**T.C.**
**NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

# KONSTA-DEVİRLİ KODLAR

**Tezi Hazırlayan**
**Bahar KULOĞLU**

**Tez Danışmanı**
**Doç. Dr. Sezer SORGUN**

**Matematik Anabilim Dalı**
**Yüksek Lisans Tezi**

**Mayıs 2016**
**NEVŞEHİR**

**T.C.**
**NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

# KONSTA-DEVİRLİ KODLAR

**Tezi Hazırlayan**
**Bahar KULOĞLU**

**Tez Danışmanı**
**Doç. Dr. Sezer SORGUN**

**Matematik Anabilim Dalı**
**Yüksek Lisans Tezi**

**Mayıs 2016**
**NEVŞEHİR**

Doç. Dr. Sezer SORGUN danışmanlığında **Bahar KULOĞLU** tarafından hazırlanan "**Konsta-Devirli Kodlar**" başlıklı bu çalışma, jürimiz tarafından Nevşehir Hacı Bektaş Veli Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında **Yüksek Lisans Tezi** olarak kabul edilmiştir.

23/05/2016

**JÜRİ**

Başkan : Doç. Dr. Hacı AKTAŞ

Üye : Doç. Dr. Sezer SORGUN

Üye : Doç. Dr. Yasin YAZLIK

ONAY:

Bu tezin kabulü Enstitü Yönetim Kurulunun 23.05.2016...tarih ve...20-182...
sayılı kararı ile onaylanmıştır.

25/05/2016
Doç.Dr. Şahlan ÖZTÜRK
Müdür

Enstitü Müdürü

## TEZ BİLDİRİM SAYFASI

Tez yazım kurallarına uygun olarak hazırlanan bu çalışmada yer alan bütün bilgilerin bilimsel ve akademik kurallar çerçevesinde elde edilerek sunulduğunu ve bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Bahar KULOĞLU

# TEŞEKKÜR

Tezimin konusunun belirlenmesinde, araştırma aşamasında yön tayininde ve tamamlanmasında destek olan değerli hocam Doç. Dr. Hacı AKTAŞ ve tez danışmanım Doç. Dr. Sezer SORGUN'a bana ayırdıkları değerli zamanları ve sağladıkları destekler için teşekkür ederim.

Gösterdikleri sabır ve verdikleri her türlü destekle yanımda olan aileme de ayrıca teşekkür ederim.

**KONSTA-DEVİRLİ KODLAR**

**(Yüksek Lisans Tezi)**

**Bahar KULOĞLU**

**NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**Mayıs 2016**

## ÖZET

Bu tezde ele alınan konular genel itibari ile "J. Qian, Li Zhang, Shi Zhu, Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$, *Oxfored Journals Mathematics and Physical Sciences IEICE-Tran Fund Elec*, Comm and Comp Sci E89-A, 6, 2006. 1863-1865" ve "Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu, $(1 + u) -$ constacyclic and cyclic over $F_2 + uF_2$, *Applied Mathematics Letters*, 19 (18) 2006, 820-823" makalelerinden derlenmiştir.

Tezin birinci bölümünde kodlamanın doğuşu ve amacı ile ilgili bilgiler, ikinci bölümünde kodlama teorisi ile ilgili temel tanım ve kavramlar verilmiştir.

Üçüncü bölümde, sonlu zincir halkaları üzerindeki konsta-devirli kodlar ele alınmıştır. $Z_4$ üzerinde *n* uzunluğunda bir lineer konsta-devirli kodun Gray görüntüsünün bir ikili uzaklığa sahip değişmez devirli kod olduğu ve $R_2 = F_2 + uF_2$ ve $R_3 = F_2 + uF_2 + u^2F_2$ üzerinde sırası ile $(1 + u) -$ konsta devirli ve $(1 - u^2)$-konsta-devirli kodların genel tanımları verilmiştir.

***Anahtar kelimeler: Devirli kod, Konsta-devirli kod, Kuasi-devirli kod, Gray dönüşüm***
**Tez Danışman: Doç. Dr. Sezer SORGUN**
**Sayfa Adeti: 58**

**CONSTA-CYCLIC CODES**

**(M. Sc. Thesis)**

**Bahar KULOĞLU**

**NEVŞEHİR HACI BEKTAŞ VELI UNIVERSITY**

**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**

**May 2016**

## ABSTRACT

The topics discussed in this thesis has generally been compiled from "J. Qian, Li Zhang, Shi Zhu, Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$, *Oxfored Journals Mathematics and Physical Sciences IEICE-Tran Fund Elec*, Comm and Comp Sci E89-A, 6, 2006. 1863-1865" and "Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu, $(1+u)-$ constacyclic and cyclic over $F_2 + uF_2$, *Applied Mathematics Letters*, 19 (18) 2006, 820-823" references.

In the first section of this thesis some information about the starting of coding is given. In the second section, The basic definitions and concepts related to coding theory is determined.

The third section of the thesis is deal with consta-cyclic codes over finite chain rings. Especially, Gray image of a linear constacyclic code over $Z_4$ of lenght $n$ is a binary distance invariant cyclic code. Also $(1+u)-$ constacyclic and $(1-u^2)$-constacyclic code over the ring $R_2 = F_2 + uF_2$ and $R_3 = F_2 + uF_2 + u^2F_2$ is introduced.

***Keywords: Cyclic code, Constacyclic code, Quasi-cyclic code, Gray map***

**Thesis Supervisor: Assoc. Prof. Dr. Sezer SORGUN**

**Page Number: 58**

## İÇİNDEKİLER

## SİMGELER LİSTESİ

| | |
|---|---|
| $\boldsymbol{Z_2[x]}$ | katsayıları {0,1} elemanlarından oluşan polinom. |
| $\boldsymbol{A}$ | $\{a_1, a_2, \dots, a_q\}$, $q$ elemanlı kod kelimerinin kümesi. |
| $\boldsymbol{C}$ | $C \subset A^n$ olan bir kod kümesi. |
| $\boldsymbol{c}$ | $c \in C$ olan bir kod kelimesi. |
| $\boldsymbol{M}$ | *n* uzunluğundaki kodların boyutu. |
| $\boldsymbol{F_q^n}$ | sonlu $F_q$ cismi üzerinde *n* uzunluğunda vektör uzayı. |
| $\boldsymbol{F_2}$ | {0,1} elemanlarından oluşan bir binary (ikili) cisim. |
| $\boldsymbol{R_2 = F_2 + uF_2}$ | $\{0,1,u,1+u\}$, $u^2 = 0$ kümesi ile değişmeli halkadır. |
| $\boldsymbol{R_3 = F_2 + uF_2 + u^2F_2}$ | $\{0,1,u,u^2,v,v^2,uv,v^3\}, u^3 = 0 \ ve \ v = 1+u, v^2 = 1+u^2, v^3 = 1+u+u^2, uv = u+u^2$ elemanlarından oluşan değişmeli halkadır. |
| $\boldsymbol{d(x,y)}$ | *x* ile *y* arasındaki hamming uzaklık. |
| $\boldsymbol{d(C)}$ | *C* kodunun minimum uzaklığı. |
| $\boldsymbol{w_t(x)}$ | *x* kodunun hamming ağırlığı. |
| $\boldsymbol{w_L(x)}$ | *x* kodunun Lee ağırlığı. |
| $\boldsymbol{w_{t_L}(x)}$ | *x* kodunun Lee uzaklığı. |
| $\boldsymbol{a_r}$ | *r* elemanının Lee ağırlığı. |
| $\boldsymbol{G}$ | üreteç matrisi. |
| $\boldsymbol{H}$ | parite kontrol matrisi. |
| $\boldsymbol{g(x)}$ | üreteç polinomu. |
| $\boldsymbol{s(x)}$ | syndrome polinomu. |
| $\boldsymbol{\phi(z)}$ | $z \in R_2^n$ ve $z \in R_3^n$ ün Gray dönüşümü. |
| $\boldsymbol{\mu}$ | halka izomorfizması. |

# 1.BÖLÜM

# GİRİŞ

Claude Shannons 1948 yılında'' İletişimin Matematiksel Teorisi'' adlı makalesinde bilgi teorisi ve kodlama teorisinin doğuşuna imza attı. Temel amaç ise düşmanca bir çevre içerisinde etkili ve güvenli iletişim sağlamaktı. Bu iki amacın varlığı daima avantaj olacaktı bizim temel problemimiz ise bunları daima bağdaştırmak olmalı idi.

Kodlama teorisi temelde cebirsel anlamda inşa edilmiş modeller aracılığı ile bu bağların oluşmasını farketmemize yardımcı oldu.

Shannons'un meslektaşı Richard Hamming aslında Shannons'un 1948 deki makalesinden daha önce ilk bilgisayarlar ile ''Hata Düzeltme'' üzerinde çalışmalar yaptı. ve o kodlama teorisindeki ilk buluşları oluşturdu.

Aşağıdaki şema bize bir kaynaktan gönderilen bilginin bir kanal aracılığı ile varacağı yere ulaşma sistemini göstermektedir.

Bilgi Kaynağı → Kodlayıcı → İletişim Kanalı → Alıcı → Bilgi Alıcısı

↑

Gürültü

Bu şemanın en önemli parçası gürültüdür. Eğer gürültü ya da diğer bir değişle gürültü olmazsa teori için çalışmaya ihtiyaç kalmayacaktır.

$n$ uzunluğunda ve $M$ sayıda bir kod her biri $n$ bileşen ile $M$ vektörlerinin kümesinden oluşur. Bu bileşenler $S$ alfabe kümesinden alınır. Klasik kodlama teorisinde $S$, $|S|$ mertebeli bir cisimdir.

Bir $C$ kodu , $S^n$ in $n$ boyutlu alt kümelerinin kümesidir. Bir lineer $C$ kodu $S$ kümesi üzerinde bir üretici $G$ matrisi ile belirlenir. Yani; $C$, $G$ uzayının satırlarından oluşmaktadır.

Bu tez üç bölümden oluşmaktadır. İlk bölüm de kodlamanın tarihçesi hakkında kısa bir bilgi verilip ikinci bölümde halka, idealler ve kodlar üzerinde genel tanımlardan ve aynı zamanda üreteç ve (parite kontrol ) parity-check matrisinden bahsedilmiştir.

Son bölümde ise sonlu $R_2\ ve\ R_3$ zincir halkaları üzerinde konsta- devirli kodlar ve bunlar üzerinde tanımlanan Gray dünüşümler ile ilgili yapılan çalışmalar derlenmiştir.

# 2. BÖLÜM

# TEMEL TANIM VE KAVRAMLAR

Bu bölümde geçen teoremler ve sonuçlar [1-7] kaynaklarından alınmıştır.

## 2.1. Halkalar ve Sonlu Cisimler

Bu bölümde temel cebir yapıları, yani; halkalar, polinom halkaları, idealler, maximal idealler, temel idealler, indirgenemez polinomlar ve idempotent polinomların genel tanım ve teoremler ile ifade edilecektir.

**Tanım 2.1.1.** $\Phi$ , R halkasından S halkasına bir dönüşüm olsun. $\forall a, b \in R$ için;

1. $\Phi\ (a + b) = \Phi\ (a) + \Phi\ (b)$
2. $\Phi(a.b) = \Phi(a).\Phi(b)$

şartları sağlanıyorsa $\Phi$ ye $R$ den $S$ ye bir halka homomorfizması denir.

Örnek 2.1.1. Gerçel katsayılı bütün polinomları $R[x]$ halkası ile gösterelim.$f(x) \rightarrow f(1)$ dönüşümü $R[x] \rightarrow R$ ye bir halka homomorfizmasıdır.

**Tanım 2.1.2.** $\Phi$ ye $R$ den $S$ ye bir halka homomorfizması olmak üzere

a) $\Phi$ 1-1 ise monomorfizma
b) $\Phi$ örten ise epimorfizma
c) $\Phi$ hem bire bir hem de örten ise izomorfizma

adını alır.

**Tanım2.1.3.** $R$ bir halka olsun. $I$, $R$ nin boş olmayan bir altkümesi olsun. Eğer ;

1. $\forall a, b \in I$ için $a - b \in I$ ,
2. $\forall r \in R$ ve $\forall a \in I$ için $r.a \in I$ ve $a.r \in I$

koşulları sağlanıyor ise *I* ya *R* nin bir idealidir denir.

Örnek 2.1.2. Herhangi bir *R* halkası için $\{0\}$ ve *R*, *R* nin idealleridir.

**Tanım 2.1.4.** *I*, *R* nin bir ideali olsun. Eğer *I*, $g \in I$ olacak biçimde bir eleman tarafından üretilir ise yani; $I = \langle g \rangle = \{g.r : r \in R\}$ oluyorsa o zaman *I* ya esas (temel) ideal denir.

Bir $R$ halkasının her ideali esas ideal oluyorsa bu durumda $R$ ye esas ideal halkası denir. $g$ elemanı $I$ nın üreteciolarak adlandırlır ve $I, g$ tarafından üretilir denir.

**Tanım 2.1.5.** $R$ bir halka ve $A$ , $R$ halkasının bir ideali olsun. $\{r + A : r \in R\}$ kümesi, çarpım halkası olarak adlandırılır.

Örnek 2.1.3. $F_2[x]/(x^3 - 1)$ halkasında $I = \{0, 1 + x, x + x^2, 1 + x^2\}$ altkümesi bir idealdir.

**Tanım 2.1.6.** *R* bir halka, *M*, *N; R* nin idealleri olsun. Eğer $M \neq R$ *ve* $M \subseteq N \subseteq R$ olacak şekildelde en az bır *N* kümesi varsa ve $M=N$ veya $N=R$ oluyorsa bu durumda *M* ye *R* nin maksimal ideali denir.

Örnek 2.1.4. $\mathbb{Z}_{36}$ nın maksimal idealleri $\langle 2 \rangle$ ve $\langle 3 \rangle$ tür.

Örnek 2.1.5. $F_2[x]/(x^3 - 1)$ halkasında $I=\{0, 1 + x, x + x^2, 1 + x^2\}$ altkümesi esasdır. Yani; $I=\langle 1 + x \rangle$ dir. Şimdi dikkat edilirse;

$0.(1 + x) = 1+x^3 = 0 = (1 + x + x^2).(1 + x)$;

$1.(1 + x) = 1 + x = (x + x^2)(1 + x)$;

$x.(1 + x) = x + x^2 = (1 + x^2).(1 + x)$;

$x^2(1 + x) = 1 + x^2 = (1 + x)(1 + x)$

eşitliklerinin sağlandığı görülür.

