T.C
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$F_4 + vF_4$ HALKASI ÜZERİNDEKİ DEVİRLİ KODLARDAN KUANTUM KOD ELDE ETMEK

YÜKSEK LİSANS TEZİ

Faik Cem ERTUNÇ

Enstitü Anabilim Dalı : MATEMATİK

Enstitü Bilim Dalı : CEBİR VE SAYILAR TEORESİ

Tez Danışmanı : Prof. Dr. Mehmet ÖZEN

Temmuz 2017

T.C
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$F_4 + vF_4$ HALKASI ÜZERİNDEKİ DEVİRLİ KODLARDAN KUANTUM KOD ELDE ETMEK

YÜKSEK LİSANS TEZİ

Faik Cem ERTUNÇ

Enstitü Anabilim Dalı : MATEMATİK

Enstitü Bilim Dalı : CEBİR VE SAYILAR TEORESİ

Bu tez 07.07.2017 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr Mehmet ÖZEN Jüri Başkanı	Doç. Dr. Murat GÜZELTEPE Üye	Yrd. Doç. Dr. Hüseyin KOCAMAN Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Faik Cem ERTUNÇ

03.05.2017

TEŞEKKÜR

Derslerinde anlattığı kuantum dünyası ile benim bu konuya yönelmemi sağlayan, çalışmalarım boyunca her zaman benim ile birlikte sabırla çalışan, bilgi ve tecrübelerinden yararlandığım, saygıdeğer hocam Prof. Dr. Mehmet Özen'e şükranlarımı sunarım.

Ayrıca, takıldığım noktalarda yardımcı olan bölümümüz Araş. Gör. Halit İnce ve bölümümüz doktora öğrencisi Tuğba Özzaim'e teşekkür ederim. Öte yandan bugünlere ulaşmamda maddi ve manevi destekleriyle her zaman yanımda olan çok değerli aileme ve özellikle eşime teşekkürü bir borç bilirim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

C	: Kod
$C^{\perp}$	: C kodunun diki
d_L	: Lee uzaklık
F	: Cisim
G	: Grup
I	: İdeal
R	: Halka
$\langle u, v \rangle$	: u ile v ' nin iç çarpımı
V	: Vektör uzayı
$V(n,q)$	: Elemanları $\mathbb{F}_q$' dan alınan n −lilerin kümesi
w	: Hamming Ağırlık
ψ	: Gray Dönüşümü
F_q	: q elemanlı sonlu cisim

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Kuantum kod, lineer kod, devirli kod, $F_4 + vF_4$ üzerindeki kodlar

Bu çalışmada $v^2 = v$ iken $R = F_4 + vF_4$ halkası üzerindeki devirli kodlar çalışılmıştır. Bu devirli kodlar üzerinde kendine dual kodların nasıl elde edileceği belirlenmiştir. Bu kodlar sayesinde R üzerinde kuantum kod üretilmesi çalışılmıştır. Ayrıca F_4, 4 elemanlı bir sonlu cisim olmak üzere R ile F_4^2 arasında bir Gray dönüşüm tanımlanmıştır. Tezin son kısmında da bazı optimal kuantum kodlar için parametreleri ve üreteç polinomları MAGMA bilgisayar programı yardımı ile hesaplanmış ve tablo halinde verilmiştir.

QUANTUM CODES FROM CYCLIC CODES OVER $F_4 + vF_4$

SUMMARY

Keywords: Quantum codes, Linear codes, Cyclic codes, Gray map, Codes over $F_4 + vF_4$, where $v^2 = v$.

In this thesis, cyclic codes over $F_4 + vF_4$, where $v^2 = v$ are studied. A method is given to construct quantum codes from cyclic codes over $F_4 + vF_4$, where $v^2 = v$ and a Gray map is defined between R and F_4^2, where F_4 is the field with 4 elements. Some optimal quantum code parameters and others will be presented at the end of the paper by using MAGMA computational algebra system.

BÖLÜM 1. GİRİŞ

Bu bölümde verilecek tanım, teorem ve önermeler diğer bölümler için bir hazırlık mahiyetinde olup diğer bölümlerde bu tanım ve teoremler kullanılacaktır.

1.1. Cebirsel Tanımlar

Tanım 1.1.1 A boştan farklı bir küme olmak üzere A kümesinin sıralı ikililerden oluşan her elemanını A'da bir ve yalnız bir elemana karşılık getiren bir fonksiyona A kümesi üzerinde bir ikili işlem denir. Bu işlem " $*$" sembolü ile gösterilirse

$$A \times A \to A$$
$$(a,b) \to a * b$$

olarak tanımlanır [1].

Tanım 1.1.2 G kümesi boş olmayan bir küme ve $*$, G kümesinde bir ikili işlem olsun. $(G,*)$ cebirsel yapısı aşağıda verilen aksiyomları sağlıyorsa $(G,*)$ cebirsel yapısına bir grup denir.

i. $*$, G kümesinde bir ikili işlemdir.

ii. $*$ işleminin G kümesinde birleşme özelliği vardır. Yani $\forall a,b,c \in G$ için $a*(b,c) = (a,b)*c$ olur.

iii. $*$ işleminin G kümesinde birim elemanı vardır. Yani $\forall a \in G$ için $a*e = e*a = a$ olacak şekilde $\exists e \in G$ vardır.

iv. $*$ işlemine göre G kümesindeki her elemanın bir tersi vardır. Yani $\forall a \in G$ için $a*a^{-1} = a^{-1}*a = e$ olacak şekilde $\exists a^{-1} \in G$ vardır [1].

Tanım 1.1.3 G bir grup ve $a_1, a_2, \ldots, a_n \in G$ olsun. Eğer G'deki her eleman $a_1, a_2, \ldots, a_n$ elemanları sayesinde elde ediliyorsa bu elemanlara G'nin üreteçleri denir ve $G = \langle a_1, a_2, \ldots, a_n \rangle$ şeklinde gösterilir [1].

Tanım 1.1.4 G bir grup olsun. Eğer G'nin elemanları bir $a \in G$ elemanı tarafından üretilebiliyorsa bu gruba devirli grup denir ve $G = \langle a \rangle$ ile gösterilir ve $\forall g \in G$ için $g = a^n$ olacak şekilde en az bir n doğal sayısı vardır [1].

Tanım 1.1.5 $R \neq \varnothing$ kümesi üzerinde tanımlı iki ikili işlem $+$ ve $.$ olsun. Aşağıdaki aksiyomları sağlayan $(R, +, .)$ cebirsel yapısına bir halka denir.

i. $(R, +)$ bir değişmeli gruptur.

ii. $.$ işleminin R üzerinde birleşme özelliği vardır.

iii. $.$ işleminin $+$ işlemi üzerine R' de sağdan ve soldan dağılma özellikleri vardır [1].

Tanım 1.1.6 R halkası üzerinde $\forall a, b \in R$ için $a.b = b.a$ olması durumunda R halkasına değişmeli halka, $\forall a \in R$ için $1_R.a = a.1_R = a$ olacak şekilde $1_R \in R$ varsa R halkasına birimli halka, 1_R'ye de halkanın birim elemanı denir [15].

Tanım 1.1.7 R halkasında, $0_R \neq a \in R$ elemanı için $ab = 0_R$ (veya $ba = 0_R$) olacak şekilde $\exists 0_R \neq b \in R$ bulunabilirse a'ya, halkanın sıfır böleni denir [1].

Tanım 1.1.8 Bir halkanın sıfır böleni yoksa o halkaya tam halka denir. Birimli, değişmeli ve sıfır bölensiz bir halkaya da tamlık bölgesi denir.

Tanım 1.1.9 R birimli ve değişmeli bir halka olsun. Eğer $R - \{0_R\} = R^*$ kümesi $.$ işlemine göre bir grup ise R'ye bir cisim denir [1].

Tanım 1.1.10 R bir halka ve $0 \neq S \subset R$ olsun. R üzerindeki işlemlere göre S alt kümesi de kendi başına bir halka oluşturuyorsa S halkasına R halkasının bir alt halkası denir [15].

Tanım 1.1.11 R bir halka ve $\varnothing \neq I \subseteq R$ olsun.

i. $\forall a,b \in I$ için $a-b \in I$ ve

ii. $\forall a \in I$ ve $\forall r \in R$ için, $ra \in I$ (veya $ar \in I$) ise I , R ' nin bir sol (veya sağ) ideali olarak adlandırılır. Hem sol ideal hem de sağ ideal oluyorsa iki taraflı ideal veya kısaca ideal denir [1].

Tanım 1.1.12 R bir halka olsun. I , R 'nin bir ideali olmak üzere $\forall a,b \in R$ için, R halkasının, bir I idealine göre denklik bağıntısı,

$$a \equiv b \left(\operatorname{mod} I\right) \Leftrightarrow a-b \in I$$

biçiminde tanımlanır [1].

Önerme 1.1.1 R halkasının, bir I idealine göre tanımlanan $\equiv$ bağıntısı, R ' de bir denklik bağıntısıdır. $r \in R$ 'nin denklik sınıfı da

$$\overline{r} = r + I = \left\{r + a : a \in I\right\}$$

dır. Bütün denklik sınıfları kümesi R/I ile gösterilir [1].

Önerme 1.1.2 I , R halkasının bir ideali olsun. I idealine göre tanımlanan denklik sınıfları arasında;

$$\left(a+I\right) \oplus \left(b+I\right) = \left(a+b\right)+I \,, \qquad \left(a+I\right) \otimes \left(b+I\right) = \left(ab\right)+I$$

ile tanımlanan $\oplus$ ve $\otimes$ işlemlerine göre R/I bir halkadır. Bu halkaya R'nin I idealine göre bölüm halkası denir [1].

