T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

# $\mathbb{Z}_4+u\mathbb{Z}_4$ HALKASINDAKİ DEVİRLİ KODLAR, SABİT DEVİRLİ KODLAR VE KENDİNE DUAL KODLAR

**YÜKSEK LİSANS TEZİ**

**Fatma Zehra UZEKMEK**

| | | |
|---|---|---|
| **Enstitü Anabilim Dalı** | **:** | **MATEMATİK** |
| **Enstitü Bilim Dalı** | **:** | **CEBİR VE SAYILAR TEORİSİ** |
| **Tez Danışmanı** | **:** | **Prof. Dr. Mehmet ÖZEN** |

**Haziran 2015**

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

# $\mathbb{Z}_4+u\mathbb{Z}_4$ HALKASINDAKİ DEVİRLİ KODLAR, SABİT DEVİRLİ KODLAR VE KENDİNE DUAL KODLAR

## YÜKSEK LİSANS TEZİ

Fatma Zehra UZEKMEK

| | | |
|---|---|---|
| **Enstitü Anabilim Dalı** | : | **MATEMATİK** |
| **Enstitü Bilim Dalı** | : | **CEBİR VE SAYILAR TEORİSİ** |

**Bu tez 16 .06 .2015 tarihinde aşağıdaki jüri tarafından oybirliği ~~/ oyçokluğu~~ ile kabul edilmiştir.**

| | | |
|---|---|---|
| **Prof. Dr. İrfan ŞİAP** | **Prof. Dr. Mehmet ÖZEN** | **Yrd. Doç. Dr. Yusuf KARAKUŞ** |
| **Jüri Başkanı** | **Üye** | **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.

Fatma Zehra UZEKMEK

16.06.2015

# TEŞEKKÜR

Matematiğin bu alanına yönlenmemi sağlayan, çalışmalarımda her zaman yardımcı olan ve sabrını benden esirgemeyen saygıdeğer hocam Prof. Dr. Mehmet Özen'e, bilgi ve deneyimlerinden yararlanma fırsatı bulduğum, özellikle çalışmanın bilgisayar hesaplamalarında yardımcı olan Kenyon University'den Prof. Dr. Nuh Aydın'a ve savunmama katılarak bilgilerinden istifade edebilme fırsatı bulduğum saygıdeğer hocam Prof. Dr. İrfan Şiap'a teşekkürlerimi sunarım. Takıldığım yerlerde yardımcı olan bölümümüz doktora öğrencisi N. Tuğba Özzaim'e de teşekkür ederim. Ayrıca bugünlere ulaşmamda maddi ve manevi destekleriyle her zaman yanımda olan çok değerli aileme şükranlarımı sunarım.

# İÇİNDEKİLER

# SİMGELER VE KISALTMALAR LİSTESİ

| | |
|---|---|
| $C$ | : Kod |
| $C^{\perp}$ | : $C$ kodunun tümleyeni |
| $d_L$ | : Lee uzaklık |
| $d_E$ | : Öklid ağırlık |
| $F$ | : Cisim |
| G | : Grup |
| $I$ | : İdeal |
| R | : Halka |
| $\hat{R}$ | : Modül |
| $Sp(A)$ | : A kümesinin bütün lineer birleşimlerinin kümesi |
| $<u,v>$ | : $u$ ile $v$'nin iç çarpımı |
| $V$ | : Vektör uzayı |
| $V(n,q)$ | : Elemanları $F_q$'dan alınan $n-$lilerin kümesi |
| $w$ | : Ağırlık |
| $w_c(x)$ | : $C$ kodunun ağırlık sayacı |
| $\chi$ | : Halkanın bir karakteri |
| $\sigma$ | : Devirli kod |
| $\upsilon$ | : Sabit Devirli Kod |
| $\Phi$ | : Gray dönüşümü |
| $\varphi\|_C$ | : $\varphi$'nin $C$'ye kısıtlanışı |
| $\|\ \|$ | : Mertebe |

# TABLOLAR LİSTESİ

# ÖZET

Anahtar kelimeler: $u^2=1$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerindeki kodlar, Sabit devirli kodlar, Kendine dual kod, Özdeşlik anlamında kendine dual kod.

Bu tezde $u^2=1$ iken $R=\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerindeki devirli kodlar ve $(2+u)$-sabit devirli kodlar çalışılmıştır. Bu halka üzerindeki devirli kodların üreteçleri ve geren kümeleri belirlenmiştir. Tek uzunlukta olan $(2+u)$-sabit devirli kodların $\mathbb{Z}_4$ görüntülerinin $\mathbb{Z}_4$ üzerinde devirli kod olduğu ispatlanmıştır. Ayrıca bu halka üzerindeki kendine dual (self dual) kodlar, özdeşlik anlamında kendine dual (formally self dual) kodlar ve ikili dairesel (double circulant) kodlar çalışılmıştır. Önceden en iyi olarak bilinen $\mathbb{Z}_4$ lineer kodların parametrelerinden daha iyi parametrelere sahip $R$ üzerindeki devirli kodların $\mathbb{Z}_4$ görüntülerine pek çok örnek verilmiştir.

# CYCLIC CODES, CONSTACYCLIC CODES AND SELF DUAL CODES OVER THE RING $\mathbb{Z}_4 + u\mathbb{Z}_4$

## SUMMARY


Keywords: Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 1$, Cyclic codes, Constacyclic codes, Self dual, Formally self dual.

In this paper, we study cyclic codes and constacyclic codes with shift constant $(2+u)$ over $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 1$. We determine the form of the generators of the cyclic codes over this ring and their spanning sets. Considering their $\mathbb{Z}_4$ images, we prove that the $\mathbb{Z}_4$- image of a $(2+u)$- constacyclic code of odd length is a cyclic code over $\mathbb{Z}_4$. We also study self dual, formally self dual, and double circulant codes over this ring. We also present many examples of cyclic codes over $R$ whose $\mathbb{Z}_4$- images have better parameters than previously best-known $\mathbb{Z}_4$- linear codes.

# BÖLÜM 1. GİRİŞ

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

## 1.1. Cebirsel Tanımlar

**Tanım 1.1.1** $G$ boş olmayan herhangi bir küme olsun. $G$ kümesinin elemanlarından oluşan her sıralı ikiliye $G$'de bir ve yalnız bir eleman karşılık getiren bir fonksiyona $G$ üzerinde bir ikili işlem denir. Bu işlem $*$ sembolü ile gösterilirse;

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

şeklinde tanımlanır.

**Tanım 1.1.2** $G$ boştan farklı bir küme ve $*$, $G$'de tanımlı bir ikili işlem olsun. Eğer $(G,*)$ cebirsel yapısı aşağıdaki aksiyomları sağlıyorsa $(G,*)$ ikilisine bir grup denir [1] .

$G1)$ $*$, $G$'de bir ikili işlemdir.

$G2)$ $*$ işleminin $G$'de birleşme özelliği vardır. Yani, $\forall a,b,c \in G$ için, $a*(b*c)=(a*b)*c$ dir.

$G3)$ $*$ işleminin $G$'de bir birim elemanı vardır. Yani, $\forall a \in G$ için $a*e=e*a=a$ olacak şekilde bir $e \in G$ vardır.

$G4)$ $*$ işlemine göre, $G$'deki her elemanın bir tersi vardır. Yani, $a \in G$ için $a*a^{-1}=a^{-1}*a=e$ olacak şekilde bir $a^{-1} \in G$ bulunabilir.

**Tanım 1.1.3** $G$ bir grup, $X$ $G$'nin bir alt kümesi, $\{H_i \mid i \in I\}$ te $X$'i içeren $G$'nin tüm alt gruplarının bir ailesi olsun. Bu durumda, $\bigcap_{i \in I} H_i$ $X$ kümesi tarafından üretilen $G$'nin alt grubu olarak adlandırılmaktadır. $< X >$ ile gösterilmektedir. $X = \{a_1, ..., a_n\}$ olması durumunda $< X >$ yerine $< a_1, ..., a_n >$ yazılabilir. Eğer, $a \in G$ ise, $< a >$ alt grubu $a$ tarafından üretilen devirli (alt)-grup olarak adlandırılmaktadır [2] .

**Tanım 1.1.4** $R$ boştan farklı bir küme ve bu küme üzerinde tanımlı ikili işlem $+$ ve $.$ olsun. Aşağıdaki aksiyomları sağlayan $(R, +, .)$ cebirsel yapısına bir halka denir [2] .

1) $(R, +)$ bir değişmeli gruptur.
2) $\forall a, b, c \in R$ için $(a.b).c = a.(b.c)$ dir. Yani, $.$ işleminin $R$'de birleşme özelliği vardır.
3) $a.(b+c) = a.b + a.c$ ve $(a+b).c = a.c + b.c$ dir. Yani, $.$ işleminin $+$ işlemi üzerine sağdan ve soldan dağılma özelliği vardır.

**Tanım 1.1.5** $\forall a, b \in R$ için $a.b = b.a$ olması durumunda $R$'ye değişmeli halka, $\forall a \in R$ için $1_R.a = a.1_R = a$ olacak şekilde $1_R \in R$ varsa $R$'ye birimli halka, $1_R$' ye de halkanın birim elemanı denir [2] .

**Tanım 1.1.6** $R$ halkasında $0 \neq a \in R$ elemanı için, $ab = 0_R$ (veya $ba = 0_R$) olacak şekilde $\exists 0 \neq b \in R$ bulunabilirse $a$'ya halkanın sıfır böleni, böyle bir $b$ yoksa sıfır böleni değildir denir [1] .

**Tanım 1.1.7** Sıfır bölensiz bir halkaya tam halka denir. Birimli, değişmeli ve sıfır bölensiz (tam) halkaya da bir tamlık bölgesi denir [1] .

**Tanım 1.1.8** $R$ bir tamlık bölgesi olsun. $m.1_R = 0_R$ olacak şekilde bir $m > 0$ tamsayısı varsa böyle $m$'lerin en küçüğüne $R$'nin karakteristiği denir. Eğer bu özellikte hiçbir $m$ bulunamıyorsa $R$'nin karakteristiği sıfır denir [1] .

**Tanım 1.1.9** $R$ bir halka ve $0 \neq S \subset R$ olsun. $R$'deki işlemlere göre $S$ alt kümesi kendi başına bir halka ise $S$'ye $R$ halkasının bir alt halkası denir [2] .

**Tanım 1.1.10** $A$, $R$ halkasının bir alt kümesi olsun. $R$'nin $A$'yı kapsayan bütün alt halkalarının arakesitine $A$'nın ürettiği alt halka denir ve $< A >$ ile gösterilir. $A$'nın elemanlarına da $< A >$'nın üreteçleri denir [1] .

**Tanım 1.1.11** $R$ bir halka ve $I$, $R$'nin boştan farklı bir alt halkası olsun. Bu durumda,

1) $\forall x, y \in I : x - y \in I$
2) $\forall r \in R$ ve $\forall x \in I$ iken $rx \in I$ ise sol ideal;
   $\forall r \in R$ ve $\forall x \in I$ iken $xr \in I$ ise sağ ideal

olarak adlandırılmaktadır. Hem sol hem de sağ ideal mevcut ise $I$'ya ideal denir [2].

**Tanım 1.1.12** $A$, $R$ halkasının bir alt kümesi, $\{A_i \,|\, i \in I\}$ da $A$'yı kapsayan $R$'deki tüm ideallerin ailesi olsun. Bu durumda $\bigcap_{i \in I} A_i$, $A$ tarafından üretilen ideal olarak adlandırılmaktadır. $(A)$ ile gösterilir. $A$'nın elemanlarına $(A)$ idealinin üreteçleri denir. Eğer $A = \{a\}$ tek elemanlı bir küme ise $A$'nın ürettiği ideale temel ideal denir ve $(a)$ ile gösterilir [2] .

**Tanım 1.1.13** Her ideali temel ideal olan halkaya temel ideal halkası, her ideali temel ideal olan tamlık bölgesine ise temel ideal bölgesi denir [2] .

**Tanım 1.1.14** $R$ bir halka ve $I$, $R$'nin bir ideali olsun. $\forall a, b \in R$ için, $R$ halkasının, bir $I$ idealine göre denklik bağıntısı,

$$a \equiv b \pmod{I} \iff a - b \in I$$

biçiminde tanımlanır [1] .

**Önerme 1.1.1** $R$ halkasının, bir $I$ idealine göre tanımlanan denklik sınıfları arasında;

$$(a+I)\oplus(b+I)=(a+b)+I\,, \qquad (a+I)\odot(b+I)=(ab)+I$$

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

**Tanım 1.1.15** $R$ ve $S$ iki halka olsun. $\forall a,b\in R$ için,

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

$f:R\to S$ fonksiyonuna bir halka homomorfizması denir [2] .

**Tanım 1.1.16** $f:R\to S$ homomorfizması birebir ve örten ise $f$'ye bir izomorfizma, $R$ ve $S$'ye izomorf halkalar denir. $R\cong S$ ile gösterilir [1] .

**Tanım 1.1.17** $f:R\to S$ halka homomorfizmasının çekirdeği

$$çek(f)=\{\, r\in R \mid f(r)=0_S \,\}$$

dir [2] .

**Tanım 1.1.18** $R$ bir halka, $x$ bir bilinmeyen ve $a_0,a_1,...,a_k$'lar $R$'nin elemanları olmak üzere,

$$a_0+a_1x+...+a_kx^k$$

şeklindeki bir ifadeye $R$'den katsayılı bir polinom denir. $R$'den katsayılı tüm polinomlar kümesi $R[x]$ ile gösterilir [1] .

**Önerme 1.1.2** $R$ bir halka ise $R[x]$ de bir halkadır [1] .

**Önerme 1.1.3** $R$ bir halka olsun [1] .

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

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

iii. $R$ tamlık bölgesi ise $R[x]$ de tamlık bölgesidir.

**Tanım 1.1.19** Bir $R$ tamlık bölgesinin tüm elemanlarını bölen $R$'nin bir elemanına aritmetik birim veya birimsel eleman denir [1] .

**Önerme 1.1.4** $R$'nin aritmetik birimleri, $R$'deki terslenebilen elemanlardan ibarettir [1] .

**Tanım 1.1.20** $R$ değişmeli ve birimli bir halka ve $M$ de $R$'nin $(1)$ den farklı 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] .

**Önerme 1.1.5** $M$, $R$'nin bir $(1)$ den farklı bir ideali olsun. $M$'nin maksimal olması için gerek ve yeter koşul $\forall x \in R-M$ için, $M+(x)=R$ olmasıdır [1] .

**Tanım 1.1.21** Tek maksimal ideale sahip birimli değişmeli bir halkaya lokal halka denir [2] .

**Tanım 1.1.22** Bir $S$ halkasının tüm sol ideallerinin latisi zincir oluşturuyorsa $S$'ye sol zincir halkası; tüm sağ ideallerinin latisi bir zincir oluşturuyorsa $S$'ye sağ zincir halkası denir [40] .

**Tanım 1.1.23** $(M,+)$ bir değişmeli grup ve $R$ değişmeli bir halka olsun. $M$'deki elemanların, $R$'deki elemanlarla skaler çarpımı, $R\times M\to M$ fonksiyonu aşağıdaki koşulları sağlıyorsa, $M$'ye $R$ üzerinde bir modül veya kısaca, $R$ – modül denir [3].

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 1.1.24** $R$ bir halka, $M$ bir $R-$modül ve $N \subseteq M$ boş olmayan bir alt küme olsun. $N$ kendi başına bir $R-$modül ise $N$'ye, $M$'nin bir alt modülü veya $R-$alt modülü denir [3] .

**Tanım 1.1.25** $R$ bir halka, $M$ ve $N$ de $R$ – modül olsunlar. Bir $f : M \to N$ fonksiyonu,

i. $\forall m, m' \in M$ için, $f(m+m') = f(m) + f(m')$

ii. $\forall r \in R$ için, $f(rm) = r f(m)$

koşullarını sağlıyorsa, $f$'ye bir modül homomorfizması veya $R-$homomorfizma denir [3] .

**Tanım 1.1.26** $f$, $R[x]$'te bir polinom olmak üzere $f$ sıfır bölen değil ise $f$'ye regüler polinom denir [4] .

**Tanım 1.1.27** $F$ bir cisim, $f$ $F$'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 [9] .

**Tanım 1.1.28** $f$ ve $g$ $R[x]$'te sıfırdan farklı polinomlar olsun. $g$ regüler ise $f = gq + r$ , $der(r) < der(g)$ olacak şekilde $q, r \in R[x]$ vardır. Bu ifade Öklid algoritması olarak adlandırılmaktadır [4] .

**Teorem 1.1.1** $f$, $R[x]$'te regüler bir polinom olsun. Bu durumda $a \in R$ için, $f(a) = 0 \Leftrightarrow f^*(a) = 0$ olacak şekilde $\mu f = \mu f^*$ olan monik polinomu vardır. Ayrıca $v f = f^*$ olacak şekilde $v \in R[x]$ birimsel elemanı vardır [4] .

**Teorem 1.1.2** $R$ sonlu bir halka ise aşağıdaki ifadeler denktir [41] .

a) $R$ bir Frobenius halkadır.

b) Bir sol modül olarak, $\hat{R} \cong {}_R R$ dir.

c) Bir sağ modül olarak, $\hat{R} \cong R_R$ dir.

## 1.2. Lineer Kodlar

**Tanım 1.2.1** $F$ cismi üzerinde tanımlı elemanları vektörler olan $V$ kümesi aşağıdaki aksiyomları sağlıyorsa $V$ kümesine vektör uzayı denir [5] .

$V1)$ $V$ kümesi toplama işlemine göre değişmeli bir gruptur.

$V2)$ $\forall a \in F$ ve $u \in V$ için $au \in V$ dir.

$V3)$ $\forall a,b \in F$ ve $\forall u,v \in V$ için $a(u+v) = au + av$ ve $(a+b)v = av + bv$ dir.

$V4)$ $\forall a,b \in F$ ve $\forall u \in V$ için $(ab)u = a(bu)$ dir.