**Tanım 2.1.7.** *R* bir değişmeli halka olsun. $a, b \in R$ için $a \neq 0, b \neq 0$ olmak üzere $a.b = 0$ ise $a$ ve $b$ elemanlarının her birine bir sıfır bölen denir.

**Tanım 2.1.8.** Eğer $\langle f_1 \rangle + \langle f_2 \rangle = R[x]$ veya eşit olarak $f_1 g_1 + f_2 g_2 = 1$, $g_1, g_2 \in R[x]$ varsa $f_1, f_2 \in R[x]$ polinomları aralarında asal polinomlardır denir. Eğer $f \in R[x]$ bir sıfır bölen değilse o zaman regüler olarak adlandırılır.

**Tanım 2.1.9.** Herhangi bir $f(x) \in F[x]$ polinomu için eğer $f(x) = a(x).b(x), a(x), b(x) \in F[x]$ ve $a(x)$ veya $b(x)$ ten biri 0 derecesine sahip yani sabit ise o zaman $f(x)$ polinomuna $F$ cismi üzerinde indirgenemez polinom denir. Aksi taktirde $f(x)$ polinomu indirgenebilirdir.

Örnek 2.1.6. $g(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$ polinomunun derecesi 2 ve bu polinom indirgenemez bir polinomdur. Aksi takirde bu polinom $x$ veya $x + 1$ gibi bir lineer çarpana sahip olabilirdi. Yani; *0* veya *1* $g(x)$ polinomunun bir kökü olabilirdi. Fakat $g(0) = g(1) = 1 \in \mathbb{Z}_2$ dir.

Örnek 2.1.7. $f(x) = x^4 + 2x^6 \in \mathbb{Z}_2[x]$ polinomunun derecesi *6* dır. Bu polinom $f(x) = x^4(1 + 2x^2)$ olacak şekilde indirgenebilir bir polinomdur.

**Tanım 2.1.10.** Bütün polinomların halkasını $F_q$ cismi üzerinde ve mod $(1 + x^n)$ bağıntısına göre $F_q[x]/(1 + x^n)$ olarak tanımlayalım.

Eğer $I^2(x) \equiv I(x) \ \ (mod(1 + x^2))$ ise o zaman $I(x) \in R_n$ polinomu idempotent olarak adlandırılır.

Örnek 2.1.8. $x^3 + x^6 \in \mathbb{Z}_2[x]/(x^9 + 1)$, $(x^3 + x^6)$ polinomu $mod(1 + x^9)$ için bir idempotent elemandır. Çünkü $\mathbb{Z}_2$ üzerinde;

$$(x^3 + x^6)^2 \equiv x^6 + 2x^9 + x^{12} \ \ \big(mod(1 + x^9)\big)$$

$$\equiv x^3 + x^6 \qquad\qquad (mod(1 + x^9))$$

dir.

**Tanım 2.1.11.** Sıfır bölensiz birimli ve değişmeli halkaya tamlık bölgesi denir. Eğer *R* birimli ve sıfırdan farklı her elemanı tersinir olan bir halka ise *R* ye bölünme halkası; ayrıca değişmeli bölünme halkasına da cisim denir.

## 2.2 Kodlar İle İlgili Genel Tanımlar

Bu bölümde biz alfabe, kodlar, kod kelimeleri, cisimler üzerindeki kodlar, Hamming ağırlık ve Hamming uzaklıkları ele alacağız.

**Tanım 2.2.1.** $A = \{a_1, a_2, \dots, a_q\}$, $q$ elemanlı bir küme olsun. Bu küme alfabe kodu ve bu kümenin tüm elemanları da kod sembolleri olarak adlandırılır. Bir $n$ uzunluğunda $A$ üzerinde $q-$ lu kelime, $\forall i \in I$ ve her bir $w_i \in A$ için

$W = w_1 w_2 \dots w_n$

şeklinde bir dizidir.

$A$ üzerinde $n$ uzunluğunda bir $q-$ lu blok kod yine aynı uzunluklu $q-$ lu kelimelerinin boş olmayan bir $C$ kümesidir ve $C \subset A^n$ dir.

**Tanım 2.2.2.** $C$ nin bir elemanı $C$ de bir kod kelimesi olarak adlandırılır. $C$ deki kod kelimelerinin sayısı $|C|$ ile gösterilir ve $C$ nin boyutu olarak adlandırılır. $n$ uzunluğunda ve eleman sayısı $M$ olan bir kod $(n, M)$ koddur.

Örnek 2.2.1. $C = \{00,10,01,11\}$ olsun. 01 bir kod kelimesi ve $|C| = 4$ tür.

**Tanım 2.2.3.** $\mathbb{Z}_4$ , $mod4$ ile bir halkadır. Bu halka 4 tane eleman içerir. Bunlar;

$\{0, 1, 2, 3\}$ veya $\{0, 1, 2, -1\}$ dir.

**Tanım 2.2.4.** $F_q^n$, sonlu $F_q$ cismi üzerinde tüm $n-$uzunluğunda vektör uzaylarını tanımlar.

**Tanım 2.2.5.** $R_2 = F_2 + uF_2$ ; $\{0, 1, u, 1+u\}$, $u^2 = 0$ kümesi ile bir değişmeli halkadır. Burada $F_2$, $\{0,1\}$ elemanları ile bir binary (ikili) cisimdir $F_2 + uF_2$ için toplam ve çarpım işlemleri aşağıdaki tablolarda verilmiştir.

| + | 0 | 1 | u | 1+u |
|---|---|---|---|---|
| 0 | 0 | 1 | u | 1+u |
| 1 | 1 | 0 | 1+u | u |
| u | u | 1+u | 0 | 1 |
| 1+u | 1+u | u | 1 | 0 |

| . | 0 | 1 | u | 1+u |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | u | 1+u |
| u | 0 | u | 0 | u |
| 1+u | 0 | 1+u | u | 1 |

**Tanım 2.2.6.** $R_3 = F_2 + uF_2 + u^2F_2$; $\{0, 1, u, u^2, v, v^2, uv, v^3\}, u^3 = 0$ kümesi ile bir değişmeli halkadır. Burada $v = 1 + u$, $v^2 = 1 + u^2, v^3 = 1 + u + u^2, uv = u + u^2$ dir.

*R* üzerinde toplamsal ve çarpımsal işlemler aşağıdaki tabloda verilmiştir.

| + | 0 | 1 | u | v | $u^2$ | uv | $v^2$ | $v^3$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | u | v | $u^2$ | uv | $v^2$ | $v^3$ |
| 1 | 1 | 0 | v | u | $v^2$ | $v^3$ | $u^2$ | uv |
| u | U | v | 0 | 1 | uv | $u^2$ | $v^3$ | $v^2$ |
| v | v | u | 1 | 0 | $v^3$ | $v^2$ | uv | $u^2$ |
| $u^2$ | $u^2$ | $v^2$ | uv | $v^3$ | 0 | u | 1 | v |
| uv | uv | $v^3$ | $u^2$ | $v^2$ | u | 0 | v | 1 |
| $v^2$ | $v^2$ | $u^2$ | $v^3$ | uv | 1 | v | 0 | u |
| $v^3$ | $v^3$ | uv | $v^2$ | $u^2$ | v | 1 | u | 0 |

| . | 0 | 1 | u | v | $u^2$ | uv | $v^2$ | $v^3$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | u | v | $u^2$ | uv | $v^2$ | $v^3$ |
| u | 0 | u | $u^2$ | uv | 0 | $u^2$ | u | uv |
| v | 0 | uv | v | $v^2$ | $u^2$ | u | $v^3$ | 1 |
| $u^2$ | 0 | $u^2$ | 0 | $u^2$ | 0 | 0 | $u^2$ | $u^2$ |
| uv | 0 | uv | $u^2$ | u | 0 | $u^2$ | uv | u |
| $v^2$ | 0 | $v^2$ | u | $v^3$ | $u^2$ | uv | 1 | v |
| $v^3$ | 0 | $v^3$ | uv | 1 | $u^2$ | u | v | $v^2$ |

**Tanım 2.2.7.** $x$ ve $y$, *A* alfabe kümesi üzerinde *n* uzunluğunda kelimeler olsun.

$x = x_1 x_2 \dots x_n$

$y = y_1 y_2 \dots y_n$

olmak üzere $x$ ile $y$ arasındaki uzaklık karşılıklı farklı sembollerin sayısı olarak tanımlanır ve $d(x, y)$ ile gösterilir. Bu uzaklığa ise Hamming uzaklık adı verilir.

Eğer; $x = x_1 x_2 \dots x_n$ ve $y = y_1 y_2 \dots y_n$ ise o zaman

$$d(x, y) = d(x_1, y_1) + \cdots + d(x_n, y_n) \tag{2.2.1}$$

burada $x_i, y_i$ *1* uzunluğunda kelimelerdir. ve

$$d(x_i, y_i) = \begin{cases} 1, & eğer\ x_i \neq y_i \\ 0, & eğer\ x_i = y_i \end{cases}$$

dir.

Örnek 2.2.2. $A = \{0, 1\}$ ; $x = 01010$ ve $y = 11101$ olsun. O zaman $d(x, y) = 4$ olur.

Örnek 2.2.3. $A = \{0, 1, 2, 3\} = \mathbb{Z}_4$ ve $x = 1230,\ y = 1023$ olsun. O zaman $d(x, y) = 3$ olur.

**Önerme 2.2.1**. $x, y, z$ ; $A$ üzerinde $n$ uzunluğunda kelimeler olsun. o zaman;

1. $0 \leq d(x, y) \leq n$
2. $d(x, y) = 0 \iff x = y$
3. $d(x, y) = d(y, x)$ , $\forall x, y \in A$ için
4. $d(x, z) \leq d(x, y) + d(y, z)$ (üçgen eşitsizliği) $\forall x, y, z \in A$ için

uzaklık fonsiyonunun bu 4 özelliği sağlanır [6].

**Tanım 2.2.8.** $C$ bir kod olsun. $x, y \in C$ için $d(x, y)$ ile $x, y$ kodları arasındaki uzaklığı gösterelim. $C$ deki min $d(x, y)$ ye $C$ kodunun minimum uzaklığı denir ve $d(C)$ ile gösterilir. Yani;

$$d(C) = min\{d(x, y) : x, y \in C,\ x \neq y\}$$

dir.

Örnek 2.2.4. $C = \{00000, 11111, 00111\}$ bir binary (ikili) kod olsun. O zaman $d(C) = 2$ dir. Çünkü;

$d(00000, 00111) = 3$; $d(00000, 11111) = 5$; $d(00111, 11111) = 2$

eşitliklerinden dolayı $C$ bir ikili (binary) $[5, 3, 2]$- koddur.

Örnek.2.2.5. $C = \{000000, 000111, 111222\}$ bir ternary kod olsun. (yani; $\{0, 1, 2\}$ alfabe kodu ile ) o zaman $d(C) = 3$ tür. Çünkü;

$d(000000, 000111) = 3$; $d(000000, 111222) = 6$; $d(000111, 111222) = 6$

eşitliklerinden dolayı, *C* bir üçlü (ternary) $[6, 3, 3]$– koddur.

**Tanım.2.2.9.** $x, y \in C$ olan bir $C$ kodu için $x + y$ de $C$ nin elemanı oluyorsa (yani *C* de bir kelime oluyorsa) o zaman $C$ koduna bir lineer koddur denir. Yani; bir lineer kod, kelimeleri toplama işlemine göre kapalı olan koddur.

Örnek 2.2.6. $C = \{000, 111\}$ , $F_2$ üzerinde bir lineer koddur. Çünkü;

$000 + 000 = 000$

$111 + 000 = 111$

$000 + 111 = 111$

$111 + 111 = 000$

dir. Yukarıdaki toplamlar yine *C* içindedir. Bir lineer kod *000* kelimesini içermek zorundadır.

**Tanım 2.2.10.** $n$ uzunluğunda $F_q$ üzerinde bir lineer $C$ kodu $F_q^n$ nin bir alt uzayıdır.

Örnek 2.2.7**.** $C = \{(\lambda, \lambda, \dots, \lambda): \lambda \in F_q\}$ bir lineer koddur. Bu kod tekrarlayan kod olarak adlandırılır.

**Tanım 2.2.11.** $x \in F_q^n$ olsun. $x$ in Hamming ağırlığı $x$ de sıfırdan farklı bileşenlerin sayısı olarak ifade edilir ve $wt(x)$ olarak gösterilir. Yani;

$wt(x) = d(x, 0)$

dir. Burada ‘’$0$’’ sıfır kelimesidir.

Örnek 2.2.8. $x = (1010111) \in F_2^7,\ y = (00111010111) \in F_2^{11}$ olsun. o zaman

$wt(x) = 5\ ve\ wt(y) = 7$ dir.

**Not 2.2.2.** Bir $x \in \mathbb{Z}_4$ ün Lee ağırlığı ;

$wL(0) = 0; wL(1) = 1; wL(2) = 2; wL(3) = 1$

şeklinde tanımlanır.

**Tanım 2.2.12.** $x \in \mathbb{Z}_4^n$ elemanının Lee ağırlığı $wL = n_1(x) + 2n_2(x) + n_3(x)$ dir. Burada $n_a(x)$, $\forall a \in \mathbb{Z}_4$ için $x$ in $a$ ya eşit bileşenlerinin sayısıdır.

**Uyarı 2.2.1.** $\mathbb{Z}_4^n$, $\mathbb{Z}_4$ üzerinde bir modüldür. $\mathbb{Z}_4$ üzerinde *n* uzunluğunda bir *C* lineer kodu $\mathbb{Z}_4^n$ nin bir altkümesi $\mathbb{Z}_4$ moddur.

Örnek 2.2.9. $x = (12301322) \in \mathbb{Z}_4^8$ olsun. O zaman;

$wL = n_1(x) + 2n_2(x) + n_3(x) = 2 + 2.3 + 2 = 10$

**Tanım 2.2.13** $\forall x, y \in \mathbb{Z}_4^n$ için $d_L = wt_L(x - y)$ olarak tanımlanan ifadeye Lee uzaklık denir ve $d_L$ ile gösterilir.

