FEN BİLİMLERİ ENSTİTÜLERİ
ORTAK YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

Nesibe YILMAZ

BAZI HALKALAR ÜZERİNDEKİ AYKIRI DEVİRLİ KODLAR

MATEMATİK ANABİLİM DALI

OSMANİYE – 2022

FEN BİLİMLERİ ENSTİTÜSÜ
ORTAK YÜKSEK LİSANS PROGRAMI

BAZI HALKALAR ÜZERİNDEKİ AYKIRI DEVİRLİ KODLAR

Nesibe YILMAZ

MATEMATİK ANABİLİM DALI

OSMANİYE
AĞUSTOS-2022

TEZ ONAYI

BAZI HALKALAR ÜZERİNDEKİ AYKIRI DEVİRLİ KODLAR

Nesibe YILMAZ tarafından Dr. Öğr. Üyesi Cennet ESKAL danışmanlığında, Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü **Matematik** Anabilim Dalı'nda hazırlanan bu çalışma, aşağıda imzaları bulunan jüri üyeleri tarafından oy birliği/çokluğu ile **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Danışman: Dr. Öğr. Üyesi Cennet ESKAL ……...
Matematik Anabilim Dalı, OKÜ

Üye: Doç. Dr. Özge ÖZTEKİN ……...
Matematik Anabilim Dalı, GAÜN

Üye: Dr. Öğr. Üyesi Mehmet ÇİTİL ……...
Matematik Anabilim Dalı, KSÜ

Yukarıdaki jüri kararı Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ...../...../..... tarih ve ..... /……..... sayılı kararı ile onaylanmıştır.

Doç. Dr. Bülent YANIKTEPE ……...

Enstitü Müdürü, **Fen Bilimleri Enstitüsü**

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, bu çalışma sonucunda elde edilmeyen her türlü bilgi ve ifade için ilgili kaynağa eksiksiz atıf yapıldığını ve bu tezin Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Nesibe YILMAZ

ÖZET

BAZI HALKALAR ÜZERİNDEKİ AYKIRI DEVİRLİ KODLAR

Nesibe YILMAZ
Yüksek Lisans, Matematik Anabilim Dalı
Danışman: Dr. Öğr. Üyesi Cennet ESKAL

Ağustos 2022, 68 sayfa

Bu tezde önce devirli kodların genellemesi olan aykırı devirli kodların özellikleri incelenmiştir. $u^2 = 1$ olmak üzere bir δ_θ türetimi ve θ otomorfizmi kullanılarak $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerindeki aykırı devirli polinom halkası tanımlanmış, bu halkanın cebirsel özellikleri incelenmiş, bu halka üzerideki aykırı devirli kodlar derlemiştir. Son olarak ise $u^2 = u,\ v^2 = v,\ uv = vu = 0$ ve $u^2 = 1,\ v^2 = 1,\ uv = vu = 0$ durumlarında $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki aykırı polinom halkası tanımlanmış, bu halka üzerindeki aykırı devirli kodlar çalışılmış ve bu kodların üreteç ve kontrol matrisleri verilmiştir.

Anahtar Kelimeler: Devirli kod, aykırı polinom halkası, aykırı devirli kodlar

ABSTRACT

SKEW CYCLIC CODES OVER SOME RINGS

Nesibe YILMAZ
M.Sc., Department of Mathematics
Supervisor: Assist. Prof. Dr. Cennet ESKAL

August 2022, 68 pages

In this thesis, firstly it is investigated properties of skew cyclic codes, which are generalizations of cyclic codes. Skew polynomial ring over $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 1$ with a derivation δ_θ and an automorphism θ is defined, properties of algebraic are investigated, skew cyclic codes over R is compiled. In case of $u^2 = u$, $v^2 = v$, $uv = vu = 0$ and $u^2 = 1$, $v^2 = 1$, $uv = vu = 0$, skew polynomial ring over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is defined, skew cyclic ring over the ring is studied and its parity-check matrix is given.

Key Words: Cyclic code, skew polynomial ring, skew cyclis codes

Çok kıymetli kendime…

TEŞEKKÜR

Yüksek Lisans tez konumun belirlenerek tez çalışmamın yürütülmesini üstlenen, çalışmalarım süresince değerli bilgi ve tecrübeleriyle katkılarını esirgemeyen, kendisine ne zaman danışsam sabırla bana faydalı olabilmek için elinden geleni yapan danışman hocam Sayın Dr. Öğr. Üyesi Cennet ESKAL'a ve Osmaniye Korkut Ata Üniversitesi Matematik Bölümü öğretim elemanlarına, ayrıca başta Kahramanmaraş Sütçü İmam Üniversitesi Matematik Bölüm Başkanı Prof. Dr. Hüseyin YILDIRIM olmak üzere tüm öğretim elemanlarına teşekkürlerimi sunarım.

Ayrıca hayatım boyunca her konuda maddi ve manevi desteklerini esirgemeyen kıymetli annem, babam başta olmak üzere bu hayattaki en büyük şansım olan ve tezimin her aşamasında bana yardımcı olan kıymetli eşim M. Yunus YILMAZ' a, moral kaynağım kızım Hatice Zeynep'e ve bütün aileme sonsuz sevgi ve teşekkürlerimi sunarım.

İÇİNDEKİLER

ÇİZELGELER DİZİNİ

ŞEKİLLER DİZİNİ

SİMGELER ve KISALTMALAR

$\mathrm{Aut}\,(R)$ R halkasının otomorfizm grubu

$C^{\perp}$ C kodunun dual kodu

$d(C)$ C kodunun minimum uzaklığı

$d(x,y)$ x ile y kodsözleri arasındaki uzaklık

$\mathrm{der}\, f$ f polinomunun derecesi

$GF(q)$ p asal sayı olmak üzere $q = p^n$ elemanlı Galois cismi

F_q q elemanlı sonlu cisim

R/I R halkasının I idealine göre bölüm halkası

$R[x]$ Katsayıları R halkasında olan polinomlar halkası

$R[x,\theta]$ R halkası üzerindeki aykırı polinom halkası

$Z(R)$ R halkasının merkezi

$w(C)$ C kodunun (Hamming) ağırlığı

$w_L(C)$ C kodunun Lee ağırlığı

$\mathbb{Z}$ Tamsayılar halkası

$\mathbb{Z}_n$ Mod n ye göre tamsayılar halkası

$\Phi(C)$ C kodunun Gray görüntüsü

$[n,M]$ n uzunluklu M tane kodsözden oluşan lineer kod

$\langle S \rangle$ S kümesi tarafından üretilen ideal

1. GİRİŞ

Kaliteli ve güvenli iletişim ihtiyacından ortaya çıkan kodlama teorisinin başlangıç noktası olarak Shannon'ın [1] 1948 tarihli "A mathematical theory of communication" makalesi kabul edilmektedir. Shannon bu çalışmasında gürültülü bir iletişim kanalında, kanal kapasitesi denilen bir sayının altındaki bir oran için güvenilir iletişimin uygun kodlama ve kod çözme teknikleri kullanılarak gerçekleşetirilebileceğini göstermiştir. Fakat Shannon sadece uygun kodlamanın varlığını göstermiş, kodlamanın nasıl yapılacağına dair bir yöntem vermemiştir. Shannon bu çalışması ile, kanalda değişime uğrayacak olan bilginin bir doğruluk değeri ile dekodlanması sağlanacak şekilde bilginin gönderilmeden önce kodlanabilmesi garanti altına alınmıştır.

1950 de Hamming [2] hata tespit eden ve hata düzelten kodları vermiştir. Bir kodun minimum uzaklığı ne kadar büyük olursa o kadar fazla hata düzeltmektedir. Gilbert [3] ve Varshanov [4], verilen herhangi bir uzunuluktaki ve minimum uzaklıktaki kodlar için alt sınırları belirlemişlerdir.

Kodlama teorisinde mesajın şifrelenmesinde kullanılan alfabe bir sonlu küme olduğundan kodlama teorisi sonlu cisimler, sonlu halkalar gibi sonlu cebirsel yapılar üzerinde çalışılmaktadır. Kodlama teorisnde en çok $\mathbb{Z}_2^n$ nin bir alt kümesi olan ikili kodlar çalışılmıştır. En çok çalışılan bir diğer kodlama sınıfı da F_q^n vektör uzayının alt vektör uzayı olarak tanımlanan lineer kodlar olup cebirsel yapısından dolayı lineer olmayan kodlara göre kodlama ve dekodlama işlemleri açısından daha avantajlıdır. Lineer bir kod için tüm kodsözleri veren bir bazdan, dolayısıyla bir üreteç matrisinden sözedilebilir.

Lineer kodların özel bir sınıfı olan devirli kodlar, ilk olarak 1957 yılında Prange [5] tarafından tanımlanmıştır. Prange sonlu bir F cismi üzrinde n uzunluklu bir devirli koda karşılık gelen $F[x]/\langle x^n - 1\rangle$ halkasının bir idealinin varlığını göstermiştir. İdealler ile devirli kodlar arasındaki bu ilişki Hamming kodlarının genellemesi olan BCH kodlarının oluşturulmasına yol açmıştır.

Hammons ve ark. [6] $\mathbb{Z}_4$ halkası üzerindeki lineer kodların Gray dönüşümü altındaki görüntüsü sayesinde iyi hata düzeltme kapasitesine sahip lineer olmayan kodlar elde

etmişlerdir. Bu çalışma ile sonlu cisimler üzerindeki kodlarla ilgili çalışmalar değişmeli halkalar üzerine aktarılmaya başlanmış oldu.

Özen ve ark. [7] de $\mathbb{Z}_4[u]/\langle u^2-1\rangle$ halkası üzerindeki devirli ve sabit devirli (constacyclic) kodları çalışmışlardır. Yıldız ve Aydın [8], $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerindeki kodları, Yıldız ve Karadeniz [9], $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerindeki lineer kodları çalışmışlardır.

