir. C kodunun duali de R üzerinde n uzunluğa sahip lineer bir koddur. Eğer $C \subset C^{\perp}$ ise C koduna self ortogonal kod, $C = C^{\perp}$ ise C koduna self dual kod denir.

Teorem 3: C, R üzerinde n uzunluğa sahip lineer bir kod olsun. Bu durumda $\Phi(C)^{\perp} = \Phi(C^{\perp})$. Ayrıca, C self dual kod ise $\Phi(C)$ kodu da self dual koddur (Liu ve ark., 2017).

(Liu ve ark., 2017), Çin Kalan Teoremini kullanarak R halkasını aşağıdaki şekilde ifade etmiştir.

$$R = 2^{-1}(1+u)(1-v^2)F_q \oplus 2^{-1}(1-u)(1-v^2)F_q \oplus 4^{-1}(1+u)(v+v^2)F_q$$
$$\oplus 4^{-1}(1-u)(v+v^2)F_q \oplus 4^{-1}(1+u)(-v+v^2)F_q \oplus 4^{-1}(1-u)(-v+v^2)F_q$$

$$\eta_1 = 2^{-1}(1+u)(1-v^2), \eta_2 = 2^{-1}(1-u)(1-v^2)$$
$$\eta_3 = 4^{-1}(1+u)(v+v^2), \eta_4 = 4^{-1}(1-u)(v+v^2)$$
$$\eta_5 = 4^{-1}(1+u)(-v+v^2), \eta_6 = 4^{-1}(1-u)(-v+v^2)$$

olmak üzere R üzerinde n uzunluğa sahip C lineer kodu

$$C = \sum_{j=1}^{6} \eta_j C_j$$

şeklinde ifade edilir. Burada ki $C_j = \{x_j \in F_q^n : \exists x_i \in F_q^n, i \in \{1,2,...,6\} \setminus \{j\}, \sum_{i=1}^{6} \eta_i x_i \in C\}$ kodları F_q üzerinde n uzunluğa sahip lineer kodlardır (Liu ve ark., 2017).

$G_1, G_2, ..., G_6$, sırasıyla $C_1, C_2, ..., C_6$ kodlarının üreteç matrisleri ise C kodunun üreteç matrisi

$$G = \begin{bmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \vdots \\ \eta_6 G_6 \end{bmatrix}$$

dir. d_L, C kodunun minimum Lee ağırlığı olsun. $d_H(C_i)$, sırasıyla $C_1, C_2, ..., C_6$ kodlarının minimum Hamming ağırlığı olmak üzere,

$$d_L = d_H(\Phi(C)) = \min\{d_H(C_1), d_H(C_2), ..., d_H(C_6)\}$$

dir (Liu ve ark., 2017).

Önerme 4: $i = 1,2,...,6$ için C_i, F_q üzerinde n uzunluğa sahip lineer kodlar olmak üzere $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$, R üzerinde n uzunluğa sahip lineer bir kod olsun. C kodunun devirli bir kod olması için gerekli ve yeterli koşul $i = 1,2,...,6$ için C_i kodlarının devirli kod olmasıdır.

İspat: C devirli bir kod, $(a_0^1, a_1^1, ..., a_{n-1}^1) \in C_1$, $(a_0^2, a_1^2, ..., a_{n-1}^2) \in C_2, ..., (a_0^6, a_1^6, ..., a_{n-1}^6) \in C_6$ olmak üzere $i = 0,1,...,n-1$ için $m_i = \eta_1 a_i^1 + \eta_2 a_i^2 + ... + \eta_6 a_i^6$ olsun. C kodu devirli bir kod olduğundan $(m_0, m_1, ..., m_{n-1}) \in C$ için $(m_{n-1}, m_0, ..., m_{n-2}) \in C$ dir. Bu durumda,

$$(m_{n-1}, m_0, ..., m_{n-2}) = \eta_1(a_{n-1}^1, a_0^1, ..., a_{n-2}^1) + \eta_2(a_{n-1}^2, a_0^2, ..., a_{n-2}^2) + ... + \eta_6(a_{n-1}^6, a_0^6, ..., a_{n-2}^6)$$

eşitliği elde edilir. Böylece $(a_{n-1}^1, a_0^1, ..., a_{n-2}^1) \in C_1$, ..., $(a_{n-1}^6, a_0^6, ..., a_{n-2}^6) \in C_6$. O halde C_1, C_2, ... , C_6 kodları devirli koddur.