Tanım 1.1.13 R ve S iki halka olsun. $\forall a,b \in R$ için $f : R \to S$ fonksiyonu aşağıdaki şartı sağlıyorsa bir halka homomorfizması denir [15].

$$f(a+b) = f(a) + f(b) \text{ ve } f(ab) = f(a)\,f(b)$$

Tanım 1.1.14 $f : R \to S$ halka homomorfizması birebir ve örten olma özelliklerini sağlarsa f'ye bir izomorfizma denir. R ve S halkalarına da izomorf halkalar denir ve $R \cong S$ ile gösterilir [1].

Tanım 1.1.15 R değişmeli ve birimli bir halka ve $(1) \neq M$'de R'nin bir ideali olsun. R'nin, M'yi kapsayan M ve R'den başka hiçbir ideali yoksa, M'ye R'nin bir maksimal ideali denir [1].

Tanım 1.1.16 M, R'nin (1) den farklı bir ideali olsun. M'nin maksimal olması için gerek ve yeter şart $\forall x \in R - M$ için, $M + (x) = R$ olmasıdır [1].

Tanım 1.1.17 $(M,+)$ bir değişmeli grup ve R değişmeli ve birimli bir halka olsun. M'deki elemanların, R'deki elemanlarla skaler çarpımı olan, $R \times M \to M$ fonksiyonu aşağıdaki koşulları sağlıyorsa, M'ye R üzerinde bir modül veya kısaca, $R-$ modül denir [16].

i. $\forall r \in R$ ve $\forall m, m' \in M$ için, $r(m+m') = rm + rm'$,

ii. $\forall r, r' \in R$ ve $\forall m \in M$ için, $(r+r')m = rm + r'm$,

iii. $\forall r, r' \in R$ ve $\forall m \in M$ için, $(rr')m = r(r'm)$,

iv. $\forall m \in M$ için, $1_R m = m$.

Tanım 1.1.18 R halkasının I ve J idealleri için, $I+J=R$ ise I ve J ideallerine aralarında maksimal idealler denir [16].

Teorem 1.1.1 (Çinlilerin Kalan Teoremi) $n \geq 2$ olmak üzere, $I_1, I_2, \ldots, I_n$ ler R halkasının, ikişer ikişer aralarında maksimal idealleri olsunlar. O zaman

i. Eğer $a_1, a_2, \ldots, a_n$ R'nin elemanları ise herhangi bir $a \in R$ vardır, öyle ki

$$a \equiv a_i \pmod{I_i}, \qquad i = 1, 2, \ldots, n$$

ii. $f(a) = (a + I_1, a + I_2, \ldots, a + I_n)$ ile tanımlı

$$f : R \to R/I_1 \times R/I_2 \times \ldots \times R/I_n$$

fonksiyonu bir örten homomorfizmadır.

iii. $R\Big/\bigcap_{i=1}^{n} I_i \cong \prod_{i=1}^{n} R/I_i$ izomorfturlar [16].

Tanım 1.1.19 Sonlu ve değişmeli bir halkanın idealleri birbirlerini kapsamaya göre doğrusal sıralı ise bu halkaya sonlu zincir halkası denir [23].

Tanım 1.1.20 R bir halka, x bir bilinmeyen ve $a_0, a_1, \ldots, a_n$ ler R'nin elemanları olmak üzere

$$a_0 + a_1 x + \ldots + a_n x^n$$

olarak tanımlanan ifadeye R'den katsayılı bir polinom denir. Katsayıları R'den alınan bütün polinomlar kümesi de $R[x]$ ile gösterilir [1].

Tanım 1.1.21 $\rho(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ ve $a_n \neq 0$ ise a_n ye polinomun baş katsayısı ve n ye de polinomun derecesi denir [1].

Önerme 1.1.3 R bir halka ise $R[x]$ de bir halkadır [1].

Önerme 1.1.4 R bir halka olsun.

i. R birimli bir halka ise $R[x]$ de birimli,

ii. R değişmeli bir halka ise $R[x]$ de değişmeli,

iii. R tamlık bölgesi ise $R[x]$ de tamlık bölgesi olur [1].

Tanım 1.1.22 Bir R tamlık bölgesinin bütün elemanlarını bölen R'nin bir elemanına birimsel eleman veya aritmetik birim denir [1].

Tanım 1.1.23 f, $R[x]$'te bir polinom olmak üzere f sıfır bölen değil ise f'ye regüler polinom denir [17].

Tanım 1.1.24 F bir cisim, f 'de $F[x]$'de bir polinom olsun. $a_i \in F$ olmak üzere,

$$f(x) = \sum_{i=0}^{n} a_i x_i$$

yazılsın. $a_n = 1$ olması durumunda f polinomuna monik polinom denir [14].

Tanım 1.1.25 f ve g polinomları $R[x]$'te sıfırdan farklı polinomlar olsun. g regüler polinom ise $f = gq + r$, $der(r) < der(g)$ olacak şekilde $q, r \in R[x]$ vardır. Bu ifade Öklid algoritması olarak adlandırılmaktadır [17].

1.2. Lineer Kodlar

Tanım 1.2.1 F cismi üzerinde tanımlı olan ve elemanları vektörler olan V kümesi aşağıdaki aksiyomları sağladığı durumda V kümesine bir vektör uzayı denir [18].

i. V kümesi toplama işlemine göre değişmeli gruptur.

ii. $\forall m \in F$ ve $u \in V$ için $mu \in V$ dir.

iii. $\forall m,n \in F$ ve $\forall u,v \in V$ için $m(u+v) = mu + mv$ ve $(m+n)v = mv + nv$ dir.

iv. $\forall m,n \in F$ ve $\forall u \in V$ için $(mn)u = m(nu)$ dir.

v. $\forall u \in V$ için $1u = u$ dur.

Tanım 1.2.2 V bir vektör uzayı ve $0 \neq Y \subset V$ olsun. Eğer Y, bütün vektör uzayı olma aksiyomlarını sağlıyorsa Y'ye V'nin bir alt uzayı denir [18].

Teorem 1.2.1 V bir vektör uzayı ve $0 \neq Y \subset V$ olsun. Y, aşağıdaki aksiyomları sağladığı durumda V vektör uzayının bir alt uzayıdır[18].

i. $\forall x,y \in Y$ için $x + y \in Y$ dir.

ii. $\forall a \in F$ için $ax \in Y$ dir.

Tanım 1.2.3 k_i'ler birer skaler olmak üzere, n tane $v_1, v_2, \ldots, v_n$ vektörlerinin birleşimi

$$v = k_1 v_1 + k_2 v_2 + \ldots + k_n v_n$$

şeklindedir. Eğer $A = \{v_1, v_2, \ldots, v_n\}$ ise A kümesinin tüm lineer birleşimlerinin kümesi $Sp(A)$ ile ifade edilir. Ayrıca $Sp(A)$, V vektör uzayının bir alt uzayıdır[18].

Tanım 1.2.4 $A=\{v_1,v_2,\ldots,v_n\}$ olsun. A kümesinin tüm lineer birleşimlerinin kümesi $Sp(A)$ olmak üzere, $Sp(A)$ uzayına A kümesinin gerdiği (ürettiği) alt uzay denir. A kümesine de $Sp(A)$ alt uzayının bir üreteci denir [18].

Tanım 1.2.5 V vektör uzayında $v_1,v_2,\ldots,v_n$ vektörleri verilsin. $\{v_1,v_2,\ldots,v_n\}$ vektörlerinin kümesinin lineer bağımlı olması için $k_1v_1+k_2v_2+\ldots+k_nv_n=0$ olacak şekilde en az biri sıfırdan farklı olan $k_1,k_2,\ldots,k_n$ sayılarının var olması gerekir. Eğer, $k_1v_1+k_2v_2+\ldots+k_nv_n=0\Rightarrow k_1=k_2=\ldots=k_n=0$ ise $\{v_1,v_2,\ldots,v_n\}$ vektörlerinin kümesi lineer bağımsızdır denir [19].

Tanım 1.2.6 V vektör uzayı ve $A=\{v_1,v_2,\ldots,v_n\}$ olsun. Eğer A kümesinin V 'nin bir tabanı veya bazı olması için aşağıdaki koşulları sağlaması gerekir.

i. A lineer bağımsız bir kümedir.
ii. A, V 'yi geren bir kümedir [19].

Tanım 1.2.7 V vektör uzayının tabanlarının herhangi birindeki tüm vektörlerinin sayısına V 'nin boyutu denir [18].

Tanım 1.2.8 $A=\{a_1,a_2,\ldots,a_q\}$ sonlu cümlesine $q-$lu alfabe ya da kısaca alfabe denir. A^n kümesine, A cümlesinin elemanlarından elde edilen $n-$lilerin oluşturduğu sözler ailesi denir. A^n 'nin herhangi bir C alt kümesine $q-$lu blok kodu denir. C 'nin elemanlarına ise kodsöz denir. $C\subset A^n$'nin M tane elemanı varsa C ye n uzunluğunda, M büyüklüğünde bir kod denir ve (n,M) parametreleri ile gösterilir [12].

Tanım 1.2.9 u ve v aynı uzunlukta ve aynı alfabe üzerinde tanımlanmış $n-$liler olsun. u ile v' nin farklı bileşenlerinin sayısına u ile v arasındaki Hamming mesafesi denir ve $d(u,v)$ ile gösterilir. $d: A^n \times A^n \to \mathbb{N}$, $d(u,v) = \{i : u_i \neq v_i, 1 \leq i \leq n\}$ olmak üzere (A^n, d) ikilisi bir metrik uzay oluşturur [20].