**Uyarı 2.2.2.** $\forall x \in F_q$ için Hamming ağırlık

$$wt(x) = d(x, 0) = \begin{cases} 1, & x \neq 0\ ise \\ 0, & x = 0\ ise \end{cases}$$

olarak tanımlanır [6].

| X | Y | x●y | $wt(x) + wt(y) - 2wt(x \bullet y)$ | $wt(x + y)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 |

| | | | | |
|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 |

Tablo(1)

$x \in F_q^n$ , $x = (x_1, x_2, \ldots, x_n)$ alarak x in Hamming ağırlığı ini ayrıca aşağıdaki gibi de tanımlayabiliriz;

$$wt(x) = wt(x_1) + wt(x_2) + \ldots + wt(x_n) \quad (2.2.2)$$

**Önerme 2.2.3.** [1] $x, y, z$; $n$ uzunluklu kelimeler ve $a$ bir sayı olsun. şimdi biz ağırlık ve uzaklıkla ilgili birkaç özelliği listeleyelim;

1. $0 \leq wt(x) \leq n$
2. $wt(x) = 0 \Leftrightarrow x = 0$
3. $0 \leq d(x, y) \leq n$
4. Eğer $d(x, y) = 0 \Leftrightarrow x = y$
5. $d(x, y) = d(y, x)$
6. $wt(x + y) \leq wt(x) + wt(y)$
7. $d(x, z) \leq d(x, y) + d(y, z)$
8. $wt(a.x) = a.wt(x), a \neq 0 \; ve \; a \in F_q$
9. $d(ax, az) = a.d(x, z), a \neq 0 \; ve \; a \in F_q$

**Lemma 2.2.4.** Eğer $x, y \in F_q^n$ ise o zaman $d(x, y) = wt(x - y)$ dir [1].

İspat. $x, y \in F_q, d(x, y) = 0 \Leftrightarrow x = y$ ve bu denklem ancak ve ancak $x - y = 0$ veya eşit olarak $wt(x - y) = 0$ anlamına gelir.

Şimdi 2.2.1 ve 2.2.2 denklemlerinden biz;

$$d(x, y) = d(x_1, y_1) + d(x_2, y_2) + \cdots + d(x_n, y_n) \quad (2.2.3)$$

$$wt(x) = wt(x_1) + wt(x_2) + \cdots + wt(x_n) \quad (2.2.4)$$

denklemlerini elde ederiz ve benzer olarak ;

$$wt(x-y) = wt(x_1 - y_1) + wt(x_2 - y_2) + \cdots + wt(x_n - y_n) \quad (2.2.5)$$

$$wt(x-y) = d(x_1, y_1) + d(x_2, y_2) + \cdots + d(x_n, y_n) \quad (2.2.6)$$

elde edilir. 2.2.3 ve 2.2.6 dan;

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

elde edilir.

□

**Lemma 2.2.5**. $x, y \in F_2^n$ olsun. $x = (x_1, x_2, \dots, x_n)$ ve $y = (y_1, y_2, \dots, y_n)$ için;

$$wt(x+y) = wt(x) + wt(y) - 2wt(x \bullet y) \quad (2.2.7)$$

ve burada $x \bullet y = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$ dir [6].

İspat. (2.2.2) den (2.2.7) nin doğru olduğunun ispatı açıktır. Bu tablo1 den kolaylıkla doğrulanır.

**Tanım 2.2.14.** $C$ bir kod olsun. $wt(C)$ ile tanımlanan $C$ nin minimum(Hamming) ağırlığı; $C$ de sıfırdan farklı kod kelimelerinin en küçük weghtidir.

**Teorem 2.2.6.** $C$, $F_q$ üzerinde bir lineer kod olsun. o zaman $d(C) = wt(C)$ dir [6].

İspat. Lemma2.2.4 ten $d(x,y) = wt(x-y)$ dir. Tanım 2.2.14 ten $d(\acute{x}, \acute{y}) = d(C)$ olacak biçimde $\acute{x}, \acute{y} \in C$ vardır. $\acute{x} - \acute{y} \in C$ olduğundan dolayı;

$$d(C) = d(\acute{x}, \acute{y}) = wt(\acute{x} - \acute{y}) \geq wt(C) \text{ dir.} \quad (2.2.8)$$

Tersine; bir $z \in C \backslash \{0\}$ vardır öyle ki; $wt(C) = wt(z)$ dir. Böylece;

$$wt(C) = wt(z) = d(z, 0) \geq d(C) \quad (2.2.9)$$

dir. 2.2.8 ve 2.2.9 dan;

$$d(C) = wt(C)$$

elde edilir.

□

Örnek 2.2.10. $C = \{0000,1000,0100,1100\}$ bir ikili (binary) lineer kod olsun. Şimdi;

$wt(1000) = 1; wt(0100) = 1; wt(1100) = 2$

olsun. Buradan $d(C) = 1$ dir.

**Tanım 2.2.15.** $C$ bir lineer $[n, k]$-kod olsun.

$C^{\perp} = \{x \in F_q^n : \ x.c = 0, \forall c \in C\}$

kümesi $C$ için dual kod olarak adlandırılır. Burada $x.c, x \ ve \ c$ vektörlerinin $x_1c_1 + x_2c_2 + \cdots + x_nc_n$ şeklindeki genel skaler çarpımıdır. Dikkat edilirse $C^{\perp}$ bir $[n, n-k]$-koddur.

**Tanım 2.2.16.** $x = x_1x_2, \dots, x_n$ ve $y = y_1y_2, \dots, y_n$ binary kelimeler olsun. $x \ ve \ y$ nin kesişimi;

$x \cap y = (x_1y_1, x_2y_2, \dots, x_ny_n)$

şeklinde tanımlanır.

$x \ ve \ y$ nin çarpımı;

$x.y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$

şeklinde yazılır.

**Teorem 2.2.7**

1. Eğer $x, y \in F_2^n$ ise $wt(x + y) = wt(x) + wt(y) - 2wt(x \cap y)$
2. Eğer $x, y \in F_2^n$ ise $wt(x \cap y) \equiv x.y \ \ (mod 2)$
3. Eğer $x \in F_2^n$ ise ise $wt(x) \equiv x.x \ \ (mod 2)$
4. Eğer $x \in F_3^n$ ise $wt(x) \equiv x.x \quad (mod 3)$
5. Eğer $x \in F_4^n$ ise $wt(x) \equiv x.x \quad (mod 2)$

şartları sağlanır [7].

**Tanım 2.2.17.** $R_2 = F_2 + uF_2$ olsun. $R_2$ halkasında bir $r$ elemanının Lee ağırlığı

$a_r$ aşağıdaki denklemlerle ifade edilir;

$$a_{r=}\begin{cases} 0, & r=0\ ise \\ 1, & r=1\ veya\ 1+u\ ise \\ 2, & r=u\ ise \end{cases}$$

Buradan bir $x=(x_1,x_{2,}\dots,x_n)\in R_2^n$ elemanının Lee ağırlığı;

$$wt_L(x)=\sum_{i=1}^{n} a_r$$

biçiminde olur.

**Tanım 2.2.18.** $R_3=F_2+uF_2+u^2F_2$ olsun. $R_3$ halkasında bir $r$ elemanının Lee ağırlığı $a_r$ aşağıdaki denklemlerle elde edilir.

$$a_r=\begin{cases} 0; & r=0 \text{ ise} \\ 1; & r=1 \text{ veya } v^2\ ise \\ 2; & r=u \text{ veya } uv\ ise \\ 3; & r=v \text{ veya } v^3\ ise \\ 4; & r=u^2 \text{ise} \end{cases}$$

Örnek 2.2.11. $x=(1,0,0,u,v,u^2,v^2,uv)$ olsun. Buradan $wt_L(x)=13$ elde edilir.

**Tanım 2.2.19.** $x,y\in R^n$ arasındaki Lee uzaklık;

$$d_L(x,y)=wt_L(x-y)$$

şeklinde tanımlanır.

**Tanım 2.2.20.** $X;\ F_q$ üzerinde bir vektör uzayı olsun. Eğer ;

$$\lambda_1x_1+\cdots+\lambda_rx_r=0$$

$$\lambda_1=\cdots=\lambda_n=0$$

ise o zaman . $X$ de $\{x_1,\dots,x_r\}$ vöktörlerinin kümesi lineer bağımsızdır denir.

Örnek 2.2.12. Herhangi $F_q\ için$ $\{(0,0,0,1),(0,0,1,0),(0,1,0,0)\}$ kümesi lineer bağımsızdır.

**Tanım 2.2.21.** $V, F_q$ üzerinde bir vektör uzayı ve $S = \{v_1, v_2, \dots, v_k\}$ kümesi $V$ nin boş olmayan bir altkümesi olsun. $S$ nin lineer gereni;

$$\langle S \rangle = \{\lambda_1 v_1 + \cdots + \lambda_k v_k : \lambda_i \in F_q\}$$

olarak tanımlanır. $C, V$ nin bir altuzayı ve $S\ de\ C$ nin bir alt kümesi olsun. Eğer $C = \langle S \rangle$ ise o zaman $S\ ye\ C$ kümesinin gereni adı verilir.

**Tanım 2.2.22.** $X, F_q$ üzerinde bir vektör uzayı olsun. $X = \langle B \rangle$; $B$ lineer bağımsız ve $X$ için bir geren küme ise $X$ in boş olmayan bir $B = \{x_1, \dots, x_r\}$ kümesi $X$ için bir baz olarak adlandırılır.

**Tanım 2.2.23.** Sonlu $F_q$ cismi üzerinde $X$ bir vektör uzayı olsun. Bu uzay birçok baza sahip olabilir fakat bütün bazlar aynı sayıda elemana sahiptirler. Bu sayıya $X$ in $F_q$ üzerinde boyutu denir ve $dim(X)$ ile gösterilir.

**Tanım 2.2.24.** $a$, $M$ maksimal idealinin bir sabit üreteci olsun. o zaman $a$ bir nilpotent tir.

Buradan $a$ nın nilpotent indeksini $t$ alarak $a^t = 0$ tanımlarız. $R$ nin idealleri ;

$$R = \langle a^0 \rangle \supsetneq \langle a^1 \rangle \supsetneq \cdots \supsetneq \langle a^{t-1} \rangle \supsetneq \langle a^t \rangle = \langle 0 \rangle$$

şeklinde zincirdir.

**Tanım 2.2.25**. Eğer herhangi bir R halkasının bütün sağ ve sol ideallerinin kümesi bir sonlu zincir oluşturuyorsa R halkasına zincir halkası adı verilir.

## 2.3. Üreteç ve Parite Kontrol (Parity Check) Matrisi

Bir lineer kod için bazları bilmek bize onun kod kelimelerini açıkça tanımlama imkanı sağlar. Kodlama teorisinde, bir lineer kod için baz sıkça matris formunda temsil edilir ve üreteç matrisi olarak adlandırılır. Dual kod için matris gösterimi parite kontrol matrisi olarak adlandırılır. Bu matrisler kodlama teorisinde önemli rol oynar. *K* üzerinde bir matrisin rankı; herhangi eşelon formdaki bir matrisin sıfırdan farklı satır sayısıdır. *C* kodunun boyutu olan k; *C* nin boyutudur.

**Tanım 2.3.1.** Eğer *C; n* uzunluğunda boyutu *k* olan bir lineer kod ise; satırları *C* için bir baz oluşturan herhangi bir matris, *C* için üreteç matrisi olarak adlandırılır. *C* için üreteç matrisinin *k* sayıda satıra ne *n* sayıda sütuna sahip olması gerektiği unutulmamalıdır.

**Tanım 2.3.2.** *K* üzerindeki bir matrisin rankı bir matrisin herhangi bir eşelon formdaki sıfırdan farklı satır sayısıdır.

**Teorem 2.3.1.** *G* matrisi bazı lineer *C* kodu için üreteç matrisidir ancak ve ancak *G* nin satırları lineer bağımsızdır. Yani; *G* nin rankı *G* nin satırlarının sayısına eşittir. [6]

**Tanım 2.3.3.** Herhangi bir $k < n$, $k \times n$ tipinde bir *G* matrisinin ilk $k$ sütunu $k \times k$ tipinde $I_k$ birim matrisidir. Böylece;

$$G = (I_k|X)$$

indirgenmiş eşelon formda lineer bağımsız satırlara sahiptir. Böylece *G* matrisi *n* uzunluğunda ve *k* boyutlu bazı lineer kodlar için üreteç matrisidir.

Bir *G* üreteç matrisi standart form olarak adlandırılır ve *G* tarafından üretilen *C* kodu sistematik kod olarak adlandırılır.

**Teorem 2.3.2.** Eğer $G = (I_k|X)$ standart formda *C* $[n, k]$ kodu için bir üreteç matrisi olsun. o zaman $H = (-X^{\perp}|I_{n-k})$ , C için bir parite kontrol matrisidir. [6]

**Teorem 2.3.3.** Eğer *G*, bir lineer *C* kodu için üreteç matrisi ise o zaman satırları *G* ye denk herhangi bir matris de aynı zamanda *C* kodu için üreteç matrisidir. Özellikle, herhangi bir lineer kod indirgenmiş eşelon formda bir üreteç matrisine sahiptir. [6]

Örnek 2.3.1. $S = \{11101, 10110, 01011, 11010\}$ ve $C = \langle S \rangle$ olan bir lineer kodun üreteç matrisini bulmak için, elemanter satır işlemlerinden;

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

yazılır. Böylece;

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} = (I_3|X)$$

*C* için bir standart form olur.

**Tanım 2.3.4.** Eğer bir lineer *C* kodu için herhangi bir *H* matrisinin satırları $C^{\perp}$ nin kodu için bir baz oluyorsa o zaman *H* matrisine parite kontrol matrisi denir ve ;

$$C^{\perp} = \{x \in F_q^n | \, Hx^{\perp} = 0\}$$

ile ifade edilir.

Eğer $C$ kodu $n$ uzunluğunda ve $k$ boyutlu bir kod ise o zaman $C$ ve $C^{\perp}$ nin boyutlarının toplamı $n$ dir ve $C$ için herhangi bir parite kontrol matrisi $n$ sayda satıra, $n-k$ sayıda sütuna sahip olup rankı $n-k$ dır.

Örnek 2.3.2. $S = \{11101, 10110, 01011, 11010\}$ ve $C = \langle S \rangle$ olan bir *C* lineer kodunun parite kontrol matrisini bulmak için elemanter satır işlemlerinden;

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

buradan;

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$= (I_3 | X)$$

*C* kodu için bir üreteç matrisi olur ve;

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} = (X^{\perp} \backslash I_2)$$

*C* kodu için bir parite kontrol matrisi olur.