$V5)$ $\forall u \in V$ için $1u = u$ dur.

**Tanım 1.2.2** $V$ bir vektör uzayı ve $0 \neq W \subset V$ olsun. Eğer $W$, vektör uzayının bütün aksiyomlarını sağlıyorsa $W$'ya $V$'nin bir alt uzayı denir [5] .

**Teorem 1.2.1** $V$ bir vektör uzayı ve $0 \neq W \subset V$ olsun. $W$, aşağıdaki aksiyomları sağlıyorsa $V$ vektör uzayının bir alt uzayıdır [5] .

i. $\forall x, y \in W$ için $x + y \in W$ dır.

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

**Tanım 1.2.3** $r_i$'ler skaler olmak üzere, $n$ tane $v_1, v_2, ..., v_n$ vektörlerinin lineer birleşimi

$$v = r_1 v_1 + r_2 v_2 + ... + r_n v_n$$

şeklindedir. Eğer $A=\{v_1,v_2,...,v_n\}$ ise $A$ kümesinin bütün lineer birleşimlerinin kümesi $Sp(A)$ ile ifade edilmektedir. Ayrıca $Sp(A)$, $V$ vektör uzayının bir alt uzayıdır [5] .

**Tanım 1.2.4** $A=\{v_1,v_2,...,v_n\}$ olsun. $Sp(A)$, $A$ kümesinin bütün lineer birleşimlerinin kümesi olmak üzere, $Sp(A)$ uzayına $A$ kümesinin gerdiği (ürettiği) alt uzay denir. $A$ kümesine de $Sp(A)$ alt uzayının bir üreteci denir [5] .

**Tanım 1.2.5** $V$ vektör uzayında $v_1,v_2,...,v_n$ vektörleri verilsin. Eğer, $r_1v_1+r_2v_2+...+r_nv_n=0$ olacak şekilde en az biri sıfırdan farklı olan $r_1,r_2,...,r_n$ sayıları varsa $\{v_1,v_2,...,v_n\}$ vektörlerinin kümesi lineer bağımlıdır denir. Eğer, $r_1v_1+r_2v_2+...+r_nv_n=0 \Rightarrow r_1=r_2=...=r_n=0$ ise lineer bağımsızdır denir [6] .

**Tanım 1.2.6** $V$ bir vektör uzayı ve $A=\{v_1,v_2,...,v_n\}$ olsun. Eğer $A$ kümesi aşağıdaki koşulları sağlıyorsa $A$'ya $V$'nin bir tabanı veya bazı denir [6] .

i. $A$ lineer bağımsız bir kümedir.

ii. $A$, $V$'yi geren bir kümedir.

**Tanım 1.2.7** $V$ vektör uzayının herhangi bir tabanındaki vektörlerinin sayısına $V$'nin boyutu denir [5] .

**Tanım 1.2.8** $A=\{a_1,a_2,...,a_q\}$ sonlu bir küme olsun. Bu kümeye alfabe yada $q$ - lu alfabe denir. $A^n$ ise $A$ kümesinden alınan $n$-lileri temsil etsin. Bu durumda $A^n$ kümesine sözler ailesi denir. $A^n$'nin herhangi bir $C$ alt kümesine $q$-lu blok kodu, $C$'nin elemanlarına da kodsöz denir. $C\subset A^n$'nin $M$ tane elemanı varsa $C$'ye, $n$ uzunluğunda $M$ elemanlı bir kod denir ve $(n,M)$ ile gösterilir [8].

**Tanım 1.2.9** $x$ ve $y$ aynı uzunlukta ve aynı alfabe üzerinde tanımlanmış $n$-liler olsun. $x$ ve $y$'nin farklı bileşenlerinin sayısına, $x$ ile $y$ arasındaki Hamming uzaklık denir. $d(x,y)$ ile gösterilir [8] .

**Tanım 1.2.10** $d(C)=\min_{x,y\in C, x\neq y} d(x,y)$ sayısına $C$ kodunun minimum uzaklığı denir. $n$ uzunluğunda $M$ elemana sahip ve minimum uzaklığı $d$ olan bir kod $(n,M,d)$ ile gösterilir [8] .

**Teorem 1.2.2** $A^n$, $A$ alfabesinden oluşan $n$-lilerin kümesi olsun. Hamming uzaklık aşağıdaki özelliklere sahiptir. $\forall x,y,z\in A$ için,

I) ( Pozitif Tanımlılık )

$$d(x,y)\geq 0 \text{ ve } d(x,y)=0 \Leftrightarrow x=y$$

II) ( Simetri )

$$d(x,y)=d(y,x)$$

III) ( Üçgen Eşitsizliği )

$$d(x,y)\leq d(x,z)+d(z,y)$$

$(A^n,d)$ ikilisi metrik uzaydır [8] .

**Tanım 1.2.11** $(X,d)$ ve $(X',d')$ iki metrik uzay ve $f:X\to X'$ bir dönüşüm olsun. $\forall x,y\in X$ için,

$$d'(f(x),f(y))=d(x,y)$$

eşitliği sağlanırsa, $f$ dönüşümüne bir izometri denir [30] .

Diğer bir deyişle, metrik uzaylar arasındaki bir $f$ dönüşümü, elemanlar arasındaki uzaklıkları koruyorsa izometri adını alır [30] .

**Tanım 1.2.12** Bir $x=(x_1,x_2,...,x_n)$ vektörünün sıfırdan farklı elemanlarının sayısı $x$ vektörünün Hamming ağırlığını verir. $w(x)$ ile gösterilir. Buradan, $d(x,y)=w(x-y)$ olduğu görülür [8] .

**Tanım 1.2.13** Bir $C$ kodunun sıfırdan farklı kodsözlerinin ağırlıklarının en küçüğüne o kodun minimum ağırlığı denir [8] .

**Tanım 1.2.14** $C\subset V(n,q)$ alt kümesi $V(n,q)$ vektör uzayının bir alt uzayı ise $C$'ye bir lineer kod denir. $C$'nin boyutunun $k$ olması durumunda $C$'ye $[n,k]$-kodu denir. $C$ kodunun minimum uzaklığı $d$ ise $C$'ye $[n,k,d]$-kodu denir [8] .

**Teorem 1.2.3** $C$ bir lineer kod ise $d(C)=w(C)$ dir [8] .

**Tanım 1.2.15** $C$ bir $[n,k]$- kodu olsun. Satırları $C$ kodunun bazlarından oluşan $k\times n$ tipinde bir $D$ matrisine $C$'nin bir üreteç matrisi denir [8] .

**Teorem 1.2.4** $F_q$ cismi üzerinde bir $[n,k,d]$- kodu verildiğinde, ilk $k$ sütunu $k$ boyutlu $I_k$ birim matris olan $G=[I_k\,|\,A]$ standart formdaki üreteç matrisine sahip bir koda denktir [8] .

**Teorem 1.2.5** $C$ kodu $G=[I_k\,|\,A]$ standart formdaki üreteç matrisine sahip $[n,k]$ parametreli lineer bir kod ise $C$'nin dik tümleyeni de $H=[-A^T\,|\,I_{n-k}]$ üreteç matrisine sahip bir $[n,n-k]$ lineer kod olur. $H$ matrisine $C$ kodunun kontrol matrisi denir [8] .

**Tanım 1.2.16** $V$ bir vektör uzayı olsun. Aşağıdaki aksiyomlar sağlanıyorsa bu vektör uzayına iç çarpım uzayı denir [5] .

$c$ 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. $\langle u,v\rangle = \langle v,u\rangle$

iii. $\langle u+v,w\rangle = \langle u,w\rangle + \langle v,w\rangle$ ve $\langle u,v+w\rangle = \langle u,v\rangle + \langle u,w\rangle$

iv. $\langle cu,v\rangle = c\langle u,v\rangle$ ve $\langle u,cv\rangle = c\langle u,v\rangle$.

**Tanım 1.2.17** $V$ iç çarpım uzayında $\langle u,v\rangle = 0$ ise $u$ vektörü, $v$ vektörüne diktir (veya ortogonaldir) denir [5] .

**Tanım 1.2.18** $V(n,q)$ vektör uzayında doğal olan bir iç çarpım tanımlı olmak üzere, $u = (u_1,u_2,...,u_n)$ , $v = (v_1,v_2,...,v_n) \in V(n,q)$ için $u$ ve $v$ 'nin iç çarpımı,

$$< u,v > = u_1v_1 + u_2v_2 + ... + u_nv_n$$

şeklinde tanımlanır [8] .

**Tanım 1.2.19** $C$ kodu bir $[n,k]$ lineer kod olsun.

$$C^{\perp} = \{u \in V(n,q) : < u,v >= 0, v \in C\}$$

kümesine $C$ 'nin dik tümleyeni (dual kodu) denir [8] .

**Teorem 1.2.6** [8]

1. Eğer $G = [I_k \mid A]$, $C$ kodunun bir üreteç matrisi ise o zaman

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

dir.

2. Lineer bir $[n,k]$- kodunun duali de bir $[n,n-k]$- koddur.

3. Eğer $C$ lineer bir kod ise $(C^{\perp})^{\perp} = C$ dir.

**Tanım 1.2.20** $C = C^{\perp}$ olması durumunda $C$ koduna kendine dual, $C \subset C^{\perp}$ olması durumunda ise $C$'ye kendine dik kod (self ortogonal) denir [8] .

**Tanım 1.2.21** $q > 1$ 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 $(M = A_q(n, d))$ optimal kod denir [10] .

**Tanım 1.2.22** $R$ üzerinde $n$ uzunluğunda lineer bir kod $C$ olsun. Herhangi bir $c = (c_0, c_1, ..., c_{n-1})$ kodsözü için $c$'nin Lee ağırlığı $w_L = \sum_{i=0}^{n-1} w_L(c_i)$ olarak tanımlanmaktadır [11] .

**Tanım 1.2.23** Herhangi bir $c' \in C$ ve $c \neq c'$ için, $d_L(c, c')$ iki kodsöz arasındaki Lee uzaklık olmak üzere $d_L(c, c') = w_L(c - c')$ ifadesine $C$'nin Lee uzaklığı, $d_L = \min d_L(c, c')$ ifadesine de $C$'nin minimum Lee uzaklığı denir [11] .

**Tanım 1.2.24** $R$'de $n$ uzunluğundaki bir $C$ kodu için, $C$'nin üreteçlerinin en küçük sayısına rank denir. $rank(C)$ ile gösterilir [7] .

**Tanım 1.2.25** $i, j.$ elemanı $a_{ij}$ olan $k \times k$ tipindeki bir matris $A$ olsun. $(i - j) \mid k = (q - p) \mid k$ iken $a_{ij} = a_{pq}$ ise $A$ matrisine dairesel matris denir.

Bu durumda dairesel bir matrisin en fazla $k$ farklı elemanı yani $a_0, a_1, ..., a_{k-1}$ elemanları vardır ve $A$ matrisi,

$$A=\begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{k-1} \\ a_{k-1} & a_0 & a_1 & \dots & a_{k-2} \\ a_{k-2} & a_{k-2} & a_0 & \dots & a_{k-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}$$

şeklinde ifade edilir [12] .

### 1.3. Devirli Kodlar

**Tanım 1.3.1** $V(n,q)$, bileşenleri $F_q$ cisminden olan, $n$ - lilerden oluşan bir vektör uzayıdır.

**Tanım 1.3.2** $C \subset V(n,q)$ lineer kodu için, eğer $c_0 c_1 ... c_{n-1} \in C$ iken $c_{n-1} c_0 c_1 ... c_{n-2} \in C$ ise, bu lineer koda devirli bir kod denir [8] .

$F_q$ üzerinde derecesi $n$'den daha küçük polinomlar ile $V(n,q)$ vektör uzayı arasında bir izomorfizma kurulabilir.

$R_n = \dfrac{F_q[x]}{\langle x^n - 1 \rangle}$ olmak üzere,

$$\phi : V(n,q) \to R_n$$
$$\phi\left((c_0 c_1 ... c_{n-1})\right) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

şeklinde tanımlanan $\phi$ fonksiyonu $V(n,q)$ ile $R_n$ arasında bir izomorfizmadır.

Eğer $C$, $R_n = \dfrac{F_q[x]}{\langle x^n - 1 \rangle}$ halkasının bir ideali ise devirli bir kod olur. $R_n$, $F_q$ üzerinde derecesi $n$'den küçük olan tüm polinomların kümesidir. Tüm polimomlar mod $x^n - 1$' e göre olacaktır [8] .

### 1.3.1. Devirli bir kodun üreteç polinomu

Aşağıdaki teorem devirli kodlar hakkındaki bazı gerçekleri içerir. $R_n$ halkası temel ideal bölgesidir.

**Teorem 1.3.1.1** $C$, $R_n$' de bir ideal yani $n$ uzunluğunda devirli bir kod olsun [8] .

1) $C$'de minimum dereceli tek bir monik $g(x)$ polinomu vardır. Bu polinomu $C$'yi üretir yani $C=\langle g(x)\rangle$ tir. $g(x)$ polinomuna, $C$'nin üreteç polinomu denir.

2) Üreteç polinomu $g(x)$, $x^n-1$ 'i böler.

3) $der(g(x))=r$ ise $C$'nin boyutu $n-r$ dir. Yani,

$$C=\langle g(x)\rangle=\{r(x)g(x)\,|\,der(r(x))<n-r\}$$

dir.

4) $g(x)=g_0+g_1x+g_2x^2+...+g_rx^r$ ise bu durumda $g_0\neq 0$ dır ve $C$'nin üreteç matrisi

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_r & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{bmatrix}$$

olur. Burada $G$ nin herbir satırı önceki satırın devirli bir ötelemesidir.

**Teorem 1.3.1.2** $R^n$ 'deki monik bir polinomun devirli bir kodun üreteç polinomu olması için gerek yeter koşul $p(x) \mid x^n - 1$ olmasıdır [8] .

### 1.3.2. Devirli bir kodun kontrol polinomu

$R^n$ 'deki devirli bir $[n, n-r]$- kodunun üreteç polinomu $g(x)$, $x^n - 1$ 'i böldüğü için, $x^n - 1 = g(x)h(x)$ olarak yazılır. $h(x)$ polinomuna $C$'nin kontrol polinomu denir ve $h(x)$ polinomunun derecesi $n-r$ dir [8] .

**Teorem 1.3.2.1** $h(x)$, $R^n$ 'deki devirli bir $C$ kodunun kontrol polinomu olsun [8] .

1) $C$ kodu,

$$C = \left\{ p(x) \in R^n \mid p(x)h(x) \equiv 0 \right\}$$

olur.

2) Eğer $h(x) = h_0 + h_1 x + \cdots + h_{n-r} x^{n-r}$ ise $C$'nin kısmi kontrol matrisi,

$$H = \begin{bmatrix} h_{n-r} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_{n-r} & \dots & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_{n-r} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \dots & \ddots & 0 \\ 0 & 0 & \dots & 0 & h_{n-r} & \dots & h_0 \end{bmatrix}$$

ile tanımlanmaktadır.

3) $C^{\perp}$ dual kodu

$$h^{\perp}(x) = h_0^{-1} x^{n-r} h\left(x^{-1}\right) = h_0^{-1}\left(h_0 x^{n-r} + h_1 x^{n-r-1} + \ldots + h_{n-r}\right)$$

üreteç polinomu ile $r$ boyutlu devirli bir koddur.

## 1.4. Ağırlık Sayaçları, Karakterler ve MacWilliams Özdeşliği

**Tanım 1.4.1** $(G,+)$ sonlu değişmeli bir grup ve $(\mathbb{C}-\{0\},.)$ kompleks sayıların çarpımsal grubu olsun. $\chi: G \to \mathbb{C}-\{0\}$ homomorfizması varsa $\chi$'e $G$ grubunun karakteri denir. $G$'nin tüm karakterlerinin kümesi $G$ ile gösterilir. Eğer $n$, $G$ grubunun mertebesi ise $x \in G$ için $x^n = e$ dir. Böylece $1 = \chi(e) = \chi(x^n) = \chi(x)^n$ yani $\chi(x)$ birimin $n$. köküdür [29] .

$\chi$ homomorfizma olduğundan $\forall u, v \in G$ için, $\chi(u+v) = \chi(u).\chi(v)$ ve $\chi(0) = 1$ dir. Eğer $\forall u \in G : \chi(u) = 1$ ise $\chi$ özel olarak $G$ grubunun temel karakteridir [8] .

**Teorem 1.4.1** $G$ bir grup ve $\chi$ de $G$ grubunun bir karakteri olsun. O halde,

$$\sum_{u \in G} \chi(u) = \begin{cases} |G|, & \chi \text{ temel karakter ise} \\ 0, & \text{diğer} \end{cases}$$

$\chi: F_q \to \mathbb{C}-\{0\}$ karakteri $(F_q,+)$ grubu üzerinde temel karakter olmasın. $u \in V(n,q)$ olmak üzere herhangi bir $C \subset V(n,q)$ lineer kodu için $\chi_u : C \to \mathbb{C}-\{0\}$ fonksiyonu $c = (c_1, c_2, \ldots, c_n)$ ve $u = (u_1, u_2, \ldots, u_n)$ olmak üzere, $\chi_u(c) = \chi(\langle c,u \rangle) = \chi(c_1u_1 + c_2u_2 + \ldots + c_nu_n)$ şeklinde tanımlanabilir. İç çarpım özellikleri ve $\chi_u$ için verilen tanım kullanılarak $\chi_u$ fonksiyonunun $C$ kodu için karakter olduğu aşağıdaki gibi gösterilir [8] :

$$\chi_u(c+d) = \chi(\langle c+d,u \rangle) = \chi(\langle c,u \rangle + \langle d,u \rangle)$$

$$= \chi(\langle c,u \rangle).\chi(\langle d,u \rangle) = \chi_u(c).\chi_u(d)$$

**Teorem 1.4.2** $\chi_u : C \to \mathbb{C} - \{0\}$ karakterinin temel karakter olabilmesi için gerek yeter koşul $u \in C^{\perp}$ olmasıdır [8] .