Tanım 1.2.10 (n,M) parametrelerine sahip bir C kodunun minimum mesafesi $d(C)$ ile gösterilir ve $d(C) = \min_{\forall u,v \in C} d(u,v)$ şeklinde tanımlanır. n uzunluğunda, M elemanına sahip ve minimum mesafesi d olan bir kod kısaca (n,M,d) şeklinde gösterilir [20].

Tanım 1.2.11 (X,d_1) ve (Y,d_2) iki metrik uzay ve $f: X \to Y$ bir dönüşüm olmak üzere $\forall x, y \in X$ için

$$d_2(f(x), f(y)) = d_1(x,y)$$

şeklinde bir eşitlik sağlanırsa, f dönüşümüne izometri denir. Yani f dönüşümü metrik uzaylardaki elemanlar arası uzaklıkları koruyorsa izometri olarak adlandırılır [21].

Tanım 1.2.12 q elemanlı F_q cismi üzerinde bulunan n uzunluklu bütün vektörlerden oluşan F_q^n kümesi bir vektör uzayıdır ve bu vektör uzay $V(n,q)$ ile gösterilir. C kümesi $V(n,q)$ vektör uzayının k boyutlu bir alt uzayı olsun. C' ye k boyutlu ve n uzunluğunda bir lineer kod denir ve $[n,k]$ ile gösterilir. Eğer C kodunun minimum mesafesi d ise bu kod $[n,k,d]$ parametreleri ile gösterilir. $c \in C$'nin Hamming ağırlığı bu koddaki sıfırdan farklı bileşenlerin sayısı olarak tanımlanır ve $w(c)$ biçiminde gösterilir. C' nin sıfır vektörü hariç geri kalan ağırlıklarının en

küçüğüne ise C kodunun minimum ağırlığı denir ve $w(C)$ ile gösterilir. Lineer kodlarda $d(C) = w(C)$'dir [12].

Tanım 1.2.13 V vektör uzayı aşağıdaki şartları sağlıyorsa V vektör uzayına bir iç çarpım uzayı denir [18].

k bir skaler ve $u, v, w \in V$ olmak üzere;

i. $\langle u, u \rangle \geq 0; u = 0_V \Rightarrow \langle u, u \rangle = 0$

ii. $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$ ve $\langle u + v, w \rangle = \langle u, \mathrm{w} \rangle + \langle \mathrm{v}, w \rangle$

iii. $\langle ku, v \rangle = k \langle u, \mathrm{v} \rangle$ ve $\langle u, kv \rangle = k \langle u, \mathrm{v} \rangle$

Tanım 1.2.14 V iç çarpım uzayı olmak üzere $u, v \in V$ için $\langle u, \mathrm{v} \rangle = 0$ ise u vektörü, v vektörüne diktir (veya ortogonaldir) denir [18].

Tanım 1.2.15 $V(n, q)$ vektör uzayında doğal bir iç çarpım tanımlı olsun. $u = (u_1, u_2, \ldots, u_n), v = (v_1, v_2, \ldots, v_n) \in V(n, q)$ için u ile v'nin iç çarpımı

$$\langle u, \mathrm{v} \rangle = \sum_{i=1}^{n} u_i v_i$$

şeklinde tanımlanır [12].

Tanım 1.2.16 C kodu bir $[n, k]$ lineer kod olsun.

$$C^{\perp} = \{u \in V(n, q) : \langle u, v \rangle = 0, \forall v \in C\}$$

kümesine C kodunun diki (duali) denir [12].

Tanım 1.2.17 C kodu bir $[n,k]$ lineer kod olsun. Eğer bir D matrisi C kodunun bazlarından oluşan $k \times n$ tipinde bir matris ise bu D matrisine C kodunun üreteç matrisi denir [12].

Teorem 1.2.2 F_q cismi üzerinde bir lineer $[n,k,d]$ kodu verildiğinde, ilk k sütunu k boyutlu I_k birim matrisi olan $G=[I_k, A]$ standart formda ki üreteç matrisine sahip bir koda denktir [12].

Teorem 1.2.3 C kodu $G=[I_k, A]$ standart formdaki üreteç matrisine sahip $[n,k]$ parametreli bir lineer kod ise C 'nin diki de $H=\left[-A^{tr}, I_{n-k}\right]$ üreteç matrisine sahip bir $[n,n-k]$ lineer kod olur. H matrisine C kodunun kontrol matrisi denir [12].

Tanım 1.2.18 $q>1$ olmak üzere, q boyutlu bir kod alfabesi A, n ve d değerleri verilsin. A üzerinde mümkün olan en büyük boyuta sahip bir $(n,M,d)-$kodu $A_q(n,d)$ olsun. Bu durumda

$$A_q(n,d) = max\{\, M : A \text{ üzerinde bir } [n,M,d]-\text{kodu mevcuttur.}\}$$

maksimum boyutlu herhangi bir $(n,M,d)-C$ koduna $\left(M = A_q(n,d)\right)$ optimal kod denir [13].

Tanım 1.2.21 R 'de n uzunluğunda bir C kodu için, C 'nin üreteçlerinin en küçük sayısına rank denir ve $rank(C)$ ile gösterilir [22].

1.3. Devirli Kodlar

Tanım 1.3.1 $V(n,q)$, elemanları F_q cisminden alınan $n-$li elemanların oluşturduğu bir vektör uzayıdır [12].

Tanım 1.3.2 Eğer $(c_0,c_1,\ldots,c_{n-1})\in C$ iken $(c_{n-1},c_0,\ldots,c_{n-2})\in C$ oluyorsa $C\subset V(n,q)$ lineer koduna devirli kod denir [12].

Önerme 1.3.1 $R_n=F_q[x]/\langle x^n-1\rangle$ polinom halkası bir temel ideal halkasıdır.

$$\theta: V(n,q)\to R_n$$

$$(u_0,u_1,\ldots,u_{n-1})\to u_0+u_1 x+\ldots+u_{n-1}x^{n-1}$$

olarak bir izomorfizma tanımlansın. Bu izomorfizma kullanılarak iki kodsözün çarpımı sağlanmış olur. C, n uzunluğunda bir devirli kod ise $\theta(C)$, R_n'de bir ideal olur [12].

Teorem 1.3.1 C, R_n'de bir ideal olsun. Bu durumda C, n uzunluğunda bir devirli kod olmak üzere,

i. C'de derecesi minimum olacak şekilde tek bir monik polinom $g(x)$ vardır. Bu polinomdan üretilen ideal de C koduna karşılık gelir. Bu $g(x)$ polinomuna da C kodunun üreteç polinomu denir.

ii. $g(x)$ polinomu x^n-1 polinomu böler.

iii. $g(x) = g_0 + g_1 x + \ldots + g_r x^{n-r}$ polinomu bir devirli kodun üreteci ise $g_0 \neq 0$ olur ve bu polinomun ürettiği kod;

$$G = \begin{pmatrix} g_0 & \ldots & g_r & 0 & 0 & 0 & 0 \\ 0 & g_0 & \ldots & g_r & 0 & 0 & 0 \\ 0 & 0 & g_0 & \ldots & g_r & 0 & 0 \\ 0 & 0 & 0 & g_0 & \ldots & g_r & 0 \\ 0 & 0 & 0 & 0 & g_0 & \ldots & g_r \end{pmatrix}$$

matrisinin ürettiği koda karşılık gelir [12].

Önerme 1.3.2 $p(x)$ polinomu R_n' de monik bir polinom olsun. $p(x)$ polinomunun bir devirli C kodunun üreteci olabilmesi için gerek ve yeter şart $p(x) \mid x^n - 1$ olmasıdır. R_n' de bir devirli kodun üreteç polinomu olan $p(x)$, $x^n - 1$ polinomunu böldüğünden $x^n - 1 = g(x)h(x)$ olur. $h(x)$ polinomuna C' nin kontrol polinomu denir [12].

Teorem 1.3.3 $h(x)$ polinomu R_n' de C devirli kodunun kontrol polinomu olsun. Bu durumda;

i. C devirli kodu

$$C = \left\{ p(x) \in R_n : p(x)h(x) \equiv 0 \bmod \left(x^n - 1\right) \right\}$$

olarak tanımlanır.

ii. Eğer $h(x)=h_0+h_1x+\ldots+h_{n-r}x^{n-r}$ ise bu durumda C kodunun kontrol matrisi

$$H=\begin{pmatrix} h_{n-r} & \ldots & h_0 & 0 & 0 & 0 & 0 \\ 0 & h_{n-r} & \ldots & h_0 & 0 & 0 & 0 \\ 0 & 0 & h_{n-r} & \ldots & h_0 & 0 & 0 \\ 0 & 0 & 0 & h_{n-r} & \ldots & h_0 & 0 \\ 0 & 0 & 0 & 0 & h_{n-r} & \ldots & h_0 \end{pmatrix}$$

olur.

iii. C kodunun diki olan $C^{\perp}$ kodu da r boyutlu bir devirli koddur ve

$$h^{\perp}=h_0^{-1}x^{n-r}h\left(x^{-1}\right)$$

polinomu $C^{\perp}$'in üreteç polinomudur [12].

Tanım 1.3.3 C kodu $g(x)$ polinomu ile üretilen $[n,n-r]$ parametreli bir devirli kod ve $g(x)$ polinomunun derecesi r olsun. Bir $u(x)$ polinomunun sendromu $S(u(x))$ ile gösterilir ve bu sendrom $u(x)$ polinomunun $g(x)$ polinomuna bölümünden elde edilen kalana eşittir. Yani

$$u(x)=q(x)g(x)+S(u(x)),\ der(S(u(x)))<1$$

dir [12].