**Teorem 2.3.4.** Bir *C* lineer kodu için *H* bir parite kontrol matrisidir ancak ve ancak *H* ın sütunları lineer bağımsızdır. [1]

**Teorem 2.3.5.** Eğer *n* uzunluğunda bir lineer *C* kodu için *H* parite kontrol matrisi ise o zaman *C* kodu $K^n$ deki tüm *x* kelimelerinden oluşur. Buradan ;

$xH^T = 0$

deklemi elde edilir. [1]

Örnek 2.3.3. $G = (I_4|X)$ olsun. Burada ;

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$[7, 4]$ binary (ikili) kod için standart formda bir üreteç matrisidir. Parite kontrol matrisi ise;

$H = (X^T|I_3)$

$$= \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

şeklinde elde edilir.

**Tanım 2.3.5.** $n$ uzunluğunda bir lineer $C$ kodu bir devirli değişim altında invaryant ise o zaman $C$ koduna $R$ üzerinde devirli kod denir. Yani;

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

ancak ve ancak

$\tilde{c} = (c_{n-1}, c_0, c_1, \dots, c_{n-3}, c_{n-2}) \in C$

dir.

Örnek 2.3.4. $\{11111, 00000\} \subset F_2^5$ kümesi bir devirli koddur.

Örnek 2.3.5. Aşağıdaki kodlar devirli kodlardır:

- üç aşikar kod: $\{0\}, \{\lambda.1 : \lambda \in F_q\}$ $ve$ $F_q^n$
- $[3, 2, 2]$ binary (ikili) lineer kodu $\{000, 110, 101, 011\}$

**Teorem 2.3.6.** $C$ , üreteç matrisi $g(x) = g_1 + g_2x + \cdots + g_kx^{k-1}$ olan devirli kod olsun.

O zaman verilen kod için üreteç matrisi;

$$G = \begin{pmatrix} g_1 & g_2 & g_3 & \cdots & g_k & 0 & 0 & \cdots & 0 \\ 0 & g_1 & g_2 & \cdots & g_{k-1} & g_k & 0 & \cdots & 0 \\ 0 & 0 & g_1 & \cdots & g_{k-2} & g_{k-1} & g_k & \cdots & 0 \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\ 0 & 0 & \cdots & \cdots & g_1 & \cdots & \cdots & \cdots & g_k \end{pmatrix}$$

şeklinde olur. [6]

**Uyarı 2.3.1.** $n$ uzunluğunda $F_q$ üzerinde bir devirli $C$ kodunun üreteç poliomu $g(x)$, $x^n - 1$ polinomunun bir bölenidir.

**Tanım 2.3.6.** Polinomların halkası x bilinmeyenine göre $F(x)$ olarak yazılır. Yani $F(x)$ ten kasıt olarak $a_0 + a_1x + \cdots + a_nx^n$ olan bütün polinomların kümesini ele almış oluyoruz. Burada $n$ negatif olmayan herhangi bir tamsayı; $a_0, a_1, \ldots, a_n \in F$ tir.

**Tanım 2.3.7**. Eğer ; $p(x) = a_0 + a_1x + \cdots + a_mx^m$ ve $q(x) = b_0 + b_1x + \cdots + b_nx^n$ $F[x]$ de polinomlar ise o zaman $q(x) = p(x) \Leftrightarrow \forall i \geq 0$ için $a_i = b_i$ dir.

**Tanım 2.3.8.** Eğer $p(x) = a_0 + a_1x + \cdots + a_mx^m$ ve $q(x) = b_0 + b_1x + \cdots + b_nx^n$ $F[x]$ te polinomlar ise o zaman $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$ dir. burada $\forall i$ için $a_i + b_i = c_i$ dir.

**Tanım 2.3.9.** Eğer $p(x) = a_0 + a_1x + \cdots + a_mx^m$ ve $q(x) = b_0 + b_1x + \cdots + b_nx^n$ $F[x]$ te polinomlar ise o zaman $p(x)q(x) = c_0 + c_1x + \cdots + c_kx^k$ dır. Burada

$c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t$ dir.

**Tanım 2.3.10.** Bir $n$. dereceden sıfırdan farklı $f(x) = \sum_{i=0}^{n} a_ix^i$ polinomu eğer $a_n = 1$ ise o zaman $f(x)$ polinomuna monik polinom denir.

**Tanım 2.3.11.** $g(x), h(x) \in \mathbb{Z}_4[x]$ olacak şekilde iki polinom olsun. Eğer $f(x) = g(x)h(x)$ ve $g(x)$ veya $h(x)$ ten biri birim ise o zaman $f(x) \in \mathbb{Z}_4[x]$ polinomuna indirgenemez polinom denir.

Örnek 2.3.6. $x^4 - 1$ in indirgenemez polinomlar halindeki $\mathbb{Z}_4$ deki çarpanları $(x - 1)(x + 1)(x^2 + 1)$

**Tanım 2.3.12.** $f(x), g(x) \in \mathbb{Z}_4[x]$ sıfırdan farklı iki polinom olsun. $f(x), g(x) \in \mathbb{Z}_4[x]$ nin en büyük ortak böleni; $(f(x), g(x))$ ile gösterilir. $f(x), g(x) \in \mathbb{Z}_4[x]$ in en büyük ortak böleni en yüksek dereceli monik polinomdur. Eğer $\big(f(x), g(x)\big) = 1$ ise o zaman $f(x)\ ve\ g(x)$ polinomları aralarında asaldır denir.

**Lemma 2.3.7.** $f(x), g(x) \in \mathbb{Z}_4[x]$ polinomlar olsun. $f(x)\ ve\ g(x)$ aralarında asaldır ancak ve ancak $\mu(f(x))\ ve\ \mu(g(x))$, $F_2[x]$ üzerinde aralarında asal polinomlardır. [7]

**Tanım 2.3.13.** . $\mu: \mathbb{Z}_4[x] \longrightarrow F_2[x]\ ve$

$\mu\big(f(x)\big) \equiv f(x)\ \ (mod 2)$ yani; $\mu(0) = \mu(2) = 0, \mu(1) = \mu(3) = 1$ ve $\mu(x) = x$ olarak belirlenen dönüşüm indirgenmiş homomorfizma olarak adlandırılır.

**Tanım 2.3.14.** Eğer $C$ kodu $n$ uzunluğunda, boyutu $k$ olan ve uzaklığı $d$ olan bir kod ise ozaman bu kod $[n, k, d]$ şeklinde ifade edilir ve bu üç parametre herhangi bir $C$ kodu için önemli bilgiler verir.

**Teorem 2.3.8 (Hensel).** $f(x) \in \mathbb{Z}_4[x]$ olsun. $h_1(x)h_2(x) \dots h_k(x)$ polinomları $F_2[x]$ de ikişer ikişer aralarında asal polinomlar olsunlar. Kabul edelim ki $\mu(f(x)) = h_1(x)h_2(x) \dots h_k(x)$ olsun o zaman;

1. $\mu\big(g_i(x)\big) = h_i(x)$
2. $g_1(x)g_2(x) \dots g_k(x)$ fonksiyonları ikişer ikişer aralarında asaldır
3. $f(x) = g_1(x)g_2(x) \dots g_k(x)$ olacak şekilde $g_1(x), g_2(x), \dots, g_k(x) \in \mathbb{Z}_4[x]$ fonksiyonları vardır. [7]

**Tanım 2.3.15.( Graeffe metodu)**

1. $h(x)$, $x^n + 1$ in $F_2[x]$ te indirgenemez çarpanı olsun.

   $h(x) = e(x) + o(x)$; $e(x)$ , $h(x)$ terimlerinin çift kuvvetli üslerinin toplamı ve $o(x)$, $h(x)$ terimlerinin tek kuvvetli üslerinin toplamıdır.

2. $g(x)$, $\mathbb{Z}_4[x]$ te $\mu\big(g(x)\big) = h(x)$ şartıyla $x^n - 1$ in indirgenemez çarpanı olsun. burada $g(x^2) = \pm(e(x))^2 - (o(x))^2$ dir.

Örnek 2.3.7 . $x^7 + 1$ polinomunun $F_2$ de indirgenemez polinomlar halinde çarpanları;

$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$

olsun. $x^7 - 1$ in monik indirgenemez polinomlar halinde $\mathbb{Z}_4[x]$ te çarpanlarını bulmak için Graeffe nin metodunu uygulayalım.

Çözüm.

● Eğer $h(x) = x + 1$ ise $e(x) = 1$ ve $o(x) = x$. Buradan

$g(x^2) = -(1 - x^2) = x^2 - 1$ ve böylece $g(x) = x - 1$ dir.

● Eğer $h(x) = x^3 + x + 1$ ise $e(x) = 1\ ve\ o(x) = x^3 + x$. Buradan

$g(x^2) = -(1 - (x^3 + x)^2) = x^6 + 2x^4 + x^2 - 1$

ve böylece $g(x) = x^3 + 2x^2 + 2x - 1$ dir.

● Eğer $h(x) = x^3 + x^2 + 1$ ise $e(x) = x^2 + 1\ ve\ o(x^3)$. Buradan

$g(x^2) = -((x^2 + 1)^2 - (x^3)^2) = x^6 - x^4 - 2x^2 - 1$ ve böylece

$g(x) = x^3 - x^2 - 2x - 1$ dir.

Böylece $x^7 - 1$ in $\mathbb{Z}_4[x]$ teki monik indirgenemez polinomlar halindeki çarpımı;

$x^7 - 1 = (x - 1)(x^3 + 2x^2 + 2x - 1)(x^3 - x^2 + 2x - 1)$ şeklindedir.

Örnek 2.3.8. $x^9 + 1$ in $F_2$ deki indirgenemez monik polinomlar halindeki çarpımı;

$x^9 + 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$

şeklindedir. $x^9 - 1$ in $\mathbb{Z}_4[x]$ te indirgenemez monik polinomlar halindeki çarpanlarını Graeffe metodunu kullanarak bulalım

Çözüm**.**

● Eğer $h(x) = x + 1$ ise $e(x) = 1\ ve\ o(x) = x$ dir. Buradan

$g(x^2) = -(1 - x^2) = x^2 - 1$ ve böylece $g(x) = x - 1$ dir.

● Eğer $h(x) = x^2 + x + 1$ ise $e(x) = x^2 + 1\ ve\ o(x) = x$ dir. Buradan

$g(x^2) = -((x^2+1)^2 - x^2) = -x^4 - x^2 - 1$ ve böylece $g(x) = -x^2 - x - 1$ dir.

● Eğer $h(x) = x^6 + x^3 + 1$ ise $e(x) = x^6 + 1$ $ve$ $o(x) = x^3$ tür. Buradan

$g(x^2) = -((x^6+1)^2 - (x^3)^2) = -x^{12} - x^6 - 1$ ve böylece $g(x) = -x^6 - x^3 - 1$ dir.

Böylece $x^9 - 1$ in $\mathbb{Z}_4[x]$ teki monik indirgenemez polinomlar halindeki çarpımı;

$x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$ şeklindedir.

### 2.4. Polinom Kodlama ve Kod Çözme

Lineer devirli kodlar için çeşitli üreteç matrisleri bulunabilir bunun en basiti satırları üreteç polinomuna karşılık gelen kod kelimeridir ve onun ilk $k-1$ sütunu devirli değişimdir. Yani;

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ . \\ . \\ . \\ x^{k-1}g(x) \end{pmatrix}$$

dir.

Örnek 2.4.1. $C$ lineer devirli kodu $n = 7$ uzunluğunda ve derecesi $n - k = 3$ olan $g(x) = 1 + x + x^3$ üreteç polinomuna sahip olsun. Buradan $k = 4$ olur. Böylece *C* için bir baz ;

$g(x) = 1 + x + x^3$

$xg(x) = x + x^2 + x^4$

$x^2g(x) = x^2 + x^3 + x^5$

$x^3g(x) = x^3 + x^4 + x^6$

ve *C* için bir üreteç matris;

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

şeklinde olur.

$C$ bir $n$ uzunluğunda ve $k$ boyutlu bir lineer devirli kod olsun. $k$ basamak olan $(a_0, a_1, \dots, a_{k-1})$, $a(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ gibi bir polinom olarak kodlama yapmak için düşünülebilir. Bu polinom ise bilgi mesaj polinomu olarak adlandırılır. Kodlama, polinom çarpımından oluşur yani; $a(x)$ polinomu $a(x)g(x) = c(x)$ olarak kodlanır. Polinom çarpımı için ters işlem polinom bölümüdür. Dolayısıyla en yakın kod kelimesi $c(x)$ e karşılık gelen mesajı bulmak için alınan kelime $c(x)\ in\ g(x)$ e bölünmesi ile oluşur. Böylece düzeltme mesaj polinomu $a(x)$ bulunur.

Örnek 2.4.2. $g(x) = 1 + x + x^3\ ve\ n = 7$ olsun. buradan $k = 7 - 3 = 4$ tür. $a(x) = 1 + x^2$ mesaj polinomu olsun karşılık gelen kelime $a = 1010$ olur. $a(x)$ mesajı $c(x) = a(x)g(x)$ olarak kodlanır. Böylece;

$$c(x) = (1 + x^2)(1 + x + x^3) = 1 + x + x^2 + x^5$$

$c = 1110010$ karşılık gelen kod kelimesidir.

Eğer $c(x) = 1 + x + x^4 + x^6$ ise karşılık gelen mesaj polinomu $\frac{c(x)}{g(x)} = a(x) = 1 + x^3$ , karşılık gelen mesaj ise $a = 1001$ dir.

**Tanım 2.4.1.** Syndrome polinomu, $s(x) \equiv w(x) \pmod{g(x)}$ olarak tanımlanır burada $w(x)$ alınan, $g(x)$ üreteç polinomudur.

Eğer $w(x) = c(x) + e(x)$ işlemi ile $c(x)$ gönderilen ve $w(x)$ alınan polinomlar olsun. o zaman biz syndrome polinomunu ve büyük olasılıkla hata polinomu $e(x)$ i hesaplayabiliriz. Toplam $g(x)$ polinomu $n - k$ dereceye sahiptir. O zaman $s(x)$ polinomu $n - k$ dan daha az dereceye sahip olacaktır ve $n - k$ uzunluğunda bir ikili $s$ kelimesine karşılık gelecektir.

$w(x) = c(x) + e(x)$ ve $c(x) = a(x)g(x)$ den biz $s(x) = e(x)\ mod\ g(x)$ olduğunu söyleyebiliriz.

$i.$ sırası $r_i$ , $n-k$ uzunluğundaki kelime ve $r_i(x) \equiv x^i \; mod \; g(x)$ e karşılık gelen satırları olan bir $H$ matrisini tanımlayabiliriz.