Aykırı devirli kodlar, ilk kez 2007 yılında Boucher, Geiselmann ve Ulmer [10] tarafından devirli kodların genellemesi olarak verilmiştir. Aykırı devirli kodlar bazı kaynaklarda θ −devirli kodlar olarak isimlendirilmiştir. Aykırı polinom halkalarında sağ ve sol bölme algoritmasının sağlanması ve çarpanlara ayırmanın tek türlü olmaması nedeniyle aykırı devirli kodlar optimal kod elde edilmesi bakımından devirli kodlara gore avantajlıdır.

Sharma ve Bhaintwal [11], $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerindeki aykırı devirli kodları türetim ile tanımlamışlardır. Çalışkan [12] de bunu $\mathbb{Z}_{2^s}+u\mathbb{Z}_{2^s}$ halkası için genellemiştir. Dertli ve Çengellenmiş [13] $u^2=u,\ v^2=v,\ uv=vu=0$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4$ halkası üzerindeki aykırı devirli kodları çalışmışlardır. Mohammadi ve ark. [14] te p bir asal sayı ve $v^3=v$ olmak üzere $F_p+vF_p+v^2F_p$ halkası üzerindeki aykırı devirli kodları çalışmışlardır.

Bu tezin amacı, bazı halkalar üzerindeki aykırı devirli kodları tanımlamak, bu kodların üreteç ve kontrol matrislerini elde etmektir.

Bu tez beş bölümden oluşmaktadır.

İkinci bölümde kodlama teorisi ile ilgili temel tanım ve teoremler verilmiştir.

Üçüncü bölümde türetim kullanılarak $u^2=1$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerindeki aykırı polinom halkasının cebirsel özellikleri araştırılmış, bu halka üzerindeki aykırı devirli kodlar çalışılarak bu kodların üreteç ve kontrol matrisleri derlenmiştir.

Dördüncü bölümün ilk kısmında $u^2=u,\ v^2=v,\ uv=vu=0$ olmak üzere $\theta(a+ub+vc)=a+uc+vb$ otomorfizmi kullanılarak $\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4$ halkası üzerindeki aykırı polinom halkası üzerindeki aykırı devirli kodlar çalışılmış ve bu

kodların üreteç ve kontrol matrislerinin formları belirlenmiştir. Bu bölümün ikinci kısmında ise $u^2 = 1,\ v^2 = 1,\ uv = vu = 0$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki aykırı polinom halkası $\theta(a + ub + vc) = a + u(3b) + v(3c)$ otomorfizmi kullanılarak tanımlanmış ve bu halkanın özellikleri incelenmiş, bu halka üzerindeki aykırı devirli kodlar çalışılmış ve bu kodların üreteç ve kontrol matrisleri verilmiştir.

2. TEMEL TANIM ve TEOREMLER

Bu bölümde önce aykırı polinom halkalarının cebirsel yapısı, daha sonra ise lineer kodlar, devirli kodlar ve aykırı devirli kodlar ile ilgili temel tanım ve teoremler verilmiştir. Kodlama teorisi ile ilgili temel bilgiler için Roman'ın [15] deki kitabından faydanılabilir.

2.1 Aykırı Polinom Halkaları

Aykırı polinom halkalarının teorisi 1933 te ilk kez Ore [16] tarafından ortaya atılmış ve Jacobson [17] ve McDonald [18] tarafından geliştirilmiştir.

F_q, q elemanlı bir sonlu cisim ve $\mathrm{Aut}(F_q)$, F_q cisminin otomorfizmlerinin kümesi olsun. $\theta \in \mathrm{Aut}(F_q)$ ve θ otomorfizminin mertebesi $|\langle\theta\rangle| = m$ olsun. $q = p^t$ ise F_q cisminin θ otomorfizmi tarafından sabit bırakılan alt cismi, $p^{t/m}$ elemanlı sonlu cisimdir.

Tanım 2.1.1 $F_q[x;\theta] = \{k_0 + k_1x + \cdots + k_nx^n \ : \ k_i \in F_q, \ 0 \le i \le n\}$ kümesi üzerindeki toplama işlemini polinomlardaki bilinen toplama işlemi olarak alalım. Çarpma işlemini ise $a_1, a_2 \in F_q$ için

$$(a_1x^i)(a_2x^j) = a_1\theta^i(a_2)x^{i+j} \tag{2.1}$$

olarak tanımlayalım. Dağılma özelliği kullanılarak (2.1) de tanımlanan çarpma işlemi, $F_q[x;\theta]$ kümesi üzerindeki tüm elemanlara genişletilebilir.

Teorem 2.1.2 (2.1) de tanımlanan çarpma ve polinomların bilinen toplama işlemiyle $F_q[x;\theta]$ kümesi, değişmeli olmayan bir halkadır [18].

Tanım 2.1.3 Eğer θ birim otomorfizmden farklı ise değişmeli olmayan $F_q[x;\theta]$ halkasına *aykırı (skew) polinom halkası* denir.

$f(x)$ polinomunun derecesini $der(f(x))$ ile gösterelim. $F_q[x;\theta]$ aykırı polinom halkasının özellikleri aşağıda verilmiştir.

i. $F_q[x;\theta]$ halkasının sıfır böleni yoktur.

ii. $F_q[x;\theta]$ halkasının birimselleri, F_q cisminin birimselleridir.

iii. $f(x),\ g(x) \in F_q[x;\theta]$ olmak üzere

$$\text{der}(f(x)+g(x)) \leq \max\{f(x),\ g(x)\}$$

$$\text{der}(f(x)\cdot g(x)) = \text{der}(f(x)) + \text{der}(g(x)) \text{ dir.}$$

Teorem 2.1.4 (Bölme Algoritması) $f(x) \neq 0$ ve $g(x)$, $F_q[x;\theta]$ halkasında herhangi iki polinom olsun.

$$g(x) = q(x).f(x) + r(x), \quad \text{der}(r(x)) < \text{der}(f(x)) \text{veya} \quad r(x) = 0$$

olacak şekilde tek türlü $q(x),\ r(x) \in F_q[x;\theta]$ vardır [18].

Yukarıdaki teoremde, $g(x)$ polinomu, $f(x)$ polinomu ile sağdan bölünmüştür. $F_q[x;\theta]$ halkasındaki bölme algoritması soldan bölme için de geçerlidir. Dolayısıyla bölme algoritması $F_q[x;\theta]$ halkasında hem sağdan hem de soldan sağlanır.

I, $F_q[x;\theta]$ halkasının bir sol ideali olsun. I idealindeki en küçük dereceli sıfırdan farklı bir $f(x)$ ve herhangi bir $g(x)$ polinomları için bölme algoritmasından

$$g(x) = q(x)\cdot f(x) + r(x), \quad \text{der}(r(x)) < \text{der}(f(x)) \quad \text{veya} \quad r(x) = 0$$

sağlanır. Ancak $r(x) = g(x) - q(x)\cdot f(x) \in I$ olup I idealindeki en küçük dereceye sahip polinom $f(x)$ olduğundan $r(x) = 0$ olur. Bu nedenle her $g(x) \in I$ için $g(x) = q(x)\cdot f(x)$ eşitliği sağlanır. Böylece I ideali, bir $f(x) \in F_q[x;\theta]$ polinomu tarafından üretildiğinden I bir esas ideal olup $I = \langle f(x)\rangle$ şeklindedir. Benzer şekilde $F_q[x;\theta]$ halkasının tüm sağ idealleri de bir esas idealdir.

Teorem 2.1.5 $F_q[x;\theta]$ halkasında x^n-1 polinomu tarafından üretilen sol ideal $\langle x^n-1\rangle$ ve $|\langle\theta\rangle|=m$ olsun. $\langle x^n-1\rangle$ idealinin iki taraflı ideal olması için gerek ve yeter koşul $m|n$ olmasıdır.

Teorem 2.1.6 K, F_q cisminin θ otomorfizmi tarafından sabit bırakılan alt cismi olmak üzere $F_q[x;\theta]$ halkasının merkezi,

$$Z\big(F_q[x;\theta]\big)=\{a_0+a_1x^m+\cdots+a_rx^{mr}:\ a_i\in K,\quad |\langle\theta\rangle|=m\}$$

kümesidir [18].

Önerme 2.1.7 [18] θ, F_q cisminin derecesi m olan bir otomorfizmi ve $m|n$ olsun. Eğer $x^n-1=h(x)\cdot g(x)\in F_q[x;\theta]$ ise $x^n-1=g(x)\cdot h(x)\in F_q[x;\theta]$ dir.

2.2 Lineer Kodlar

Cebirsel yapısından dolayı, lineer olmayan kodlara göre kodlama ve dekodlama işlemleri açısından avantajından dolayı en çok çalışılan bir kodlama sınıfı lineer kodlardır.

Tanım 2.2.1 q elemanlı $A=\{a_1,a_2,..,a_q\}$ kümesine *alfabe* ve bu kümenin elemanlarına da *kod sembolleri* denir. $A^n=\{w_1w_2\dots w_n:\ w_1,w_2,\dots,w_n\in A\}$ kümesinin elemanlarına *söz (kelime)* denir. A^n nin boş kümeden farklı herhangi bir C alt kümesine A üzerinde n uzunluklu *kod*, C nin herhangi bir elemanına bir *kodsöz (kod kelimesi*) denir. C nin kodsözlerinin sayısına C nin eleman sayısı denir ve $|C|$ ile gösterilir. n uzunluğu ve $|C|=M$ olan koda $[n,M]-kod$ denir. $\mathbb{Z}_2=\{0,1\}$ üzerindeki bir koda *ikili (binary) kod* denir.