**Teorem 1.4.3** (MacWiliams Özdeşliği) $R$ üzerinde tanımlı $[n,k,d]$ lineer kodu $C$ olsun. Bu durumda,

$$W_{C^{\perp}}(z) = \frac{1}{|C|} \cdot \sum_{c \in C} \left(1 + (q-1)z\right)^{n-w(c)} (1-z)^{w(c)}$$

dir [14] .

# BÖLÜM 2. $u^2=1$; $\mathbb{Z}_4+u\mathbb{Z}_4$ HALKASI

Tezde $R=\frac{\mathbb{Z}_4[u]}{<u^2-1>}\cong\mathbb{Z}_4+u\mathbb{Z}_4$, $u^2=1$ halkası çalışılacaktır. Bu halka $u\to u+1$ yoluyla [39] daki $\frac{\mathbb{Z}_4[u]}{<u^2+2u>}$ halkasına izomorf olan, 16 mertebeli 7 tane LFNCR halkadan biridir.

## 2.1. $u^2=1$; $\mathbb{Z}_4+u\mathbb{Z}_4$ Halkasının Yapısı

$u^2=1$ için $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası aşağıdaki gibi tanımlanır:

$$\mathbb{Z}_4+u\mathbb{Z}_4=\{0,1,2,3,u,2u,3u,1+u,2+u,3+u,1+2u,2+2u,3+2u,1+3u,2+3u,3+3u\}$$

Bu durumda $\mathbb{Z}_4+u\mathbb{Z}_4$ halkasının 16 elemanlı olduğu görülür.

$u^2=1$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası $R$ ile gösterilsin.

$\langle 0\rangle,\langle 1\rangle,\langle 2u\rangle,\langle 1+u\rangle,\langle 3+u\rangle,\langle 2+2u\rangle,\langle 2u,1+u\rangle$ olmak üzere $R$'nin 7 tane ideali mevcut olup bu ideallerin elemanları aşağıdaki gibidir :

$$\langle 0\rangle=\{0\}$$

$$\langle 1\rangle=\langle u\rangle=\langle 3\rangle=\langle 3u\rangle=\langle 2+u\rangle=\langle 1+2u\rangle=\langle 3+2u\rangle=\langle 2+3u\rangle=R$$

$$\langle 2\rangle=\langle 2u\rangle=\langle 2,2+2u\rangle=\langle 2u,2+2u\rangle=\{0,2,2u,2+2u\}$$

$$\langle 1+u\rangle=\langle 3+3u\rangle=\langle 1+u,2+2u\rangle=\langle 3+3u,2+2u\rangle=\{0,1+u,2+2u,3+3u\}$$

$$\langle 3+u\rangle=\langle 1+3u\rangle=\langle 3+u,2+2u\rangle=\langle 1+3u,2+2u\rangle=\{0,3+u,2+2u,1+3u\}$$

$$\langle 2+2u\rangle=\{0,2+2u\}$$

$$\begin{aligned}\langle 2,1+u\rangle &= \langle 2u,1+u\rangle = \langle 2u,3+3u\rangle = \langle 2,3+3u\rangle = \langle 2u,3+u\rangle = \langle 2,3+u\rangle = \langle 2u,1+3u\rangle \\ &= \langle 2,1+3u\rangle = \langle 1+u,3+u\rangle = \langle 3+3u,3+u\rangle = \langle 1+u,1+3u\rangle = \langle 3+3u,1+3u\rangle \\ &= \{0,1+u,2+2u,3+3u,2,3+u,2u,1+3u\}\end{aligned}$$

$R$ 'nin terslenebilen elemanları $\{1,3,u,3u,2+u,1+2u,3+2u,2+3u\}$, karakteristiği 4, maksimal ideali de $\langle 2,\, 1+u\rangle$ dur. $R$ tek maksimal ideale sahip olduğundan lokal bir halkadır.

$R$ üzerinde $n$ uzunluğunda lineer bir $C$ kodu, $R^n$ 'nin bir $R$ alt modülüdür. $C$ 'nin bir elemanı kodsöz olarak adlandırılmaktadır. $R$ bir zincir halka olmadığından $R$ üzerindeki lineer bir kodun üreteç matrisi için kanonik bir form yoktur. Ancak bu kodlar için üreteç kümesi bulunabilir.

$R^n$ 'de bir Gray dönüşümü, $a,b\in\mathbb{Z}_4$ ve herhangi bir $z\in R$ için $z=b+(a-b)u$ olacak şekilde $\Phi: R\to\mathbb{Z}_4$ , $\Phi(z)=(b,\, b+a)$ formunda tanımlansın. Bu dönüşüm $R^n$ 'den $\mathbb{Z}_4^{2n}$ 'e genişletilebilir.

Bu durumda, $z=(z_1,z_2,...,z_n)\in R^n$ için $\Phi$, $R^n$ 'e aşağıdaki gibi genişletilmektedir.

$1\le i\le n$ iken, $z_i=b_i+(a_i-b_i)u$ için,

$$\Phi: R^n\to\mathbb{Z}_4^{2n}$$

$$(z_1,z_2,...,z_n)\to(b_1,b_2,...,b_n,b_1+a_1,b_2+a_2,...,b_n+a_n)$$

dir.

$\mathbb{Z}_4$ üzerindeki kodlar için en önemli ağırlıkların ikisi Lee ve Öklid ağırlıklarıdır. $x\in\mathbb{Z}_4$ 'ün Lee ağırlığı $w_L(x)=\min\{x,\,4-x\}$ dir. Böylece $0,1,2,3$ 'ün Lee ağırlıkları, sırasıyla, $0,1,2,1$ dir. $x\in\mathbb{Z}_4$ 'ün Öklid ağırlığı $w_E(x)=\min\left\{x^2,\,(4-x)^2\right\}$

dir. Böylece $0,1,2,3$ 'ün Öklid ağırlıkları, sırasıyla, $0,1,4,1$ dir. $x \in \mathbb{Z}_4^{\,n}$ 'deki bir kodsözün Lee (yada Öklid) ağırlığı, koordinatlarının Lee (yada Öklid) ağırlıklarının rasyonel toplamı olarak tanımlanır.

$z = b + (a-b)u \in R$ elemanının Lee ve Öklid ağırlıkları aşağıdaki gibi tanımlansın:

$w_L(b+(a-b)u) = w_L(\Phi(z)) = w_L(b, a+b)$

$w_E(b+(a-b)u) = w_E(\Phi(z)) = w_E(b, a+b)$.

$p,t,r,s \in \mathbb{Z}_4$ olmak üzere $x = p + (t-p)u$ , $y = s + (r-s)u$ olsun. Bu durumda,

$\forall x, y \in R^n$: $\Phi(x) = (p, p+t), \Phi(y) = (s, s+r)$ için,

$$\begin{aligned} d_{L'}(x,y) = w_{L'}(x-y) &= w_{L'}\left(\left(p+(t-p)u\right) - \left(s+(r-s)u\right)\right) \\ &= w_{L'}\left(\Phi\left(p-s+u(t-p-r+s)\right)\right) \\ &= w_L\left(p-s,\, p-s+t-r\right) \\ &= w_L\left(\Phi(x) - \Phi(y)\right) \\ &= d_L\left(\Phi(x), \Phi(y)\right) \end{aligned}$$

olduğundan yani uzaklık korunduğundan $\Phi$ , $\left(R^n, d_{L'}\right) \to \left(\mathbb{Z}_4^{2n}, d_L\right)$ bir izometridir.

$\forall x, y \in R^n, k \in \mathbb{Z}_4$ için, $x = p + (t-p)u$ , $y = s + (r-s)u$ olmak üzere,

a) $$\begin{aligned} \Phi(x+y) &= \Phi\left(\left(p+(t-p)u\right) + \left(s+(r-s)u\right)\right) \\ &= \left((p+s) + (t-p+r-s)u\right) \\ &= \left(p+s,\ p+s+r+t\right) \\ &= (p,\ p+t) + (s,\ s+r) = \Phi(x) + \Phi(y) \end{aligned}$$ ve

b) $$\begin{aligned} \Phi(kx) = \Phi\left(k\left(p+(t-p)u\right)\right) &= \Phi\left(kp + k(t-p)u\right) \\ &= \left(kp,\ k(p+t)\right) = k(p,\ p+t) = k\,\Phi(x) \end{aligned}$$

olduğundan $\Phi$ Gray dönüşümü lineerdir.

$\Phi$ dönüşümünün lineer ve izometri olduğu Lee ağırlığa göre gösterilmiştir. Benzer şekilde Öklid ağırlık için de gösterilebilir.

# BÖLÜM 3. $u^2=1$; $\mathbb{Z}_4+u\mathbb{Z}_4$ HALKASINDA DEVİRLİ KODLAR

Devirli kodlar en çok çalışılan cebirsel yapılar arasındadır. Bundan dolayı, devirli kodlar üzerine literatürde pek çok çalışma vardır. Son iki yılda pek çok kodlama teorisi araştırmacısının dikkatini çeken diğer kod sınıfları, halkalar üzerindeki kodlardır. Halka üzerindeki kodlara ilgi, ufuk açıcı bir çalışmayla başlamış ([39]) ve pek çok yönde genişlemiştir.

Mertebesi 16 olan halkalar özel bir öneme sahiptir. En küçük sonlu lokal değişmeli zincir olmayan Frobenius halkasının (LFNCR) 16 mertebeli olduğu bilinmektedir [39] . Kodlama teorisinde ilgi çeken 16 mertebeli pek çok halka $\mathbb{Z}_4$ genişlemesidir. Örneğin son zamanlarda $\mathbb{Z}_4+u\mathbb{Z}_4$ olarak ifade edilen, $u^2=0$ iken $\mathbb{Z}_4/<u^2>$ üzerindeki kodlar ele alınmaktadır ([25]) ve bu halkalar üzerindeki devirli kodlar yakın zamanda [27]'de çalışılmıştır. [27]'de Yıldız ve Aydın $u^2=0$ için $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerinde devirli kodların cebirsel yapısını belirleyerek, üreteçlerini araştırmışlardır.

$u^2=0$ iken cebirsel yapılar kullanılarak $\mathbb{Z}_4$ üzerinde pek çok yeni lineer kod elde edilmiştir. [21]'de T. Abualrup ve I. Siap tarafından $\mathbb{Z}_2+u\mathbb{Z}_2$ ve $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$ deki devirli kodların üreteç kümeleri bulunmuştur ve bu halkalar üzerindeki rank, dual ve Hamming uzaklık konuları çalışılmıştır. [16]'da Wolfmann devirli kodlara yoğunlaşmış ve üreteç polinomlarını kullanarak $\mathbb{Z}_4$ üzerindeki Gray görüntüleri lineer kodlar olan yada Nechaev görüntüleri lineer devirli kodlar olan tüm lineer devirli kodları incelemiştir.

Bu bölümde $u^2=1$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerindeki devirli kodlar incelenecektir. Bu halka üzerindeki devirli kodların üreteçleri araştırılıp geren kümeler oluşturulacaktır.

### 3.1. $\mathbb{Z}_4+u\mathbb{Z}_4$ Halkasında Devirli Kodlar

$R^n$ 'de devirli öteleme operatörü $\sigma(c_0,c_1,...,c_{n-1})=(c_{n-1},c_0,...,c_{n-2})$ olsun. $\sigma$ altında korunan lineer $C$ koduna yani $\sigma(C)=C$ ifadesine devirli bir kod denir. Vektörleri $\vec{c}=(c_0,c_1,...,c_{n-1})$ olarak bilinen $c_0+c_1x+...+c_{n-1}x^{n-1}$ polinomu $R$ üzerinde $n$ uzunluğundaki devirli kodlar olan $R_n=\dfrac{R[x]}{<x^n-1>}$ halkasının idealleridir.

$R_n$ 'deki ideallerin yapısını belirlemek için, [27] 'de ele alındığı gibi, $R$ 'den $\mathbb{Z}_4$ 'e $\varphi(a+ub)=a-b \pmod{(1+u)}$ dönüşümü tanımlansın.

$\varphi$ 'nin $çek(\varphi)=<1+u>=(1+u)\mathbb{Z}_4$ ile örten halka homomorfizması olduğu açıktır.

$\varphi$ dönüşümü ilk olarak $R[x]$ 'ten $\mathbb{Z}_4[x]$ 'e daha sonra da $\varphi(a_0+a_1x+...+a_{n-1}x^{n-1})=\varphi(a_0)+\varphi(a_1)x+...+\varphi(a_{n-1})x^{n-1}$ ile $R_n$ 'den $\mathbb{Z}_4[x]/<x^n-1>$ 'e genişletilsin.

$C$, $R^n$ 'de $n$ uzunluğunda devirli bir kod olsun. $\varphi$ 'nin tanım kümesi de $C$ 'ye kısıtlandırılsın. Bu durumda $\varphi(C)$, $\mathbb{Z}_4[x]/<x^n-1>$ 'in bir idealidir ve $çek(\varphi|_C)$ de $(1+u)\mathbb{Z}_4[x]/<x^n-1>$ 'in bir idealidir. Böylece $\varphi(C)$, $\mathbb{Z}_4[x]/<x^n-1>$ 'deki bazı $I$ idealleri için $(1+u)I$ formundadır.

$\mathbb{Z}_4[x]/<x^n-1>$ 'deki ideallerin tanımlaması yapıldığına göre $C$ 'nin idealleri oluşturulabilir. $\mathbb{Z}_4[x]/<x^n-1>$ 'deki idealler $n$ tek ve $n$ çift olması durumunda farklı tanımlamalara sahiptir ([32], [33]) :

**Teorem 3.1.1** [32] $n$ tek pozitif tamsayı ve $C$, $\mathbb{Z}_4[x]/<x^n-1>$ 'in bir ideali olsun. Bu durumda $x^n-1=g(x)f(x)h(x)$ iken $g(x)$ ile $h(x)$ polinomları $\mathbb{Z}_4$ üzerinde aralarında asal olacak şekilde $f(x), g(x)$ ve $h(x)$ monik polinomları vardır. Bu durumda

$$C=<f(x)h(x)+2f(x)>$$

dir.

Bu teoreme ve yukarıdaki tartışmaya dayanarak $R$ üzerinde tek uzunlukta olan devirli kodlar aşağıdaki gibi tanımlanabilir:

**Teorem 3.1.2** $R$ üzerinde $n$ uzunluğunda devirli bir kod $C$ ve $n$ pozitif tek tamsayı olsun. Bu durumda, Teorem 3.1.1'deki gibi elde edilen $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerindeki herhangi $g_2(x)$ polinomu ve $\mathbb{Z}_4$ üzerindeki herhangi $g_1(x)$ ve $g_3(x)$ polinomları için,

$$C=<g_1(x)+(1+u)g_2(x),(1+u)g_3(x)>$$

dir.

$\mathbb{Z}_4$ üzerinde çift uzunluktaki devirli kodların yapısı [33]te verilmiştir:

**Teorem 3.1.3** [33] $C$, $\mathbb{Z}_4$ üzerinde $n$ uzunluğunda devirli bir kod ve $n$ çift olsun. Bu durumda ya

a) $g(x)\,|\,(x^n-1) \pmod 2$ ve $(g(x)+2p(x))\,|\,(x^n-1) \pmod 4$ iken

$$C=<g(x)+2p(x)>$$

formundaki bir üreteçle $C$ bir serbest modüldür, yada

b) $(g(x)+2p(x))\big|(x^n-1) \pmod 4$, $a(x)\big|g(x) \pmod 2$, $a(x)\big|p(x)\left(\frac{x^n-1}{g(x)}\right)$ $\pmod 2$ ve $der(g(x)) > der(a(x))$ iken

$$C =< g(x)+2p(x),\ 2a(x) >$$

formundaki üreteçle $C$ bir serbest modüldür.

Böylece $R$ üzerinde çift uzunluktaki devirli kodlar aşağıdaki gibi tanımlanabilir:

**Teorem 3.1.4** $C$, $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $n$ uzunluğunda devirli bir kod olsun. $g_i(x)$, $p_i(x)$ ve $a_i(x)$'ler Teorem 3.1.3'teki şartları sağlaması ve $g_2(x),\ a_2(x)\in\mathbb{Z}_4+u\mathbb{Z}_4$ olması durumunda,

$$C =< g_1(x)+2p_1(x)+(1+u)g_2(x),\ 2a_1(x)+(1+u)a_2(x),$$

$$(1+u)(g_3(x)+2p_3(x)),\ 2(1+u)a_3(x) >$$

formundadır.

**Lemma 3.1.1** $f(x)$ ve $f_1(x)+(1+u)f_2(x)$, $R[x]$'te iki polinom olmak üzere, $f_1(x)+(1+u)f_2(x)$ regüler ise, $f(x)=(f_1(x)+(1+u)f_2(x)).q(x)+p(x)$ olacak şekilde $q(x)$ ve $p(x)$ polinomları vardır ve $der\,p(x) < der(f_1(x)+(1+u)f_2(x))$ tir.

**İspat** $f_1(x)+(1+u)f_2(x)$ regüler olduğundan [4, Teorem XIII.6]'dan $f_1(x)+(1+u)f_2(x)=v(x).g^*(x)$ olacak şekilde $g^*(x)\in R[x]$ monik ve $v(x)\in R[x]$ birimsel polinomu vardır.

$g^*(x)$ monik olduğundan [4, sf.273] ten, $der\,p(x)<der\,g^*(x)$ olacak şekilde $f(x)=g^*(x).q'(x)+p(x)$ yazılır. Her iki taraf $v(x)$ ile çarpılarak,

$q'(x)=q(x).v(x)$ olacak şekilde $f(x)=\left(f_1(x)+(1+u)f_2(x)\right).q(x)+p(x)$ elde edilir. $g^*(x)$ monik ve $f_1(x)+(1+u)f_2(x)=v(x).g^*(x)$ olduğundan, $der\,g^*(x)<der\left(f_1(x)+(1+u)f_2(x)\right)$ dır.