Eğer $w$ alınan bir kelime ise o zaman ;

$$w(x) = c(x) + e(x)$$

Böylece;

$$wH = (c+e)H = s(x)$$

dir.

Buradan $s(x) = 0$ ancak ve ancak $w(x)$ bir kod kelimesi ve böylece $H$ bir parite kontrol matrisidir. Aynı zamanda eğer $wH = s$ ise o zaman $s$; $s(x) = w(x) \; mod \; g(x)$ e karşılık gelir.

Örnek 2.4.3. $n = 7$ ve $g(x) = 1 + x + x^3$ olsun. o zaman $n - k = 3$ tür. Biz $H$' ı aşağıdaki gibi üretebiliriz:

$$r_0(x) \equiv 1 \; mod \; g(x) = 1 \; \leftrightarrow 100$$

$$r_1(x) \equiv x \; mod \; g(x) = x \; \leftrightarrow 010$$

$$r_2(x) \equiv x^2 \; mod \; g(x) = x^2 \; \leftrightarrow 001$$

$$r_3(x) \equiv x^3 \; mod \; g(x) = x^3 \; \leftrightarrow 110$$

$$r_4(x) \equiv x^4 \; mod \; g(x) = x^4 \; \leftrightarrow 011$$

$$r_5(x) \equiv x^5 \; mod \; g(x) = x^5 \; \leftrightarrow 111$$

$$r_6(x) \equiv x^6 \; mod \; g(x) = x^6 \; \leftrightarrow 101$$

Böylece;

$$H = \begin{pmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 111 \\ 101 \end{pmatrix}$$

olur. Eğer $w(x) = 1 + x^5 + x^6$ alınırsa $w = 1000011$ olur. o zaman $wH = s = 110$ ve $s(x) = 1 + x = 1 + x^5 + x^6 mod(1 + x + x^3)$ elde edilir.

# 3. BÖLÜM

# SONLU ZİNCİR HALKALARI ÜZERİNDE KONSTA-DEVİRLİ KODLAR

Bu bölümde geçen kavramlar ve sonuçlar [8-13] kaynaklarından alınmıştır.

Sonlu halkalar üzerinde kodlama ile ilgili çok fazla araştırma ve inceleme yapılmıştır. Özellikle $Z_4$ halkası ve bunun yanında $F_2 + uF_2$ halkası üzerinde birkaç araştırma yapılmıştır. Wolfmann [13] $Z_4$ üzerinde $n$ uzunluğunda ve $n$ tek olmak üzere lineer devirli kodların Gray görüntüsünün bir ikili devirli koda denk olduğunu göstermiştir.

Bu bölümde $R_2 = F_2 + uF_2$ ve $R_3 = F_2 + uF_2 + u^2F_2$ üzerindeki konsta-devirli kodlar ile ilgili bazı tanım teoremler incelenecektir.

Ayrıca konsta-devirli kodlar hakkında bazı tanım ve önermeler, konsta-devirli kodların Gray dönüşümler altındaki kodları ile ikili kuasi-devirli kodlar incelenecektir.

## 3.1 Konsta-Devirli Kodlar ve Kuasi -Devirli Kodlar

Bu bölümde $\beta$-konsta-devirli kodlar ve $t$-kuasi devirli kodlar hakkında bazı tanım ve notlar incelenecektir.

**Tanım 3.1.1.** Her $(a_0, a_1, \dots, a_{n-1})$ kod kelimesi, $\beta \in F_q^* \setminus \{0\}$ olacak şekilde konsta-devirli değişim vektörleri tarafından $(\beta a_{n-1}, a_0, a_1, \dots, a_{n-2})$ şeklinde elde edilen ifade de bir kod kelimesi ise o zaman bu koda $\beta$-konsta -devirli kod denir.

Bunlar $F_q[x]/(x^n - \beta)$ halkasında ideallerdir.

**Not 3.1.1**. $\beta = 1$ olduğu zaman bu koda devirli kod adı verilir.

**Not 3.1.2.** $\beta = -1$ olduğu zaman bu koda negatif devirli kod adı verilir.

**Tanım 3.1.2.** $C$ bir kod ve her $(a_0, a_1, \dots, a_{n-1})$ kod kelimesi için $t$ tamsayı olmak üzere $(a_{n-t}, \dots, a_{n-1}, a_0, a_1, \dots, a_{n-t-1})$ de aynı zamanda bir kod kelimesi ise o zaman bu koda $t$-kuasi devirli kod denir.

$\sigma$ ve $\nu$ $F_2^{2n}$ $ve$ $\mathbb{Z}_{2^{k+1}}^n$ üzerinde alışılmış değişim olsun;

$$\psi_t\left(a^{(1)}\middle|a^{(2)}\middle|\dots\middle|a^{(t)}\right) = \sigma\left(a^{(1)}\right)|\sigma\left(a^{(2)}\right)|\dots|\,\sigma\left(a^{(t)}\right),$$

$$\delta_t\left(\tilde{a}^{(1)}\middle|\tilde{a}^{(2)}\middle|\dots|\tilde{a}^{(t)}\right) = \nu\left(\tilde{a}^{(1)}\right)|\nu\left(\tilde{a}^{(2)}\right)|\dots|\nu\left(\tilde{a}^{(t)}\right)\Big),$$

verilenler ile herhangi bir pozitif $t$ sayısı için, $\psi_t, (F_2^{2n})^t$ üzerinde bir kuasi-değişim ve $\delta_t$ , $(\mathbb{Z}_4^n)$ üzerinde bir kuasi-negatif değişim olsun. Burada $a^{(i)} \in F_2^{2n}, \tilde{a}^{(i)} \in \mathbb{Z}_4^n,\ i = 1, 2, \dots, t$ için ve "|" ise alışılmış vektör birleştirmesini tanımlar.

**Not 3.1.3.** $t = 1$ ise o zaman bu kod devirli kod olarak adlandırılır.

## 3.2. $F_2 + uF_2$ Üzerinde $(1 + u)$ −Konsta-Devirli Kodlar

$R_3^n$ nin alt kümesi $C\ nin\ (1 + u)$ −konsta -devirli $n$ uzunluğunda bir kod olması için gerek ve yeter şartın onun polinom gösteriminin $R_2[x]/(x^n - (1 + u))$ nun bir ideali olması gerektiğini ve yine bu bölümde $F_2 + uF_2$ üzerinde $n$ uzunluğunda $(1 + u)$ −konsta lineer devirli kodun Gray görüntüsünün bir ikili uzaklıklı değişmez lineer devirli kod olduğu ve aynı zamanda eğer *n* tek ise $F_2 + uF_2$ üzerinde *n* uzunluğunda bir lineer devirli kodun Gray görüntüsü olan her ikili kodun bir lineer devirli koda denk olduğu ispatlanacaktır.

$R_2 = F_2 + uF_2 = F_2[u]/(u^2)$ değişmeli halkası aşikar toplam ve çarpım işlemlerini $u^2 = 0$ özelliği ile sağlamaktadır. Burada $R_2$ nin elemanları *0,1,u,1+u* olup *1* ve *1+u* $R_2$ de birim elemanlardır. Bu yüzden $R_2$; *(0), (1), (u)* ideallerine sahiptir.

**Tanım 3.2.1.** $R_2 = F_2 + uF_2$ olsun. Eğer $n$ uzunluğunda $R_2$ üzerinde bir kod

$$\nu(a_0, a_1, \dots, a_{n-1}) = ((1 + u)a_{n-1}, a_0, \dots, a_{n-2}),$$

ν otomorfizmi ile değişmez ise o zaman bu kod $(1 + u)$ −konsta-devirli kod olarak tanımlanır.

**Önerme 3.2.1.** $R^n$ nin bir alt kümesi $C, (1+u)$-konsta $n$ uzunluğunda devirli koddur ancak ve ancak onun polinom gösterimi $R_2[x]/(x^n-(1+u))$ nun bir idealidir.[10]

İspat. Kabul edelim ki $\pi(C), R_2[x]/(x^n-(1+u))$ in ideali olsun. O zaman herhangi $\alpha, \beta \in R_2^n \subset R_2[x]/(x^n-(1+u))$ ve $a, b \in C$ için tanım 2.1.3, 2. maddeden $\alpha\pi(a), \beta\pi(b) \in \pi(C)$ bulunur. Böylece Tanım 2.1.3, 1. maddeden $\alpha\pi(a) + \beta\pi(b) \in \pi(C)$ yani;

$\alpha\pi(a) + \beta\pi(b) = \pi(\alpha a + \beta b) \in \pi(C)$ dolayısıyla $\alpha(a) + \beta(b), C$ nin bir kod kelimesidir. Bu da gösterirki *C* lineer koddur.

Şimdi $c = (c_0, c_1, \dots, c_{n-1}), C$ nin bir kod kelimesi olsun o zaman *C*'nin polinom gösterimi;

$\pi(c) = (c_0 + c_1x + \cdots + c_{n-1}x^{n-1}), \pi(C)$ nin bir elemanıdır.$\pi(C), R_2[x]/(x^n-(1+u)$ nun ideali olduğundan;

$x\pi(c) = c_0x + c_1x^2 + \cdots + c_{n-1}x^n \in \pi(C)$ dir.

Fakat $\pi(C), R_2[x]/(x^n-(1+u))$ nin bir ideali olduğu için ve

$x^n-(1+u) = 0 \Longrightarrow x^n = (1+u)$ olduğundan dolayı

$$x\pi(c) = c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}\big((1+u)\big)$$

$$= (1+u)c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}$$

$\pi(C)$ nin elemanıdır yani; $\big((1+u)c_{n-1}, c_0, c_1, \dots, c_{n-2}\big), C$ nin bir kod kelimesidir. Bu da $C$ nin $(1+u)$ −konsta- devirli kod olduğu anlamına gelir.

Tersine; Kabul edelim ki $C$, $R$ üzerinde $(1+u)-$konsta-devirli kod olsun. Tanım 2.1.3, madde 1 $\pi(C)$ için doğrulanır. $(f_0, f_1, \dots, f_{n-2}, f_{n-1}) \in C$ ile $\pi(C)$ nin herhangi $f(x)$ polinomu için;

$$f(x) = f_0 + f_1x + \cdots + f_{n-2}x^{n-2} + f_{n-1}x^{n-1}$$

$$= \pi(f_0, f_1, \dots, f_{n-2}, f_{n-1})$$

ve böylece

$$xf(x) = x^n f_{n-1} + f_0 x + f_1 x^2 + \cdots + f_{n-2} x^{n-1}$$

$$= (1+u) f_{n-1} + f_0 x + f_1 x^2 + \cdots + x^{n-1} f_{n-2}$$

polinomu da aynı zamanda $C, (1+u)-$konsta-devirli kod olduğundan $\pi(C)$ nin elemanıdır. Böylece $x^2 f(x) = x\big(xf(x)\big)$, $\pi(C)$ nin bir elemanıdır. Tümevarımdan kabul edilir ki $\forall j \geq 0$ için $x^j f(x)$, $\pi(C)$ ye aittir. *C* bir lineer kod ve π bir lineer dönüşüm olduğundan $\pi(C)$, $R_2$ üzerinde bir modüldür. Dolayısıyla herhangi

$$g(x) = g_0 + g_1 x + \cdots + g_{n-1} x^{n-1} \in R_2[x]/(x^n - (1+u))$$

polinomu için;

$$g(x) f(x) = \sum_{i=0}^{n-1} g_i (x^i f(x))$$

polinomu da $\pi(C)$ nin elemanıdır. Böyce ideal tanımından $\pi(C)$, $R_2[x]/(x^n - (1+u)$ nin bir ideali olduğu kolaylıkla görülür.

**Tanım 3.2.2.** $R_2 = F_2 + uF_2$ bir değişmeli halka olsun. Herhangi bir $z \in R_2$, $z = r + uq$ olarak ifade edilebilir burada $r, q \in F_2$.

$\phi(z) = (q, q+r)$ tarafından $\phi$: $R_2 \to F_2$ gray dönüşümü tanımlanır.

Bu dönüşüm doğal bir yolla $R_2^n$ e genişletilebilir. $z = (z_1, z_2, \ldots, z_n) \in R_2^n$ için $\phi$, $R_2^n$'e aşağıdaki gibi genişletilebilir:

$\phi$: $R_2^n \to F_2^{2n}$

$(z_1, z_2, \ldots, z_n) \to (q_1, q_2, \ldots, q_n, q_1 \oplus r_1, \ldots, q_n \oplus r_n)$

Burada $1 \leq i \leq n$ için $z_i = r_i + uq_i$, ve $\oplus$ ikili toplamı ifade eder.

Örnek 3.2.1. $\phi(1) = 01 \quad q = 0,\ r = 1$

$\phi(u) = 11 \quad q = 1, \quad r = 0$

$\phi(0) = 00 \quad q = 0, \quad r = 0$

$\phi(1+u) = 10 \quad q = 1, \quad r = 1$

**Not 3.2.2.** $(1+u)^n = 1+u$ , $n$ tek ise

$(1+u)^n = 1,\ n$ çift ise

### 3.2.1 Tek Uzunluklu $(1+u)$ −Konsta-Devirli Kodlar

Bu bölümde tek uzunluklu $(1+u)-$konsta-devirli kodlar ile ilgili bazı önermeler incelenecektir.

**Önerme 3.2.3.** $\mu$; $\mu\big(f(x)\big) = f((1+u)x)$ olacak şekilde

$R_2[x]/(x^n-1) \to R_2[x]/(x^n-(1+u))$ ye bir dönüşüm olsun. Eğer $n$ tek ise o zaman $\mu$ bir halka izomorfizmasıdır. [10]

İspat**.** İlk olarak $\mu$ nin bir halka homomorfizması olduğunu gösterelim.

$f(x), g(x) \in R_2[x]/\ x^n-1$ polinomları için

$$\mu\big(f(x)+g(x)\big) = \mu\big((f+g)(x)\big)$$

$$= (f+g)\big((1+u)x\big)$$

$$= f\big((1+u)x\big) + g\big((1+u)x\big)$$

$$= \mu\big(f(x)\big) + \mu\big(g(x)\big)$$

ve

$$\mu\big(f(x)g(x)\big) = \mu\big((fg)(x)\big)$$

$$= (fg)\big((1+u)x\big)$$

$$= f\big((1+u)x\big)g\big((1+u)x\big)$$

$$= \mu\big(f(x)\big)\mu\big(g(x)\big)$$

ifadeleri elde edilir. Böylece $\mu$ bir halka homomorfizmasıdır.