BÖLÜM 2. $F_4 + vF_4$ HALKASI ÜZERİNDEKİ DEVİRLİ KODLARDAN KUANTUM KOD ELDE ETME

Lineer kodların cebirsel kodlama teorisi 20. Yüzyılın son yarısında kayda değer bir gelişme göstermiştir. Cisimler üzerindeki lineer kodlar için birçok makale yazılmıştır. Özellikle basit pratiksel uygulamalarından dolayı binary (ikili) kodlar üzerinde çalışılmıştır. Devirli kodlar lineer kodların bir alt ailesi olup cebirsel yapısı ve pratikteki özellikleri ile lineer kodların önemli bir kısmını oluşturur. Kuantum hata düzeltebilen kodlar, artan kuantum bilgisayarların icadı ile oluşan sorunlara çözüm üretmiştir. Bu konuda ilk hata düzeltebilen kuantum kod Shor tarafından üretilmiştir [11]. Sonra Steane basit bir kuantum hata düzeltebilen kod üzerine çalışma yapmıştır [3]. Daha sonra Calderbank, Rains, Shor ve Sloane yaygın olarak kullanılan klasik hata düzeltebilen kodlar sayesinde kuantum kod üretmiştir [2]. Son zamanlarda q bir asalın kuvveti olmak üzere F_q cismi üzerindeki devirli kodlar sayesinde kuantum hata düzeltebilen kodlar üretilmiştir. [6] da Qian tarafından $F_2 + uF_2$, $u^2 = 0$ sonlu halkası üzerinde hata düzelten kuantum kodlar için bir teknik vermiştir. [7] de Kai ve Zhu tarafından n tek olmak üzere $F_4 + uF_4$, $u^2 = 0$ sonlu zincir halkasında n uzunluğundaki devirli kodlar sayesinde kuantum kod üretilmiştir. Qian, $F_2 + vF_2$, $v^2 = v$ sonlu halkası üzerindeki devirli kodlardan yeni bir teknik vermiştir [5]. Bu makaleden yola çıkarak M. Ashraf $F_3 + vF_3$, $v^2 = 1$ sonlu halkası üzerindeki devirli kodlardan benzer bir hata düzeltebilen kod yapısı vermiştir [8].

Bu çalışmada $F_4 + vF_4$, $v^2 = v$ sonlu halkası üzerindeki devirli kodlar sayesinde F_4 üzerinde kuantum kodlar elde edilecektir. $F_4 + vF_4$, $v^2 = v$ sonlu halkası üzerindeki

devirli kodların yapısı ve bu halkanın $F_4 \times F_4$ e izomorf olduğu A. Bayram tarafından [9] da verilmiştir. Bu çalışmada da $F_4 + vF_4,\ v^2 = v$ sonlu halkası üzerindeki devirli ve lineer kodların Gray görüntülerinden F_4 üzerinde kendine dik kodlar üretilecektir. $F_4 + vF_4,\ v^2 = v$ sonlu halkası üzerindeki devirli kodların kendine dik kodları içermesi için bir koşul verilecektir. Çalışmanın sonunda hata düzeltebilen kuantum kodların parametreleri verilecektir. Bunlardan bazıları [10]'daki tabloya gore optimal kodlardır.

2.1. $F_4 + vF_4$ Halkası Üzerindeki Lineer Kodlar

Tanım 2.1.1 $R = F_4 + vF_4 = \{0,1,w,w^2,v,1+v,w+v,w^2+v,wv,1+wv,w+wv$ $w^2+wv, w^2v, 1+w^2v, w+w^2v, w^2+w^2v\}$ olarak R halkasının tüm elemanlarını gösteririz. Burada $v^2 = v$, $F_4 = \{0,1,w,w^2\}$ ve $w^2 = w+1$ dir. R, 16 elemanı ile zincir oluşturmayan bir sonlu halkadır.

Tanım 2.1.2 R halkasının bütün idealleri;

i. $R = (1) = (w) = (w+1) = (v+w) = (1+v+w) = (1+vw)$
$= (1+v+vw) = (1+w+vw) = (v+w+vw)$

ii. $(v) = (vw) = (v(w+1)) = \{0, v, vw, v(w+1)\}$,

iii. $(v+1) = ((v+1)w) = ((v+1)(w+1)) = \{0, v+1, (v+1)w, (v+1)(w+1)\}$,

iv. $(0) = \{0\}$

şeklindedir. Ayrıca R halkası,

$(v) = \{0, v, vw, v(w+1)\}$ ve $(v+1) = \{0, v+1, (v+1)w, (v+1)(w+1)\}$

maksimal ideallerine sahiptir. Çinlilerin Kalan Teoreminden

$$R \cong F_4[v]/(v+1) \oplus F_4[v]/(v) \cong F_4 \oplus F_4 \cong \langle v \rangle + \langle v+1 \rangle$$

olacağından R'nin her elemanını $\exists x, y \in F_4$ için $x + vy = v(x+y) + (v+1)x$ olarak tek türlü gösterilebilmesi anlamına gelmektedir [9].

Tanım 2.1.3 $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ ve $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$ R^n'nin herhangi iki elemanı olsun. R^n'de γ ve δ elemanlarının Öklid iç çarpımları

$$\gamma \cdot \delta = \gamma_1\delta_1 + \gamma_2\delta_2 + \ldots + \gamma_n\delta_n$$

olarak tanımlanır [12].

Tanım 2.1.4 R'nin birim grubu, dir. Buradan $U_R = \{1, w, w+1, v+w, 1+w+v, 1+vw$ $1+v+vw, 1+w+vw, v+w+vw\}$ dir. 9 elemanlı U_R kümesi $Z_3 \times Z_3$ ile izomorf olurlar [9].

Tanım 2.1.5 R üzerindeki n uzunluğunda bir C kodunun dik kodu;

$$C^{\perp} = \left\{ \delta \in R^n \middle| \langle \gamma, \delta \rangle = 0, \forall \gamma \in C \right\}$$

olarak tanımlanır. Eğer $C \subseteq C^{\perp}$ ise C koduna kendine dik, eğer $C = C^{\perp}$ ise kendine dual kod denir [12].

2.2. $F_4 + vF_4$ Halkası Üzerindeki Lineer Kodlar İçin Gray Dönüşümü

Bu bölümde $F_4 + vF_4$ halkası üzerindeki devirli kodlardan kuantum kod elde edilme yöntemi verilmektedir. Bundan sonraki bölümlerde $F_4 + vF_4$ halkası R ile gösterilecektir ve $v^2 = v$ alınacaktır.

$R = F_4 + vF_4$ halkasının her elemanı $a, b \in F_4$ olmak üzere $a + vb$ şeklinde tanımlanır. R'den F_4^2 üzerine bir ψ Gray Dönüşümü ;

$$\psi(a + vb) = (a + b, a)$$

olarak tanımlansın. Burada ψ lineer olup R^n'den F_4^{2n} üzerine genişletilebilir.

Önerme 2.2.1 ψ Gray dönüşümü bir izomorfizmadır.

İspat r ve r', R nin iki elemanı olsun. $r = a + vb$ ve $r' = a' + vb'$ olmak üzere

$$\begin{aligned}
\psi(r + r') &= \psi\left(a + a' + v(b + b')\right) \\
&= (a + a' + b + b', a + a') \\
&= (a + b, a) + (a' + b', a') \\
&= \psi(r) + \psi(r')
\end{aligned}$$

olur. Diğer taraftan

$$\begin{aligned}\psi(rr') &= \psi\big((a+vb)(a'+vb')\big)\\ &= \psi\left(aa'+ab'v+ba'v+bb'v\right)\\ &= \psi\left(aa'+\left(ab'+ba'+bb'\right)v\right)\\ &= \left(aa'+ab'+ba'+bb', aa'\right)\\ &= \big((a+b)(a'+b'), aa'\big)\\ &= \big((a+b), a\big)\big((a'+b'), a'\big)\\ &= \psi(r)\psi(r')\end{aligned}$$

olduğundan ψ Gray dönüşümü bir homomorfizma olur. Birebir ve örtenlik kısmı kolaylıkla görülebileceğinden dolayı ψ Gray dönüşümü bir izomorfizma olur.

Bu çalışmada herhangi bir $x \in R$'nin Lee ağırlığı $w_L(x) = w_H\left(\psi(x)\right)$ olarak tanımlanacaktır. Herhangi $x, y \in R$ içinde Lee uzaklık $d_L(x,y) = w_L(x-y)$ olarak tanımlanır [24].

Teorem 2.2.1 (R^n, Lee uzaklık)'tan (F_4^{2n}, Hamming uzaklık)'a tanımlanan Gray dönüşümü bir izometridir.

İspat Herhangi $x_{1,}x_2 \in R$ ve $\lambda \in F_4$ için $\psi(x_1+x_2) = \psi(x_1)+\psi(x_2)$ ve $\psi(\lambda x_1) = \lambda\psi(x_1)$ olduğundan ψ lineer olur. Tanımdan,

$$d_L(x_{1,}x_2) = w_L(x_1-x_2) = w_H\left(\psi(x_1-x_2)\right) = w_H\left(\psi(x_1)-\psi(x_2)\right) = d_H\left(\psi(x_1)-\psi(x_2)\right)$$

olarak elde edilir. Dolayısıyla ψ 'nin uzaklık koruduğu gösterilmiş olur.

Önerme 2.2.2 R üzerinde n uzunluğunda bir C kodu için eğer C kendine dik olursa o zaman $\psi(C)$ kodu da kendine dik olur.