Tersine, $C_1, C_2, ..., C_6$ kodları devirli kod olsun. Bu durumda $i = 0,1,...,n-1$ için $m_i = \eta_1 a_i^1 + \eta_2 a_i^2 + ... + \eta_6 a_i^6$ olmak üzere $(m_0, m_1, ..., m_{n-1}) \in C$ ve $(a_0^1, a_1^1, ..., a_{n-1}^1) \in C_1$, ..., $(a_0^6, a_1^6, ..., a_{n-1}^6) \in C_6$ olur. Buradan

$$(m_{n-1}, m_0, ..., m_{n-2}) = \eta_1(a_{n-1}^1, a_0^1, ..., a_{n-2}^1) + \eta_2(a_{n-1}^2, a_0^2, ..., a_{n-2}^2) + ... + \eta_6(a_{n-1}^6, a_0^6, ..., a_{n-2}^6) \in C$$

elde edilir. O halde C devirli bir koddur.

Önerme 5: $C = \sum_{j=1}^{6} \eta_j C_j$, R üzerinde n uzunluğa sahip devirli bir kod olsun. O zaman f_1, f_2, ..., f_6 sırasıyla $C_1, C_2, ..., C_6$ kodlarının üreteç polinoları olmak üzere

$$C = \langle \eta_1 f_1, \eta_2 f_2, ..., \eta_6 f_6 \rangle$$

dir.

Lemma 6: $C=\sum_{j=1}^{6}\eta_j C_j$, R üzerinde n uzunluğa sahip devirli bir kod olsun. Bu durumda f_1, f_2,..., f_6 sırasıyla $C_1, C_2, ..., C_6$ kodlarının üreteç polinoları ve

$$f(x)=\eta_1 f_1(x)+\eta_2 f_2(x)+...+\eta_6 f_6(x)$$

olmak üzere $C=\langle f(x)\rangle$ olacak şekilde tek bir $f(x)$ polinomu vardır ve $f(x)\,|\,x^n-1$.

Lemma 7: $C=\sum_{j=1}^{6}\eta_j C_j$, R üzerinde n uzunluğa sahip devirli bir kod olsun. Bu durumda $i=1,2,...,6$ için $h_i^*(x)=x^{\deg h_i(x)}h_i(x^{-1})$, $h_i(x)=(x^n-1)/f_i(x)$, reciprocal polinomları olmak üzere

$$C^{\perp}=\langle \eta_1 h_1^*+\eta_2 h_2^*+...+\eta_6 h_6^*\rangle$$

eşitliği elde edilir.

Lemma 8: $f^*(x)$, $f(x)$ polinomunun reciprocal polinomu olmak üzere $f(x)$ polinomu ile üretilen devirli bir C kodunun dualini içermesi için gerekli ve yeterli koşul

$$x^n-1\equiv 0\pmod{ff^*}$$

olmasıdır (Ashraf ve Mohammed, 2017).

BULGULAR VE TARTIŞMA

Lemma 9: C_1 ve C_2, F_q üzerinde tanımlı sırasıyla $[n,k_1,d_1]_q$ ve $[n,k_2,d_2]_q$ parametrelerine sahip lineer kod, $C_2^{\perp}\subseteq C_1$,

$$d=\min\{w_t(v):\ v\in(C_1\setminus C_2^{\perp})\cup(C_2\setminus C_1^{\perp})\}\geq\min\{d_1,d_2\}$$

olsun. Bu durumda $[[n,k_1+k_2-n,d]]_q$ parametrelerine sahip bir C kuantum hata düzeltici kod vardır (Ashraf ve Mohammed, 2017).

Teorem 10: $f(x)=\eta_1 f_1(x)+\eta_2 f_2(x)+...+\eta_6 f_6(x)$ olmak üzere $C=\langle f(x)\rangle$, R üzerinde keyfi n uzunluğa sahip devirli bir kod olsun. Bu durumda $C^{\perp}\subseteq C$ olması için gerekli ve yeterli koşul $i=1,...,6$ için $f^*(x)$, $f(x)$ polinomunun reciprocal polinomu olmak üzere $x^n-1\equiv 0\pmod{f_i(x)f_i^*(x)}$ olmasıdır.