Örnek 2.2.2 $A=\{0,1,2\}$ üzerindeki $C=\{0100,1020,2112\}$ kümesi 4 uzunluklu bir kod ve $0100,\ 1020,\ 2112$ ifadeleri birer kodsöz olup C kodu $[4,3]-$koddur.

Tanım 2.2.3 $x, y \in A^n$ olmak üzere x ve y nin birbirinden farklı bileşenlerinin (koordinatlarının) sayısına x ve y nin *Hamming uzaklığı* denir ve $d(x,y)$ ile gösterilir. $x = x_1x_2 \dots x_n$, $y = y_1y_2 \dots y_n \in A^n$ için

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

olmak üzere

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

dir. Bir C kodunun ayrık kodsözlerinin arasındaki uzaklıkların en küçüğüne 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. n uzunluğunda M elemana sahip ve minimum uzaklığı d olan bir kod $[n, M, d]$ −kodu olarak ifade edilir. $n,\ M,\ d$ sayıları kodun parametreleridir.

Örnek 2.2.4 $\mathbb{Z}_2^6$ de $d(101001, 000111) = 4$ ve $d(100001, 000001) = 1$ dir.

Önerme 2.2.6 A alfabesi üzerinde n uzunluğundaki üç kodsöz $x,\ y,\ z$ olsun. O zaman aşağıdakiler sağlanır.

- **i.** $0 \leq d(x,y) \leq n$
- **ii.** $d(x,y) = 0 \Leftrightarrow x = y$
- **iii.** $d(x,y) = d(y,x)$
- **iv.** $d(x,z) \leq d(x,y) + d(y,z)$ (üçgen eşitsizliği)

Yukarıdaki önerme, d fonksiyonunun A^n üzerinde bir metrik olduğunu gösterir.

Örnek 2.2.7 $C = \{0000,\ 1100,\ 1111\}$ ikili kodu için $d(0000, 1100) = 2$, $d(0000, 1111) = 4$, $d(1100, 1111) = 2$ olduğundan $d(C) = 2$ olur. C kodunun parametreleri $n = 4$, $M = 3$, $d = 2$ olup C kodu $[4,3,2] -$ koddur.

$V(n, q) = F_q^n$, uzunlukları n olan vektörlerden oluşan bir vektör uzayı olsun.

Tanım 2.2.8 F_q^n vektör uzayının bir C alt uzayına *lineer kod* denir. Eğer C nin boyutu k ve C nin minimum uzaklığı d ise C ye bir $[n, k, d] -$kod denir.

Not 2.2.9 0 vektörü lineer kodun bir elemanıdır. Bir q lu $[n, k, d] -$kod aynı zamanda bir q lu $[n, q^k, d] -$koddur, fakat her $[n, q^k, d] -$kod, bir $[n, k, d] -$kod olmayabilir.

Örnek 2.2.10

1. $C = \{(\lambda, \lambda, \dots, \lambda) : \lambda \in F_q\}$ bir tekrarlı lineer koddur.
2. $C = \{000,\ 001,\ 022,\ 002,\ 003,\ 023,\ 020,\ 021\}$ bir dörtlü lineer koddur.
3. $C = \{0000,\ 1001,\ 1011,\ 0110,\ 1111,\ 1101,\ 0100\}$ bir ikili lineer koddur.

Teorem 2.2.11 C bir $[n, k, d] -$kod olsun. $d = 2t + 1$ ya da $d = 2t + 2$ olacak şekilde bir $t \in \mathbb{Z}^+$ vardır. C koduna t *hata düzelten kod* denir. Ayrıca $d \geq s + 1$ ise C koduna $s \in \mathbb{Z}^+$ *hatayı tespit eden kod* denir.

Tanım 2.2.12 $x \in F_q^n$ elemanının sıfırdan farklı bileşenlerinin sayısına x in *(Hamming) ağırlığı (weight)* denir ve $w(x)$ ile gösterilir. Yani;

$$w(x) = d(x, 0) = \left|\{ i :\ x_i \neq 0,\quad i = 1,2, \dots, n,\quad x_i \in F_q \}\right|$$

dir. Bir C kodunun sıfırdan farklı kodsözlerinin ağırlıklarının en küçüğüne C kodunun *minimum (Hamming) ağırlığı* denir ve $w(C)$ ile gösterilir.

$$w(C) = \min\{ w(x) :\ x \neq 0,\ x \in C \}$$

Önerme 2.2.13 Her $x, y \in F_q^n$ için $d(x,y) = w(x-y)$ dir.

Teorem 2.2.14 C, F_q üzerinde bir n uzunluğunda lineer kod ise $d(C) = w(C)$ dir.

İspat. $x = (x_1, x_2, \dots, x_n)$, $y = (y_1, y_2, \dots, y_n) \in C$ olmak üzere

$$d(C) = d(x,y) = w(x-y) \geq min\{w(x) : x_i \neq 0, x \in C\} = w(C)$$

olup buradan $d(C) \geq w(C)$ elde edilir. $w(C) = min\{w(x) : x_i \neq 0,\ x \in C\}$ olduğundan $w(C) = w(x)$ olacak şekilde bir $x \in C$ vardır. $\exists x \in C$ için

$$w(C) = w(x) = w(x-0) \geq min\{d(x,y) : x \neq y,\ \ x, y \in C\} = d(C)$$

olup buradan $w(C) \geq d(C)$ bulunur. O halde $d(C) = w(C)$ elde edilir.

Not 2.2.15 Genel olarak M tane kodsözden oluşan bir genel kod için minimum uzaklığı bulmak için

$$\binom{M}{2} = \frac{1}{2}M(M-1)$$

tane Hamming uzaklığının hesap edilmesi gerekir. Ancak kod bir lineer kod ise $M-1$ tane sıfırdan farklı kodsözün ağırlığının bulunması yeterlidir.

Örnek 2.2.16 $C = \{0000,\ 1000,\ 0100,\ 1100\}$ ikili lineer kodunu ele alalım. Buna göre $w(1000) = 1,\ w(0100) = 1\,,\ w(1100) = 2$ olduğundan $d(C) = 1$ dir.

n uzunluğundaki bir kodun parametrelerini taşıyan kodun ağırlık sayacı olarak tanımlanan n −yinci dereceden homojen polinom aşağıdaki gibi tanımlanır.

Tanım 2.2.17 C, n −uzunluğunda bir kod olsun. C kodunda ağırlığı i olan kodsözlerin sayısı A_i, yani ;

$$A_i = |\{c \ : \ w(c) = i, \quad c \in C\}|$$

olsun. O zaman

$$w_C(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)} = \sum_{i=1}^{n} A_i x^{n-i}\, y^i$$

polinomuna C kodunun *Hamming ağırlık sayacı* denir.

Ağırlık sayacında y nin en küçük pozitif kuvveti kodun minimum uzaklığını, homojenlik derecesi kodun uzunluğunu ve katsayılarının toplamı kodsözlerin sayısını vermektedir.

Tanım 2.2.18 C, F_q^n üzerinde bir lineer kod olsun. C nin tüm elemanlarına ortogonal olan elemanların kümesine C nin *dual kodu* denir ve $C^{\perp}$ ile gösterilir. O zaman $C^{\perp}$, C alt uzayının ortogonal tümleyeni olup $x = (x_1, x_2, \dots, x_n),\ y = (y_1, y_2, \dots, y_n) \in F_q^n$ için

$$\langle x, y \rangle \ = \ \sum_{i=1}^{n} x_i y_i$$

F_q^n üzerindeki elemanların standart iç çarpımı olmak üzere

$$C^{\perp} = \{ y \in F_q^n : \ \langle x, y \rangle = 0, \quad \forall x \in C \}$$

şeklindedir.

Teorem 2.2.19 C, F_q^n üzerinde n uzunluğunda bir lineer kod olsun. Bu durumda

- **i.** $|C| = q^{\dim(C)}$, yani $\dim(C) = \log_q |C|$ dir.
- **ii.** $C^{\perp}$ bir lineer koddur ve $\dim(C) + \dim(C^{\perp}) = n$ dir.
- **iii.** $(C^{\perp})^{\perp} = C$ dir.

Tanım 2.2.20 C bir lineer kod olsun. Eğer $C \subseteq C^{\perp}$ ise C koduna *kendine dik kod*, $C = C^{\perp}$ ise C koduna *kendine dual kod* denir.

Örnek 2.2.21 F_2^4 deki $C = \{0000,\ 1010,\ 0101,\ 1111\}$ kodunu düşünelim. O zaman $C^{\perp} = \{0000,\ 1010,\ 1111\} = C$ olduğundan C kendine dual koddur. Ayrıca $\dim(C) = \log_2|C| = \log_2 4 = 2$ dir.

Önerme 2.2.22 n uzunluklu kendine dik kodun boyutu $n/2$ den küçük veya eşittir. n uzunluklu bir kendine dual kodun boyutu $n/2$ ye eşittir.

2.3 Lineer Kodun Üreteç ve Kontrol Matrisi

Lineer kodlar bir alt vektör uzayı olduklarından bazları vasıtasıyla temsil edilebilirler. Kodlama teorisinde lineer kodun bir bazı genel olarak matris formunda yazılır.

Tanım 2.3.1 C bir $[n, k]$ −kod olsun. Satırları C lineer kodunun tüm kodsözlerini üreten, yani C lineer kodu için baz olan $k\ x\ n$ tipindeki G matrisine *üreteç matrisi* denir. C kodunun kodsözleri, G üreteç matrisinin satırlarının lineer kombinasyonlarından oluşur.

Örnek 2.3.2 F_2^3 deki $C = \{000,\ 011,\ 101,\ 110\}$ kodu için $011 + 101 = 110$, $011 + 011 = 000$ olduğundan $G = \{011,\ 101\}$, C kodu için bir bazdır. C kodunun üreteç matrisi,

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

olur.