İspat $c_1 = \gamma_1 + v\delta_1$ ve $c_2 = \gamma_2 + v\delta_2 \in C$ olsun, burada $\gamma_1, \delta_1, \gamma_2, \delta_2 \in F_4^n$ ' dir. O zaman c_1 ve c_2 nin Öklid İç Çarpımından;

$$c_1 c_2 = \gamma_1\gamma_2 + (\gamma_1\delta_2 + \gamma_2\delta_1 + \delta_1\delta_2)v$$

olur. C kendine dik olduğundan $\gamma_1\gamma_2 = \gamma_1\delta_2 + \gamma_2\delta_1 + \delta_1\delta_2 = 0$ olur.

Diğer taraftan

$$\psi(c_1)\psi(c_2) = (\gamma_1 + \delta_1, \gamma_1)(\gamma_2 + \delta_2, \gamma_2) = (\gamma_1\gamma_2 + \gamma_1\delta_2 + \gamma_2\delta_1 + \delta_1\delta_2, \gamma_1\gamma_2)$$

olur. Böylece $\psi(C)$ koduda kendine dik olur.

Tanım 2.2.1 A_1 ve A_2 iki lineer kod olmak üzere bu kodların direk ve kartezyen çarpımları sırasıyla,

$$A_1 \otimes A_2 = \{(a_1, a_2) \mid a_1 \in A_1, a_2 \in A_2\} \text{ ve } A_1 \oplus A_2 = \{a_1 + a_2 \mid a_1 \in A_1, a_2 \in A_2\}$$

olarak tanımlanır. C , R üzerinde n uzunluğunda lineer bir kod olmak üzere

$$C_1 = \{a + b \in F_4^n \mid (a+b)v + a(v+1) \in C, \exists a, b \in F_4^n\}$$

ve

$$C_2 = \left\{ a \in F_4^n \middle| (a+b)v + a(v+1) \in C, \exists a,b \in F_4^n \right\}$$

için C_1 ve C_2 kodları F_4 üzerinde lineer kodlar olarak tanımlayalım [9].

Teorem 2.2.2 C, R üzerinde n uzunluğunda lineer bir kod olsun. $\psi(C) = C_1 \otimes C_2$ olur ve $|C| = |C_1||C_2|$ olur.

İspat $C_1 = \left\{ a+b \in F_4^n \middle| (a+b)v + a(v+1) = a + vb \in C, \exists a,b \in F_4^n \right\}$ ve $C_2 = \left\{ a \in F_4^n \middle| (a+b)v + a(v+1) = a + vb \in C, \exists a,b \in F_4^n \right\}$ olsun. $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in \psi(C)$ ve $i = 1,2,\ldots,n$ için $c_i = r_i v + q_i(1+v) = q_i + (q_i + r_i)v$ olarak alınabilir. ψ birebir ve örten olduğundan $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ olur. C_1 ve C_2 kodlarının tanımından dolayı $r = (r_1, r_2, \ldots, r_n) \in C_1$ ve $q = (q_1, q_2, \ldots, q_n) \in C_2$ olur. Böylece $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in C_1 \otimes C_2$ olur. Yani $\psi(C) \subseteq C_1 \otimes C_2$ olur. Diğer taraftan herhangi $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in C_1 \otimes C_2$ olarak alınsın. $a = (a_1, a_2, \ldots, a_n)$ ve $b = (b_1, b_2, \ldots, b_n)$, C kodunun elemanları olmak üzere $1 \le i \le n$ için $m_i, n_i \in F_4$ elemanları $a_i = q_i + vm_i$ ve $b_i = r_i + (1+v)n_i$ olacak şekilde vardır. C lineer bir kod olduğundan dolayı

$$\begin{aligned} c &= (1+v)a + vb \\ &= (1+v)(q+vm) + v(r+n+nv) \\ &= q + qv + vm + v^2 m + vr + vn + v^2 n \\ &= q + qv + vm + vm + vr + vn + vn \end{aligned}$$

$$= q + (q + r)v$$

olup C nin elemanı olur. $\psi(c) = (q + q + r, q) = (r, q) = (r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n)$ olur. $C_1 \otimes C_2 \subseteq \psi(C)$ olur. Böylece $\psi(C) = C_1 \otimes C_2$ olur. Diğer taraftan $|C| = |\psi(C)| = |C_1 \otimes C_2| = |C_1||C_2|$ olarak elde edilir.

Sonuç 2.2.1 G_1 ve G_2 sırasıyla C_1 ve C_2 kodlarının üreteç matrisleri olsun. O zaman C kodunun üreteç matrisi

$$\begin{pmatrix} vG_1 \\ (1+v)G_2 \end{pmatrix}$$

olur.

İspat: Eğer G_1 ve G_2 sırasıyla C_1 ve C_2 kodlarının üreteç matrisleri ise o zaman $\psi(C) = C_1 \otimes C_2$ nin üreteç matrisi

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

olur. Teorem 2.2.1 den dolayı C matrisinin üreteç matrisi

$$\begin{pmatrix} vG_1 \\ (1+v)G_2 \end{pmatrix}$$

olur.

Sonuç 2.2.2 Eğer $\psi(C) = C_1 \otimes C_2$ ise o zaman C kodu $C = vC_1 \oplus (1+v)C_2$ olacak şekilde tek türlü yazılabilir [4].

Önerme 2.2.3 d_H ve d_L sırasıyla R üzerindeki C lineer kodunun Hamming uzaklığı ve Lee uzaklığı olsunlar. O zaman $d(C_i)$, C_i kodunun minimum uzaklığı olmak üzere $d_H = d_L = \min\{d(C_1), d(C_2)\}$ olur .

İspat ψ dönüşümü uzaklık koruduğundan dolayı $d_H(\psi(C)) = d_H(C_1 \otimes C_2) = \min\{d(C_1), d(C_2)\} = d_L$ olur ve $d_H = d_L$ olduğu görülür.

Önerme 2.2.4 $C^{\perp}$, C kodunun dual kodu olsun. O zaman $\psi(C^{\perp}) = \psi(C)^{\perp}$ olur.

İspat $r_1, r_2, q_1, q_2 \in F_4^n$ olmak üzere $c_1 = r_1 + vq_1 \in C$ ve $c_2 = r_2 + vq_2 \in C^{\perp}$ olsun. $c_1.c_2 = 0$ olduğundan $r_1r_2 = r_1q_2 + r_2q_1 + q_1q_2 = 0$ olur. Buradan $\psi(c_1).\psi(c_2) = 2r_1r_2 + r_1q_2 + r_2q_1 + q_1q_2 = 0$ olarak elde edilir. Dolayısıyla $\psi(C^{\perp}) \subseteq \psi(C)^{\perp}$ elde edilir.Diğer taraftan $|C| = 16^{k_1}4^{k_2}4^{k_3}$ ve $|\psi(C)| = |C|$ olması bakımından $\psi(C)$, $[2n, 4k_1 + 2k_2 + 2k_3]$ parametrelerine sahip bir lineer kod olur. Buradan $|\psi(C)^{\perp}| = 2^{2n-4k_1-2k_2-2k_3}$ olur ve $|\psi(C)^{\perp}| = |C^{\perp}| = 4^n/|C| = 2^{2n-4k_1-2k_2-2k_3}$ olarak elde edilir. Böylece $\psi(C^{\perp}) = \psi(C)^{\perp}$ olur.

Önerme 2.2.5 C, R üzerinde n uzunluğunda bir lineer kod ve $\psi(C)=C_1\otimes C_2$ olduğundan $C=vC_1\oplus(1+v)C_2$ olur. O zaman $\psi(C^{\perp})=C_1^{\perp}\otimes C_2^{\perp}$ ve $C^{\perp}=vC_1^{\perp}\oplus(1+v)C_2^{\perp}$ olarak elde edilir.

İspat Önerme 2.2.3'den $\psi(C^{\perp})=\psi(C)^{\perp}=(C_1\otimes C_2)^{\perp}$ olur. Sadece $C_1^{\perp}\otimes C_2^{\perp}=(C_1\otimes C_2)^{\perp}$ olduğunu göstermemiz yeterli olacaktır. $C_1^{\perp}\otimes C_2^{\perp}\subseteq(C_1\otimes C_2)^{\perp}$ olduğu açıktır. Diğer taraftan varsayalım ki sırasıyla C_1 ve C_2 kodları $[n,k_1]$ ve $[n,k_2]$parametrelerine sahip lineer kodlar olsunlar. O zaman $C_1^{\perp}$, $C_2^{\perp}$ ve $C_1\otimes C_2$ kodları sırasıyla $[n,n-k_1],[n,n-k_2]$ ve $[2n,k_1+k_2]$ parametrelerine sahip lineer kodlar olurlar. $|C_1^{\perp}\otimes C_2^{\perp}|=|C_1^{\perp}|.|C_2^{\perp}|=2^{2n-k_1-k_2}=|(C_1\otimes C_2)^{\perp}|$ olur. Böylece $C_1^{\perp}\otimes C_2^{\perp}=(C_1\otimes C_2)^{\perp}$ olarak elde edilir. Sonuç 2.2.1'den diğer sonucu da elde ederiz.

Önerme 2.2.6 $C=vC_1\oplus(1+v)C_2$ kodu R üzerinde *n* uzunluğunda bir lineer kod, C_i, $i=1,2$ için $[n,k_i,d(C_i)]$ parametrelerine sahip lineer kod olsunlar. O zaman $\psi(C)$, F_4 üzerinde $[2n,k_1+k_2,\min\{d(C_1),d(C_2)\}]$ parametrelerine sahip bir kod olur [24].