İspat: $x^n-1\equiv 0\pmod{f_i(x)f_i^*(x)}$ olsun. Lemma 8 den $C_i^{\perp}\subseteq C_i$ dir. Buradan $\eta_i C_i^{\perp}\subseteq\eta_i C_i$ ve $\sum_{j=1}^{6}\eta_j C_j^{\perp}\subseteq\sum_{j=1}^{6}\eta_j C_j$ elde edilir. Böylece $\left\langle\sum_{j=1}^{6}\eta_j h_j^*(x)\right\rangle\subseteq\left\langle\sum_{j=1}^{6}\eta_j f_j(x)\right\rangle$. Yani, $C^{\perp}\subseteq C$ dir.

Tersine, $C^{\perp}\subseteq C$ olsun. Bu durumda $\sum_{j=1}^{6}\eta_j C_j^{\perp}\subseteq\sum_{j=1}^{6}\eta_j C_j$. C_i koları F_q üzerinde tanımlı olduğundan $\eta_i C_i$, modulo η_i ye göre C koduna denktir. O halde $C_i^{\perp}\subseteq C_i$. Böylece $x^n-1\equiv 0\pmod{f_i(x)f_i^*(x)}$ dir.

Lemmma 9 ve Teorem 10 u kullanarak kuantum kodların parametrelerini aşağıdaki gibi elde ederiz.

Teorem 11: $C=\sum_{j=1}^{6}\eta_j C_j$, R üzerinde n uzunluğa sahip devirli bir kod olsun. Eğer $i=1,2,...,6$, için $C_i^{\perp}\subseteq C_i$ ise $C^{\perp}\subseteq C$ dir ve d_L, C kodunun minimum Lee ağırlığı, k, $\Phi(C)$ kodunun boyutu olmak üzere $[[6n,2k-6n,d_L]]$ parametrelerine sahip bir kuantum hata düzeltici kod vardır.

Örnek 1: $F_9 = \{x + ay \ : \ x, y \in F_3, a^2 + a + 2 = 0\}$ olmak üzere $x^6 - 1 = (x+1)^3 (x+2)^3 \in F_9[x]$

$$f_1(x) = f_2(x) = f_3(x) = f_4(x) = f_5(x) = f_6(x) = x + 1$$

olsun. Böylece $C = \langle \eta_1 f_1, \eta_2 f_2, ..., \eta_6 f_6 \rangle$. C_i kodları 6 uzunluğunda $[6,5,2]$-koddur. Bu durumda $\Phi(C)$, $[36,30,2]$ parametreye sahip lineer bir koddur. Teorem 10 dan, $C^{\perp} \subseteq C$. Teorem 11 i kullanarak, $[[36,24,2]]$ parametrelerine sahip kuantum kod elde ederiz.

Örnek 2: $x^{10} - 1 = (x+1)^5 (x+4)^5 \in F_5[x]$

$$f_1(x) = f_2(x) = (x+4)^2, \ f_3(x) = f_4(x) = f_5(x) = f_6(x) = (x+1)^2$$

olsun. Böylece $C = \langle \eta_1 f_1, \eta_2 f_2, ..., \eta_6 f_6 \rangle$. C_i kodları 10 uzunluğunda $[10,8,2]$-koddur. Bu durumda $\Phi(C)$, $[60,48,2]$ parametreye sahip lineer bir koddur. Teorem 10 dan, $C^{\perp} \subseteq C$. Teorem 11 i kullanarak, $[[60,36,2]]$ parametrelerine sahip kuantum kod elde ederiz.