Tanım 2.3.3 C bir lineer kod olsun. $C^{\perp}$ dual kodun üreteç matrisine C kodunun *kontrol matrisi* denir.

Not 2.3.4

i. Eğer C bir $[n,k]$ −lineer kodunun üreteç matrisi $k \times n$ boyutunda ve kontrol matrisi de $(n-k) \times n$ boyutundadır.

ii. Bir vektör uzayının birden fazla bazı olduğundan lineer bir kodun da birden fazla üreteç matrisi olabilir. Eğer sabit bir baz seçilirse, bu bazla ifade edilen üreteç matrisinin satırlarının permütasyonu ile farklı üreteç matrisleri elde edilebilir.

iii. Üreteç matrislerinin satırları lineer bağımsızdır. Aynı şekilde kontrol matrisinin satırları da lineer bağımsızdır. $k \times n$ boyutundaki bir G matrisinin verilen bir $[n,k]$ −lineer kodunun üreteç matrisi olduğunu göstermek için G matrisinin satırlarının G nin kodsözleri olması ve lineer bağımsız olması yeterlidir.

Tanım 2.3.5 Bir C $[n,k]$ −lineer kodunun üreteç matrisi G, I_k, $k \times k$ tipindeki birim matris ve A da $k \times (n-k)$ tipinde bir matris olsun. G matrisi, elemanter satır işlemleri kullanılarak dönüştürülen $[I_k \mid X]$ formundaki matrise *üreteç matrisin standart formu* denir. I_{n-k}, $(n-k) \times (n-k)$ tipindeki birim matris ve Y de $(n-k) \times k$ tipinde bir matris olmak üzere $[Y \mid I_{n-k}]$ matrisine *kontrol matrisin standart formu* denir.

Örnek 2.3.6 F_5 üzerinde üreteç matrisi $G = \begin{bmatrix} 2 & 3 & 0 & 1 & 4 \\ 1 & 2 & 0 & 4 & 3 \\ 2 & 2 & 1 & 1 & 0 \end{bmatrix}$ olan C lineer kodu için G nin standart formunu bulalım.

$$G = \left(\begin{array}{ccc|cc} 2 & 3 & 0 & 1 & 4 \\ 1 & 2 & 0 & 4 & 3 \\ 2 & 2 & 1 & 1 & 0 \end{array}\right) S_1 \leftrightarrow S_2 \left(\begin{array}{ccc|cc} 1 & 2 & 0 & 4 & 3 \\ 2 & 3 & 0 & 1 & 4 \\ 2 & 2 & 1 & 1 & 0 \end{array}\right)$$

$$\begin{matrix} 3S_1 + S_2 \to S_2 \\ 3S_1 + S_3 \to S_3 \end{matrix} \left(\begin{array}{ccc|cc} 1 & 2 & 0 & 4 & 3 \\ 0 & 4 & 0 & 3 & 3 \\ 0 & 3 & 1 & 3 & 4 \end{array}\right)$$

$$4S_2 \leftrightarrow S_2 \left(\begin{array}{ccc|cc} 1 & 2 & 0 & 4 & 3 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 3 & 1 & 3 & 4 \end{array}\right)$$

$$\begin{matrix} 3S_2 + S_1 \to S_1 \\ 2S_2 + S_3 \to S_3 \end{matrix} \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 2 & 3 \end{array}\right)$$

Önerme 2.3.7 C, F_q üzerinde bir $[n, M]$ lineer kodu ve C kodunun üreteç matrisi G olsun. $v \in F_q^n$ elemanının $C^\perp$ dual kodunun bir elemanı olması için gerek ve yeter koşul v nin G deki her satıra dik olmasıdır. Yani $v \in C^\perp$ olması için gerek ve yeter koşul $v.G^T = 0$ olmasıdır. Özel olarak $(n-k) \times n$ boyutlu H matrisinin C lineer kodunun kontrol matrisi olabilmesi için gerek ve yeter koşul H nin satırlarının lineer bağımsız olması ve $H.G^T = 0$ olmasıdır.

Teorem 2.3.8 C lineer kodunun kontrol matrisi H olsun.

- **i.** C kodunun uzaklığının d ye eşit veya d den büyük olması için gerek ve yeter koşul H nin tüm $d-1$ sütunlu kümelerinin lineer bağımsız olmasıdır.
- **ii.** C kodunun uzaklığının d ye eşit veya d den küçük olması için gerek ve yeter koşul H nin d sütundan oluşan bir sütun kümesinin lineer bağımlı olmasıdır.

Sonuç 2.3.9 C bir lineer kod ve H, C kodunun kontrol matrisi olsun. Aşağıdakiler birbirine denktir.

- **i.** C, d uzaklığına sahiptir.
- **ii.** H matrisinin herhangi $d-1$ sütunu lineer bağımsızdır ve H, d adet lineer bağımlı sütuna sahiptir.

Teorem 2.3.10 Eğer C bir $[n,k]$ −lineer kodunun standart formdaki üreteç matrisi $G = [I_k \mid A]$ ise C kodunun kontrol matrisi $H = [-A^T \mid I_{n-k}]$ formundadır.

Örnek 2.3.11 F_5 üzerindeki standart formdaki üreteç matrisi

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 2 & 3 \end{array}\right)$$

olan C lineer kodunu düşünelim. $k = 3$ ve dolayısıyla $|C| = q^k = 5^3 = 125$ tir. $w(C) = d(C) = 2$ dir. C bir $[5,3,2]$ −koddur. C kodunun kontrol matrisi

$$H = [-A^T | I_{5-3}] = \left(\begin{array}{ccc|cc} 0 & 3 & 3 & 1 & 0 \\ 1 & 3 & 2 & 0 & 1 \end{array}\right)$$

formundadır.

Bazı kodların üreteç matrisleri standart formda olmayabilir. Ancak kodsözlerin koordinatlarında yapılacak uygun permütasyonlarla bu matris standart forma dönüştürülebilir ve standart haldeki bu matris, yeni kodun üreteç matrisidir.

Tanım 2.3.12 F_q üzerinde verilen iki $[n, M]$ −koddan birisi, diğerine

i. Kodsözlerin n bileşenlerinin permütasyonu

ii. Sabit bir koordinattaki tüm elemanların sıfırdan farklı sabit bir skalerle çarpılması.

işlemlerinden birisine maruz kalmasıyla elde edilebiliyorsa bu iki koda *denk* ya da *permütasyon denk* denir.

Örnek 2.3.13 $C = \{00000, 10010, 01011, 11101, 11001, 01111, 10110, 00100\}$ ikili kodunun koordinatlarına $\lambda = (24153)$ permütasyonunu uygulayalım.

$$C' = \{00000, 01100, 11010, 1011, 10110, 11011, 01101, 00001\}$$

kodu, C koduna denk olan bir koddur.

Not 2.3.14 Denk kodların tüm parametreleri aynıdır. Kodlama açısından aralarında hiçbir fark yoktur. Ancak uygulama esnasında bazı özel durumlar (örneğin standart formda üreteç matrisine sahip lineer kodlar) tercih edilebilir.

Teorem 2.3.15 Herhangi bir C lineer kodu standart formda üreteç matrisine sahip bir C' lineer koduna denktir.

Yukarıdaki teoremden; bir lineer kod için üreteç matrisin standart formda seçilmesi genelliği bozmayacağından genel olarak üreteç matrisin standart formda olduğu düşünülür.

2.4 Devirli Kodlar

Devirli kodlar, lineer kodların özel bir alt ailesidir. Devirli kodlar ilk olarak Prange [5] tarafından 1957 yılında ortaya konulmuştur. Bu çalışma cebirsel kodlama teorisi alanında çok önemli gelişmelere yol açmıştır. Devirli kodlar, özellikle verimli kodlama ve dekodlama algoritmaları sağlaması nedeniyle avantajlıdır. n uzunluğundaki k boyutlu bir lineer kodu temsil edebilmek için $k\ x\ n$ lik bir matrise ihtiyaç duyulurken aynı parametrelere sahip bir devirli kod sadece derecesi $n-k$ olan bir polinom tarafından temsil edilebilmektedir. Önemli kod ailelerinden olan Hamming, Golay ve BCH kodlar, devirli kodlardandır.

Tanım 2.4.1 C, F_q^n nin bir alt kümesi olsun. Her $c=(c_0,c_1,c_2,\dots,c_{n-1})\in C$ için

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

oluyorsa C kümesine *devirli (cyclic) küme* denir. σ dönüşümüne *devirsel öteleme (cyclic shift)* denir. C bir lineer kod olmak üzere C bir devirli küme ise C ye *devirli kod (cyclic cod)* denir.

Örnek 2.4.2 $C=\{(0,1,1,2),\ (2,0,1,1),\ (1,2,0,1),\ (1,1,2,0)\}\subseteq F_3^4$ kümesi bir devirli küme olmasına rağmen bir lineer kod olmadığı için bir devirli kod değildir. Çünkü $(0,0,0,0)\notin C$ dir.

Kodlar polinomlar cinsinden aşağıdaki şekilde ifade edilebilir:

$$\begin{array}{rcl} \Pi\ :\ F_q^n & \to & F_q[x]\,/\langle x^n-1\rangle \\ c=(c_0,c_1,c_2,\dots,c_{n-1}) & \to & c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1} \end{array}$$

olarak tanımlanan Π fonksiyonu bir lineer dönüşümdür. Bu durumda $c \in C$ kodsözünün devirsel ötelemesi $F_q[x]\,/\langle x^n - 1\rangle$ bölüm halkasında

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

polinomuna karşılık gelir.

Örnek 2.4.3 $C = \{000,\ 110,\ 101,\ 011\}$ devirli kodunu düşünelim. Buna göre

$$\Pi(C) \;=\; \{0,\quad 1+x,\quad 1+x^2,\quad x+x^2\} \;\subset\; F_2[x]\,/\,\langle x^3-1\rangle$$

olur.