Ayrıca, $der(f_1(x)+(1+u)f_2(x))=der(v(x))+der(g^*(x))$ dir. Bölme algoritmasından $der(p(x))<der(g^*(x))<der\left(f_1(x)+(1+u)f_2(x)\right)$ bulunarak $der\,p(x)<der\left(f_1(x)+(1+u)f_2(x)\right)$ olduğu görülür.

Devirli bir kod için geren küme aşağıdaki gibi tanımlanabilir:

**Teorem 3.1.6** $n$ tek uzunlukta olmak üzere $C=\left\langle f_1(x)+(1+u)f_2(x),(1+u)s(x)\right\rangle$, $R$ üzerinde $n$ uzunluğunda devirli bir kod olsun. $der\,f_1(x)+(1+u)f_2(x)=r_1$, $der\,s(x)=r_2$ olmak üzere, $f_1(x)+(1+u)f_2(x)$ $R[x]$'te regüler bir polinom ve $s(x)$ $\mathbb{Z}_4$ üzerinde monik bir polinom ise $r_1>r_2$, $C$'nin rankı $n-r_2$ ve $C$'yi geren minimal küme

$B=\{f_1(x)+(1+u)f_2(x),x\left(f_1(x)+(1+u)f_2(x)\right),...,x^{n-r_1-1}\left(f_1(x)+(1+u)f_2(x)\right),$
$(1+u)s(x),x(1+u)s(x),...,x^{r_1-r_2-1}(1+u)s(x)\}$

dir.

**İspat** $C=\left\langle f_1(x)+(1+u)f_2(x),(1+u)s(x)\right\rangle$ iken, $f_1(x)+(1+u)f_2(x)$ regüler ve $s(x)$ de monik bir polinom, $der\,f_1(x)+(1+u)f_2(x)=r_1$, $der\,s(x)=r_2$ olsun. İlk olarak $r_1>r_2$ olduğu gösterilsin.

Bunu göstermek için öncelikle $x^k\left((1+u)s\right)$, $B$'nin lineer kombinasyonu olarak yazılmalıdır. $f_1+(1+u)f_2$ regüler olduğundan Lemma 3.1.1'den $x^ks=(f_1+(1+u)f_2).q+p$, $der(p)<der(f_1+(1+u)f_2)=r_1$ olacak şekilde $q,p\in R[x]$ polinomları vardır. Her iki taraf $(1+u)$ ile çarpılarak, $(1+u)x^ks=(1+u)\left(f_1+(1+u)f_2\right).q+(1+u)p$ ve $der\left((1+u)p\right)<r_1$ elde edillir.

Buradan, $(1+u)p = x^k(1+u)s - (1+u)\left(f_1 + (1+u)f_2\right).q \in C$ dir. Böylece, herhangi $a,b \in R[x]$ için, $(1+u)p = a.\left(f_1 + (1+u)f_2\right) + b.\left((1+u)s\right)$ yazılabilir. $der(p) < r_1$ olduğundan $a = 0$ olmalıdır. Öyleyse, $(1+u)p = b.(1+u)s$ tir. $s$ monik olduğundan $der(p) = der(b) + der(s) = der(b) + r_2$ dir. Buradan $der\left((1+u)p\right) \geq r_2$ dir. Dolayısıyla, $r_2 \leq der\left((1+u)p\right) < r_1$ elde edilir. Aynı zamanda, $der(b) < r_1 - r_2$ olduğu görülür.

Böylece, $(1+u)p = b_0\left((1+u)s\right) + b_1 x\left((1+u)s\right) + \ldots + b_{r_1-r_2-1}x^{r_1-r_2-1}\left((1+u)s\right)$ ve

$$x^k\left((1+u)s\right) = (1+u)\left(f_1 + (1+u)f_2\right)q + \underbrace{b_0\left((1+u)s\right) + b_1 x\left((1+u)s\right) + \ldots + b_{r_1-r_2-1}x^{r_1-r_2-1}\left((1+u)s\right)}$$

$$\downarrow \qquad \downarrow \qquad\qquad\qquad \downarrow$$
$$k + r_2 \qquad r_1 \qquad\qquad\qquad \leq r_1 - 1$$

tir.

1. Durum : $q(x)$ sabit bir polinom ise $der\left(q(x)\right) = 0$ dır. Bu durumda $k + r_2 = r_1$ olur. Öyleyse $k = r_1 - r_2$ dir.

2. Durum : $q(x)$ sabit polinom olmasın. $der\left(q(x)\right) = m$ olsun. Bu durumda $k + r_2 = r_1 + m$ olur. Öyleyse, $k = r_1 - r_2 + m > r_1 - r_2$ elde edilir.

Her iki durum incelendiğinde $k \geq r_1 - r_2$ olması durumunda $x^k(us)$ ifadesi

$\{f_1(x) + (1+u)f_2(x), x\left(f_1(x) + (1+u)f_2(x)\right), \ldots, x^{n-r_1-1}\left(f_1(x) + (1+u)f_2(x)\right),$
$(1+u)s(x), x(1+u)s(x), \ldots, x^{r_1-r_2-1}(1+u)s(x)\}$

elemanlarının lineer kombinasyonu olarak yazılabilir. Böylece, $x^{r_1-r_2}(us) \in span(B)$ elde edilir. Herhangi bir $k > r_1 - r_2$ için $x^k\left((1+u)s\right) \in span(B)$ olduğu da benzer şekilde gösterilebilir. Bu durumda $B$, $C$'nin bir üreteç kümesi olur.

$B$'nin lineer bağımsız olması için, $d(x),h(x)\in R[x]$ olacak şekilde $d(x).(f_1+(1+u)f_2)+h(x).(1+u)s(x)=0\in R_n$ olmalıdır. $der\left(d\left(x\right)\right)=n-r_1-1$ ve $der\left(h\left(x\right)\right)=r_1-r_2-1$ olsun. Bu durumda, $d\left(x\right)=d_0+d_1x+d_2x^2+...+d_{n-r_1-1}x^{n-r_1-1}$ ve $h\left(x\right)=h_0+h_1x+h_2x^2+...+h_{r_1-r_2-1}x^{r_1-r_2-1}$ dir.

$f_1\left(x\right)+\left(1+u\right)f_2\left(x\right)$ regüler olduğundan, $\left(f_1\left(x\right)+\left(1+u\right)f_2\left(x\right)\right)=v\left(x\right).g^*\left(x\right)$ olacak şekilde $g^*\left(x\right)\in R\left[x\right]$ monik polinomu ve $v\left(x\right)\in R\left[x\right]$ birimsel polinomu vardır. $g^*\left(x\right)$ monik olduğundan $g^*\left(x\right)=g_0^*+g_1^*x+...+g_{n-r_1-1}^*x^{n-r_1-1}$ polinomunda $g_{n-r_1-1}$ birimsel elemandır. Başlangıçta $d(x).(f_1+(1+u)f_2)+h(x).(1+u)s(x)=0$ eşitliği $d\left(x\right).\left(v\left(x\right).g^*\left(x\right)\right)+h\left(x\right).\left(1+u\right)s\left(x\right)=0$ olarak yazılabilir. $d\left(x\right)$ ve $h\left(x\right)$ polinomları yerine yazılarak, $\left(d_0+d_1x+d_2x^2+...+d_{n-r_1-1}x^{n-r_1-1}\right)\left(v\left(x\right).g^*\left(x\right)\right)+$ $\left(h_0+h_1x+h_2x^2+...+h_{r_1-r_2-1}x^{r_1-r_2-1}\right)\left(\left(1+u\right)s\left(x\right)\right)=0$ elde edilir.

Bu durumda, $r_1-r_2\le i\le n-r_1-1$ için katsayılar $x^i.v\left(x\right).g^*\left(x\right).d_i=0$ olur. Yani, $v\left(x\right).g^*\left(x\right).d_i=0$ dir. $v\left(x\right)$ birimsel polinom olduğundan $g^*\left(x\right).d_i=0$ dır. $g^*\left(x\right)$ polinomu yerine yazılırsa, $\left(g_0^*+g_1^*x+g_2^*x^2+\ldots+g_{n-r_1-1}^*x^{n-r_1-1}\right).d_i=0$ elde edilir. Bu eşitliğin en büyük dereceli katsayısı $g_{n-r_1-1}^*.d_i=0$ dır. Buradan $g_{n-r_1-1}^*=1$ olduğundan $d_i=0$ bulunur.

$0\le j\le r_1-r_2-1$ için katsayılar $x^j.\left(v\left(x\right).g^*\left(x\right).d_j+\left(1+u\right)s\left(x\right).h_j\right)=0$ olur. Yani, $v\left(x\right).g^*\left(x\right).d_j+\left(1+u\right)s\left(x\right).h_j=0$ dır. $g^*\left(x\right)$ ve $s\left(x\right)$ polinomları yerine yazılırsa, $v\left(x\right).\left(\left(g_0^*+g_1^*x+g_2^*x^2+\ldots+x^{n-r_1-1}\right).d_j+\left(1+u\right)\left(s_0+s_1x+s_2x^2+\ldots+x^{r_2}\right)\right).h_j=0$ elde edilir. $r_2<n-r_1-1$ olduğundan bu ifade iki durumda incelenir:

1. Durum : $x$ 'in kuvveti $r_2$ 'den büyükse, $d_j.v\left(x\right).g_{n-r_1-1}=0$ dır. $g_{n-r_1-1}=1$ ve $v\left(x\right)$ te birimsel polinom olduğundan $d_j=0$ bulunur.

2. Durum : $x$ 'in kuvveti $r_2$ 'den küçükse, $x^{r_2}\left(v(x).g_{r_2}.d_j+(1+u)h_j\right)=0$ dır. Buradan $v(x).g_{r_2}.d_j+(1+u)h_j=0$ dır. $d_j=0$ bulunduğundan $(1+u)h_j=0$ dır. Böylece, $h_j=0$ elde edilir.

Sonuç olarak, $i=0,1,\ldots,n-r_1-1$ ve $j=0,1,\ldots,r_1-r_2-1$ için $d_i=0$ ve $h_j=0$ bulunur. Dolayısıyla $B$ lineer bağımsızdır.

**Teorem 3.1.7** $f(x)$ derecesi $n-k$ olan monik bir polinom olmak üzere, $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerinde $n$ uzunluğunda devirli bir kod $C=<f(x)>$ olsun. Bu durumda $C$ 'nin $k$ ranklı free modül olması için gerek yeter koşul $f(x)\left|\left(x^n-1\right)\right.$ olmasıdır.

**İspat** [26]'daki Teorem 1'in ispatına benzer şekilde yapılır.

**Lemma 3.1.2** $\left(\mathbb{Z}_4+u\mathbb{Z}_4\right)[x]$ 'te $x^m-1=g(x)h(x)$ ve $C$, $g(x)$ tarafından üretilen devirli bir kod olsun. Eğer $f(x)$ ile $h(x)$ aralarında asal ise $C=<g(x)f(x)>$ dir [26] .

**İspat** [26]'daki Lemma 2'nin ispatına benzer şekilde yapılır.

# BÖLÜM 4. $u^2=1$; $\mathbb{Z}_4+u\mathbb{Z}_4$: SABİT DEVİRLİ KODLAR

Devirli kodlar pek çok genelleştirmeye sahiptir. Bunlardan biri de sabit devirli kodlardır. Kodlama teorisinde 1950 sonlarından beri çalışılan lineer kodların, önemli bir sınıfını sabit devirli kodlar oluşturmaktadır.

[38]'deki çalışma sonrasında sabit devirli kodlar üzerinde pek çok çalışma yapılmıştır. Çeşitli halkalar üzerindeki sabit devirli kodlar da son yıllarda geniş ölçüde çalışma alanı bulmuştur (13, 20, 21, 22). Gray dönüşümü ile $\mathbb{Z}_4$ üzerindeki devirli kodlardan inşa edilebilen lineer olmayan devirli kodların keşfinden sonra, 1970'lerden beri çalışılan sonlu halkalar üzerindeki kodlara dikkat çekilmiştir. Sonlu değişmeli halka üzerindeki sabit devirli kodlar ilk olarak Wolfmann tarafından [15]'te incelenmiştir. Burada $\mathbb{Z}_4$ üzerindeki lineer nega devirli (negacyclic) bir kodun ikili görüntüsünün uzaklığı koruyan devirli bir kod olduğu çalışılmıştır. Dikkat edilmelidir ki bu çalışmada devirli kod bulunurken bu devirli kodun lineer olma şartı yoktur. Daha sonra Blackford bu dönüşümü kullanarak $\mathbb{Z}_4$ üzerinde çift uzunluktaki tüm nega devirli kodları sınıflandırmıştır [18]. 2001 yılında Wolfmann, $\mathbb{Z}_4$ üzerindeki devirli kodların ikili görüntülerini incelemiş [16], Ling ve Blackford da [15] ile [16]'daki sonuçların çoğunu [17]'de $\mathbb{Z}_{p^{k+1}}$ halkasına genişletmiştir. 1990 sonlarından itibaren, [19]'daki $F_p+uF_p$ üzerindeki lineer kodlar kullanılarak $F_p[u]/\langle u^m\rangle$ sonlu halkalarının bir sınıfına dikkat çekilmiş olup, $F_p[u]/\langle u^m\rangle$ üzerindeki lineer kodlara odaklanılmıştır. $F_2+uF_2$ halkası hem $\mathbb{Z}_4$ halkası hemde $F_4$ Galois cisminin bazı iyi özelliklerini sağladığından ciddi çalışma alanı bulmuştur. $F_2+uF_2$ üzerindeki devirli ve kendine dual kodlar pek çok araştırmacı tarafından çalışılmış olup ( örn. [20], [21], [22], [23] ) $F_2+uF_2$ üzerindeki tek uzunlukta olan

$(1+u)$- sabit devirli kodlar ilk olarak Qian tarafından [13]'te çalışılmıştır. Bu çalışmada $F_2+uF_2$ üzerindeki tek uzunlukta olan $(1+u)$- sabit devirli bir kodun Gray görüntüsünün uzaklığı koruyan lineer devirli bir kod olduğu ispatlanmıştır. Minjia [31]'de zincir olmayan $F_p+vF_p$ halkası üzerindeki sabit devirli kodlara yoğunlaşmış, Gray dönüşümü belirlemiş ve $p$'nin tek olması durumunda Gray dönüşümle optimal $p$-li lineer (devirli) kod elde etmiştir. [20]'de ise Abualrup ve Şiap tarafından $F_2+uF_2$ rastgele bir $n$ uzunluğunda olan $(1+u)$- sabit devirli bir koda odaklanılmış, $(1+u)$- sabit devirli kodların ve bu ikili kodların Gray görüntüsü ispatlanmıştır. Ayrıca herbir $(1+u)$- sabit devirli kodların ve duallerinin üreteç kümesi bulunmuştur.

Bu bölümde $u^2=1$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerinde uzunluğu tek olan $(2+u)$- sabit devirli kodlar incelenip, sabit devirli kodlar için Gray dönüşümü tanımlanarak uzunluğu tek olan devirli bir kodun Gray görüntüsünün devirli bir koda eşit olduğunu ispatlanacaktır. Ayrıca sabit devirli kodların üreteç polinomları da belirlenecektir.

Öncelikle sabit devirli kodun tanımı verilsin:

$\lambda$, $R$'de birimsel eleman olmak üzere, $\upsilon(c_0,c_1,...,c_{n-1})=(\lambda c_{n-1},c_0,...,c_{n-2})$ sabit devirli öteleme operatörü altında $R$ üzerinde $n$ uzunluğunda lineer bir $C$ koduna $\lambda$ - sabit devirli bir kod, $\lambda$ sabitine de $C$'nin devir sabiti denir. Sabit devirli kodların en temel sonuçlarından biri $R_{n,\lambda}=R[x]/(x^n-\lambda)$ üzerinde ideallerinin olmasıdır. Ayrıca $\lambda=1$ olması durumunda, devirli kodlar sabit devirli kodların özel bir durumu olmaktadır.

## 4.1. $R$ Halkasındaki $(2+u)$- Sabit Devirli Kodların Gray Görüntüleri

$\Phi$ $R^n$ 'den $\mathbb{Z}_4^{2n}$ 'e bir dönüşüm, $\sigma$ devirli öteleme operatörü ve $\upsilon$ 'nin de sabit devirli öteleme operatörü olduğu hatırlatılsın. $(2+u)$- sabit devirli kodlardaki temel sonuç $(2+u)$- sabit devirli kodların Gray görüntülerinin $\mathbb{Z}_4$ üzerinde devirli kod olmasıdır.

**Önerme 4.1.1** Herhangi bir $\vec{c} \in R^n$ için, $\Phi\upsilon\left(\vec{c}\right) = \sigma\,\Phi\left(\vec{c}\right)$ dir.

**İspat** $\vec{c} = (c_0, c_1, \ldots c_{n-1})$, $R^n$ 'de bir kod olsun. $a_i$ ve $b_i$ 'ler $\mathbb{Z}_4$'te olmak üzere, $c_i = b_i + (a_i - b_i)u$ şeklinde tanımlansın. Tanımdan,

$\Phi\left(\vec{c}\right) = (b_0, b_1, ..., b_{n-1}, b_0 + a_0, b_1 + a_1, ..., b_{n-1} + a_{n-1})$ ve

$\sigma\Phi\left(\vec{c}\right) = (b_{n-1} + a_{n-1}, b_0, b_1, ..., b_{n-1}, b_0 + a_0, ..., b_{n-2} + a_{n-2})$ elde edilir.

Diğer yandan,

$$\upsilon\left(\vec{c}\right) = \left((2+u)c_{n-1}, c_0, ..., c_{n-2}\right)$$

$$= \left(a_{n-1} + b_{n-1} + u\left(2a_{n-1} - b_{n-1}\right), \ldots, b_{n-2} + u\left(a_{n-2} - b_{n-2}\right)\right)$$

dir. Buradan,

$$\Phi\left(\upsilon\left(\vec{c}\right)\right) = (b_{n-1} + a_{n-1}, b_0, b_1, ..., b_{n-1}, b_0 + a_0, ..., b_{n-2} + a_{n-2})$$

olduğu görülür. Böylece, $\Phi\upsilon(c) = \sigma\,\Phi(c)$ elde edilir.