Çizelge 1. Kuantum Kodlar

n	q	$C_1 = C_2 = C_3$	$C_4 = C_5 = C_6$	$\Phi(C)$	$[[N, K, D]]$
3	19	[3, 2, 2]	[3, 2, 2]	[18,12, 2]	[[18, 6, 2]]
4	9	[4, 3, 2]	[4, 3, 2]	[24,18, 2]	[[24,12, 2]]
12	3	[12, 9, 2]	[12, 9, 2]	[72, 54, 2]	[[72, 36, 2]]
20	9	[20,16, 4]	[20,16, 4]	[120, 96, 4]	[[120, 72, 4]]
27	3	[27, 21, 2]	[27, 21, 2]	[162,126, 2]	[[162, 90, 2]]
30	5	[30, 29, 2]	[30, 29, 2]	[180,174, 2]	[[180,168, 2]]
36	5	[36, 34, 2]	[36, 34, 2]	[216, 204, 2]	[[216,192, 2]]

SONUÇ

Bu çalışmada, $u^2 = 1$, $v^3 = v$, $uv = vu$, $q = p^m$ ve p tek asal sayı olmak üzere $R = F_q + uF_q + vF_q + uvF_q + v^2F_q + uv^2F_q$ halkası üzerindeki devirli kodlar kullanılarak F_q üzerindeki kuantum kodların parametreleri elde edilerek bazı sonlu cisimler üzerinde örnekler verildi. Yapılan bu çalışma farklı halkalara taşınarak yeni optimal kuantum kodlar elde edilebilir.

KAYNAKLAR

Ashraf M, Mohammad G, 2014. Quantum codes from cyclic codes over $F_3 + vF_3$. International Journal of Quantum Information, 12 (6):1450042.

Ashraf M, Mohammad G, 2015. Construction of quantum codes from cyclic codes over $F_p + vF_p$. International Journal of Information and Coding Theory, 2 : 137-144.

Ashraf M, Mohammad G, Quantum codes from cyclic codes over $F_q + uF_q + vF_q + uvF_q$. Quantum Information Processing, DOI:10.1007/s11128-016-1379-8.

Calderbank A R, Rains E M, Shor P M, Sloane N J A, 1998. Quantum error correction via codes over GF(4). IEEE Transactions on Information Theory, 44:1369-1387.

Dertli A, Cengellenmis Y, Eren S, 2015a. On quantum codes obtained from cyclic codes over A_2. International Journal of Quantum Information, 13: 1550031.

Dertli A, Cengellenmis Y, Eren S, 2015b. Quantum Codes over the Ring $F_2 + uF_2 + u^2F_2 + ... + u^mF_2$. International Journal of Algebra, 9: 115-121.

Dertli A, Cengellenmis Y, Eren S, 2016a. On the linear codes over the ring R_p. Discrete Mathematics, Algorithms and Applications, 1650036.

Dertli A, Cengellenmis Y, Eren S, 2015c. On the Codes over a Semilocal Finite Ring. Intern. J. of Adv. Computer Science & Application, DOI: 10.14569/IJACSA.2015.061038.

Dertli A, Cengellenmis Y, Eren S, 2016b. Some results on the linear codes over the finite ring $F_2 + v_1F_2 + ... + v_rF_2$. International Journal of Quantum Information, 1650012.

Dertli A, Cengellenmis Y, Eren S, 2015d. Quantum Codes Over $F_2 + uF_2 + vF_2$. Palestine Journal of Mathematics, 4: 547-552.

Kai X, Zhu S, 2011. Quaternary construction bof quantum codes from cyclic codes over $F_4 + uF_4$. International Journal of Quantum Information, 9:689-700.

Liu Y, Shi M, Lu Z, 2017. Skew cyclic codes over $F_q[u,v]/ < u^2 - 1, v^3 - v, uv - vu >$. IEICE Transactions Fundamentals, DOI:101587/transfun.E0.A.1.

Qian J, 2013. Quantum codes from cyclic codes over $F_2 + vF_2$. Journal of Information & computational Science, 10:1715-1722.

Qian J, Ma W, Gou W, 2009. Quantum codes from cyclic codes over finite ring. International Journal of Quantum Information, 7:1277-1283.

Shor P W, 1995. Scheme for reducing decoherence in quantum memory. Phys. Rev. A, 52:2493-2496.

Steane A M, 1996. Simple quantum error correcting codes. Phys. Rev. A, 54:4741-4751.

Yin X, Ma W, 2011. Gray map and quantum codes over the ring $F_2 + uF_2 + u^2F_2$. In Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE 10th International Conference on, p:897-899.