Teorem 2.4.4 $C \subseteq F_q^n$ lineer kodunun devirli kod olması için gerek ve yeter koşul $\Pi(C) \lhd F_q[x]/\langle x^n - 1\rangle$ olmasıdır.

Teorem 2.4.5 I, $F_q[x]/\langle x^n - 1\rangle$ halkasının sıfırdan farklı bir ideali ve $g(x)$ polinomu da I idealindeki sıfırdan farklı en küçük dereceye sahip monik polinom olsun. Bu durumda $g(x)$ polinomu, I idealinin üretecidir ve $x^n - 1$ polinomunu böler.

$C \subseteq F_q^n$ bir devirli kod ve $\Pi(C) = \langle\, g(x)\rangle$ ise $g(x)$ polinomuna C kodunun *üreteç polinomu* denir ve $C = \langle\, g(x)\rangle$ yazılır.

Teorem 2.4.6 $F_q[x]/\langle x^n - 1\rangle$ halkasının sıfırdan farklı herhangi bir I idealindeki sıfırdan farklı en küçük dereceli monik polinom tektir.

Örnek 2.4.7 $C = \{000,\ 101,\ 011,\ 110\}$ devirli kodunu düşünelim. Bu durumda $\Pi : F_2^3 \to F_2[x]/\langle x^3 - 1\rangle$ dönüşümü için $\Pi(C) = \{\overline{0},\ \overline{1+x},\ \overline{1+x^2},\ \overline{x+x^2}\}$, $F_2[x]/\langle x^3 - 1\rangle$ halkasının idealidir.

$$\bar{0} \cdot (\overline{1+x}) = \bar{0} = (\overline{1+x})\left(\overline{1+x+x^2}\right)$$

$$\bar{1} \cdot (\overline{1+x}) = \overline{1+x} = (\overline{1+x})\left(\overline{x+x^2}\right)$$

$$\bar{x} \cdot (\overline{1+x}) = \overline{x+x^2} = \left(\overline{1+x^2}\right)(\overline{1+x})$$

$$\overline{x^2} \cdot (\overline{1+x}) = \overline{1+x^2} = (\overline{1+x})(\overline{1+x})$$

olup

$$F_2[x]/\langle x^3-1\rangle = \{a_0 + a_1x + a_2x^2 : a_i \in F_2\}$$

$$= \left\{\bar{0}, \bar{1}, \overline{x}, \overline{1+x^2}, \overline{1+x+x^2}, \overline{x+x^2}\right\}$$

dir. $\langle\overline{1+x}\rangle = \left\{\overline{(1+x).f(x)} : \overline{f(x)} \in F_2[x]/\langle x^3-1\rangle\right\}$ olduğundan $\Pi(C) = \langle\overline{1+x}\rangle$ olup $\Pi(C)$ aynı zamanda bir esas idealdir.

Teorem 2.4.8 $F_q[x]$ halkasında $x^n - 1$ polinomunun her bir monik böleni, F_q üzerinde bir devirli kod üretir.

Teorem 2.4.9 $g(x) \in F_q[x]$, $g(x)|(x^n-1)$ ve $\text{der}\big(g(x)\big) = k$ olsun. Bu durumda $g(x)$ tarafından üretilen ideale karşılık gelen kod, n −uzunluğunda boyutu $n-k$ olan bir devirli koddur.

Tanım 2.4.10 $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k \in F_q[x]$ derecesi k olan bir polinom olsun. $f(x)$ in *ters sıralı polinomu (reciprocal)*,

$$f^R(x) = x^k.f\left(\frac{1}{x}\right) = \sum_{i=0}^{k} a_{k-i}x^i = a_k + a_{k-1}x + a_{k-2}x^2 + \cdots + a_0x^k$$

şeklinde tanımlıdır.

Önerme 2.4.11 $x^n - 1 = h(x)g(x) \in F_q[x]$ ve $C = \langle g(x)\rangle$, F_q üzerinde n uzunluğunda bir devirli kod olsun. Bu durumda C kodunun duali, $h^R(x)$ polinomu tarafından üretilen devirli koddur. Yani; $C^{\perp} = \langle h^R(x)\rangle$ dir.

Not 2.4.12 $h(x) = h_0 + h_1x + \cdots + h_kx_k$ iken $h^R(x)$ polinomu monik olmayabilir. Bu durumda $h_0 \neq 0$ iken ${h_0}^{-1}h^R(x)$ polinomu, monik polinomdur. $h^R(x)$ polinomunun ürettiği ideal ile ${h_0}^{-1}h^R(x)$ polinomunun ürettiği ideal aynı olduğundan $C^{\perp} = \langle h^R(x) \rangle$ yazılır.

Önerme 2.4.13 $x^n - 1 = h(x)g(x) \in F_q[x]$ ve $C = \langle g(x) \rangle$, F_q üzerinde n uzunluğunda bir devirli kod olsun.

i. $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ ve der $g(x) = n - k$ olmak üzere

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{bmatrix}$$

matrisi, C kodunun üreteç matrisidir.

ii. $h(x) = h_0 + h_1x + \cdots + h_kx^k$ ve der $h(x) = k$ olmak üzere

$$H = \begin{bmatrix} h(x) \\ xh(x) \\ \vdots \\ x^{n-k-1}h(x) \end{bmatrix} = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & h_{k-2} & h_0 \end{bmatrix}$$

matrisi C kodunun kontrol matrisidir. H matrisi aynı zamanda $C^{\perp}$ kodunun üreteç matrisidir.

Örnek 2.4.14 $F_2[x]$ halkasında $x^7 - 1 = (1 + x + x^3)(1 + x + x^2 + x^4)$ olup $g(x) = 1 + x + x^2 + x^4$ polinomu, $F_2[x]$ halkasında $x^7 - 1$ polinomunun bir bölenidir. Bu durumda $g(x)$ polinomu, $n = 7$ uzunluğunda boyutu $n - k = 7 - 4 = 3$ olan bir devirli kod üretir. $C = \langle g(x) \rangle$ devirli kodunun üreteç matrisi,

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

dir. C kodunun parametreleri $[7,3,4]$ dir. $h(x) = (x^7 - 1)/g(x) = 1 + x + x^3$ ve $h^R(x) = 1 + x^2 + x^3$ olup $C^\perp = \langle h^R(x) \rangle$ kodunun üreteç matrisi;

$$H = \begin{bmatrix} h^R(x) \\ xh^R(x) \\ x^2h^R(x) \\ x^3h^R(x) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

şeklindedir.

Tanım 2.4.15 R bir halka, $\lambda \in R$ ve $C \subseteq R^n$ bir lineer kod olmak üzere

$$\begin{array}{rcl} v & : & R^n \to R^n \\ (c_0, c_1, \dots, c_{n-1}) & \to & v(c_0, c_1, \dots, c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \end{array}$$

dönüşümü için $v(C) = C$ oluyorsa C koduna R halkası üzerinde bir λ*−sabit devirli (constacylic) kod* denir. Özel olarak $\lambda = -1$ ise C koduna R halkası üzerinde *negacyclic kod* denir.

Önerme 2.4.16 $C \subseteq R^n$ bir lineer kod olsun. C kodunun bir devirli kod olması için gerek ve yeter koşul

$$\sigma: C \to C, \ \ \sigma(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, \dots, c_{n-2})$$

olarak tanımlanan dönüşümün, bir otomorfizm olmasıdır.

Önerme 2.4.17 $C \subseteq R^n$ bir lineer kod olsun. C nin bir λ−sabit devirli kod olması için gerek ve yeter şart

$$v : C \to C, \quad v(c_0, c_1, \dots, c_{n-1}) = (\lambda c_{n-1}, c_0, \dots, c_{n-2})$$

dönüşümünün bir otomorfizm olmasıdır.

2.5 Aykırı Devirli Kodlar

Aykırı (skew) devirli kodlar, ilk kez 2007 yılında Boucher, Geiselmann ve Ulmer [10] tarafından devirli kodların genellemesi olarak verilmiştir. Aykırı devirli kodlar bazı kaynaklarda θ −devirli kodlar olarak isimlendirilmiştir. Aykırı polinom halkalarında sağ ve sol bölme algoritmasının sağlanması ve çarpanlara ayırmanın tek türlü olmaması nedeniyle aykırı devirli kodlar optimal kod elde edilmesi bakımından devirli kodlara göre avantajlıdır.

Tanım 2.5.1 [10] C, F_q cismi üzerinde n uzunluğunda bir lineer kod ve θ, F_q cisminin bir otomorfizmi olsun. Her $c = (c_0, c_1, c_2, \dots, c_{n-1}) \in C$ için

$$\sigma(c) = \big(\theta(c_{n-1}), \theta(c_0), \theta(c_1), \cdots, \theta(c_{n-2})\big) \in C$$

oluyorsa C koduna n uzunluğunda *aykırı devirli (skew cyclic) kod*, σ dönüşümüne ise *aykırı devirsel öteleme (skew cyclic shift)* denir.

Eğer θ birim otomorfizm ise aykırı devirli kod, bir devirli koddur. Bu nedenle aykırı devirli kod ailesi, devirli kod ailesini içerir.

C aykırı devirli kodunun kodsözleri, polinomlar şeklinde aşağıdaki gibi ifade edilebilir:

$$\begin{aligned} \Pi_1 \ : \ C \quad &\rightarrow \quad F_q[x;\theta]/\langle x^n - 1\rangle \\ c = (c_0, c_1, \cdots, c_{n-1}) \quad &\rightarrow \quad c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \end{aligned}$$

şeklinde tanımlanan Π_1 dönüşümü bir izomorfizmdir. $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ kodsözünün $\sigma(c)$ aykırı devirsel ötelemesi

$$xc(x) = \theta(c_{n-1}) + \theta(c_0)x + \cdots + \theta(c_{n-2})x^{n-1}$$

polinom şeklinde yazılır.