**Teorem 4.1.1** $R$ üzerindeki $(2+u)$- sabit devirli bir $C$ kodunun Gray dönüşüm altındaki görüntüsü $\left(\Phi(C)\right)$, $\mathbb{Z}_4$ üzerinde devirli bir koddur.

**İspat** $C$, $R$ üzerinde $(2+u)$- sabit devirli bir kod olsun. Bu durumda $\upsilon(C)=C$ dir. Her iki tarafın $\Phi$ altındaki görüntüsü alınırsa, $(\Phi\upsilon)C=\Phi(C)$ elde edilir. Önerme 4.1.1'den yararlanarak $\sigma(\Phi(C))=\Phi(C)$ olduğu bulunur. Yani, $\Phi(C)$ devirli bir koddur.

**Önerme 4.1.2** $\Phi$ özel olarak, $\Phi(c_0,c_1,\ldots c_{n-1})=(b_0,b_0+a_0,b_1,\ldots b_{n-1},b_{n-1}+a_{n-1})$ şeklinde tanımlanırsa, herhangi bir $\vec{c}\in R^n$ için $\Phi\sigma(\vec{c})=\sigma^2\Phi(\vec{c})$ dir.

**İspat** $\Phi(\sigma(c_0,c_1,...,c_{n-1}))=(c_{n-1},c_0,c_1,...,c_{n-2})$

$=(b_{n-1},b_{n-1}+a_{n-1},b_0,b_0+a_0,...,b_{n-2},b_{n-2}+a_{n-2})$ elde edilir.

Diğer taraftan,

$$\sigma^2\left(\Phi\left(\vec{c}\right)\right)=\sigma^2\left(\left(b_0,b_0+a_0,b_1,...,b_{n-1},b_{n-1}+a_{n-1}\right)\right)$$

$$=\sigma\left(b_{n-1}+a_{n-1},b_0,b_0+a_0,b_1,...,b_{n-1}\right)$$

$$=\left(b_{n-1},b_{n-1}+a_{n-1},b_0,b_0+a_0,...,b_{n-2},b_{n-2}+a_{n-2}\right)$$

dir. Buradan $\Phi\sigma(\vec{c})=\sigma^2\Phi(\vec{c})$ eşitliği elde edilir.

Son önermenin sonucu aşağıdaki gibi ifade edilebilir:

**Sonuç 4.1.1** $C$, $R$ üzerinde $n$ uzunluğunda devirli bir kod olsun. Bu durumda $\Phi(C)$ de $\mathbb{Z}_4$ üzerinde $2n$ uzunluğunda 2- parçalı devirli (quasicyclic) koddur.

## 4.2. $R$ Halkasında Tek Uzunlukta olan $(2+u)$- Sabit Devirli Kodlar

Bu bölümde, tek uzunluktaki $(2+u)$- sabit devirli kodlar çalışılacaktır. Öncelikle,

$(2+u)^n = \begin{cases} 1 & n \text{ çift ise} \\ 2+u & n \text{ tek ise} \end{cases}$ tanımlansın.

**Önerme 4.2.1** $\mu : R[x]/\langle x^n-1\rangle \to R[x]/\langle x^n-(2+u)\rangle$ dönüşümü tanımlansın. $\mu(c(x)) = c((2+u)x)$ olsun. $n$ tek olması durumunda, $\mu$ bir halka izomorfizmasıdır.

**İspat**

İyi tanımlılık: $\forall c(x), b(x) \in \dfrac{R[x]}{\langle x^n-1\rangle}$ : $b(x) = c(x) \pmod{x^n-1}$ iken,

$\mu(b(x)) = \mu(c(x)) \pmod{(x^n-(2+u))}$ midir?

$b(x) = c(x) \pmod{x^n-1}$ ise $b(x) = (x^n-1).q(x)+c(x)$ dir. $x \mapsto (2+u)x$ yazılırsa,

$$\begin{aligned} b((2+u)x) &= (((2+u)x)^n-1).q((2+u)x)+c((2+u)x) \\ &= ((2+u)^n x^n-(2+u)^2).q((2+u)x)+c((2+u)x) \\ &= (2+u)(x^n-(2+u)).q((2+u)x)+c((2+u)x) \end{aligned}$$

elde edilir. Buradan,

$b((2+u)x) = (2+u)(x^n-(2+u)).q((2+u)x)+c((2+u)x)$ olduğu görülür. Yani, $\mu(b(x)) = \mu(c(x)) \pmod{(x^n-(2+u))}$ dur. Öyleyse, $\mu$ fonksiyonu iyi tanımlıdır.

Birebirlik:

$$\forall c(x), b(x) \in {R[x]}/{\langle x^n - 1 \rangle} : \mu(b(x)) = \mu(c(x)) \pmod{(x^n - (2+u))} \Rightarrow$$

$b(x) = c(x) \pmod{x^n - 1}$ mi?

$\mu(b(x)) = \mu(c(x)) \Rightarrow b((2+u)x) = c((2+u)x) \pmod{x^n - (2+u)}$ yani,

$b((2+u)x) = q((2+u)x).(x^n - (2+u)) + c((2+u)x) \pmod{(x^n - (2+u))}$ iken,

$x \mapsto (2+u)x$ yazılırsa,

$$\begin{aligned} b(x) &= \left(((2+u)x)^n - (2+u)\right).q(x) + c(x) \\ &= \left((2+u)^n x^n - (2+u)\right).q(x) + c(x) \\ &\overset{n \text{ tek}}{=} \left((2+u)x^n - (2+u)\right).q(x) + c(x) \\ &= (2+u)\left(x^n - 1\right).q(x) + c(x) \end{aligned}$$

elde edilir. Yani, $b(x) = c(x) \pmod{x^n - 1}$ dir. Bu da $\mu$ fonksiyonunun birebir olduğunu gösterir.

Örtenlik: Sonlu ve birebir olduğundan örtendir.

Homomorfizma: $\forall c(x), b(x) \in {R[x]}/{\langle x^n - 1 \rangle}$ :

$\mu(b(x) + c(x)) = \mu(b(x)) + \mu(c(x))$ ve $\mu(b(x).c(x)) = \mu(b(x)).\mu(c(x))$ mi?

$\forall c(x), b(x) \in {R[x]}/{\langle x^n - 1 \rangle}$ :

I) $$\begin{aligned} \mu(b(x) + c(x)) = \mu((b+c)(x)) &= (b+c)((2+u)x) \\ &= b((2+u)x) + c((2+u)x) \\ &= \mu(b(x)) + \mu(c(x)) \end{aligned}$$

ii) $\mu\big(b(x).c(x)\big)=\mu\big((b.c)(x)\big)=(b.c)\big((2+u)x\big)$

$$=b\big((2+u)x\big)+c\big((2+u)x\big)$$

$$=\mu\big(b(x)\big)+\mu\big(c(x)\big)$$

olduğundan $\mu$ fonksiyonu bir halka homomorfizmadır.

$n$ tek olması durumunda tanımlanan $\mu$ fonksiyonu; iyi tanımlılık, birebir, örten ve homomorfizma şartlarını sağladığından $\mu$ bir halka izomorfizmasıdır.

Bunun sonucunda,

**Sonuç 4.2.1** $I$ 'nın $R[x]/\langle x^n-1\rangle$ 'nin bir ideali olması için gerek yeter koşul $\mu(I)$ 'nın $R[x]/\langle x^n-(2+u)\rangle$ 'nın bir ideali olmasıdır.

**İspat** $(\Rightarrow)$: $I$, $R[x]/\langle x^n-1\rangle$ 'nin bir ideali olsun. Bu durumda aşağıdaki özellikler sağlanır:

$\forall a(x),b(x)\in I : a(x)-b(x)\in I$

$\forall a(x)\in I, \forall r(x)\in R[x]/\langle x^n-1\rangle : a(x)r(x)\in I,\ r(x)a(x)\in I.$

$\mu(I)$ 'nın $R[x]/\langle x^n-(2+u)\rangle$ 'nin bir ideali olduğu gösterilsin.

Bu durumda,

i. $\forall a(x),b(x)\in I$ *ve* $\forall \mu\big(a(x)\big)=a\big((2+u)x\big),\ \mu\big(b(x)\big)=b\big((2+u)x\big)\in\mu(I)$ :

$$\mu\big(a(x)-b(x)\big)\overset{\mu\ \text{hom}}{=}\mu\big(a(x)\big)-\mu\big(b(x)\big)\in\mu(I)$$

dır.

ii. $\forall \mu(a(x)) = a((2+u)x) \in \mu(I)$ *ve* $\forall r(x) \in \dfrac{R[x]}{\langle x^n-(2+u)\rangle}$ :

$\mu(a(x)r(x)) \overset{\mu \text{ hom}}{=} \mu(a(x)).r(x) \in \mu(I)$ *ve* $\mu(r(x)a) \overset{\mu \text{ hom}}{=} r(x)\mu(a(x)) \in \mu(I)$

olduğundan, $\mu(I)$, $\dfrac{R[x]}{\langle x^n-(2+u)\rangle}$ 'nın bir idealidir.

$(\Leftarrow)$: $\mu(I)$, $\dfrac{R[x]}{\langle x^n-(2+u)\rangle}$ 'nın bir ideali olsun. Bu durumda,

$\forall \mu(a(x)), \mu(b(x)) \in \mu(I) : \mu(a(x)) - \mu(b(x)) \in \mu(I)$ ve

$\forall \mu(a(x)) \in \mu(I)$ *ve* $\forall r(x) \in \dfrac{R[x]}{\langle x^n-(2+u)\rangle}$ : $\mu(a(x)).r(x) \in I$ *ve*

$r(x).\mu(a(x)) \in I$ sağlanır.

$I$ 'nın $\dfrac{R[x]}{\langle x^n-1\rangle}$ 'nin bir ideali olduğu gösterilsin.

$\mu(a(x)-b(x)) \overset{\mu \text{ hom}}{=} \mu(a(x)) - \mu(b(x)) \in \mu(I)$ ve

$\mu(a(x)r(x)) \overset{\mu \text{ hom}}{=} \mu(a(x)).r(x) \in \mu(I)$ olduğu bilinmektedir.

Bu durumda, $\forall a(x), b(x) \in I$: $a(x)-b(x) \in I$ ve $r(x).a(x) \in I$ dır.

$\mu(r(x)a(x)) = r(x).\mu(a(x)) \in \mu(I)$ ise $a(x).r(x) \in I$ dır. Buradan, $I$ 'nın $\dfrac{R[x]}{\langle x^n-1\rangle}$ 'nın bir ideali olduğu görülür.

**Sonuç 4.2.2** $n$ tek olması durumunda,

$$\overline{\mu}(c_0, c_1, ..., c_{n-1}) = \left(c_0, (2+u)c_1, (2+u)^2 c_2, ..., (2+u)^i c_i, ..., (2+u)^{n-1} c_{n-1}\right)$$

olacak şekilde, $R^n$ 'de bir $\bar{\mu}$ permütasyonu tanımlansın ve $D$, $R^n$ 'nin bir alt kümesi olsun. Bu durumda, $D$'nin devirli bir kod olması için gerek ve yeter koşul $\bar{\mu}(D)$ 'nin $(2+u)$- sabit devirli bir kod olmasıdır.

**İspat** $D$ devirli ise $(c_0,c_1,...,c_{n-1})\in D$ iken $(c_{n-1},c_0,c_1,...,c_{n-2})\in D$ dir. $(c_0,c_1,...,c_{n-1})$ nin $\bar{\mu}$ altında görüntüsü alınırsa, $(c_0,(2+u)c_1,c_2,...,c_{n-1})\in\bar{\mu}(D)$ elde edilir. $\bar{\mu}(D)$'nin $(2+u)$- sabit devirli olması $((2+u)c_{n-1},c_0,(2+u)c_1,\ldots,c_{n-2})=\upsilon(\bar{\mu}(D))$ yani $(2+u)(c_{n-1},(2+u)c_0,c_1,...,c_{n-2})$ demektir. $(2+u).\upsilon(\bar{\mu}(D))=(c_{n-1},(2+u)c_0,c_1,...,c_{n-2})\in\bar{\mu}(D)$ olup $\bar{\mu}(D)$ ideal olduğundan $\upsilon(\bar{\mu}(D))\in\bar{\mu}(D)$ dir. Yani $\bar{\mu}(D)$, $(2+u)$- sabit devirli bir koddur.

Teorem 3.1.1, Teorem 3.1.2 ve $\bar{\mu}$ homomorfizması kullanılarak $R$ üzerinde tek uzunluktaki $(2+u)$- sabit devirli kodlar aşağıdaki gibi ifade edilir:

**Teorem 4.2.1** $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerinde $n$ uzunluğunda $(2+u)$- sabit devirli bir kod $C$ ve $n$ tek olsun. Bu durumda $x^n-1=t_i(x).p_i(x).g_i(x)$ olacak şekilde $\tilde{x}=(2+u)x, t_i(x), p_i(x), g_i(x)$ $\mathbb{Z}_4[x]$'te aralarında asal polinom çiftleri olan monik polinomlar ve $t_2(x)\in\mathbb{Z}_4+u\mathbb{Z}_4$ iken

$$C=<t_1(\tilde{x})(p_1(\tilde{x})+2)+(1+u)t_2(\tilde{x}),(1+u)t_3(\tilde{x})(p_3(\tilde{x})+2)>$$

tarafından üretilen $C$, $R[x]/<x^n-(2+u)>$'da bir idealdir.

$\tilde{x}=(2+u)x$ iken, yukarıdaki teoremle verilen $(2+u)$- sabit devirli kodların üreteçleri

$$C=<f_1(\tilde{x})+(1+u)f_2(\tilde{x}),(1+u)s(\tilde{x})>$$

dir.

$R$ üzerindeki devirli kodların temel iki sonucu aşağıdaki gibidir. Benzer sonuçlar [26] da $u^2 = 0$ iken $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası için ispatlanmıştır.

[27]'deki Yıldız ve Aydın'ın çalışmasından yararlanarak $R$ üzerinde $n$ uzunluğunda tek üreteçli $(2+u)$- sabit devirli kodlar ele alınsın. Yani $a(x), b(x) \in \mathbb{Z}_4[x]$, $der\, a(x) < n$ ve $der\, b(x) < n$ iken $b(x) + u(a(x) - b(x)) \in R[x]/< x^n - (2+u) >$ polinomları tarafından üretilen $R[x]/< x^n - (2+u) >$ 'de bir idealdir. Sonuç olarak aşağıdaki teorem elde edilir:

**Teorem 4.2.2** $C =< b(x) + (a(x) - b(x))u >$, $R$ üzerinde $n$ tek uzunlukta $(2+u)$- sabit devirli kod olsun. Bu durumda $\phi(C)$, $b(x) + x^n(a(x) + b(x))$ ve $(a(x) - b(x)) + x^n(2a(x) - b(x))$ polinomları tarafından üretilen $2n$ uzunluğunda $\mathbb{Z}_4$ üzerinde devirli bir koddur.

**İspat** İlk olarak polinomlar için aşağıdaki gibi Gray dönüşümler tanımlansın:

$$\phi_1 : R[x]/< x^n - (2+u) > \to \mathbb{Z}_4[x]/< x^n - 1 > \times \mathbb{Z}_4[x]/< x^n - 1 >$$

$$\phi_1(b(x) + u(a(x) - b(x)) = (b(x),\ a(x) + b(x))$$

ve

$$\phi_2 : \mathbb{Z}_4[x]/< x^n - 1 > \times \mathbb{Z}_4[x]/< x^n - 1 > \to \mathbb{Z}_4[x]/< x^{2n} - 1 >$$

$$\phi_2(p(x), q(x)) = p(x) + x^n q(x)$$

$\phi_1$ ve $\phi_2$ 'nin iyi tanımlı olduğu açıktır. $\phi_1$ ve $\phi_2$, $\mathbb{Z}_4[x]$ modül homomorfizması ve $\phi_1$ örtendir. Böylece $\phi_1(\phi_2(c))$, $\mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ 'in $\mathbb{Z}_4[x]$- modülü ve

$\mathbb{Z}_4[x]/\langle x^n-1\rangle$ 'in $\mathbb{Z}_4[x]$- modülü de bir idealdir. Buradan $\mathbb{Z}_4$ üzerinde $2n$ uzunluğunda devirli bir koddur.

$\big(b(x),\ a(x)+b(x)\big)$, $\mathbb{Z}_4[x]/_{<x^{2n}-1>}$ 'deki $b(x)+u(a(x)+b(x))$ vektörünü verir.

Her $r(x)\in\mathbb{Z}_4[x]$ için $C$, $\mathbb{Z}_4[x]/_{<x^n-(2+u)>}$ halkasında bir ideal olduğundan $ur\big(x\big)\big(b(x)+u\big(a(x)-b(x)\big)\big)\in C$ dir.

Buradan $\phi\big(ur(x)\big(b(x)+u\big(a(x)-b(x)\big)\big)\big)=r(x)\big(a(x)-b(x),\ 2a(x)-b(x)\big)$ elde edilir. Bunun sonucunda $\mathbb{Z}_4[x]/_{<x^{2n}-1>}$ halkasındaki $r(x)(a(x)-b(x)+x^n(2a(x)-b(x)))$ vektörü bulunur. $q(x)$ ve $r(x)$, $\mathbb{Z}_4[x]$ 'te derecesi $n$ 'den küçük rastgele alınan polinomlar olmak üzere,

$$(r(x)+uq(x))(b(x)+u(a(x)-b(x)))=r(x)b(x)+a(x)q(x)-q(x)b(x)+$$

$$+u(a(x)r(x)-r(x)b(x)+q(x)b(x))$$

$$\overset{\phi_1}{=}(r(x)b(x)+q(x)(a(x)-b(x)),\ \ r(x)(b(x)+a(x))+q(x)(2a(x)-b(x)))$$

$$=r(x)(b(x),\ (b(x)+a(x)))+\ q(x)((a(x)-b(x)),\ (2a(x)-b(x)))$$

elde edilir. Böylece

$$\phi_2[(r(x)+uq(x))(b(x)+u(a(x)-b(x)))]=r(x)(b(x)+x^n(a(x)+b(x))+$$

$$+q(x)((a(x)-b(x))+x^n(2a(x)-b(x)))$$

bulunur. Yani, $b\big(x\big)+x^n\big(a(x)+b(x)\big)$ ve $(a(x)-b(x))+x^n(2a(x)-b(x))$ polinomları $\mathbb{Z}_4[x]/_{<x^{2n}-1>}$ 'te $\phi_1\big(\phi_2\big(c\big)\big)$ 'yi üretir.