2.3. $F_4 + vF_4$ Halkası Üzerindeki Devirli Kodlar

Önerme 2.3.1 $C = vC_1 \oplus (1+v)C_2$ kodu $R = F_4 + vF_4$ üzerinde lineer bir kod olsun. C'nin R üzerinde bir devirli kod olması için gerek ve yeter şart C_1 ve C_2 kodlarının F_4 üzerinde devirli kod olmalarıdır.

İspat $i = 1,2,\ldots,n-1$ ve $c_i = r_i + vq_i$ olmak üzere $(c_0, c_1, \ldots, c_{n-1}) \in C$ olarak alalım. $r = (r_0, r_1, \ldots, r_{n-1})$ ve $q = (q_0, q_1, \ldots, q_{n-1})$ olarak alırsak $r + q \in C_1$, ve $r \in C_2$ olur. Eğer C_1 ve C_2 devirli kod olarak alınırsa $\sigma(r+q) \in C_1$ ve $\sigma(r) \in C_2$ olur. $c = v(r+q) + (1+v)r$ olarak yazılacağından dolayı $\sigma(c) = v\sigma(r+q) + (1+v)\sigma(r) \in C$ olup C de bir devirli kod olur. Diğer taraftan herhangi $r = (r_0, r_1, \ldots, r_{n-1}) \in C_1$ ve $q = (q_0, q_1, \ldots, q_{n-1}) \in C_2$ elemanları için $(c_0, c_1, \ldots, c_{n-1}) \in C$ ve $c_i = vr_i + (1+v)q_i = q_i + (q_i + r_i)v$ olarak tanımlanacağından dolayı eğer C bir devirli kod ise $\sigma(c) = \sigma(q) + v(\sigma(r) + \sigma(q))$ olur. $\psi(\sigma(c)) = (\sigma(r), \sigma(q)) \in C_1 \otimes C_2$ olacağından $\sigma(r) \in C_1$ ve $\sigma(q) \in C_2$ olur. Buradan da C_1 ve C_2 kodlarının devirli kod olduğu görülür.

Sonuç 2.3.1 C, R üzerinde bir devirli kod ise C'nin dual kodu olan $C^{\perp}$ de bir devirli kod olur.

İspat Önerme 2.2.5'den $C^{\perp} = vC_1^{\perp} \oplus (1+v)C_2^{\perp}$ dual kodu bir devirli kod olur ve Önerme 2.3.1'den $C^{\perp}$ de bir devirli kod olur.

Önerme 2.3.2 $C = vC_1 \oplus (1+v)C_2$, R üzerinde n uzunluğunda bir devirli kod olsun. O zaman $g_1(x)$ ve $g_2(x)$ sırasıyla C_1 ve C_2 kodlarının üreteç polinomları olmak üzere $C = \langle vg_1(x), (1+v)g_2(x) \rangle$ ve $|C| = 4^{2n-\deg(g_1(x))-\deg(g_2(x))}$ olarak elde edilir.

İspat $C_1 = \langle g_1(x) \rangle$, $C_2 = \langle g_2(x) \rangle$ ve $C = vC_1 \oplus (1+v)C_2$ olsun. Buradan $C = \{c(x) = vg_1(x)r_1(x) + (1+v)g_2(x)r_2(x); r_1(x), r_2(x) \in F_4[x]\}$ olarak alınırsa $C \subseteq \langle vg_1(x), (1+v)g_2(x) \rangle \subseteq R_n$ olarak elde edilir. Diğer taraftan $k_1(x), k_2(x) \in R_n$ olmak üzere herhangi bir $vg_1(x)k_1(x) + (1+v)g_2(x)k_2(x) \in \langle vg_1(x), (1+v)g_2(x) \rangle$ elemanını alalım. Burada her elemanı v katsayısını içereceğinden dolayı v parantezine alındığında tüm katsayıları $F_4[x]$'in elemanı olur. Aynı şekilde $(1+v)$ içinde düşünülürse $vk_1(x) = vr_1(x)$ ve $(1+v)k_2(x) = (1+v)r_2(x)$ olacak şekilde $r_1(x), r_2(x) \in F_4[x]$ vardır. Böylece $\langle vg_1(x), (1+v)g_2(x) \rangle \subseteq C$ olacak şekilde elde ederiz. Buradan da $C = \langle vg_1(x), (1+v)g_2(x) \rangle$ olur. $|C| = |C_1||C_2|$ olduğundan $|C| = 4^{2n-\deg(g_1(x))-\deg(g_2(x))}$ olarak elde edilir.

Önerme 2.3.3 C, R üzerinde n uzunluğunda bir devirli kod olsun. O zaman tek bir $g(x)$ polinomu, $C = \langle g(x) \rangle$ olacak şekilde vardır, burada $g(x) | x^n - 1$ ve $g(x) = vg_1(x) + (1+v)g_2(x)$ dir.

İspat Önerme 2.3.2'den $C = \langle vg_1(x), (1+v)g_2(x) \rangle$ olduğunu söyleyebiliriz. O zaman $g_1(x), g_2(x)$ polinomları sırasıyla C_1 ve C_2 kodlarının üreteç polinomları olmak üzere $g(x) = vg_1(x) + (1+v)g_2(x)$ olarak alalım. Buradan kolayca görülür ki $\langle g(x) \rangle \subseteq C$ dir. Diğer taraftan $vg_1(x) = vg(x)$ ve $(1+v)g_2(x) = (1+v)g(x)$ olarak

yazılacağından dolayı $C \subseteq \langle g(x) \rangle$ olur. Böylece $C = \langle g(x) \rangle$ olarak elde edilir. $g_1(x) \mid x^n - 1$ ve $g_2(x) \mid x^n - 1$ olduğundan dolayı $x^n - 1 = g_1(x) r_1(x) = g_2(x) r_2(x)$ olacak şekilde $r_1(x), r_2(x) \in R_n$ vardır. Buradan görülür ki

$$x^n - 1 = g(x)\left[v r_1(x) + (1+v) r_2(x) \right]$$

$$= g_2(x) r_2(x) + v\left(g_1(x) r_1(x) + g_2(x) r_2(x) \right)$$

$$= g_2(x) r_2(x)$$

olarak elde edilir. Böylece $g(x) \mid x^n - 1$ olur.

Sonuç 2.3.2 Önerme 2.3.3'den $C = vC_1 \oplus (1+v)C_2$ kodu R üzerinde n uzunluğunda bir devirli kod ise, o zaman $C^{\perp} = \langle v h_1^*(x) + (1+v) h_2^*(x) \rangle$ ve $|C^{\perp}| = 4^{\deg(g_1(x)) + \deg(g_2(x))}$ olur, burada $h_i(x) = x^n - 1 / g_i(x)$ ve $h_i^*(x) = x^{\deg(h_i(x))} h_i(x^{-1})$ olmak üzere $h_i^*(x)$, $h_i(x)$' in reciprocal polinomudur.

Teorem 2.3.1 C, $[n,k,d]$ parametrelerine ve C', $[n,k',d']$ parametrelerine sahip iki kod olsunlar. Eğer $C'^{\perp} \subseteq C$ ise o zaman $[n, k+k'-n, \min\{d,d'\}]$ parametrelerine sahip bir kuantum kod elde edilir. Özel olarak, eğer $C^{\perp} \subseteq C$ olarak alınırsa o zaman $[n, 2k-n, d]$ parametrelerine sahip bir kuantum kod elde edilir [5].

2.4. $F_4 + vF_4$ Halkası Üzerindeki Devirli Kodlardan Kuantum Kod Elde Edilmesi

Bu bölümde R üzerinde n uzunluğunda ki devirli kodlar kullanılarak F_4 üzerinde kendine dik kodlar elde edilmeye çalışılacaktır. Bu kendine dik kodlar kullanılarak kuantum kod parametrelerine karşılık gelen kodlar tanımlanacaktır.

Şimdi verilecek Lemma bir devirli kodun kendine dik olması için gerek ve yeter şartı verecektir.

Önerme 2.4.1 C, $g(x)$ üreteç polinomu ile bir devirli kod olsun. O zaman C kodunun kendi dualini kapsaması için gerek ve yeter koşul

$$x^n - 1 \equiv 0 \bmod \left(g(x) g^*(x) \right)$$

olmasıdır, burada $g^*(x)$ polinomu $g(x)$ polinomunun reciprocal polinomudur.

Şimdi R üzerinde bir devirli kodun kendi dualini içermesi için gerek ve yeter şartı vereceğiz.

Teorem 2.4.1 $C = \langle g(x) \rangle$, R üzerinde n uzunluğunda bir devirli kod olsun, burada $g(x) = vg_1(x) + (1+v) g_2(x)$ dir. O zaman $C^{\perp} \subseteq C$ olması için gerek ve yeter şart

$$x^n - 1 \equiv 0 \bmod \left(g_i(x) g_i^*(x) \right) \qquad i = 1, 2$$

olmasıdır.