C, F_q cismi üzerinde n uzunluğunda bir devirli kod olduğunda $\Pi(C)$, $F_q[x;\theta]/\langle x^n-1\rangle$ halkasının ideali idi. Aykırı devirli kodlar tanımlanırken iki durum söz konusudur:

C, F_q cismi üzerinde n uzunluğunda bir aykırı devirli kod ve $|\langle\theta\rangle| = m$ olsun.

i. $m|n$ ise $F_q[x;\theta]/\langle x^n-1\rangle$ bir halka olup $\Pi_1(C)$, $F_q[x;\theta]/\langle x^n-1\rangle$ halkasının idealidir [10].

ii. $m \nmid n$ ise $F_q[x;\theta]/\langle x^n-1\rangle$ bir halka değildir. Fakat $F_q[x;\theta]/\langle x^n-1\rangle$ bir sol $F_q[x;\theta]$ −modül olup olup $\Pi_1(C)$, $F_q[x;\theta]/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$ −altmodülüdür [19].

Teorem 2.5.2 [19] C, F_q cismi üzerinde n uzunluğunda bir lineer kod olsun. C kodunun bir aykırı devirli kod olması için gerek ve yeter koşul C kodunun $F_q[x;\theta]/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$ −altmodülü olmasıdır.

Önerme 2.5.3 [19] C, $F_q[x;\theta]/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$ −altmodülü olsun. O zaman C bir devirli altmodüldür ve C deki sıfırdan farklı en küçük dereceli monik polinom tarafından üretilir.

Teorem 2.5.4 [19] C, $F_q[x;\theta]/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$ −altmodülü ve C deki sıfırdan farklı en küçük dereceli monik polinom $f(x)$ olsun. O zaman $f(x)$ polinomu, x^n-1 polinomunun bir sağ bölenidir.

Teorem 2.5.5 [19] $F_q[x;\theta]$ halkasında $x^n-1 = h(x)g(x)$, $\text{der}\big(g(x)\big) = r$ ve $C = \langle g(x)\rangle$, $F_q[x;\theta]/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$ −altmodülü olsun. O zaman C bir serbest sol F_q −altmodüldür. C nin bir bazı

$$\beta = \{g(x),\ xg(x),\ x^2g(x),\cdots,x^{n-r-1}g(x)\}$$

şeklindedir, yani her $c \in C$ elemanı $\alpha_i \in F_q$ olmak üzere

$$c = \sum_{i=0}^{n-r-1} \alpha_i \, x^i g(x)$$

şeklinde bir sonlu toplam olarak yazılabilir ve bu yazılış tek türlüdür.

Sonuç olarak; $x^n - 1$ polinomunun sağ bölenleri $F_q[x;\theta]/\langle x^n - 1\rangle$ modülünde birer sol $F_q[x;\theta]$ −altmodül üretir ve $F_q[x;\theta]/\langle x^n - 1\rangle$ modülünün sol $F_q[x;\theta]$ −altmodülleri birer aykırı devirli koda karşılık gelir. $x^n - 1$ polinomunun derecesi $n-k$ olan her bir sağ böleni, n uzunluğında boyutu k olan bir aykırı devirli kod üretir.

Teorem 2.5.6 [20] $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$ polinomu $F_q[x;\theta]$ halkasında $x^n - 1$ polinomunun bir sağ böleni ve $\text{der}\big(g(x)\big) = n-k$ olsun. O zaman n uzunluğunda olan $C = \langle g(x)\rangle$ aykırı devirli kodunun üreteç matrisi

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \cdots & \theta(g_{n-k}) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \theta^k(g_0) & \theta^k(g_1) & \cdots & \cdots & \theta^{k-1}(g_{n-k}) \end{bmatrix}$$

şeklindedir.

$F_q[x;\theta]$ halkasında polinomların çarpanlara ayrılışının tek türlü olmaması daha fazla sayıda sağ bölen bulunmasını, dolayısıyla daha fazla sayıda kod üretilmesini sağlar.

Örnek 2.5.7 [21] $F_4 = \{0,1,a,a^2\}$, $\theta \in Aut(F_4)$ ve $\theta(a) = a^2$ olsun. F_4 üzerinde uzunluğu 4, boyutu 2 olan aykırı devirli kod bulmak için öncelikle $F_q[x;\theta]$ de $x^4 - 1$ polinomunun derecesi 2 olan sağ böleni bulunmalıdır.

$$x^4 - 1 = (x^2 + ax + a)(x^2 + ax + a^2)$$

olduğundan $g(x) = x^2 + ax + a^2$ polinomu [4,2,3] parametrelerine sahip aykırı devirli kod üretir. $C = \langle g(x) \rangle = \langle x^2 + ax + a^2 \rangle$ aykırı devirli kodunun üreteç matrisi,

$$G = \begin{bmatrix} a^2 & a & 1 & 0 \\ 0 & \theta(a^2) & \theta(a) & \theta(1) \end{bmatrix} = \begin{bmatrix} a^2 & a & 1 & 0 \\ 0 & a & a^2 & 1 \end{bmatrix}$$

şeklindedir.

$F_4[x]/\langle x^4 - 1 \rangle$ değişmeli polinom halkasında $x^4 - 1$ polinomunun derecesi 2 olan böleni sadece $x^2 + 1$ olup $x^2 + 1$ tarafından üretilen ideal, F_4 üzerinde [4,2,2] parametrelerine sahip devirli koda karşılık gelir. $F_4[x]/\langle x^4 - 1 \rangle$ halkasında $x^4 - 1$ polinomunun $x^2 + 1$ den başka ikinci dereceden böleni olmadığından başka bir devirli kod yoktur. Brouwer'a göre F_4 üzerinde optimal kod, [4,2,3] parametrelerine sahip koddur. Yukarıdaki örnekte görüldüğü üzere; aykırı devirli kod ailesi, optimal kodlar elde etme bakımından devirli kodlar ailesine göre daha avantajlıdır.

Tanım 2.5.8 $k_t \neq 0$ olmak üzere $f(x) = k_0 + k_1 x + \cdots + k_t x^t \in F_q[x; \theta]$ polinomunun *aykırı ters sıralısı (skew reciprocal)*

$$f^{RS}(x) = \sum_{i=0}^{t} x^i k_{t-i} = \sum_{i=0}^{t} \theta^i(k_{t-i}) x^i$$

şeklinde tanımlanır.

Örnek 2.5.9 $F_4 = \{0,1,a,a^2\}$ cismi üzerinde $\theta(y) = y^2$ olarak tanımlanan dönüşüm bir otomorfizmdir. $f(x) = a^2 + ax + x^2 \in F_4[x; \theta]$ polinomunun aykırı ters sıralısını bulalım. $k_0 = a^2,\ k_1 = a,\ k_2 = 1$ olmak üzere

$$f^{RS}(x) = \sum_{i=0}^{2} x^i k_{2-i} = k_2 + x k_1 + x^2 k_0$$

$$= k_2 + \theta(k_1)x + \theta^2(k_0)x^2$$

$$= 1 + \theta(a)x + \theta^2(a^2)x^2$$

$$= 1 + a^2x + a^2x^2$$

Önerme 2.5.10 [22] F_q cismindeki θ otomorfizminin derecesi m ve $m|n$ olsun. $x^n - 1 = h(x)g(x) \in F_q[x;\theta]$ ve $C = \langle g(x)\rangle$, F_q üzerinde n uzunluğunda bir aykırı devirli kod olsun. O zaman C kodunun duali; $h^{RS}(x)$ polinomu tarafından üretilen aykırı devirli koddur, yani; $C^{\perp} = \langle h^{RS}(x)\rangle$ tir.

Teorem 2.5.11 [19] C, F_q cismi üzerinde n uzunluğunda bir aykırı devirli kod ve $|\langle\theta\rangle| = m$ olsun. Eğer $(m,n) = 1$, yani m ile n aralarında asal ise C bir devirli koddur.

Teorem 2.5.12 [23] $g(x) \in F_q[x;\theta]$ polinomu, $x^n - 1$ polinomunun bir sağ böleni ve K, F_q cisminin θ otomorfizmi tarafından sabit bırakılan alt cismi olsun. Eğer m ile n aralarında asal ise $g(x) \in K[x]$ olur.

Teorem 2.5.13 [20] $g(x)$, $h(x) \in F_q[x;\theta]$ ve $k \le n$ için $\text{der}\big(h(x)\big) = k$ ve $\text{der}\big(g(x)\big) = n - k$ olsun. $\theta^n\big(g(x)\big) = \theta^n(g_0) + \theta^n(g_1)x + \cdots + \theta^n(g_{n-k})x^{n-k}$ olmak üzere $x^n - 1 = h(x)g(x)$ olması için gerek ve yeter koşul $x^n - 1 = \theta^n\big(g(x)\big)h(x)$ olmasıdır.

Teorem 2.5.14 [21] K, F_q cisminin m dereceli θ otomorfizmi tarafından sabit bırakılan alt cismi olsun. Eğer $(m,n) = 1$ ise $x^n - 1$ polinomunun $F_q[x;\theta]$ halkasındaki parçalanışı, $K[x]$ değişmeli halkasındaki parçalanışından ibarettir.

3. $\mathbb{Z}_4 + u\mathbb{Z}_4$ HALKASI ÜZERİNDEKİ AYKIRI DEVİRLİ KODLAR

Bu bölümde $u^2 = 1$ olmak üzere $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ halkasının yapısı incelenmiş, türetim kullanılarak R halkası üzerindeki aykırı devirli kodlar tanımlanmış, bu kodların üreteç ve kontrol matrisleri verilmiştir.