$\mathbb{Z}_4^{2n}$ 'nin özel bir permütasyonu olan Nechaev permütasyonu aşağıdaki gibi tanımlansın:

**Tanım 4.2.1** $n$ tek iken $\{0,1,2,...,2n-1\}$'in bir permütasyonu, $\tau=(1,n+1)(3,n+3)...(2i+1,n+2i+1)...(n-2,2n-2)$ olsun. $\mathbb{Z}_4^{2n}$'nin bir $\pi(c_0,c_1,...,c_{2n-1})=(c_{\tau(0)},c_{\tau(1)},...,c_{\tau(2n-1)})$ permütasyonuna Nechaev permütasyonu denir.

**Önerme 4.2.2** $\bar{\mu}$ yukarıdaki gibi tanımlansın.

$n$ tek ve $\pi$ Nechaev permütasyonu olmak üzere, $\Phi\,\bar{\mu}=\pi\,\Phi$ dir.

**İspat** $c_i=b_i+u(a_i-b_i)$ iken, $R^n$'de $\vec{c}=(c_0,c_1,...,c_i,...,c_{n-1})$ olsun.

$$\bar{\mu}(c_0,c_1,...,c_{n-1})=\left(c_0,(2+u)c_1,(2+u)^2c_2,...,(2+u)^ic_i,...,(2+u)^{n-1}c_{n-1}\right)$$
$$=\left(b_0+u(a_0-b_0),a_1+b_1+u(2a_1-b_1),\ldots,b_{n-1}+u(a_{n-1}-b_{n-1})\right)$$

$\vec{s}=(s_0,\ldots,s_{2n-1})\in\mathbb{Z}_4^{2n}$ aşağıdaki gibi tanımlansın:

$\forall\, j=0,1,2,\ldots,n-1$ için; $n$ çift ise $s_j=b_j$ ve $s_{n+j}=b_j+a_j$,

$n$ tek ise $s_j=a_j+b_j$ ve $s_{n+j}=b_j$ dir.

$$\Phi\left(\bar{\mu}\left(\vec{c}\right)\right)=(b_0,a_1+b_1,b_2,\ldots,b_{n-1},a_0+b_0,b_1,\ldots,a_{n-1}+b_{n-1})$$
$$\downarrow\ \downarrow\ \downarrow\quad\downarrow\quad\downarrow\ \downarrow\qquad\downarrow$$
$$s_0\ \ s_1\ \ s_2\quad s_{n-1}\quad s_n\ \ s_{n+1}\qquad s_{2n-1}$$

den,

$\Phi\left(\bar{\mu}\left(\vec{c}\right)\right)=(s_0,s_1,...,s_{n-1},s_n,...,s_{2n-1})$ elde edilir.

$\Phi\left(\vec{c}\right)=(b_0,b_1,\ldots,b_{n-1},b_0+a_0,\ldots,b_{n-1}+a_{n-1})$ den,

$\pi\left(\Phi\left(\vec{c}\right)\right)=(b_0,b_1+a_1,b_2,\ldots,b_{n-1},b_0+a_0,b_1,\ldots,b_{n-1}+a_{n-1})$ bulunur.

$\vec{s}$'nin tanımından, $\Phi\left(\overline{\mu}\left(\vec{c}\right)\right)$ ile $\Phi\left(\vec{c}\right)$ kıyaslanarak $\Phi\overline{\mu} = \pi\Phi$ elde edilir.

**Sonuç 4.2.3** $\pi$ Nechaev permütasyonu, $n$ tek tamsayı, $\Gamma$ da $R$'deki devirli bir kodun Gray görüntüsü ($\mathbb{Z}_4$ görüntüsü) olsun. Bu durumda $\pi\left(\Gamma\right)$ devirli bir koddur.

**İspat** $D$, $R$'de devirli bir kod olmak üzere, $\Gamma = \Phi\left(D\right)$ olsun. Önerme 4.2.2'den $\Phi(\overline{\mu}\left(D\right)) = \pi(\Phi\left(D\right)) = \pi\left(\Gamma\right)$ elde edilir. Sonuç 4.2.2'den $\overline{\mu}\left(D\right)$, $\left(2+u\right)$- sabit devirli bir koddur. Buradan $\Phi(\overline{\mu}\left(D\right)) = \Phi\left(C\right)$ elde edilir. Teorem 4.1.1'i kullanarak $\Phi\left(C\right)$'nin devirli olduğu görülür. $\Phi\left(C\right)$ devirli ise $\pi\left(\Gamma\right)$ de devirlidir.

**Sonuç 4.2.4** $R$ üzerinde uzunluğu tek olan devirli bir kodun Gray görüntüsü devirli bir koddur.

# BÖLÜM 5. $u^2=1$; $\mathbb{Z}_4+u\mathbb{Z}_4$: KENDİNE DUAL KODLAR, ÖZDEŞLİK ANLAMINDA KENDİNE DUAL KODLAR, AĞIRLIK SAYAÇLARI VE MACWILLIAMS ÖZDEŞLİĞİ

Kendine dual kodlar lineer kodların önemli bir sınıfıdır ve pek çok araştırma alanıyla bağlantılıdır. Bu yüzden uzun süreden beri pek çok araştırmacı tarafından çalışılmaktadır.

[24]'teki çalışmanın yapılmasından sonra, $\mathbb{Z}_4$ üzerinde çalışılan kodlar üzerine pek çok çalışma yapılmıştır. Halkaların zengin cebirsel yapısı, araştırmacıların kodlama teorisinde iyi sonuçlar elde etmesine olanak tanımıştır. Çalışılan halkalar son yıllarda değişmiştir ancak pek çok alan ile uygulama bağlantısından dolayı $\mathbb{Z}_4$ üzerindeki kodlar kodlama teorisinde özel bir başlık olarak kalmıştır.

Sonlu halkalar üzerindeki kodlar, 1970'lerin başından beri çalışılmaktadır. $\mathbb{Z}_4$ üzerindeki devirli kodlardan Gray dönüşüm ile lineer olmayan bazı iyi kodlar inşa edilebildikten sonra, sonlu halkalar üzerindeki kodlar üzerine pek çok çalışma yapılmıştır.

$\mathbb{Z}_4$ üzerindeki kodlar üzerinde geniş bir literatür çalışması vardır. Yıldız ve Karadeniz [25] 'te $u^2=0$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerindeki lineer kodları çalışmıştır. Bu çalışmada tüm ağırlık sayaçlarını içeren MacWilliams özdeşliği incelenmiş, $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde özdeşlik anlamında kendine dual kod oluşturmak için üç method verilmiştir. [28]'de ise $v^2=v$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkasındaki kendine dual kodlara odaklanılmış ve Gray dönüşümü kullanılarak Lee ve Gray ağırlık sayaçları için MacWilliams özdeşliği belirlenmiştir.

Bu bölümde kendine dual kodlar, projeksiyonlar, liftler ve $\mathbb{Z}_4$ görüntüleri, özdeşlik anlamında kendine dual kodlar ve ikili dairesel kodlar incelenecektir.

## 5.1. Tam Ağırlık Sayaçları ve MacWilliams Özdeşliği

$\mathbb{Z}_4+u\mathbb{Z}_4=\{0,u,2u,3u,1,1+u,1+2u,1+3u,2,2+u,2+2u,2+3u,3,3+u,3+2u,3+3u\}$ halkası $\mathbb{Z}_4+u\mathbb{Z}_4=\{g_1,g_2,\ldots,g_{16}\}$ olarak verilsin.

**Tanım 5.1.1** $\bar{c}$ vektöründeki $g_i$'lerin sayısı $n_{g_i}(\bar{c})$ olmak üzere, $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde lineer bir C kodunun tam ağırlık sayacı aşağıdaki gibi tanımlansın:

$$cwe_C(x_1,x_2,\ldots,x_{16})=\sum_{\bar{c}\in C}\left(x_1^{n_{g_1}(\bar{c})}x_2^{n_{g_2}(\bar{c})}\ldots x_{16}^{n_{g_{16}}(\bar{c})}\right)$$

**Not 5.1.1** $cwe_C(x_1,x_2,\ldots,x_{16})$. $C$'deki her bir terimi $n$ uzunluğunda olan 16 değişkenli homojen bir polinomdur. Ayrıca, $cwe_C(1,1,\ldots,1)=|C|$ ve $cwe_C(a,0,\ldots,0)=a^n$ dir.

Tam ağırlık sayaçları, kod hakkında pek çok bilgi verir. $\mathbb{Z}_4+u\mathbb{Z}_4$ bir Frobenius halkası olduğundan, tam ağırlık sayacı için MacWilliams özdeşliği korunmaktadır. Özdeşliklerin bulunması için $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerindeki karakter aşağıdaki gibi tanımlanır:

**Tanım 5.1.2** $\chi:\mathbb{Z}_4+u\mathbb{Z}_4\to\mathbb{C}^{\times}$ iken karakter $\chi(b+(a-b)u)=i^{a+b}$ şeklinde tanımlansın.

$T$, $T(i,j)=\chi(g_i.g_j)$ olacak şekilde, $16\times16$'lık bir matris olsun. Bu durumda $T$ matrisi aşağıdaki gibidir:

$$T=\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & -1 & 1 & -1 & i & -i & i & -i & -1 & 1 & -1 & 1 & -i & i & -i & i\\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\
1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & i & -i & i & -i\\
1 & i & -1 & -i & -1 & -i & 1 & i & 1 & i & -1 & -i & -1 & -i & 1 & i\\
1 & -i & -1 & i & -i & -1 & i & 1 & -1 & i & 1 & -i & i & 1 & -i & -1\\
1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i\\
1 & -i & -1 & i & i & 1 & -i & -1 & -1 & i & 1 & -i & -i & -1 & i & 1\\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\
1 & 1 & 1 & 1 & i & i & i & i & -1 & -1 & -1 & -1 & -i & -i & -i & -i\\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\
1 & 1 & 1 & 1 & -i & -i & -i & -i & -1 & -1 & -1 & -1 & i & i & i & i\\
1 & -i & -1 & i & -1 & i & 1 & -i & 1 & -i & -1 & i & -1 & i & 1 & -i\\
1 & i & -1 & -i & -i & 1 & i & -1 & -1 & -i & 1 & i & i & -1 & -i & 1\\
1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i\\
1 & i & -1 & -i & i & -1 & -i & 1 & -1 & -i & 1 & i & -i & 1 & i & -1
\end{bmatrix}$$

**Teorem 5.1.1** $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $n$ uzunluğunda lineer bir kod $C$ ve $C$'nin duali de $C^{\perp}$ olsun. Bu durumda, $T$ $|R|\times|R|$'lik bir matris ve $T(i,j)=\chi(g_i.g_j)$ olmak üzere,

$$cwe_{C^{\perp}}(x_1,x_2,\ldots,x_{16})=\frac{1}{|C|}\,cwe_C\left(T.(x_1,x_2,\ldots,x_{16})^t\right)$$

dir.

## 5.2. Simetri Ağırlık Sayaçları ve Lee Ağırlık Sayaçları

$\mathbb{Z}_4$'te $w_L(1)=w_L(3)=1$ olduğundan, $\mathbb{Z}_4$ üzerindeki kodlar için simetri ağırlık sayacı

$$swe_C(X,Y,Z)=cwe_C(X,Y,Z,Y)$$

şeklinde tanımlanır.

$\mathbb{Z}_4+u\mathbb{Z}_4$ üzerindeki kodların simetri ağırlık sayacı $\mathbb{Z}_4$'teki tanıma benzer olarak tanımlanabilir. Bunu yapmak için öncelikle aşağıdaki tablo oluşturulmalıdır.

Tablo 5.1. $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerindeki elemanların Lee ağırlıkları

| d | d'nin Lee Ağırlığı | Değişken Karşılıkları |
|---|---|---|
| 0 | 0 | $X_1$ |
| $u$ | 1 | $X_2$ |
| $2u$ | 2 | $X_3$ |
| $3u$ | 1 | $X_4$ |
| 1 | 3 | $X_5$ |
| $1+u$ | 2 | $X_6$ |
| $1+2u$ | 1 | $X_7$ |
| $1+3u$ | 2 | $X_8$ |
| 2 | 2 | $X_9$ |
| $2+u$ | 3 | $X_{10}$ |
| $2+2u$ | 4 | $X_{11}$ |
| $2+3u$ | 3 | $X_{12}$ |
| 3 | 3 | $X_{13}$ |
| $3+u$ | 2 | $X_{14}$ |
| $3+2u$ | 1 | $X_{15}$ |
| $3+3u$ | 2 | $X_{16}$ |

Aynı ağırlığa sahip elemanlar için simetri ağırlık sayacı aşağıdaki gibi tanımlanır:

**Tanım 5.2.1** $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerinde $n$ uzunluğunda lineer bir kod $C$ olsun. Bu durumda, $C$'nin simetri ağırlık sayacı

$$swe_C(X,Y,Z,W,S) = cwe_C(X,Y,Z,Y,W,Z,Y,Z,Z,W,S,W,W,Z,Y,Z)$$

şeklindedir.

Burada $X$ ağırlığı 0 olan 0 elemanını; $Y$ ağırlığı 1 olan $u, 3u, 1+2u, 3+2u$ elemanlarını; $Z$ ağırlığı 2 olan $2u, 1+u, 1+3u, 2, 3+u, 3+3u$ elemanlarını; $W$ ağırlığı 3 olan $1, 2+u, 2+3u, 3$ elemanlarını; $S$ ağırlığı 4 olan $2+2u$ elemanını temsil eder.

Önceki teoremle simetri ağırlık sayacı birleştirilerek Teorem 5.2.1 elde edilir.

**Teorem 5.2.1** $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerinde $n$ uzunluğunda lineer bir kod $C$, $C$'nin duali de $C^{\perp}$ olsun. Bu durumda,

$$swe_{C^{\perp}}(X,Y,Z,W,S) = \frac{1}{|c|}.swe_C(X+4Y+4W+6Z+S, X-2Y+2W-S, X-2Z+S, X+2Y-2W-S, X-4Y+6Z-4W+S)$$

dir.

**İspat**

$$swe_{C^{\perp}}(X,Y,Z,W,S) = cwe_{C^{\perp}}(X,Y,Z,Y,W,Z,Y,Z,Z,W,S,W,W,Z,Y,Z)$$
$$= \frac{1}{|c|}.cwe_C(T.(X,Y,Z,Y,W,Z,Y,Z,Z,W,S,W,W,Z,Y,Z)^t)$$
$$= \frac{1}{|c|}.swe_C(X+4Y+4W+6Z+S, X-2Y+2W-S, X-2Z+S, X+2Y-2W-S, X-4Y+6Z-4W+S)$$

**Tanım 5.2.2** $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerinde lineer bir kod $C$ olsun. Bu durumda $C$'nin Lee ağırlık sayacı aşağıdaki gibi tanımlanır:

$$Lee_C(Y,X) = \sum_{c \in C} Y^{4n - w_L(\bar{c})} X^{w_L(\bar{c})}.$$

**Teorem 5.2.2** $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $n$ uzunluğunda lineer bir kod $C$ olsun. Bu durumda,

$$Lee_C(Y,X)=swe_C\left(Y^4,Y^3X,Y^2X^2,YX^3,X^4\right)$$

dir.

**İspat** $\varepsilon_i$'ler $i$ ağırlığındaki kodun sayısını göstermek üzere, $(i=0,1,2,3,4)$, $C$'nin Lee ağırlığı ve uzunluğu

$w_L(C)=\varepsilon_1+2\varepsilon_2+3\varepsilon_3+4\varepsilon_4$
$n=\varepsilon_0+\varepsilon_1+\varepsilon_2+\varepsilon_3+\varepsilon_4$ olsun. Bu durumda,

$$\begin{aligned}Lee_C(Y,X)&=Y^{4\varepsilon_0+3\varepsilon_1+2\varepsilon_2+\varepsilon_3}.X^{\varepsilon_1+2\varepsilon_2+3\varepsilon_3+4\varepsilon_4}\\&=(Y^4)^{\varepsilon_0}+(Y^3X)^{\varepsilon_1}+(Y^2X^2)^{\varepsilon_2}+(YX^3)^{\varepsilon_3}+(X^4)^{\varepsilon_4}\\&=swe_C\left(Y^4,Y^3X,Y^2X^2,YX^3,X^4\right)\end{aligned}$$

dir.

**Teorem 5.2.3** $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $n$ uzunluğunda lineer bir kod $C$, $C$'nin duali de $C^{\perp}$ olsun. Bu durumda,

$$Lee_{C^{\perp}}(Y,X)=\frac{1}{|C|}.Lee_C(Y+X,Y-X)$$

dir.