Şimdi $\mu$ nin bire bir olduğunu gösterelim. $f(x), g(x) \in R_2[x]$ polinomları için

$f(x) \equiv g(x) \mod(x^n - 1) \Leftrightarrow f(x) - g(x) = h(x)(x^n - 1)$

olacak şekilde $h(x) \in R_2[x]$ vardır. $\Leftrightarrow n$ tek ve $f\big((1+u)x\big) - g\big((1+u)x\big) =$

$h((1+u)x)((1+u)x)^n - 1) \quad \Leftrightarrow (1+u)f\big((1+u)x\big) - (1+u)g\big((1+u)x\big) = (1+u)h((1+u)x)((1+u)^n x^n - 1)$

$= h((1+u)x)(x^n - (1+u)) \quad \Leftrightarrow (1+u)(\mu\big(f(x)\big) - \mu\big(g(x)\big))$

$= h((1+u)x)(x^n - (1+u)) \quad \Leftrightarrow \Big(\mu\big(f(x)\big) - \mu\big(g(x)\big)\Big)$

$= (1+u)h\big((1+u)x\big)\big(x^n - (1+u)\big) \Leftrightarrow \mu(f(x)) \equiv \mu(g(x))(mod\big(x^n - (1+u)\big))$

Bu $f, g \in R_2[x]\,/(x^n - 1)$ için $\mu(f(x)) \equiv \mu(g(x))(mod\ (x^n - (1+u)))$ ancak ve ancak $f(x) \equiv g(x)(mod\ (x^n - 1))$ anlamına gelir. Bu da $\mu$ nin birebir bir homomorfizma olması anlamına gelir.

$\mu$ nin örten olduğunu göstermek için; $f(x) \in R_2[x]/\ (x^n - (1+u))$ olsun o zaman

$f\big((1+u)x\big) \in R_2[x]/\ (x^n - 1)$ vardır öyle ki $\mu\Big(f\big((1+u)x\big)\Big) = f((1+u)^2 x) = f(x)$ dir.

Böylece; $\mu$ örtendir. Buradan $\mu$ bir halka izomorfizmasıdır.

Örnek 3.2.2**.** $n = 7$ olsun.

$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \in R_2[x]$

$\mu$ halka izomorfizmasından;

$(1+u)^7 x^7 + 1$

$= ((1+u)x + 1)((1+u)^3 x^3 + (1+u)x + 1)((1+u)^3 x^3 + (1+u)^2 x^2 + 1)$

elde edilir. Not 3.2.2 den ;

$(1+u)x^7 + 1 = \big((1+u)x + 1\big)\big((1+u)x^3 + (1+u)x + 1\big)\big((1+u)x^3 + x^2 + 1\big)$

dir. Bu ifade düzenlenerek

$(1+u)\left(x^7+(1+u)\right)$

$=(1+u)(x+(1+u))(1+u)(x^3+x+(1+u))(1+u)$

ve

$(1+u)\left(x^7+(1+u)\right)$

$=(1+u)^3(x+(1+u))(x^3+x+(1+u))(x^3+(1+u)x^2+(1+u))$

$(1+u)\left(x^7+(1+u)\right)$

$=(1+u)\left(x+(1+u)\right)\left(x^3+x+(1+u)\right)\left(x^3+(1+u)x^2+(1+u)\right)$

dir. Bu denklem $(1+u)$ ile bölünerek;

$x^7+(1+u)=(x+(1+u))(x^3+x+(1+u))(x^3+(1+u)x^2+(1+u))$

elde edilir.

Örnek 3.2.3. $n=9$ olsun.

$x^9+1=(x+1)(x^2+x+1)(x^6+x^3+1)\in R_2[x]$

$\mu$ halka izomorfizmasından;

$(1+u)^9x^9+1$

$=((1+u)x+1)((1+u)^2x^2+(1+u)x+1)((1+u)^6x^6+(1+u)^3x^3+1)$

Not 3.2.2 den ;

$(1+u)x^9+1$

$=\left((1+u)x+1\right)(x^2+(1+u)x+1)(x^6+(1+u)x^3+1)(1+u)\left(x^9+(1+u)\right)$

$=(1+u)(x+(1+u))(x^2+(1+u)x+1)(x^6+(1+u)x^3+1)$

$(1+u)$ ile bölünerek;

$\left(x^9+(1+u)\right)=(x+(1+u))(x^2+(1+u)x+1)(x^6+(1+u)x^3+1)$

elde edilir.

**Sonuç 3.2.4.** $I, R_2[x]\ /(x^n-1)$ nin bir ideali olması için gerek ve yeter şart $\mu(I)$,

$R_2[x]\ /\ (x^n-(1+u))$ nin bir ideali olmasıdır.[10]

İspat**.** Kabul edelim ki $I, R_2[x]\ /(x^n-1)$ nin bir ideali ve

$f\big((1+u)x\big), g((1+u)x) \in \mu(I)$ olsun. $I$ ideal olduğundan

$\forall f(x), g(x) \in I\ için\ f(x)+g(x) \in I$ dır. Böylece $\mu$ nin tanımından $\mu(f(x)+g(x)) \in \mu(I)$ dır. Fakat $\mu\big(f(x)+g(x)\big)=\mu\big((f+g)\big)(x)=(f+g)(1+u)(x)=f\big((1+u)x\big)+g\big((1+u)x\big) \in \mu(I),$ bu da;

$$f\big((1+u)x\big)+g((1+u)x) \in \mu(I) \tag{3.2.1}$$

şimdi $f\big((1+u)x\big), I((1+u)x) \in \mu(I)$ olsun. $\forall f(x) \in I\ için\ f(x)l(x) \in I\ ve\ l(x) \in R_2[x]$ olduğundan $\mu$ nun tanımından;

$\mu(f(x)l(x)) \in \mu(I)$ olur. Fakat $\mu\big(f(x)l(x)\big)=\mu\big((f.l)(x)\big)=(f.l)\big((1+u)x\big)=f\big((1+u)x\big).l((1+u)x) \in \mu(I)$ dır. Böylece;

$$f\big((1+u)x\big).l((1+u)x) \in \mu(I) \tag{3.2.2}$$

denklem 3.2.1 ve 3.2.2 den $\mu(I),\ R_2[x]\ /\ (x^n-(1+u))$ nin bir idealidir.

Tersine; kabul edelim ki $\mu(I),\ R_2[x]\ /\ (x^n-(1+u))$ nin bir ideali ve $f(x), g(x) \in I$ olsun. şimdi $f\big((1+u)x\big)+g\big((1+u)x\big) \in \mu(I),\ \forall f\big((1+u)x\big), g\big((1+u)x\big) \in \mu(I)\ için,$ çünkü $\mu(I), R_2[x]\ /(x^n-(1+u))$ nun idealidir. Böylece $\mu$ nın tanımından;

$$f\big((1+u)x\big)+g\big((1+u)x\big)=(f+g)\big((1+u)x\big)=\mu((f+g)x) \in \mu(I)$$

elde edilir.

$\mu$ bir halka izomorfizması olduğundan o zaman $\mu^{-1}\mu((f+g)x) \in \mu^{-1}\mu(I)$ dır. Böylece; $(f+g)(x) \in I$, yani;

$$f(x)+g(x) \in I \tag{3.2.3}$$

$f(x) \in I\ ve\ \imath(x) \in R[x]$ olsun. Şimdi $\forall f\big((1+u)x\big), l\big((1+u)x\big) \in \mu(I)\ ve\ \mu(I)$ bir ideal olsun o zaman $f\big((1+u)x\big).l((1+u)x) \in \mu(I)$ dır. Böylece $\mu$ nin tanımından;

$f\big((1+u)x\big).l\big((1+u)x\big) = (f.l)\big((1+u)x\big) = \mu((f.l)x) \in \mu(I).$

$\mu$ bir halka izomorfizması olduğundan;

$\mu^{-1}\mu((f.l)x) \in \mu^{-1}\mu(I)$ dir. Bu yüzden $(f.l)(x) \in I$ yani;

$f(x).l(x) \in I$ (3.2.4)

3.2.3 ve 3.2.4 ten $I, R_2[x]/(x^n-1)$ nin idealidir.

□

**Sonuç 3.2.5.** $\tilde{\mu}, n$ tek olacak şekilde $R_2^n$ nin bir permütasyonu olsun öyle ki;

$\tilde{\mu}(a_0, a_1, \dots, a_{n-1}) = (a_0, (1+u)a_1, (1+u)^2 a_2, \dots, (1+u)^i a_i, \dots, (1+u)^{n-1} a_{n-1})$

ve $D, R_2^n$ nin bir alt kümesi olsun o zaman $D$ bir lineer devirli koddur ancak ve ancak $\tilde{\mu}(D)$ bir $(1+u)$ −lineer konsta-devirli koddur. [10]

İspat. $R_2 = F_2 + uF_2$ olsun. $\tilde{\mu} = P^{-1}\mu P$ olduğu gösterilirse ispat açık olacaktır Eğer $D, R_2[x]$ üzerinde bir devirli kod ise o zaman $D(x)$, $R_2[x]/(x^n-(1+u))$ nin bir idealidir. Eğer $a = (a_0, a_1, \dots, a_{n-1}) \in D$ ise o zaman $a(x), xa(x), \dots, x^{n-1}a(x) \in D(x)$ dir.

Önerme 3.2.1 den

D ye karşılık gelenlerin polinom temsilcileri;

$a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$

$xa(x) = xa_0 + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n$

$xa(x) = a_{n-1}x^n + xa_0 + a_1 x^2 + \cdots + a_{n-2}x^{n-1}$

dır. Bu da;

$\mu\big(a(x)\big) = a_0 + (1+u)a_1 x + (1+u)^2 a_2 x^2 + \cdots + a_{n-1}(1+u)^{n-1}x^{n-1}$

$\mu\big(xa(x)\big) = a_{n-1}((1+u)x)^n + a_0\big((1+u)x\big) + a_1((1+u)x)^2 + \cdots + a_{n-2}(1+u)^{n-1}x^{n-2}$

$\mu\big(xa(x)\big) = a_{n-1}(1+u)^n x^n + a_0\big((1+u)x\big) + a_1x^2 + \cdots + a_{n-2}x^{n-1}$

anlamına gelmektedir.

$P: R_2^n \to R_2[x]$ bir dönüşüm olsun öyle ki $P(a_0, a_1, \dots, a_{n-1}) = \sum_{i=0}^{n-1} a_i x^i$ o zaman $\mu\big(a(x)\big)\ ve\ \mu(xa(x))$ nin vektör temsilcileri ;

$P^{-1}\mu\big(a(x)\big) = (a_0, (1+u)a_1, a_2, \dots, a_{n-1})$ ve

$P^{-1}\mu\big(xa(x)\big) = ((1+u)a_{n-1}, a_0, (1+u)a_1\,, a_2, \dots, a_{n-2})$

Bu da $\tilde{\mu} = P^{-1}\mu P$ olduğu anlamına gelir. Böylece;

$(a_0, (1+u)a_1, a_2, \dots, a_{n-1}) \in \tilde{\mu}(D)\ ve$

$((1+u)a_{n-1}, (1+u)a_0, a_1, (1+u)a_2, \dots, a_{n-2}) \in \tilde{\mu}(D)$

böylece;

$\tilde{\mu}(D), F_2 + uF_2$ üzerinde $(1+u)$ −konsta-devirli koddur.

### 3.2.2 Gray Dönüşüm ve *(1+u)*-Konsta-Devirli Kod

$(1+u)$ −konsta-devirli kodun Gray dönüşümü, Gray dönüşümün bir değişimidir**.**

**Uyarı 3.2.1.** Tanım 3.2.2 aşağıdaki gibi ifade edilebilir.

1. $r((1+u)z) = r(z)$
2. $q\big((1+u)z\big) = r(z) \oplus q(z)$

**Önerme 3.2.6.** Eğer $\nu, R_2^n$ de $(1+u)$ −konsta-devirli kod , $\sigma, F_2^{2n}$ de bir değişim ve $\phi, R_2^n\ den\ F_2^{2n}$ üzerine bir Gray dönüşüm olsun o zaman;

$\phi\nu = \sigma\phi$ dir.[10]

İspat.: $a = (a_0, a_1, \dots, a_i, \dots, a_{n-1}) \in R_2^n$ ve $r_i, q_i \in F_2$ öyle ki $a_i = uq_i + r_i$ burada

$q_i = q(a_i)\ ve\ r_i = r(a_i)$ dir. Tanım 3.2.2 den biz;

$$\phi(a) = (q_0, q_1, \dots, q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, \dots, q_{n-1} \oplus r_{n-1})$$

elde ederiz. Böylece;

$$\sigma\big(\phi(a)\big) = (q_{n-1} \oplus r_{n-1}, q_0, q_1, \dots, q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, \dots, q_{n-2} \oplus r_{n-2}) \quad (3.2.5)$$

diğer taraftan,

$$\nu(a) = ((1+u)a_{n-1}, a_0, \dots, a_i, \dots, a_{n-2})$$

olduğundan ;

$$\phi\big(\nu(a)\big)\big(q\big((1+u)a_{n-1}\big), q_0, q_1, \dots, q_{n-2}, r\big((1+u)a_{n-1}\big) \oplus q\big((1+u)a_{n-1}\big), q_0 \oplus r_0, \dots, q_{n-2} \oplus r_{n-2}\big) \quad (3.2.6)$$

Uyarı 3.2.1 den;

$$q\big((1+u)a_{n-1}\big) = q(a_{n-1}) \oplus r(a_{n-1}) = q_{n-1} \oplus r_{n-1} \quad (3.2.7)$$

ve

$$r\big((1+u)a_{n-1}\big) \oplus q\big((1+u)a_{n-1}\big) = q(a_{n-1}) = q_{n-1} \quad (3.2.8)$$

eşitlikleri elde edilir. Aynı zamanda (3.2.6), (3.2.7) ve (3.2.8) den

$$\phi\big(\nu(a)\big) = (q_{n-1} \oplus r_{n-1}, q_0, q_1, \dots, q_{n-2}, q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, q_{n-2} \oplus r_{n-2} \quad (3.2.9)$$

şimdi, (3.2.5) ve (3.2.9) dan

$$\phi\nu = \sigma\phi$$

elde edilir.