Bu bölümde Sharma ve Bhaintwal'in [11] deki makalesinden yararlanılmıştır.

3.1 $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ Halkası

Bu kısımda $u^2 = 1$ olmak üzere $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ halkasının yapısını incelenmiştir.

$a, b \in \mathbb{Z}_4$ olmak üzere R halkasının bir r elemanı, $r = a + ub$ şeklinde tek türlü yazılabilir. R halkasının 16 tane elemanı vardır. R halkası, $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$ bölüm halkasına izomorftur.

R halkasının bir r elemanının birimsel eleman olması için gerek ve yeter koşul a ya da b den birisinin $\mathbb{Z}_4$ halkasının birimsel elemanı olmasıdır. $\mathbb{Z}_4$ halkasının birimsel elemanları 1 ve 3 olduğundan R halkasının birimsel elemanları

$$1,\ 3,\ u,\ 3u,\ 2+u,\ 3+2u,\ 1+2u,\ 2+3u$$

dur. Sonlu bir halkada bir eleman ya birimsel ya da sıfır bölen olduğundan R halkasının birimsel olmayan yani sıfır bölen elemanları

$$0,\ 2,\ 2u,\ 2+2u,\ 1+u,\ 3+u,\ 1+3u,\ 3+3u$$

dur. R halkasının tüm idealleri;

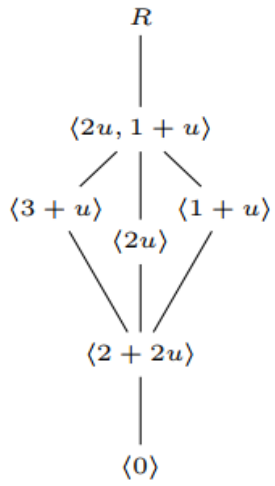
$\langle 0\rangle = \{0\}$,
$\langle 2+2u\rangle = \{0,\ 2+2u\}$
$\langle 2\rangle = \{0, 2, 2u, 2+2u\}$
$\langle 1+u\rangle = \{0, 1+u, 2+2u, 3+3u\}$

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

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

$\langle 1\rangle = R$

olup bu idealler alt küme işlemiyle bir latis formundadır. $\langle 2, 1+u\rangle$, R halkasının maksimal idealidir.



Şekil 3.1. R halkasının ideallerinin latis diyagramı

$\theta : R \to R$ dönüşümünü $\theta(a+ub) = a+(2+u)b$ olarak tanımlayalım. Her $r_1 = a_1 + ub_1$, $r_2 = a_2 + ub_2 \in R$ için

$$\begin{aligned}\theta(r_1+r_2) &= \theta\big((a_1+a_2)+u(b_1+b_2)\big)\\ &= (a_1+a_2)+(2+u)(b_1+b_2)\\ &= a_1+(2+u)b_1+a_2+(2+u)b_2\\ &= \theta(a_1+ub_1)+\theta(a_1+ub_1)\\ &= \theta(r_1)+\theta(r_2)\end{aligned}$$

ve

$$\begin{aligned}\theta(r_1\cdot r_2) &= \theta\big((a_1+ub_1)\cdot(a_2+ub_2)\big)\\ &= \theta\big((a_1a_2+b_1b_2)+u(a_1b_2+b_1a_2)\big)\\ &= (a_1a_2+b_1b_2)+(2+u)(a_1b_2+b_1a_2)\\ &= (a_1+(2+u)b_1)\cdot(a_2+(2+u)b_2)\\ &= \theta(a_1+ub_1)\cdot\theta(a_2+ub_2)\\ &= \theta(r_1)\cdot\theta(r_2)\end{aligned}$$

olduğundan θ, R halkasının bir homomorfizmidir. θ dönüşümünün birebir ve örten olduğu kolaylıkla gösterilebilir. O halde θ dönüşümü, R halkasının bir otomorfizmidir. Her $a+ub \in R$ için

$$\theta^2(a+ub) = \theta\big(\theta(a+ub)\big) = \theta(a+(2+u)b) = a+\big(2+(2+u)\big)b = a+ub$$

olduğundan θ otomorfizminin derecesi 2 dir.

Tanım 3.1.1 θ, herhangi bir H sonlu halkasının otomorfizmi olsun.

i. $\Delta_\theta(x+y) = \Delta_\theta(x) + \Delta_\theta(y)$

ii. $\Delta_\theta(x\cdot y) = \Delta_\theta(x)\cdot y + \theta(x)\cdot\Delta_\theta(y)$

koşullarını sağlayan $\Delta_\theta : H \to H$ dönüşümüne H halkasının bir *türetimi (derivation)* denir.

Teorem 3.1.2 $\delta_\theta : R \to R$ dönüşümü,

$$\delta_\theta(a+ub) = (1+u)\big(\theta(a+ub)-(a+ub)\big)$$

olarak tanımlansın. O zaman δ_θ, R halkası üzerinde bir türetimdir.

İspat: Her $r_1, r_2 \in R$ için

$$\begin{aligned}
\delta_\theta(r_1+r_2) &= (1+u)\cdot\big(\theta(r_1+r_2)-(r_1+r_2)\big)\\
&= (1+u)\cdot(\theta(r_1)+\theta(r_2)-r_1-r_2) \qquad (\theta \text{ otomorfizm})\\
&= (1+u)\cdot(\theta(r_1)-r_1+\theta(r_2)-r_2)\\
&= (1+u)\cdot(\theta(r_1)-r_1) + (1+u)\cdot(\theta(r_2)-r_2)\\
&= \delta_\theta(r_1) + \delta_\theta(r_2)
\end{aligned}$$

ve

$$\delta_\theta(r_1 \cdot r_2) = (1+u)(\theta(r_1 \cdot r_2) - r_1 \cdot r_2)$$

$$= (1+u)(\theta(r_1) \cdot \theta(yr_2) - r_1 \cdot r_2) \qquad (\theta\text{otomorfizm})$$

$$= (1+u) \cdot \theta(r_1) \cdot \theta(r_2) - (1+u) \cdot r_1 \cdot r_2$$

$$= (1+u) \cdot \theta(r_1) \cdot \theta(r_2) - (1+u) \cdot r_1 \cdot r_2 + (1+u) \cdot \theta(r_1) \cdot r_2 - (1+u) \cdot \theta(r_1) \cdot r_2$$

$$= (1+u) \cdot (\theta(r_1) - r_1) \cdot r_2 \; + \; \theta(r_1) \cdot (1+u) \cdot (\theta(r_2) - r_2)$$

$$= \delta_\theta(r_1) \cdot r_2 \; + \; \theta(r_1) \cdot \delta_\theta(r_2)$$

olduğundan δ_θ, R halkası üzerinde bir türetimdir.

R halkasının elemanlarının δ_θ türetimi altındaki görüntüleri aşağıdaki tabloda verilmiştir.

Çizelge 3.1. R halkasının elemanlarının δ_θ türetimi altındaki görüntüleri

x	0	1	2	3	u	$2u$	$3u$	$1+u$
$\delta_\theta(x)$	0	0	0	0	$2+2u$	0	$2+2u$	$2+2u$
x	$1+2u$	$1+3u$	$2+u$	$2+2u$	$2+3u$	$3+u$	$3+2u$	$3+3u$
$\delta_\theta(x)$	0	$2+2u$	$2+2u$	0	$2+2u$	$2+2u$	0	$2+2u$

Sonuç 3.1.3 $n \geq 2$ ve her $x \in R$ için $\delta_\theta^n(x) = 0$ dir.

Tanım 3.1.4 $\mathbb{Z}_4$ halkasında w_L ile gösterilen *Lee ağırlığı*

$$w_L(0) = 0, \quad w_L(1) = 1, \quad w_L(2) = 2, \quad w_L(3) = 1$$

olarak tanımlanır. $u \in \mathbb{Z}_4{}^2$ vektörünün $w_L(u)$ Lee ağırlığı; koordinatlarının Lee ağırlıklarının rasyonel toplamı olarak tanımlanır.

Tanım 3.1.5 R halkası üzerindeki Gray dönüşümü

$$\phi : R \to \mathbb{Z}_4{}^2, \quad \phi(a+ub) = (b, a+b)$$

olarak tanımlanır.

Örnek 31.6 $3+2u \in R$ elemanının Gray dönüşümü $\phi(3+2u) = (2,1)$ dir.

Tanım 3.1.7 Bir $r \in R$ elemanının $w_G(r)$ ile gösterilen *Gray ağırlığı*

$$w_G(r) = w_L(\phi(r))$$

olarak tanımlanır.

Örnek 3.1.8 $1+2u \in R$ elemanının Gray ağırlığı;

$$w_G(1+2u) = w_L(\phi(1+2u)) = w_L(2,3) = w_L(2) + w_L(3) = 2+1 = 3$$

elde edilir.

R halkasının elemanlarının Gray ağırlığı Çizelge 3.2 de verilmiştir.

Çizelge 3.2. R halkasının elemanlarının Gray ağırlığı

x	0	1	2	3	u	$2u$	$3u$	$1+u$
$w_G(x)$	0	1	2	1	2	4	2	3
x	$1+2u$	$1+3u$	$2+u$	$2+2u$	$2+3u$	$3+u$	$3+2u$	$3+3u$
$w_G(x)$	3	1	2	2	2	1	3	3

Tanım 3.1.9 ϕ dönüşümü; $\Phi : R^n \to \mathbb{Z}_4{}^{2n}$ dönüşümüne genişletilebilir. $r \in R^n$ elemanının Gray ağırlığı, r nin koordinatlarının Gray ağırlıklarının rasyonel toplamı olarak tanımlanır.