**İspat**

$$(Y+X)^4=Y^4+4Y^3X+6Y^2X^2+4YX^3+X^4$$

$$(Y-X)^3(Y+X)=Y^4-2Y^3X+2YX^3-X^4$$

$$(Y+X)^2(Y-X)^2=Y^4-2Y^2X^2+X^4$$

$$(Y+X)^3(Y-X)=Y^4+2Y^3X-2YX^3-X^4$$

$(Y-X)^4 = Y^4 - 4Y^3X + 6Y^2X^2 - 4YX^3 - X^4$ olmak üzere,

$$Lee_{C^\perp}(Y,X) = swe_{C^\perp}\left(Y^4,\ Y^3X,\ Y^2X^2,\ YX^3,\ X^4\right)$$

$$= \frac{1}{|C|}.swe_C\left(Y^4 + 4Y^3X + 4YX^3 + 6Y^2X^2 + X^4,\ Y^4 - 2Y^3X + 2YX^3 - X^4,\right.$$

$$Y^4 - 2Y^2X^2 + X^4,\ Y^4 + 2Y^3X - 2YX^3 - X^4,$$

$$\left. Y^4 - 4Y^3X - 4YX^3 + 6Y^2X^2 + X^4\right)$$

$$= \frac{1}{|C|}.Lee_C(Y+X, Y-X)$$

elde edilir.

### 5.3. Kendine Dual Kodlar, Projeksiyonlar, Liftler ve $\mathbb{Z}_4$ Görüntüleri

$C \subseteq C^\perp$ ise $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerindeki lineer $C$ kodu kendine dik, $C = C^\perp$ ise kendine dual olarak adlandırılmaktadır.

$\mho_1 = \{0, 2, 2u, 2+2u\}$

$\mho_2 = \{1+u, 1+3u, 3+u, 3+3u\}$

$\mho_3 = \{1, 3, u, 3u, 2+u, 1+2u, 3+2u, 2+3u\}$ olmak üzere,

$$a \in \mathbb{Z}_4 + u\mathbb{Z}_4 \text{ için, } a^2 = \begin{cases} 0 & a \in \mho_1 \\ 2+2u & a \in \mho_2 \\ 1 & a \in \mho_3 \end{cases} \text{ dir. } \ldots\ldots\ldots (*)$$

Burada, $\mho_3$ birimsel elemanlar kümesini; $\mho_2$ ve $\mho_1$ birimsel olmayan elemanlar kümesini temsil etmektedir.

**Teorem 5.3.1**

$\bar{c}$ 'de bulunan $\mathfrak{V}_i$ 'deki elemanların sayısı $\eta_{\mathfrak{V}_i}(\bar{c})$ olmak üzere,

**(i)** $C$ kendine dik ise, her $\bar{c} \in C$ için , $\eta_{\mathfrak{V}_2}(\bar{c})$ çift, $\eta_{\mathfrak{V}_3}(\bar{c})$ te 4 ün katı olmalıdır.

**(ii)** $n$ uzunluğundaki $C$ kodu kendine dual ise, $n$ uzunluğundaki tüm $2+2u$ - vektörleri $C$ 'de olmalıdır.

**İspat** **(i)** $C$ kendine dik olduğundan, her $\bar{c} \in C$ için, $\langle \bar{c}, \bar{c} \rangle = 0$ dır. (*) dan $\langle \bar{c}, \bar{c} \rangle = (2+2u)\eta_{\mathfrak{V}_2}(\bar{c}) + \eta_{\mathfrak{V}_3}(\bar{c})$ yazılabilir. Bu durumda,

$$\langle \bar{c}, \bar{c} \rangle = (2+2u)\eta_{\mathfrak{V}_2}(\bar{c}) + \eta_{\mathfrak{V}_3}(\bar{c})$$
$$= 2(1+u)\eta_{\mathfrak{V}_2}(\bar{c}) + \eta_{\mathfrak{V}_3}(\bar{c}) = 0$$

dır. Öyleyse $\eta_{\mathfrak{V}_2}(\bar{c})$ çift, $\eta_{\mathfrak{V}_3}(\bar{c})$ 4'ün katı olmalıdır.

**(ii)** $C$ kendine dual ise $C = C^{\perp}$ ve dolayısıyla her $\bar{c} \in C$ için $\langle \bar{c}, \bar{c} \rangle = 0$ dır. Yukarıdaki eşitlikten $\eta_{\mathfrak{V}_2}$ çift, $\eta_{\mathfrak{V}_3}$ 4'ün katı olmalıdır. Halka yapısından $\mathfrak{V}_3.(2+2u) = 2+2u$ , $\mathfrak{V}_1.(2+2u) = 0$ ve $\mathfrak{V}_2.(2+2u) = 0$ dır. Buradan $C$ 'nin $n$ uzunluktaki $2+2u$ - vektörü olduğu görülür.

$\langle \bar{c}, \overline{2+2u} \rangle = \eta_{\mathfrak{V}}(\bar{c}).(2+2u) = 0$ ve $\eta_{\mathfrak{V}}$ çift olduğundan $\overline{2+2u} \in C^{\perp} = C$ dir.

Yani, $C$ kendine dualdir. •

$\xi$ , $\mathbb{Z}_4 + u\mathbb{Z}_4$ 'ten $\mathbb{Z}_4$ 'e bir projeksiyon olmak üzere,

$(\mathbb{Z}_4 + u\mathbb{Z}_4)^n$ 'den ${\mathbb{Z}_4}^n$ 'e ;

$\xi(\bar{b} + (\bar{a} - \bar{b})u) = \bar{a}$ ve $\zeta(\bar{b} + (\bar{a} - \bar{b})u) = \bar{a} - \bar{b}$ lineer dönüşümleri ve mod 2 'de $\alpha : \mathbb{Z}_4 + u\mathbb{Z}_4 \to F_2 + uF_2$ projeksiyonu tanımlansın.

**Teorem 5.3.2** $C$, $R$'de $n$ uzunluğunda lineer bir kod, $\alpha(C)$ de $F_2+uF_2$'de $n$ uzunlukta lineer bir kod olmak üzere $\xi(C)$ ve $\zeta(C)$ $\mathbb{Z}_4$'te lineer bir koddur.

**Teorem 5.3.3** $C$, $\mathbb{Z}_4+u\mathbb{Z}_4$'te $n$ uzunluğunda kendine dual kod olsun. Bu durumda,

**i)** $\Phi(C)$, $\mathbb{Z}_4$'te $2n$ uzunluğunda özdeşlik anlamında kendine dual koddur.

**ii)** $\xi(C)$, $\mathbb{Z}_4$'te $n$ uzunluğunda kendine dik ve $\alpha(C)$ $F_2+uF_2$'de kendine diktir.

**iii)** $\zeta(C)$, kendine dik ise $2n$ uzunluğundaki $\Phi(C)$ kendine dualdir.

**İspat (i)** $\Phi(C)$, $\mathbb{Z}_4$'te $2n$ uzunluğunda lineer bir koddur. $C$ kendine dual olduğundan $C$'nin ağırlık sayacı MacWilliams dönüşümü altında sabittir. Böylece, $\Phi$ ağırlık koruyandır.

**(ii)** $\overline{a_1},\overline{a_2}\in\xi(C)$ olsun. O halde $\overline{b_1}+(\overline{a_1}-\overline{b_1})u,\overline{b_2}+(\overline{a_2}-\overline{b_2})u\in C$ olmak üzere $\overline{b_1},\overline{b_2}\in\mathbb{Z}_4{}^n$ vardır. $C$ kendine dual ise,

$$\Rightarrow \quad \left\langle \overline{b_1}+(\overline{a_1}-\overline{b_1})u,\overline{b_2}+(\overline{a_2}-\overline{b_2})u \right\rangle = 0$$

$$\Rightarrow \quad 2\overline{b_1}\overline{b_2}+\overline{a_1}\overline{a_2}-\overline{a_1}\overline{b_2}-\overline{a_2}\overline{b_1}+u\left(\overline{b_1}\overline{a_2}-\overline{b_1}\overline{b_2}+\overline{a_1}\overline{b_2}-\overline{b_1}\overline{b_2}\right)=0$$

$$\Rightarrow \quad \begin{aligned} &2\overline{b_1}\overline{b_2}+\overline{a_1}\overline{a_2}-\overline{a_1}\overline{b_2}-\overline{a_2}\overline{b_1}=0 \\ &\overline{b_1}\overline{a_2}-\overline{b_1}\overline{b_2}+\overline{a_1}\overline{b_2}-\overline{b_1}\overline{b_2}=0 \end{aligned}$$

$$\Rightarrow \quad \overline{a_1}\overline{a_2}=0$$

olduğundan $C\subseteq C^{\perp}$ elde edilir. Yani $\xi(C)$ kendine diktir. $\alpha(C)$'nin kendine dik olduğu da benzer şekilde gösterilir.

(iii) $\overline{b_1}+\left(\overline{a_1}-\overline{b_1}\right)u, \overline{b_2}+\left(\overline{a_2}-\overline{b_2}\right)u \in C$ için,

$C$ kendine dual olduğundan, $\left\langle \overline{b_1}+\left(\overline{a_1}-\overline{b_1}\right)u,\ \overline{b_2}+\left(\overline{a_2}-\overline{b_2}\right)u \right\rangle = 0$ olup,

$\left.\begin{array}{l} 2\overline{b_1}\,\overline{b_2}+\overline{a_1}\,\overline{a_2}-\overline{a_1}\,\overline{b_2}-\overline{a_2}\,\overline{b_1}=0 \\ \overline{b_1}\,\overline{a_2}-\overline{b_1}\,\overline{b_2}+\overline{a_1}\,\overline{b_2}-\overline{b_1}\,\overline{b_2}=0 \end{array}\right\}$ ve $\overline{a_1}\,\overline{a_2}=0$ dır. $\zeta(C)$ kendine dik olduğundan $\left(\overline{a_1}-\overline{b_1}\right).\left(\overline{a_2}-\overline{b_2}\right)=0$ dır. Buradan $\overline{a_1}\,\overline{a_2}-\overline{a_1}\,\overline{b_2}-\overline{a_2}\,\overline{b_1}+\overline{b_1}\,\overline{b_2}=0$ dır. $\overline{a_1}.\overline{a_2}=0$ ve $\overline{a_1}\,\overline{b_2}-\overline{a_2}\,\overline{b_1}=0$ olduğundan $\overline{b_1}.\overline{b_2}=0$ elde edilir.

$\left\langle \Phi\left(\overline{b_1}+\left(\overline{a_1}-\overline{b_1}\right)u\right).\Phi\left(\overline{b_2}+\left(\overline{a_2}-\overline{b_2}\right)u\right)\right\rangle = \left\langle \left(\overline{b_1},\left(\overline{a_1}+\overline{b_1}\right)\right).\left(\overline{b_2},\left(\overline{a_2}+\overline{b_2}\right)\right)\right\rangle = 0$ ve

$\overline{b_1}.\overline{b_2}=0$, $\overline{a_1}.\overline{a_2}=0$, $\overline{a_1}.\overline{b_2}+\overline{a_2}.\overline{b_1}=2\overline{b_1}.\overline{b_2}$ olduğundan

$\left\langle \Phi\left(\overline{b_1}+\left(\overline{a_1}-\overline{b_1}\right)u\right).\Phi\left(\overline{b_2}+\left(\overline{a_2}-\overline{b_2}\right)u\right)\right\rangle = 0$ dır. Yani, $\Phi(C)$ kendine diktir.

$\Phi$ izometri olduğundan, $C$ ve $\Phi(C)$'nin boyutları aynıdır. Yani, $|C|=|\Phi(C)|=16^{n/2}=4^n$ dir. Böylece, $\Phi(C)$'nin kendine dual olduğu gösterilmiş olur.

**Sonuç 5.3.1** $\mathbb{Z}_4+u\mathbb{Z}_4$'te $\left[I_n|A\right]$ tarafından üretilen kendine dual bir kod $C$ ise; $\xi(C)$ $\mathbb{Z}_4$'te, $\alpha(C)$ de $F_2+uF_2$'de kendine dualdir.

**İspat** $C$, $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $\left[I_n|A\right]$ tarafından üretilen kendine dual bir kod olduğundan $C$'nin herhangi bir $i$ ve $j.$ satırının iç çarpımı $0$ olmalıdır.

$i=1,2,\ldots,n$ için, $c_{in}=b_{in}+u\left(a_{in}-b_{in}\right)$ olmak üzere,

$C$'nin $i.$ satırı $\left(0,0,\ldots,1,0,\ldots,0,c_{i1},c_{i2},\ldots,c_{in}\right)$,

$C$'nin $j.$ satırı da $\left(0,0,\ldots,1,0,\ldots,0,c_{j1},c_{j2},\ldots,c_{jn}\right)$ olsun.

Bu durumda, $i$ ve $j$. satırın $\xi$ dönüşümü altındaki görüntüleri, sırasıyla, $a_{i1}+a_{i2}+\ldots+a_{in}=0$ ve $a_{j1}+a_{j2}+\ldots+a_{jn}=0$ dır. $C$ kendine dual olduğundan, $\left\langle (0,0,\ldots,1,0,\ldots,0,c_{i1},c_{i2},\ldots,c_{in}),(0,0,\ldots,1,0,\ldots,0,c_{j1},c_{j2},\ldots,c_{jn})\right\rangle =$

$$0+0+\ldots+b_{i1}b_{j1}+a_{i1}a_{j1}-a_{i1}b_{j1}-b_{i1}b_{j1}+u\left(b_{i1}a_{j1}-b_{i1}b_{j1}+a_{i1}b_{j1}-b_{i1}b_{j1}\right)+\ldots=0$$

elde edilir.

## 5.4. Özdeşlik Anlamında Kendine Dual Kodlar

Teorem 5.4.1 $A$, $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $n\times n$ tipinde bir matris olmak üzere, $A$ simetrik bir matris ise $\left[I_n\middle|A\right]$ tarafından üretilen kod $2n$ uzunluğunda özdeşlik anlamında kendine dualdir [25] .

**İspat** $G$ ve $G'$ $16^n$ uzunluğunda üreteç kodlar ve $\left[-A^T\middle|I_n\right]=\left[-A\middle|I_n\right]=G'$ ve $\left[I_n\middle|A\right]=G$ olsun. Üreteç kodlar $\mathbb{Z}_4+u\mathbb{Z}_4$'e eşittir.

$C=<G>$ ve $C'=<G'>$ olsun. Bu durumda,

$$G=\left[\begin{array}{cccc|cccc} 1 & 0 & \ldots & 0 & a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 1 & a_{n1} & a_{n2} & \ldots & a_{nn} \end{array}\right] \text{ ve}$$

$$G'=\left[\begin{array}{cccc|cccc} -a_{11} & -a_{12} & \ldots & -a_{1n} & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ -a_{n1} & -a_{n2} & \ldots & -a_{nn} & 0 & 0 & \ldots & 1 \end{array}\right] \text{ dır.}$$

$C'=C^{\perp}$ olduğu aşağıdaki gibi gösterilsin:

$G$'nin $i$. satırı $v$, $G'$'nün de $j$. satırı $w$ olsun. Bu durumda,

$v=(0,0,\ldots,1,\ldots,0,a_{i1},a_{i2},\ldots,a_{in})$, $w=(-a_{j1},-a_{j2},\ldots,-a_{jn},0,0,\ldots,1,\ldots,0,)$ dir.

$\langle v,w\rangle=-a_{ji}+a_{ij}=-A_{ji}+A_{ij}\overset{A=A^T}{=}0$ elde edilir. Bu da $C'=C^{\perp}$ demektir.

$\forall a \in \mathbb{Z}_4 + u\mathbb{Z}_4 : w_L(-a) = w_L(a)$ olduğundan, ağırlık korunur. Öyleyse $G$, $2n$ uzunluğunda özdeşlik anlamında kendine dualdir.

**Teorem 5.4.2** $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerinde derecesi $n$ olan dairesel bir matris $A$ olsun. Bu durumda $\left[ I_n \middle| A \right]$ matrisi $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerinde özdeşlik anlamında kendine dual bir kod üretir. Buna ikili dairesel yapı denir [25] .

**İspat** $G = \left[ I_n \middle| A \right]$ tarafından üretilen kod $C$, $G' = \left[ -A^T \middle| I_n \right]$ tarafından üretilen kod da $C'$ olsun. $C' = C^{\perp}$ olduğu yukarıdakine benzer şekilde gösterilir.
$\mathbb{Z}_4 + u\mathbb{Z}_4$'te $C'$, $G'' = \left[ A^T \middle| I_n \right]$ tarafından üretilen $C''$ koduna denktir. $C$ ve $C''$ denkliğini göstermek için, $C$ ile $C''$ denkliği gösterilmelidir.

$\gamma$ satır permütasyonu alınsın. Bu permütasyon $G''$ ne uygulandıktan sonra $\gamma(A)$'nın ilk sütununu $A$'nın ilk sütununa eşit olur.
Yani, $(A_{11}, A_{21}, \ldots, A_{n1}) = \left( A^T_{\gamma(1)1}, A^T_{\gamma(2)1}, \ldots, A^T_{\gamma(n)1} \right) = \left( A_{1\gamma(1)}, A_{1\gamma(2)}, \ldots, A_{1\gamma(n)} \right)$ dir.
$A$ matrisi dairesel bir matris olduğu için $A$ matrisinin her sütunu $\gamma\left(A^T\right)$'nın bir sütununa eşittir. $\delta\left(\gamma\left(A^T\right)\right)$ olacak şekilde gerekli olan $\delta$ sütun permütasyonu uygulansın. Daha sonra $\gamma(I_n)$ tarafından kurulan matris birim matris oluşturulacak şekilde diğer sütun permütasyonu $\rho$ uygulansın. $\delta$ bu kısmı etkilemeyecektir. Böylece ardarda uygulanan $\gamma, \delta, \rho$ permütasyonları ile $G''$ den $G$ elde edilir. Bu da, $C$'nin $C' = C^{\perp}$ 'ye denk olması demektir. Önceki teoremde de gösterildiği gibi bu ağırlık koruyan bir denkliktir.

**Sonuç 5.4.1** $A$, $n \times n$ tipinde bir matris olmak üzere, $\left[ I_n \middle| A \right]$ tarafından üretilen $C$, $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerinde bir kod olsun. $A$ simetrik yada dairesel matris ise $C$ özdeşlik anlamında kendine dual, $\Phi(C)$ de $\mathbb{Z}_4$ üzerinde $4n$ uzunluğunda özdeşlik anlamında kendine dualdir.