İspat $C=\langle g(x)\rangle = vC_1 \oplus (1+v)C_2$, R üzerinde n uzunluğunda bir devirli kod olsun. O zaman $C_1=\langle g_1(x)\rangle$ ve $C_2=\langle g_2(x)\rangle$ olmak üzere $C=\langle vg_1(x),(1+v)g_2(x)\rangle$ olur. Eğer

$$x^n-1\equiv 0 \bmod \left(g_i(x)g_i^*(x)\right) \qquad i=1,2$$

ise o zaman $C_1^{\perp}\subseteq C_1$ ve $C_2^{\perp}\subseteq C_2$ olur. Buradan

$$vC_1^{\perp}\subseteq vC_1, (1+v)C_2^{\perp}\subseteq (1+v)C_2$$

olur. Böylece

$$vC_1^{\perp}\oplus (1+v)C_2^{\perp}\subseteq vC_1\oplus (1+v)C_2$$

olur. Buradan da

$$\langle vh_1^*(x),(1+v)h_2^*(x)\rangle \subseteq \langle vg_1(x),(1+v)g_2(x)\rangle$$

olarak elde edilir. Böylece $C^{\perp}\subseteq C$ olur. Diğer taraftan eğer $C^{\perp}\subseteq C$ ise o zaman

$$vC_1^{\perp}\oplus (1+v)C_2^{\perp}\subseteq vC_1\oplus (1+v)C_2$$

olur. C_1 (veya C_2), F_4 üzerinde bir kod olmak üzere vC_1 (veya $(1+v)C_2$) $\bmod v$ ye (veya $\bmod(1+v)$) e göre C 'ye denk olur. $C_1^{\perp} \subseteq C_1$ ve $C_2^{\perp} \subseteq C_2$ olduğundan

$$x^n - 1 \equiv 0 \bmod\left(g_i(x) g_i^*(x)\right) \qquad i = 1, 2$$

olur.

Sonuç 2.4.1 $R = F_4 + vF_4$ üzerinde n uzunluğunda bir devirli kod $C = vC_1 \oplus (1+v)C_2$ olsun. O zaman $C^{\perp} \subseteq C$ olması için gerek ve yeter şart $C_1^{\perp} \subseteq C_1$ ve $C_2^{\perp} \subseteq C_2$ olmasıdır.

Teorem 2.5.1 ve Sonuç 2.5.1'den kuantum kod elde etmek için gerekli şart sağlanır.

Teorem 2.4.2 $C = vC_1 \oplus (1+v)C_2$, R üzerinde n uzunluğuna sahip bir devirli kod olsun ve $\psi(C)$, $[2n, k, d_L]$ parametrelerine sahip bir kod olsun, burada d_L, C kodunun minimum Lee ağırlığıdır. Eğer $C_1^{\perp} \subseteq C_1$ ve $C_2^{\perp} \subseteq C_2$ ise o zaman $C^{\perp} \subseteq C$ olur ve bu sayede parametreleri $\left[\left[2n, 2k - 2n, d_L\right]\right]$ olan bir hata düzelten kuantum kod elde edilir [5].

BÖLÜM 3. ÖRNEKLER

Bu bölümdeki örneklerin hesaplanmasında MAGMA bilgisayar programı kullanılmıştır [25].

Örnek 3.1 $R = F_4 + vF_4$ ve $n = 10$ olsun. O zaman F_4 de $x^{10} - 1 = (x+1)^2 (x^2 + wx + 1)^2 (x^2 + w^2 x + 1)^2$ olarak çarpanlarına ayrılır.

$$g_1(x) = g_2(x) = x + 1$$
$$g_1^*(x) = g_2^*(x) = x + 1$$

polinomları ile $g(x) = vg_1(x) + (1+v)g_2(x)$ polinomu elde edilir ve $C = \langle g(x) \rangle$, R üzerinde bir devirli kod olur. Açıkça görülür ki $g_i g_i^*, i = 1,2$ için $x^{10} - 1$ polinomunu böler. Sonuç 2.4.1.den $C^{\perp} \subseteq C$ olarak elde ederiz. O zaman $[[20,16,2]]$ parametrelerine sahip bir kuantum kod elde edilir.

Örnek 3.2 $R = F_4 + vF_4$ ve $n = 36$ olsun.O zaman F_4 de $x^{36} - 1 = (x+1)^4 (x+w)^4 (x+w^2)^4 (x^3+w)^4 (x^3+w^2)^4$ olarak çarpanlarına ayrılır.

$$g_1(x) = x^9 + w^2 x^8 + wx^7 + w^2 x^5 + wx^4 + w^2 x^2 + wx + 1$$
$$g_2(x) = x^{10} + x^7 + w^2 x^6 + x^4 + w^2 x^3 + w^2$$
$$g_1^*(x) = x^9 + wx^8 + w^2 x^7 + wx^5 + w^2 x^4 + wx^2 + w^2 x + 1$$

$$g_2^*(x) = w^2x^{10} + w^2x^7 + x^6 + w^2x^4 + x^3 + 1$$

polinomları ile $g(x) = vg_1(x) + (1+v)g_2(x)$ polinomu elde edilir ve $C = \langle g(x) \rangle$, R üzerinde bir devirli kod olur. Açıkça görülür ki $g_i g_i^*, i = 1,2$ için $x^{36} - 1$ polinomunu böler. Sonuç 2.4.1.den $C^\perp \subseteq C$ olarak elde ederiz. O zaman $[[72,34,4]]$ parametrelerine sahip bir kuantum kod elde edilir.

Örnek 3.3 $R = F_4 + vF_4$ ve $n = 43$ olsun. O zaman F_4 de

$$x^{43} - 1 = (x+1)(x^7 + wx^5 + x^4 + x^3 + w^2x^2 + 1)(x^7 + w^2x^5 + x^4 + x^3 + wx^2 + 1)$$
$$(x^7 + w^2x^6 + w^2x^5 + w^2x^4 + wx^3 + wx^2 + wx + 1)(x^7 + x^6 + wx^5 + w^2x^2 + x + 1)$$
$$(x^7 + x^6 + w^2x^5 + wx^2 + x + 1)(x^7 + wx^6 + wx^5 + wx^4 + w^2x^3 + w^2x^2 + w^2x + 1)$$

olarak çarpanlarına ayrılır.

$$g_1(x) = g_2(x) = x^{14} + wx^{13} + w^2x^{12} + wx^{11} + w^2x^{10} + x^8 + x^7 + x^6 + wx^4 + w^2x^3 + wx^2 + w^2x + 1$$

$$g_1^*(x) = g_2^*(x) = x^{14} + w^2x^{13} + wx^{12} + w^2x^{11} + wx^{10} + x^8 + x^7 + x^6 + w^2x^4 + wx^3 + w^2x^2 + wx + 1$$

polinomları ile $g(x) = vg_1(x) + (1+v)g_2(x)$ polinomu elde edilir ve $C = \langle g(x) \rangle$, R üzerinde bir devirli kod olur. Açıkça görülür ki $g_i g_i^*, i = 1,2$ için $x^{43} - 1$ polinomunu böler. Sonuç 2.4.1.den $C^\perp \subseteq C$ olarak elde ederiz. O zaman $[[86,30,8]]$ parametrelerine sahip bir kuantum kod elde edilir.

Örnek 3.4 $R = F_4 + vF_4$ ve $n = 57$ olsun. O zaman F_4 de

$$x^{57} - 1 = (x+1)(x+w)(x+w^2)(x^9 + x^8 + wx^6 + x^5 + x^4 + w^2x^3 + x + 1)$$

$$\left(x^9+x^8+w^2x^6+x^5+x^4+x^3+x+1\right)\left(x^9+x^8+wx^6+wx^5+w^2x^4+w^2x^3+w^2x+1\right)$$
$$\left(x^9+wx^8+w^2x^6+wx^5+w^2x^4+wx^3+w^2x+1\right)\left(x^9+w^2x^8+wx^6+w^2x^5+wx^4+w^2x^3+wx+1\right)$$
$$\left(x^9+w^2x^8+w^2x^6+w^2x^5+wx^4+wx^3+wx+1\right)$$

olarak çarpanlarına ayrılır.

$$g_1(x)=g_2(x)=x^{19}+w^2x^{18}+wx^{17}+wx^{14}+x^{10}+w^2x^9+wx^5+wx^2+x+w^2$$

$$g_1^*(x)=g_2^*(x)=w^2x^{19}+x^{18}+wx^{17}+wx^{14}+w^2x^{10}+x^9+wx^5+wx^2+w^2x+1$$

polinomları ile $g(x)=vg_1(x)+(1+v)g_2(x)$ polinomu elde edilir ve $C=\langle g(x)\rangle$, R üzerinde bir devirli kod olur. Açıkça görülür ki $g_ig_i^*, i=1,2$ için $x^{57}-1$ polinomunu böler. Sonuç 2.4.1.den $C^{\perp}\subseteq C$ olarak elde ederiz. O zaman $\left[\left[114,38,6\right]\right]$ parametrelerine sahip bir kuantum kod elde edilir.