**Teorem 3.2.7.** $R_2$ üzerinde bir $(1+u)$ −konsta-devirli lineer kodun Gray resmi bir ikili uzaklıklı değişmez lineer devirli koddur. [10]

İspat**.** $C, R_2$ üzerinde bir lineer $(1+u)$ −konsta-devirli kod olsun. o zaman $\nu(c) = c$ ve bu yüzden $\phi\big(\nu(c)\big) = \phi(c)$. Önerme 3.2.6 dan $\sigma\big(\phi(c)\big) = \phi(c)$ dir bu da $\phi(c)$ nin bir lineer devirli kod olduğu anlamına gelir.

Örnek 3.2.4**.** Örnek 3.2.2 den;

$x^7 + (1+u) = (x + (1+u))(x^3 + x + (1+u))(x^3 + (1+u)x^2 + (1+u))$

$C = \big(x + (1+u)\big)\big(x^3 + x + (1+u)\big) = 1 + x^2 + (1+u)x^3 + x^4$, yani;

*C* kodu 7 uzunluğunda ve temel kod kelimelerinin sayısı 14 tür.

| $i$ | $c_i$ | $\phi(c_i)$ |
|---|---|---|
| 1 | $(1,0,1,(1+u),1,0,0)$ | $(0,0,0,1,0,0,0,1,0,1,0,1,0,0)$ |
| 2 | $(0,1,0,1,(1+u),1,0)$ | $(0,0,0,0,1,0,0,0,1,0,1,0,1,0)$ |
| 3 | $(0,0,1,0,1,(1+u),1)$ | $(0,0,0,0,0,1,0,0,0,1,0,1,0,1)$ |
| 4 | $((1+u),0,0,1,0,1,(1+u))$ | $(1,0,0,0,0,0,1,0,0,0,1,0,1,0)$ |
| 5 | $(1,(1+u),0,0,1,0,1$ | $(0,1,0,0,0,0,0,1,0,0,0,1,0,1)$ |
| 6 | $((1+u),1,(1+u),0,0,1,0)$ | $(1,0,1,0,0,0,0,0,1,0,0,0,1,0)$ |
| 7 | $(0,(1+u),1,(1+u),0,0,1)$ | $(0,1,0,1,0,0,0,0,0,1,0,0,0,1)$ |
| 8 | $((1+u),0,(1+u),1,(1+u),0,0)$ | $(1,0,1,0,1,0,0,0,0,0,1,0,0,0)$ |
| 9 | $(0,(1+u),0,(1+u),1,(1+u),0)$ | $(0,1,0,1,0,1,0,0,0,0,0,1,0,0)$ |
| 10 | $(0,0,(1+u),0,(1+u),1,(1+u))$ | $(0,0,1,0,1,0,1,0,0,0,0,0,1,0)$ |
| 11 | $(1,0,0,(1+u),0,(1+u),1)$ | $(0,0,0,1,0,1,0,1,0,0,0,0,0,1)$ |
| 12 | $((1+u),1,0,0,(1+u),0,(1+u))$ | $(1,0,0,0,1,0,1,0,1,0,0,0,0,0)$ |
| 13 | $(1,(1+u),1,0,0,(1+u),0)$ | $(0,1,0,0,0,1,0,1,0,1,0,0,0,0)$ |
| 14 | $(0,1,(1+u),1,0,0,(1+u))$ | $(0,0,1,0,0,0,1,0,1,0,1,0,0,0)$ |

Yukarıdaki tablodan $\phi(C) = \{\phi(c_i),\ i = 1\ den\ 14\ e\}$, [14,4,4] ikili devirli koddur.

## 3.3 $F_2 + uF_2 + u^2F_2$ Üzerindeki $(1-u^2)$ −Konsta-Devirli Kodlar

$R_3 = F_2 + uF_2 + u^2F_2$, $\{0,1,u,u^2,v,v^2,uv,v^3\}$ , 8 elemanı ile bir değişmeli bir zincir olsun. Burada $u^3 = 0, v = 1+u,\ v^2 = 1+u^2,\ v^3 = 1+u+u^2,\ uv = u+u^2$ dir.

**Tanım 3.3.1.** *n* uzunluğunda bir kod eğer ν otomorfizmi ile değişmez ise o zaman bu koda $(1+u^2)$ −konsta- devirli kod denir. Burada ;

$v(a_0, a_1, \dots, a_{n-1}) = ((1-u^2)a_{n-1}, a_0, \dots, a_{n-2})$

dir.

**Önerme 3.3.1**. $C, R_3^n$ bir alt kümesi ve $n$ uzunluğunda lineer $(1-u^2)$ −konsta-devirli koddur ancak ve ancak onun polinom gösterimi $R_3[x]/(x^n-(1-u^2))$ nin bir idealidir. [11]

İspat. Önerme 3.2.1 in ispatına benzer olarak yapılabilir.

### 3.3.1 Tek uzunluklu $(1-u^2)$ −konsta-devirli kodlar

Bu bölümde $(1-u^2)-$ konsta-devirli kodlar üzerindeki bazı önermeler ve tek uzunluklu $(1-u^2)$ −konsta-devirli kodların özellikleri incelenecektir.

**Uyarı 3.3.1.** ● $(1-u^2)^n = 1-u^2$, eğer $n$ tek ise;

● $(1-u^2)^n = 1$, eğer $n$ çift ise;

**Önerme3.3.2.** $\mu$: $R_3[x]/(x^n-1) \to R_3[x]/(x^n-(1-u^2))$,

$\mu\big(f(x)\big) = f((1-u^2)x)$ şeklinde tanımlanan bir dönüşüm olsun. Eğer $n$ tek ise o zaman $\mu$ bir halka izomorfizmasıdır. [11]

İspat. ilk olarak $\mu$ nin bir halka homomorfizması olduğunu gösterelim;

$f(x), g(x) \in R_3[x]/(x^n-1)$ polinomları için;

$\mu\big(f(x)+g(x)\big) = \mu\big((f+g)(x)\big) = (f+g)((1-u^2)x)) =$

$f((1-u^2)x)) + g((1-u^2)x)) = \mu(f(x)) + \mu(g(x))$.

ve $\mu\big(f(x)g(x)\big) = \mu\big((fg)(x)\big) = (fg)\big((1-u^2)x\big) =$

$f\big((1-u^2)x\big)g\big((1-u^2)x\big) = \mu(f(x))\mu(g(x))$

dir. Bu yüzden $\mu$ bir halka homomorfizmasıdır.

Şimdi $\mu$ nin bire bir olduğunu gösterelim. $f(x), g(x) \in R_3[x]$ için $f(x) \equiv g(x) mod(x^n-1)$ dir ancak ve ancak $h(x) \in R_3[x]$ vardır öyleki $f(x)-g(x) =$

$h(x)(x^n-1)$ ancak ve ancak $n$ tek ve $f\big((1-u^2)x\big)-g\big((1-u^2)x\big)=h((1-u^2)x)((1-u^2)x^n-1)$ ancak ve ancak

$(1-u^2)f\big((1-u^2)x\big)-(1-u^2)g\big((1-u^2)x\big)$

$=\ (1-u^2)h((1-u^2)x)((1-u^2)^n x^n-1) \Leftrightarrow (1-u^2)\left(\mu\big(f(x)\big)-\mu\big(g(x)\big)\right)$

$=h\big((1-u^2)x\big)\big(x^n-(1-u^2)\big) \qquad \Leftrightarrow \left(\mu\big(f(x)\big)-\mu\big(g(x)\big)\right)$

$=(1-u^2)h((1-u^2)x)(x^n-(1-u^2)) \quad \Leftrightarrow\ \mu(f(x))\equiv\mu(g(x))(mod\big(x^n-(1-u^2)\big))$

elde edilir.

Bu da $f,g\in R_3[x]\,/(x^n-1)$ için $\mu(f(x))\equiv\mu(g(x))(mod\,\big(x^n-(1-u^2)\big))$ ancak ve ancak $f(x)\equiv g(x)(mod(x^n-1))$ anlamına gelir. Bu da $\mu$ nin birebir bir homomorfizma olduğu anlamına gelir. Şimdi $\mu$ nin örten olduğunu gösterelim.

$f(x)\in R_3[x]\,/(x^n-(1-u^2))$ olsun o zaman $f\big((1-u^2)x\big)\in R_3[x]/(x^n-1)$ vardır öyleki $\mu\left(f\big((1-u^2)x\big)\right)=f((1-u^2)^2x)=f(x)$dir. Böylece $\mu$ örten olup bir halka izomorfizmasıdır.

Örnek 3.3.1. $n=7$ olsun.

$x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1)\in R_3[x]$

halka izomorfizmasından

$(1-u^2)^7x^7+1$

$=((1-u^2)x+1)((1-u^2)^3x^3+(1-u^2)x+1)((1-u^2)^3x^3+(1-u^2)^2x^2+1)$

Uyarı 3.3.1 den;

$(1-u^2)^7x^7+1$

$=((1-u^2)x+1)((1-u^2)^3x^3+(1-u^2)x+1)((1-u^2)x^3+x^2+1)$

$(1-u^2)\big(x^7+(1-u^2)\big)$

$= (1-u^2)\big(x+(1-u^2)\big)(1-u^2)\big(x^3+x+(1-u^2)\big)(1-u^2)$

$\big(x^3+(1-u^2)x^2+(1-u^2)\big)(1-u^2)\big(x^7+(1-u^2)\big)$

$= (1-u^2)^3(x+(1-u^2))(x^3+x+(1-u^2))(x^3+(1-u^2)x^2+(1-u^2))$

$(1-u^2)(x^7+(1-u^2))$

$= (1-u^2)(x+(1-u^2))(x^3+x+(1-u^2))(x^3+(1-u^2)x^2+(1-u^2))$

$(1-u^2)$ tarafından bölünerek;

$$x^7+(1-u^2) = (x+(1-u^2))(x^3+x+(1-u^2))(x^3+(1-u^2)x^2+(1-u^2))$$

elde edilir.

**Sonuç 3.3.3.** $\tilde{\mu}, R_3^n$ ün permütasyonu ve $n$ tek olsun öyle ki;

$\tilde{\mu}(a_0, a_1, \dots, a_{n-1})$,

$= (a_0, (1-u^2)a_1, (1-u^2)^2 a_2, \dots, (1-u^2)^i a_i, \dots, (1-u^2)^{n-1} a_{n-1})$

ve $D, R_3^n$ in bir alt kümesi olsun o zaman $D$ bir lineer devirli koddur ancak ve ancak $\tilde{\mu}(D)$ bir lineer $(1-u^2)$ −konsta-devirli koddur. [11]

İspat**.** $R_3 = F_2 + uF_2 + u^2F_2$ olsun. Eğer $\tilde{\mu} = P^{-1}\mu P$ ise ispat açık olacaktır.

Eğer $D, R_3[x]$ üzerinde bir devirli kod ise o zaman $D(x)$, $R_3[x]/(x^n-(1-u^2))$ in bir idealidir. Eğer $a = (a_0, a_1, \dots, a_{n-1}) \in D$ ise o zaman $a(x), xa(x), \dots, x^{n-1}a(x) \in D(x)$ dir.

$D$ ye karşılık gelen ifadelerin polinom gösterimi;

$a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$

$xa(x) = xa_0 + a_1x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n$

$xa(x) = a_{n-1}x^n + xa_0 + a_1x^2 + \cdots + a_{n-2}x^{n-1}$

dir. Bu ifadeler de;

$\mu\big(a(x)\big) = a_0 + (1-u^2)a_1x + (1-u^2)^2a_2x^2 + \cdots + a_{n-1}(1-u^2)^{n-1}x^{n-1}$

$$\mu\big(a(x)\big) = a_{n-1}((1-u^2)x)^n + a_0\big((1-u^2)x\big) + a_1((1-u^2)x)^2 + \cdots + a_{n-2}(1 - u^2)^{n-1}x^{n-2}$$

$$\mu\big(xa(x)\big) = a_{n-1}(1-u^2)x^n + a_0\big((1-u^2)x\big) + a_1x^2 + \cdots + a_{n-2}x^{n-2}$$

anlamına gelir.

$\mu\big(a(x)\big)\ ve\ \mu\big(xa(x)\big)$ nın vektör temsilcileri;

$$P^{-1}\mu\big(a(x)\big) = (a_0, (1-u^2)a_1, a_2, \dots, (1-u^2)^{n-1}a_{n-1})\ ve$$

$$P^{-1}\mu\big(xa(x)\big) = ((1-u^2)a_{n-1}, (1-u^2)a_0, a_1, (1-u^2)a_2, \dots, (1-u^2)^{n-1}a_{n-2}$$

dir. Bu ifadelerde ;

$$\tilde{\mu} = P^{-1}\mu P$$

anlamına gelir. Böylece ;

$(a_0, (1-u^2)a_1, a_2, \dots, a_{n-1}) \in \tilde{\mu}(D)$,

$((1-u^2)a_{n-1}, (1-u^2)a_0, a_1, (1-u^2)a_2, \dots, a_{n-2}) \in \tilde{\mu}(D)$

Buradan da $\tilde{\mu}(D)$, $R_3$ üzerinde bir $(1-u^2)-$ konsta- devirli koddur.

### 3.3.2 Gray dönüşüm ve $(1-u^2)-$ konsta-devirli kodlar

Bu bölümde $R_3$ üzerinde $n$ uzunluğunda bir lineer $(1-u^2)-$konsta-devirli kodun Gray resminin bir ikili uzaklıklı değişmez lineer kuasi-devirli kod olduğu ispatlanacaktır.