**Teorem 5.4.3** $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $n-1$ boyutlu dairesel matris $A$ olsun. Bu durumda, $\ell,\kappa,\theta\in\mathbb{Z}_4+u\mathbb{Z}_4$ ve $\theta=\mp\kappa$ olmak üzere,

$$G=\left[\begin{array}{c|cccccc} & \ell & \kappa & \kappa & \dots & \kappa \\ & \theta & & & & \\ I_n & \theta & & & M & \\ & \vdots & & & & \\ & \theta & & & & \end{array}\right]$$

matrisi Gray görüntüsü $\mathbb{Z}_4$ üzerinde $4n$ uzunluğunda kendisi de $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde $2n$ uzunlukta olan özdeşlik anlamında kendine dual kod üretir. Buna genişletilmiş ikili dairesel yapı denir [25] .

**İspat**

$$G'=\left[\begin{array}{ccccc|c} -\ell & -\theta & -\theta & \dots & -\theta & \\ -\kappa & & & & & \\ -\kappa & & & -M^T & & I_n \\ \vdots & & & & & \\ -\kappa & & & & & \end{array}\right]$$

olsun. $G'$ nün $C^{\perp}$ 'i ürettiği açıktır. $\theta$ ve $\kappa$ olmaksızın $G'$ ile $C^{\perp}$ 'in denkliği, önceki teoremde $G$ ve $G'$ ne uygulanan methodla gösterilebilir. $I_n$ hariç tüm satırlar $-1$ ile çarpılarsa $C^{\perp}$ ile üreteç matrisi

$$G^*=\left[\begin{array}{c|cccccc} & \ell & \theta & \theta & \dots & \theta \\ & \kappa & & & & \\ I_n & \kappa & & & M & \\ & \vdots & & & & \\ & \kappa & & & & \end{array}\right]$$

olan $C^*$ kodu birbirine denktir.

$\theta = \kappa$ ise $C$ ile $C^*$ kodları aynıdır. $\theta = -\kappa$ ise $G^*$, ilk satırı hariç, $-1$ ile çarpımı sonucu oluşan matris te $C^*$'ı üretir. Her $a \in \mathbb{Z}_4 + u\mathbb{Z}_4$ için, $w_L(-a) = w_L(a)$ olduğundan $C$ ile $C'$ ağırlığı korur. Böylece her iki durumda da, $C$ ve $C^{\perp}$ 'te ağırlık korunmuş olur.

**Örnek 5.4.1**

| Uzunluk | $A$ 'nın ilk satırı | $d$ |
|---|---|---|
| 4 | $(2,1+2u)$ | 4 |
| 6 | $(2,3u,1+2u)$ | 6 |
| 8 | $(2,3u,2+u,2+3u)$ | 8 |
| 10 | $(1+u,2+2u,1+3u,3,3+u)$ | 8 |

Tablo 5.2. $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerindeki ikili dairesel matrislerden elde edilen özdeşlik anlamında kendine dual $\mathbb{Z}_4$ kodlar

# BÖLÜM 6. HESABA DAYALI SONUÇLAR

Sonlu cisimler üzerinde en iyi bilinen lineer kodların tablo ve veri tabanlarına uzun süreden beri ulaşılabilmektedir [35] . $\mathbb{Z}_4$ üzerindeki kodların öneminden ve $\mathbb{Z}_4$ kodlardaki yoğun çalışmadan dolayı [37] online olarak kullanılarak, $\mathbb{Z}_4$ üzerindeki kodların veritabanları [36]'da oluşturulmuştur.

Bu bölümde $R$ üzerindeki devirli kodların ve bazı tek uzunluktaki Gray görüntülerinin bilgisayar araştırma sonuçları ifade edilecektir. [34]'teki online veritabanına göre Gray görüntüsü $\mathbb{Z}_4$ üzerinde yeni lineer kodlar olan $R$ üzerinde pek çok devirli kod bulunmuştur. Aşağıdaki tablo bu kodların bir alt kümesini göstermektedir. Tek uzunluktaki devirli kodların üreteçleri Teorem 3.2.1'de verilmiştir ve $\mathbb{Z}_4$ üzerinde üç polinom belirlenmiştir. Bu polinomların katsayıları azalan sıraya göre yazılacaktır. Örneğin $2x^4+3x+1$, 20031 tarafından temsil edilmektedir. $d$ basamağı tekrar eden uzun bir dizi var olduğunda $d^n$ şeklinde yazılacaktır. Örneğin $3^4$, $3x^3+3x^2+3x+3$ polinomunu temsil etmektedir. Ayrıca, kodların Gray görüntüleri için hem Lee hem de Öklid ağırlıkları ele alınacaktır. Burada, $E$ alt indisi minimum Öklid ağırlığı göstermektedir.

Tablo 6.1. Lee ve Öklid ağırlıkları ile 7 uzunluğundaki bazı devirli kodlar

| $g_1(x)$ | $g_2(x)$ | $g_3(x)$ | $\mathbb{Z}_4$ görüntülerinin parametreleri |
|---|---|---|---|
| 22022022 | 22022022 | 22022022 | $[14,4^0 2^4,15]$ |
| $2^8$ | $2^8$ | 1001 | $[14,4^{12}2^6,2]$ |
| $3^9$ | $3^9$ | 1001 | $[14,4^{13}2^5,2]$ |
| $3^9$ | $3^9$ | 113 | $[14,4^{14}2^4,2]$ |
| 3003003 | 3003003 | 1021 | $[14,4^{15}2^2,2]$ |
| $2^9$ | $2^9$ | 11 | $[14,4^{16}2^2,2]$ |
| $3^9$ | $3^9$ | 31 | $[14,4^{17}2^0,2]$ |
| $3^9$ | $3^9$ | 3 | $[14,4^{18}2^0,1]$ |
| 22022022 | 22022022 | 22022022 | $[14,4^0 2^4,24_E]$ |
| 31031031 | 31031031 | $2^9$ | $[14,4^2 2^2,12_E]$ |
| 31031031 | 31031031 | $3^9$ | $[14,4^4 2^0,9_E]$ |
| 3001 | 3001 | 22022022 | $[14,4^6 2^4,8_E]$ |
| 333 | 333 | $2^9$ | $[14,4^7 2^1,8_E]$ |
| 3001 | 3001 | $3^9$ | $[14,4^8 2^0,8_E]$ |
| 31 | 31 | 22022022 | $[14,4^8 2^2,6_E]$ |
| 3001 | 3001 | 31031031 | $[14,4^{10}2^0,6_E]$ |
| 333 | 333 | 31031031 | $[14,4^{11}2^0,4_E]$ |
| 3001 | 3001 | 3003003 | $[14,4^{12}2^0,3_E]$ |
| $2^9$ | $2^9$ | 1001 | $[14,4^{12}2^6,2_E]$ |
| $3^9$ | $3^9$ | 1001 | $[14,4^{13}2^5,2_E]$ |
| 3003003 | 3003003 | 1021 | $[14,4^{15}2^2,2_E]$ |
| $2^9$ | $2^9$ | 11 | $[14,4^{16}2^2,2_E]$ |

Tablo 6.2. Lee ve Öklid ağırlıkları ile 23 uzunluğundaki bazı devirli kodlar

| $g_1(x)$ | $g_2(x)$ | $g_3(x)$ | $\mathbb{Z}_4$ görüntülerinin parametreleri |
|---|---|---|---|
| $202002002^5$ | $202002002^5$ | $2^{23}$ | $[46,4^0 2^{13},14]$ |
| $202002002^5$ | $202002002^5$ | $202002002^5$ | $[46,4^0 2^{22},16]$ |
| $2^{23}$ | $2^{23}$ | 220002220202 | $[46,4^0 2^{24},14]$ |
| $202002002^5$ | $202002002^5$ | $2^5 00200202$ | $[46,4^0 2^{33},4]$ |
| $3^{23}$ | $3^{23}$ | $2^{23}$ | $[46,4^1 2^1,23]$ |
| $3^{23}$ | $3^{23}$ | 220002220202 | $[46,4^1 2^{23},14]$ |
| 3230210013333 | 3230210013333 | $202002002^5$ | $[46,4^{11} 2^{11},12]$ |
| 3230210013333 | 3230210013333 | 220002220202 | $[46,4^{11} 2^{13},10]$ |
| 310023330321 | 310023330321 | 220002220202 | $[46,4^{12} 2^{12},10]$ |
| $3230210013^4$ | $3230210013^4$ | $1^{11}331113331313$ | $[46,4^{13} 2^{11},10]$ |
| $202002002^5$ | $202002002^5$ | $2^{23}$ | $[46,4^0 2^{13},28_E]$ |
| $202002002^5$ | $202002002^5$ | $202002002^5$ | $[46,4^0 2^{22},32_E]$ |
| $2^{23}$ | $2^{23}$ | $202002002^5$ | $[46,4^0 2^{24},28_E]$ |
| $3^{23}$ | $202002002^5$ | $2^5 00200202$ | $[46,4^0 2^{33},8_E]$ |
| $1^{11}331113331313$ | $1^{11}331113331313$ | $2^{23}$ | $[46,4^1 2^{12},23_E]$ |
| $3^{23}$ | $3^{23}$ | $202002002^5$ | $[46,4^1 2^{22},28_E]$ |
| $3^{23}$ | $3^{23}$ | 220002220202 | $[46,4^1 2^{23},23_E]$ |
| $202002002^5$ | $202002002^5$ | $1^{11}331113331313$ | $[46,4^2 2^{33},4_E]$ |
| $3230210013^4$ | $3230210013^4$ | $2^{23}$ | $[46,4^{11} 2^2,28_E]$ |
| 1030232211313 | 1030232211313 | $2^{23}$ | $[46,4^{11} 2^{12},12_E]$ |
| $3230210013^4$ | $3230210013^4$ | 220002220202 | $[46,4^{11} 2^{13},12_E]$ |
| 310023330321 | 310023330321 | 220002220202 | $[46,4^{12} 2^{12},12_E]$ |
| $3230210013^4$ | $3230210013^4$ | $1^{11}331113331313$ | $[46,4^{13} 2^{11},12_E]$ |

# BÖLÜM 7. SONUÇLAR VE ÖNERİLER

$\mathbb{Z}_4 + u\mathbb{Z}_4$ halkasındaki devirli kodlar incelendi ve bu halka üzerindeki devirli kodların üreteçleri araştırılıp geren kümeleri oluşturuldu.

$(2+u)$- sabit devirli kodlar için Gray dönüşümü tanımlandı ve uzunluğu tek olan $(2+u)$- sabit devirli kodların Gray görüntüsünün devirli bir koda eşit olduğu ispatlandı. Ayrıca sabit devirli kodların üreteç polinomları da belirlendi.

Kendine dual kodlar, projeksiyonlar, liftler ve $\mathbb{Z}_4$ görüntüleri, özdeşlik anlamında kendine dual ve ikili dairesel kodlar incelendi.

$R$ üzerindeki devirli kodların ve bazı tek uzunluktaki Gray görüntülerinin bilgisayar araştırma sonuçları ifade edildi.

# KAYNAKLAR


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

[2] HUNGERFORD, Thomas W., Algebra, Springer, 2000.

[3] ÇALLIALP, F., TEKİR, Ü., Değişmeli Halkalar Ve Modüller, Birsen Yayınevi, 2009.

[4] McDONALD, Bernard R., DEKKER. M., Finite Rings With Identity, QA 251.5.M3, 1974.

[5] HILL, R., KOLMAN, B., Elementary Lineer Algebra, Prentice Hall, 2000.

[6] ROMAN, S., Advanced Lineer Algebra, , Graduate Texts in Mathematics, Springer, 2000.

[7] DOUGHERTY, Steven T., SHIROMOTO, K., Maximum Distance Codes Over Rings of Order 4, IEE, Transactions on Information Theory, Vol. 47, No.1, January 2001.

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

[9] WAN, Zhe X., Finite Fields and Galois Rings, World Scientific, 2012.

[10] LING, S., XING, C., Coding Theory, Cambridge University Press, 2004.

[11] DERTLİ, A., CENGELLENMİS, Y., EREN.,S., On Quantum Codes Obtained From Cyclic Codes, arXiv:1407.1232v1 [cs. IT], 19 Jun 2014.

[12] GRAYBILL, Franklin A., Matrices With Applications In Statistics, Second Edition, Duxbury, Thomson Learning, 1983.

[13] QIAN, JF., ZHANG, LN., ZHU, SX., $(1+u)$ - Constacyclic and Cyclic Codes over $F_2+uF_2$, Applied Mathematics Letter, Volume:19, Issue:8, Pages: 820-823, Published: AUG 2006.

[14] ROTH, RON M., Introduction to Coding Theory, Cambridge University Press, 2006.

[15] WOLFMANN, J., Negacyclic and Cyclic Codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, 1999, 45(7): 2527–2532.

[16] WOLFMANN, J., Binary Images of Cyclic Codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, 2001, 47(5): 1773–1779.

[17] LING, S., and BLACKFORD, J. T., $\mathbb{Z}_{p^{k+1}}$- Linear Codes, *IEEE Trans. Inform. Theory*, 2002, 48(9): 2592–2605.

[18] BLACKFORD, T., Negacyclic Codes over $\mathbb{Z}_4$ of Even Length, IEEE Transactions on Information Theory 49(6) (2003) 1417–1424.

[19] BACHOC, C., Application of Coding Theory to the Construction of Modular lattices, Journal of Combinatorial Theory Series A 78 (1997) 92–119.

[20] ABUALRUB, T., SIAP, I., Constacyclic Codes over $F_2+uF_2$, 2009.

[21] ABUALRUB, T., SIAP, I., Cyclic Codes over the Rings $\mathbb{Z}_2+u\mathbb{Z}_2$ and $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$, Des. Codes Cryptogr., 42(2007), 273-28.

[22] KARADENİZ, S., YILDIZ, B., $(1+v)$- Constacyclic Codes over $F_2+uF_2+vF_2+uvF_2$ , J. Franklin Inst. 348 (2011), No.9, 2625-2632. (Reviewer: Irfan Siap) 94B15 (11T71).

[23] AMARRA, M.C.V., NEMENZO, F.R., On $(1-u)$- Cyclic Codes over $F_{p^k}+uF_{p^k}$ , Applied Mathematics Letters, 21 (2008), 1129–1133.

[24] HAMMONS, A.R., KUMAR, V., CALDERBANK, A.R., SLOANE, N.J.A., SOLE, P., *The $\mathbb{Z}_4$- linearity of Kerdock, Preparata, Goethals and Related codes*, IEEE Trans. Inform. Theory, 40, 301–319 (1994).

[25] YILDIZ, B., KARADENİZ, S., Linear Codes over $\mathbb{Z}_4+u\mathbb{Z}_4$: Macwilliams Identities, Projections and Formally Self-Dual Codes, Finite Fields Appl., 27(2014), 24-40.

[26] AYDIN, N., KARADENİZ, S., Bahattin Yildiz., Some New Binary Quasi-Cyclic Codes over the Ring $F_2+uF_2+vF_2+uvF_2$, AAECC (2013) 24:355-367.

[27] YILDIZ, B., AYDIN, N., On Cyclic Codes over $\mathbb{Z}_4+u\mathbb{Z}_4$ and Their $\mathbb{Z}_4$- Images, Int. J. Informatıın and Coding Theory, Vol. 2, No.4, 2014.

[28] BANDI, R.K. and BAINTWAL, M., Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, IEEE.

[29] ONO, TAKASHI., An Introduction to Algebraic Number Theory, Plenum Press, 1990.

[30] SHIRALI, SATISH., VASUDEVA, HARKRISHAN L., Metric Spaces, Springer, 2006.

[31] MINJIA, S., Optimal p-ary Codes from Constacyclic Codes over a Non-chain Ring R_, Chinese Journal of Electronics, Vol:23, No:4, Oct. 2014.

[32] PLESS, VERA S., QIAN, Z., Cyclic Codes and Quadratic Residue Codes over $\mathbb{Z}_4$, IEEE Transactions on Information Theory, Vol. 42, Issue: 5, pp. 1594-1600, 1996.

[33] ABUALRUB, T. and SIAP, I. (2007) `Reversible Cyclic Codes over $\mathbb{Z}_4$', The Australasian Journal of Combinatorics , Vol. 38, pp. 195-206.

[34] Database of $\mathbb{Z}_4$ Codes. [online] $\mathbb{Z}_4$ Codes.info (Accessed May 3, 2015).

[35] GRASSL. M., (Bounds on the minimum distance of linear codes) available at http://www.codetables.de (Accessed may 4, 2015).

[36] AYDIN, N. and ASAMOV, T. (2009) `A Database of Z4 Codes', Journal of Combinatorics, Information & System Sciences, Vol. 34 No. 1-4, pp. 1-12.

[37] Database of Z4 Codes. [online] $\mathbb{Z}_4$ Codes.info (Accessed May 4, 2015).

[38] BERLEKAMP. E.R, Algebraic Coding Theory, New York, McGraw-Hill, 1984.

[39] MARTINEZ-MORO. E., and SZABO. S., On Codes over Local Frobenius Non-chain Rings of Order 16, Contemporary Mathematics, Vol 634 (2015), 227-241.

[40] HAZEWINKEL. M., Handbook of Algebra, Elsevier, 2008.

[41] WOOD, JAY ALAN., Duality for Modules over Finite Rings and Applications to Coding Theory, American Journal of Mathematics, Vol. 121, Issue.3, pp. 555-575, 1999.

# ÖZGEÇMİŞ

Fatma Zehra Uzekmek, 07.05.1991'de Sakarya'da doğdu. İlk, orta ve lise eğitimini Sakarya'da tamamladı. 2008 yılında Özel Zaim Işık Anadolu Lisesi'nden mezun oldu. 2009 yılında başladığı Sakarya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nü 2013 yılında bölüm ikincisi olarak bitirdi. Aynı yıl içerisinde Sakarya Üniversitesi Matematik Anabilim Dalında yüksek lisansa başladı.