Tablo 2.1.Optimal kuantum kodların parametreleri

n	Üreteç Polinomları	Parametreler
4	$g_1 = g_2 = x+1$	$\left[\left[8,4,2\right]\right]$
6	$g_1 = g_2 = x+w^2$	$\left[\left[12,8,2\right]\right]$
8	$g_1 = g_2 = x+1$	$\left[\left[16,12,2\right]\right]$
9	$g_1 = g_2 = x+w^2$	$\left[\left[18,14,2\right]\right]$
12	$g_1 = g_2 = x+w^2$	$\left[\left[24,20,2\right]\right]$
14	$g_1 = g_2 = x+1$	$\left[\left[28,24,2\right]\right]$
15	$g_1 = g_2 = x+w^2$	$\left[\left[30,26,2\right]\right]$
16	$g_1 = g_2 = x+1$	$\left[\left[32,28,2\right]\right]$
18	$g_1 = g_2 = x+w^2$	$\left[\left[36,32,2\right]\right]$
20	$g_1 = g_2 = x+1$	$\left[\left[40,36,2\right]\right]$
21	$g_1 = g_2 = x+w^2$	$\left[\left[42,38,2\right]\right]$
22	$g_1 = g_2 = x+1$	$\left[\left[44,40,2\right]\right]$
24	$g_1 = g_2 = x+w^2$	$\left[\left[48,44,2\right]\right]$
26	$g_1 = g_2 = x+1$	$\left[\left[52,48,2\right]\right]$
27	$g_1 = g_2 = x+w^2$	$\left[\left[54,50,2\right]\right]$
28	$g_1 = g_2 = x+1$	$\left[\left[56,52,2\right]\right]$
33	$g_1 = g_2 = w^2x+1$	$\left[\left[66,62,2\right]\right]$
34	$g_1 = g_2 = x+1$	$\left[\left[68,64,2\right]\right]$
36	$g_1 = g_2 = w^2x+1$	$\left[\left[72,68,2\right]\right]$
39	$g_1 = g_2 = w^2x+1$	$\left[\left[78,74,2\right]\right]$
40	$g_1 = x^2+w^2x+1, g_2 = x+1$	$\left[\left[80,74,2\right]\right]$
44	$g_1 = g_2 = x+1$	$\left[\left[88,84,2\right]\right]$

Tablo 2.1. (Devamı)

48	$g_1 = g_2 = x + w^2$	$\left[\left[96, 92, 2\right]\right]$
50	$g_1 = g_2 = x + 1$	$\left[\left[100, 96, 2\right]\right]$
52	$g_1 = g_2 = x + 1$	$\left[\left[104, 100, 2\right]\right]$
54	$g_1 = g_2 = x + w^2$	$\left[\left[108, 104, 2\right]\right]$
56	$g_1 = g_2 = x + 1$	$\left[\left[112, 108, 2\right]\right]$
58	$g_1 = g_2 = x + 1$	$\left[\left[116, 112, 2\right]\right]$

Tablo 2.2. Kuantum kodların parametreleri

n	**Üreteç Polinomları**	Parametreler
11	$x^5 + w^2x^4 + x^3 + x^2 + wx + 1$	$[[22, 2, 5]]$
12	$x^4 + x^3 + w^2x^2 + wx + w$	$[[24, 8, 3]]$
15	$x^3 + x + w$	$[[30, 18, 3]]$
18	$x^5 + wx^3 + w^2x^2 + 1$	$[[36, 16, 3]]$
19	$x^9 + w^2x^8 + w^2x^6 + w^2x^5 + wx^4 + wx^3 + wx + 1$	$[[38, 2, 7]]$
21	$x^7 + wx^6 + x^4 + w^2x^3 + w^2x + w^2$	$[[42, 14, 5]]$
23	$x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$	$[[46, 2, 7]]$
28	$x^{10} + x^7 + x^5 + x^2 + 1$	$[[56, 16, 4]]$
31	$x^5 + x^4 + x^3 + x^2 + 1$	$[[62, 42, 3]]$
33	$x^{16} + wx^{15} + wx^{13} + wx^{12} + wx^{11} + wx^9 + wx^7 + wx^5 + wx^4 + wx^3 + wx + w^2$	$[[66, 2, 10]]$
33	$x^{11} + w^2x^{10} + x^8 + w^2x^7 + wx^6 + x^5 + w^2x^4 + wx^3 + w^2x + w$	$[[66, 22, 6]]$
35	$x^{12} + w^2x^{11} + wx^{10} + w^2x^9 + wx^8 + w^2x^7 + wx^5 + w^2x^4 + wx^3 + w^2x^2 + wx + 1$	$[[70, 22, 5]]$
35	$x^6 + w^2x^5 + x^4 + wx^3 + wx^2 + 1$	$[[70, 46, 3]]$
39	$x^7 + wx^5 + w^2x^4 + wx^3 + x^2 + wx + w^2$	$[[78, 50, 3]]$
42	$x^5 + wx^4 + wx^3 + wx^2 + w$	$[[84, 64, 3]]$
42	$x^8 + w^2x^7 + x^5 + w$	$[[84, 52, 4]]$
42	$x^{11} + x^8 + w^2x^6 + wx^4 + x^3 + x^2 + x + w$	$[[84, 40, 5]]$
42	$x^{14} + x^{13} + wx^{12} + wx^{11} + w^2x^{10} + x^9 + wx^8 + x^7 + x^6 + wx^5 + x^4 + wx^3 + w^2x^2 + x + w$	$[[84, 28, 6]]$
43	$x^7 + w^2x^6 + w^2x^5 + w^2x^4 + wx^3 + wx^2 + wx + 1$	$[[86, 58, 5]]$
47	$x^{23} + x^{22} + x^{21} + x^{20} + x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^5 + x^4 + 1$	$[[94, 2, 11]]$
48	$x^{11} + x^8 + wx^3 + w$	$[[96, 52, 4]]$
56	$x^{16} + x^{14} + x^{13} + x^{10} + x^9 + x^8 + x^4 + x^2 + x + 1$	$[[112, 48, 4]]$
57	$x^{27} + x^{26} + w^2x^{25} + x^{24} + wx^{23} + x^{22} + wx^{21} + w^2x^{20} + w^2x^{19} + x^{17} + wx^{16} + w^2x^{14} + wx^{13} + w^2x^{11} + x^{10} + wx^8 + wx^7 + w^2x^6 + x^5 + w^2x^4 + x^3 + wx^2 + x + 1$	$[[114, 6, 12]]$
59	$x^{29} + w^2x^{28} + x^{27} + x^{26} + w^2x^{25} + wx^{24} + x^{23} + w^2x^{21} + x^{20} + w^2x^{19} + wx^{18} + x^{17} + x^{16} + w^2x^{15} + wx^{14} + x^{13} + x^{12} + w^2x^{11} + wx^{10} + x^9 + wx^8 + x^6 + w^2x^5 + wx^4 + x^3 + x^2 + wx + 1$	$[[118, 2, 14]]$

KAYNAKLAR

[1] Çallıalp, F., Örneklerle Soyut Cebir, Birsen Yayınevi, 2009

[2] Calderbank,A.R., Rains, E.M., Shor,P.M., Sloane,N.J.A., Quantum error correction via codes over $GF(4)$, IEEE Trans. Inf. Theory, 44 (1998), 1369-1387.

[3] Steane, A.M., Simple quantum error correcting-codes,Phys. Rev. A, 54 (1996),4741-4751.

[4] Zhu, S.,Wang, Y., Shi M., Some results on cyclic codes over $F_2 + vF_2$, IEEETrans.Inf.Theory, 56 (2010), 1680-1684.

[5] Qian, J., Quantum codes from cyclic codes over $F_2 + vF_2$, Journal of Inform.&computational Science 10:6(2013), 1715-1722.

[6] Qian,J.,Ma, W., Gou, W., Quantum codes from cyclic codes over _nite ring, Int. J. Quantum Inform., 7(2009), 1277-1283.

[7] Kai, X.,Zhu, S., Quaternary construction of quantum codes from cyclic codesover $F_4 + uF_4$, Int. J. Quantum Inform., 9(2011), 92-119.

[8] Ashraf,M.,Mohammed, G., Quantum codes from cyclic codes $F_3 + vF_3$, Int.J. Quantum Inform. 12(2014) 1450042.

[9] Bayram, A.,Oztas, E.S., Siap, I., Codes over $F_4 + vF_4$ and some DNA applications, Des. Codes. Cryptogr., DOI 10.1007,2015.

[10] Graasl, M., Online Linear Code Bounds, Available Online athttp://www.codetables.de ,2011.

[11] Shor, P.W., Scheme for reducing decoherence in quantum memory, Phys. Rev.A, 52 (1995),2493-2496.

[12] Roman, S., Coding and Information Theory, Graduate Texts in Mathematics, Springer Verlag, 1992.

[13] Ling, S., Xing, C., Coding Theory, Cambridge University Press. 2004.

[14] Wan, Z. X., Finite Fields and Galois Rings, World Scientific, 2012.

[15] Hungerford, T. W., Algebra, Springer, 2000.

[16] Çallıalp, F., Tekir, Ü., Değişmeli Halkalar Ve Modüller, Birsen Yayınevi, 2009.

[17] Mcdonald, B. R., Dekker. M., Finite Rings With Identity, QA 251.5.M3, 1974.

[18] Hill, R., Kolman, B., Elementary Lineer Algebra, Prentice Hall, 2000.

[19] Roman, S., Advanced Lineer Algebra, Graduate Texts in Matematics, Springer, 2000.

[20] Özen, M., Güzeltepe, M., Quantum codes from codes over Lipschitz integers, Glob. J. Pure Appl. Math., Vol. 7, No. 2, pp, 201-206, 2011.

[21] Shirali, S., Vasudeva, H. L., Metric Spaces, Springer, 2006.

[22] Dougherty, S. T., Shiromoto, K., Maximum Distance Codes Over Rings of Order 4, IEEE, Transactions on Information Theory, Vol. 47, No. 1, January 2001.

[23] Norton, G., Salagean, A., On The Structure Of Linear And Cyclic Codes Over Finite Chain Rings, Applicable Algebra in Engineering, communication and Computing, 10, pp, 489-506, 2000.

[24] Gursoy, F., Siap, I., Yildiz, B., Construction of skew cyclic codes over $F_q + vF_q$. Adv. Math. Commun. 8, 313-322, 2014.

[25] Bosma, W., Cannon, J., Playouts, C., The Magma algebra system. I. The user language, J. Symbolic Comput., 24(1997), 235-265.

ÖZGEÇMİŞ

Faik Cem Ertunç, 04.10.1988 tarihinde İstanbul'un Beykoz ilçesinde doğmuştur. İlk, Orta ve Lise eğitimini 2005 yılında Beykoz'da tamamlamıştır. 2007 yılında Sakarya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde lisans eğitimine başladı ve buradan 2012 yılında mezun oldu. 2012 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Matematik EABD'de Yüksek Lisans eğitimine başladı. Evli ve iki çocuk babasıdır.