$R_2$ üzerinde , $(1+u)-$konsta-devirli kodun Gray dönüşümünü genelleştirelim. $\forall c \in R_3$ elemanı;

$$c = \beta_0(c) + u\beta_1(c) + u^2\beta_2(c)$$

şeklinde tek türlü olarak yazılabiliriz burada $\beta_i(c) \in F_2$ dir ve Gray dönüşümü aşağıdaki gibi tanımlarız;

$\phi: R_3 \to F_2^4$

$\phi(c) = (\beta_2(c), \beta_2(c) + \beta_0(c), \beta_2(c) + \beta_1(c), \beta_2(c) + \beta_1(c) + \beta_0(c))$

iddiamız $\phi$ lineerdir. [8]

İspat. $c_1, c \in F_2 + uF_2 + u^2F_2$ olsun o zaman $\phi(c + c_1) = (\beta_2(c + c_1), \beta_2(c + c_1) + \beta_0(c + c_1), \beta_2(c + c_1) + \beta_1(c + c_1), \beta_2(c + c_1) + \beta_1(c + c_1) + \beta_0(c + c_1),$

$\beta_i, F_2\ de\ \forall i = 0,1,2$ için lineer olduğundan o zaman;

$\phi(c + c_1) = \big(\beta_2(c), \beta_2(c) + \beta_0(c), \beta_2(c) + \beta_1(c), \beta_2(c) + \beta_1(c) + \beta_0(c)\big)$

$\oplus \big(\beta_2(c_1), \beta_2(c_1) + \beta_0(c_1), \beta_2(c_1) + \beta_1(c_1), \beta_2(c_1) + \beta_1(c_1) + \beta_0(c_1)\big)$

$= \phi(c) + \phi(c_1)$

□

Gray dönüşüm $\phi, R_3^n$ e genişletilebilir. $c = (c_0, c_1, \dots, c_{n-1}) \in R_3^n$ için;

$\beta_i(c) = \big(\beta_i(c_0), \beta_i(c_1), \dots, \beta_i(c_n)\big), 0 \le i \le 2$

Tanımlanabilir. O zaman $\phi, R_3^n$ e aşağıdaki gibi $\forall c \in R_3^n$ için genişletilebilir;

$\phi(c) = \big(\beta_2(c), \beta_2(c) + \beta_0(c), \beta_2(c) + \beta_1(c), \beta_2(c) + \beta_1(c) + \beta_0(c)\big)$

Açıkça, genişletilmiş $\phi$, $R_3^n\ ten\ F_2^{4n}$'e birebir ve örten bir foksiyondur. $\phi(c), c\ nin\ \phi$ altında ikili görüntüsü olarak adlandırılır.

**Önerme 3.3.4.** $\nu$, Tanım3.3.1 deki gibi ve $\psi_t$, Tanım 3.1.2 deki gibi olsun o zaman ;

$\phi\nu = \psi_2\phi$ dir [11]

İspat. $c = (c_0, c_1, \dots, c_{n-1}) \in R_3^n$ olsun. $c_i = \beta_0(c_i) + u\beta_1(c_i) + u^2\beta_2(c_i), \beta_i(c_i) \in F_2$ dir.

$\phi$ nin tanımından;

$$\phi(c) = \big(\beta_2(c_0), \beta_2(c_1), \dots, \beta_2(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0) + \beta_1(c_0), \dots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1})\big)$$

ve

$$\psi_2\phi(c) = \sigma\big(\beta_2(c_0), \beta_2(c_1), \dots, \beta_2(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-1}) + \beta_0(c_{n-1})\big)|, \sigma\big(\beta_2(c_0) + \beta_1(c_0), \dots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1})\big)$$

$$\psi_2\phi(c) = \big(\beta_2(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0), \beta_2(c_1), \dots, \beta_2(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-2}) + \beta_0(c_{n-2}), \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0) + \beta_1(c_0), \dots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-2}) + \beta_1(c_{n-2}) + \beta_0(c_{n-2})\big)$$

eşitlikleri elde edilir. Diğer taraftan;

$$\nu(c) = ((1-u^2)c_{n-1}, c_0, \dots, c_{n-2})$$

$$(1-u^2)c_{n-1} = \beta_0(c_{n-1}) + \beta_1(c_{n-1})u + (\beta_2(c_{n-1}) + \beta_0(c_{n-1}))u^2$$

dir ve tanımdan;

$$\phi\big(\nu(c)\big) = (\beta_2(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0), \dots, \beta_2(c_{n-2})|, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), \dots, \beta_2(c_{n-2}) + \beta_0(c_{n-2})\ |, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), \dots, \beta_2(c_{n-2}) + \beta_1(c_{n-2})|, \beta_2(c_{n-1}) + \beta_0(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), \dots, \beta_2(c_{n-2}) + \beta_1(c_{n-2}) + \beta_0(c_{n-2}))$$

elde ederiz. Şimdi;

$$\phi\big(v(c)\big) = (\beta_2(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0), \dots, \beta_2(c_{n-2})|, \beta_2(c_{n-1}) + \beta_1(n-1) + \beta_0(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-2}) + \beta_0(c_{n-2})|, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0) + \beta_1(c_0), \dots, \beta_2(c_{n-2}) + \beta_1(c_{n-2})|, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \dots, \beta_2(c_{n-2}) + \beta_1(c_{n-2}) + \beta_0(c_{n-2}))$$

böylece;

$$\phi\big(v(c)\big) = \big(\psi_2\phi(c)\big)$$

elde edilir.

□

**Teorem 3.3.5.** $R_3$ üzeinde bir lineer $(1-u^2)$-konsta-devirli kodun Gray görüntüsü mertebesi 2 olan ikili uzaklığa sahip değişmez lineer kuasi-devirli koddur. [11]

İspat. $C$ , $R_3$ üzeinde bir lineer $(1-u^2)$-konsta-devirli kod olsun o zaman

$v(C) = C$ ve bu yüzden $(\phi v)C = \phi(C)$ dir. Önerme 3.3.4 den $\psi_2\big(\phi(C)\big) = \phi(C)$ ve bu da $\phi(C)$ nin 2. mertebeden bir lineer kuasi-devirli kod olduğu anlamına gelir.

□

Örnek 3.3.2. Örnek 3.3.1 den;

$$x^7 + (1-u^2) = (x + (1-u^2))(x^3 + x + (1-u^2))(x^3 + (1-u^2)x^2 + (1-u^2))$$

$C = \big(x + (1-u^2)\big)\big(x^3 + x + (1-u^2)\big) = 1 + x^2 + (1-u^2)x^3 + x^4$ yani;

C kodu 7 uzunluğunda ve temel kod kelimelerinin sayısı 14 olan bir koddur.

Önerme 3.3.4 teki $\phi$ nin tanımından;

| i | $c_i$ | $\phi(c_i)$ |
|---|---|---|
| 1 | $(1,0,1,(1-u^2),1,0,0)$ | $(0,0,0,1,0,0,0,1,0,1,0,1,0,0$ $,0,0,0,1,0,0,0,1,0,1,0,1,0,0)$ |
| 2 | $(0,1,0,1,(1-u^2),1,0)$ | $(0,0,0,0,1,0,0,0,1,0,1,0,1,0$ $,0,0,0,0,1,0,0,0,1,0,1,0,1,0)$ |
| 3 | $(0,0,1,0,1,(1-u^2),1)$ | $(0,0,0,0,0,1,0,0,0,1,0,1,0,1$ $,0,0,0,0,0,1,0,0,0,1,0,1,0,1)$ |
| 4 | $((1-u^2),0,0,1,0,1,(1-u^2))$ | $(1,0,0,0,0,0,1,0,0,0,1,0,1,0$ $,1,0,0,0,0,0,1,0,0,0,1,0,1,0)$ |
| 5 | $(1,(1-u^2),0,0,1,0,1)$ | $(0,1,0,0,0,0,0,1,0,0,0,1,0,1$ $,0,1,0,0,0,0,0,1,0,0,0,1,0,1)$ |
| 6 | $((1-u^2),1,(1-u^2),0,0,1,0)$ | $(1,0,1,0,0,0,0,0,1,0,0,0,1,0$ $,1,0,1,0,0,0,0,0,1,0,0,0,1,0)$ |
| 7 | $(0,(1-u^2),1,(1-u^2),0,0,1)$ | $(0,1,0,1,0,0,0,0,0,1,0,0,0,1$ $,0,1,0,1,0,0,0,0,0,1,0,0,0,1)$ |
| 8 | $((1-u^2),0,(1-u^2),1,(1-u^2),0,0)$ | $(1,0,1,0,1,0,0,0,0,0,1,0,0,0$ $,1,0,1,0,1,0,0,0,0,0,1,0,0,0)$ |
| 9 | $(0,(1-u^2),0,(1-u^2),1,(1-u^2),0)$ | $(0,1,0,1,0,1,0,0,0,0,0,1,0,0$ $,0,1,0,1,0,1,0,0,0,0,0,1,0,0)$ |
| 10 | $(0,0,(1-u^2),0,(1-u^2),1,(1-u^2))$ | $(0,0,1,0,1,0,1,0,0,0,0,0,1,0$ $,0,0,1,0,1,0,1,0,0,0,0,0,1,0)$ |

| | | |
|---|---|---|
| 11 | $(1,0,0,(1-u^2),0,(1-u^2),1)$ | $(0,0,0,1,0,1,0,1,0,0,0,0,0,1$ $,0,0,0,1,0,1,0,1,0,0,0,0,0,1)$ |
| 12 | $((1-u^2),1,0,0,(1-u^2),0,(1$ $-u^2))$ | $(1,0,0,0,1,0,1,0,1,0,0,0,0,0$ $,1,0,0,0,1,0,1,0,1,0,0,0,0,0)$ |
| 13 | $(1,(1-u^2),1,0,0,(1-u^2),0)$ | $(0,1,0,0,0,1,0,1,0,1,0,0,0,0$ $,0,1,0,0,0,1,0,1,0,1,0,0,0,0)$ |
| 14 | $(0,1,(1-u^2),1,0,0,(1-u^2))$ | $(0,0,1,0,0,0,1,0,1,0,1,0,0,0$ $,0,0,1,0,0,0,1,0,1,0,1,0,0,0)$ |

Yukarıdaki tablodan $\phi(C)=\{\phi(c_i), i=1$ den 14 e$\}$ bir [28,8,8] olan 2-kuasi-devirli koddur.

# 4. BÖLÜM

# SONUÇ

Bu tezde $Z_4$ üzerinde *n* uzunluğunda bir lineer konsta-devirli kodun Gray görüntüsünün bir ikili uzaklığa sahip değişmez devirli kod olduğu ve $R_2 = F_2 + uF_2$ ve $R_3 = F_2 + uF_2 + u^2F_2$ üzerinde sırası ile *(1+u)*-konsta devirli ve $(1-u^2)$-konsta-devirli kodların genel tanımları ele alınmıştır.

$Z_4^n$ üzerinde n uzunluğunda bir lineer kontsa-devirli kodun Gray görüntüsünün bir ikili uzaklığa sahip değişmez devirli kod olduğu ve $Z_4^n$ in $\mu$ konsta yer değişiminin J. Wolfman tarafından " Negacyclic of cyclic codes over $Z_4$ " makalesinde ele alındığı gibi $\mu(a_0, a_1, \dots, a_n, \dots, a_{k-1}) = (a_{k-1}, a_0, a_1, \dots, a_n, \dots, a_{k-2})$ dönüşümünün yine $Z_4$ üzerinde n uzunluğunda bir konsta-devirli kod olduğu gösterilmiştir. $Z_4^n$, C nin alt kümesi olarak tanımlandığı taktirde $\mu(C) = C$.olduğunun ispatı gösterilmiştir.

Ayrıca $R_2 = F_2 + uF_2$ $(u^2 = 0)$ ve $R_3 = F_2 + uF_2 + u^2F_2$ $(u^3 = 0)$ üzerindeki kodlar arasında Gray dönüşüm hakkında çalışmalar yapıldı. *n* uzunluğunda $R_2$ ve $R_3$ üzerinde bir lineer $(1-u^2)$ $ve$ $(1+u)$ konsta-devirli kodların Gray görüntüsü eğer *n* tek ise bir ikili uzaklığa sahip lineer kuasi-devirli ve sırasıyla 2 ve 1 mertebeli bir kod olduğunun ispatı somut örnekler verilerek belirtilen makalelerden derlenerek oluşturulmuştur.

## KAYNAKLAR


1. D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T Phelps, C. A. Rodger, J. R. Wall, Coding Theory. *The Essentialsz Auburn University*, 1991.
2. H.Q. Dinh, S. R. López-Permouth, "Cyclic and Negacyclic Codes Over Finite Chain Rings." *IEEE transactions on information theory*. 50 (8) 2004, 1773-1741.
3. I. N. Herstein, "Topics in Algebra", *University of Chicago*, 1975.
4. M. M. Al-Ashker, "Simplex codes over rhe ring $F_2 + uF_2$", *The Arabian Journal for Science and Engineering*, 30 (2), 2005, 277-285.
5. M. M. Al-Ashker" Simplex codes over rhe ring"$\sum_{n=0}^{s} u^n F_2$ *Turk J Math,* 29(2005), 221-233 TUBITAK.
6. San ling and Chaoping xing "Coding Theory A first Course" *Cambridge University* , 2004.
7. W. C. Huffman, Vera Pless "Fundemantal Of Error Correcting Codes" *the United Kingdom Cambridge University* , 2003.
8. Dahrouj, F.M.A. " Negacyclic and Constacyclic codes over finite chain rings", *The islamic Universty of Gaza Deanery of Higher studies Faculty of Science Department of Mathematics The Degree of Master of Mathematics* s.73, Gaza, 2008
9. H. T. -Recillas, G. Vega "Some constacyclic codes over $Z_{2^k}$ and binary quasi-cyclic codes*". Discrete Applied Mathematics* 128 (2003) 305-316.
10. J . Qian, Li Zhang and Shi Zhu," Constacyclic and Cyclic codes over $F_2 + uF_2 + u^2F_2$". *Oxfored Journals Mathematics and Physical Sciences IEICE Tran Fund Elec Comm and Comp.Sci* E89-A, 6, 2006. 1863-1865
11. J. -Fa Qian, Li-Na Zhang and Shi-Xin Zhu"*(1 + u)* constacyclic and cyclic over $F_2 + uF_2$"," *Applied Mathematics Letters* 19, 8, (8) 2006, 820-823
12. K. T and B. Sundar Rajan, Senior Member," Consta-Abelian codes Over Galois Rings" *IEEE Ttransactions on information theory,*.5O, 2, (2) 2004, 367-370.

13. J. Wolfman," Negacyclic of cyclic codes over $Z_4$", *IEEE Transactions on Information Theory* 45, (1999), 2527-2532

# ÖZGEÇMİŞ

**Adı Soyadı** **:** Bahar KULOĞLU

**Baba Adı** **:** Mümin

**Ana Adı** **:** Şehnaz

**Doğum Yeri-Yılı** **:** Kayseri-14/12/1986

İlk, orta ve lise eğitimimi Kayseri'de tamamladım. 2006 yılında Cumhuriyet Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümünü kazandım. 2011 yılında Pedagojik Formasyon Eğitimi aldım ve aynı yıl Matematik Bölümü Cebir ve Sayılar Teorisi Ana Bilim Dalında Yüksek Lisans Eğitimine başladım. 2014 yılında Mardin/ Nusaybin El-Biruni Mesleki ve Teknik Anadolu Lisesinde Matematik öğretmeni olarak göreve başladım halen devam etmekteyim.