Örnek 3.1.10 $r = (1 + 3u,\ 2 + u,\ 2u) \in R^3$ elemanının Gray ağırlığı;

$$\begin{aligned} w_G(1+3u, 2+u, 2u) &= w_G(1+3u) + w_G(2+u) + w_G(2u) \\ &= w_L(\phi(1+3u)) + w_L(\phi(2+u)) + w_L(\phi(2u)) \\ &= w_L(3,0) + w_L(1,3) + w_L(2,2) \\ &= w_L(3) + w_L(0) + w_L(1) + w_L(3) + w_L(2) + w_L(2) \\ &= 1 + 0 + 1 + 1 + 2 + 2 \\ &= 3 \end{aligned}$$

elde edilir.

$\mathbb{Z}_4$ üzerindeki bir lineer kodunun parametreleri $(n, 4^{k_1}2^{k_2}, d_L)$ olarak yazılır ve kodun tipi $4^{k_1}2^{k_2}$ denir. Burada d_L, C kodunun minimum Lee uzaklığını gösterir.

3.2 $R[x, \theta, \Delta_\theta]$ Aykırı Polinom Halkası

Tanım 3.2.1 R halkasının bir otomorfizmi θ ve bir türetimi Δ_θ olsun. $R[x, \theta, \Delta_\theta]$ kümesi üzerindeki toplama işlemi, bilinen polinom toplaması olarak ve çarpma işlemi her $r \in R$ için

$$x \cdot r = \theta(r)x + \Delta_\theta(r)$$

şeklinde tanımlansın. Bu çarpma işlemi $R[x, \theta, \Delta_\theta]$ kümesinin tüm elemanlarına genişletilebilir. $R[x, \theta, \Delta_\theta]$ kümesi bu işlemlerle bir aykırı polinom halkasıdır.

Örnek 3.2.2 $f = x^2 + u, \quad g = x + u \in R[x, \theta, \delta_\theta]$ için

$$\begin{aligned} f \cdot g &= (x^2 + u) \cdot (x + u) \\ &= x^2 \cdot x + x^2 u + u \cdot x + u^2 \\ &= x^3 + x \cdot (x \cdot u) + ux + 1 \\ &= x^3 + x \cdot [\theta(u)x + \delta_\theta(u)] + ux + 1 \\ &= x^3 + x \cdot [(u+2)x + (2+2u)] + ux + 1 \\ &= x^3 + x \cdot (u+2)x + x \cdot (2+2u) + ux + 1 \\ &= x^3 + [\theta(u+2)x + \delta_\theta(u+2)]x + [\theta(2+2u)x + \delta_\theta(2+2u)] + ux + 1 \\ &= x^3 + \big[\big(2 + (u+2)\big)x + (2+2u)\big]x + [(2 + (u+2)2)x] + ux + 1 \\ &= x^3 + (ux)x + (2+2u)x + (2+2u)x + ux + 1 \\ &= x^3 + ux^2 + ux + 1 \end{aligned}$$

ve

$$\begin{aligned} g \cdot f &= (x + u) \cdot (x^2 + u) \\ &= x^2 \cdot x \ + \ x \cdot u \ + \ ux^2 \ + \ u^2 \\ &= x^3 + [\theta(u)x + \delta_\theta(u)] + ux^2 + 1 \\ &= x^3 + (2+u)x + (2+2u) + ux^2 + 1 \\ &= x^3 + ux^2 + (2+u)x + 3 + 2u \end{aligned}$$

olduğundan $f \cdot g \neq g \cdot f$ olup $R[x, \theta, \delta_\theta]$ değişmeli olmayan bir halkadır.

R halkasının $\theta(a + ub) = a + (2+u)b$ otomorfizmi altında sabit kalan elemanlarının kümesi

$$R^\theta = \{0, \quad 1, \quad 2, \quad 3, \quad 2u, \quad 3 + 2u, \quad 2 + 2u\}$$

dir. Yani her $s \in R^\theta$ için $\theta(s) = s$ ve $\delta_\theta(s) = 0$ dir. Bu nedenle her $s \in R^\theta$ için

$$xs = \theta(s)x + \delta_\theta(s) = sx$$

olur. $R[x,\theta,\delta_\theta]$ halkası bir tek çarpanlama halkası (uniquely factorization domain) değildir.

Tanım 3.2.3 $f(x) \in R[x,\theta,\delta_\theta]$ olsun. Her $a(x) \in R[x,\theta,\delta_\theta]$ için

$$f(x)\cdot a(x) = a(x)\cdot f(x)$$

oluyorsa $f(x)$ polinomuna $R[x,\theta,\delta_\theta]$ halkasının *merkezi elemanı* denir.

Lemma 3.2.4 $a \in$ R olsun. a ve b nin her ikisi de θ otomorfizmi tarafından sabit bırakılmazsa $\theta(a) - a \neq \delta_\theta(b)$ dir.

İspat. $a, b \in R$ için $\theta(a) - a = \delta_\theta(b)$ olsun. $\delta_\theta(b)$ için mümkün olan değerler 0 ve $2+2u$ dur. Eğer $\delta_\theta(b) = 0$ ise a ile b, θ otomorfizmi tarafından sabit bırakılır. $\delta_\theta(b) = 2+2u$ olduğunu kabul edelim. $\theta(a) - a$, u yu içermez. Bu ise çelişkidir. Bu da ispatı tamamlar.

Eğer R halkası üzerindeki aykırı polinom halkası, sadece θ otomorfizmi ile düşünülürse, yani $\mathrm{R}[x,\theta]$ olursa o zaman $\mathrm{R}[x,\theta]$ nın merkezi $R^\theta[x^2]$ dir.

Teorem 3.2.5 $f(x) \in R[x,\theta,\delta_\theta]$ elemanının bir merkezi eleman olması için gerek ve yeter koşul x in tüm tek kuvvetlerinin katsayıları $S = \{0,\ 2,\ 2u,\ 2+2u\}$ kümesine ait olmak üzere $f(x) \in R^\theta[x]$ olmasıdır.

İspat. İspatı tek dereceli bir polinom için yapalım. Çift dereceli polinom için de benzer şekilde yapılır. $f(x) = f_0 + f_1 x + \cdots + f_k x^k \in R[x,\theta,\delta_\theta]$ tek dereceli polinom olsun. $f(x)$ in merkezi eleman olduğunu varsayalım. O zaman

$$\begin{aligned} 0 &= xf(x) - f(x)x \\ &= \delta_\theta(f_0) + \sum_{i=0}^{k-1}\big(\theta(f_i) + \delta_\theta(f_{i+1})\big)x^{i+1} + \theta(f_k)x^{k+1} - \sum_{i=0}^{k} f_i\, x^{i+1} \end{aligned}$$

olup tüm terimlerin katsayıları sıfıra eşitlenirse

$$\delta_\theta(f_0) = 0 \tag{3.1}$$

$$\theta(f_i) - f_i + \delta_\theta(f_{i+1}) = 0, \qquad i = 0,1,2,\dots k-1 \tag{3.2}$$

$$\theta(f_k) - f_k = 0 \tag{3.3}$$

Lemma 3.2.4 ve (3.1), (3.2), (3.3) eşitliklerinden $i = 0,1,2,\dots k$ için tüm f_i ler θ otomorfizmi altında sabittir. $f(x)$ merkezi eleman olduğundan her $r \in R$ için $f(x)r = rf(x)$ olur. θ otomorfizmi altında sabit olmayan yani, $\theta(r) \neq r$ olacak şekildeki $r \in R$ elemanını alalım. O zaman

$$\begin{aligned}
0 &= rf(x) - f(x)r \\
&= \sum_{i=0}^{k} r\, f_i x^i \; - \sum_{j=0}^{\frac{k-1}{2}} \left(f_{2j} r + f_{2j+1}\delta_\theta(r)\right) x^{2j} - \sum_{l=0}^{\frac{k-1}{2}} f_{2l+1}\theta(r) x^{2l+1} \\
&= \sum_{j=0}^{\frac{k-1}{2}} \left(r f_{2j} - f_{2j} r - f_{2j+1}\delta_\theta(r)\right) x^{2j} \; + \sum_{l=0}^{\frac{k-1}{2}} \left(r f_{2l+1} - f_{2l+1}\theta(r)\right) x^{2l+1} \\
&= \sum_{j=0}^{\frac{k-1}{2}} \left(f_{2j+1}\delta_\theta(r)\right) x^{2j} - \sum_{l=0}^{\frac{k-1}{2}} f_{2l+1}\left(r - \theta(r)\right) x^{2l+1}
\end{aligned}$$

olup bu da her $j,\ l = 0,1,2,\dots,\frac{k-1}{2}$ için $f_{2l+1}\left(r - \theta(r)\right) = 0$ ve $f_{2j+1}\left(\delta_\theta(r)\right) = 0$ olmasını gerektirir. Tüm f_i ler sabit bırakıldığı için yukarıdaki koşulları sağlayan f_{2l+1} katsayıları tam olarak S nin elemanlarıdır.

Tersine, $f(x)$ in verilen koşulları sağladığını kabul edelim. Her $a(x) \in R[x, \theta, \delta_\theta]$ için $f(x)a(x) = a(x)f(x)$ olduğunu göstermek için $0 \leq i \leq \text{der}\left(a(x)\right)$ ve $0 \leq j \leq \text{der}(f(x))$ için $\left(a_i x^i\right)\left(f_j x^j\right) = \left(f_j x^j\right)\left(a_i x^i\right)$ olduğunu göstermek yeterlidir. Tüm f_i ler θ altında sabit olduğundan

$$\left(a_i x^i\right)\left(f_j x^j\right) = a_i f_j x^{i+j} \tag{3.4}$$

olur. Ayrıca

$$\left(f_j x^j\right)\left(a_i x^i\right) = \begin{cases} f_j a_i x^{i+j} & , \quad j \text{ çift ise} \\ f_j\left(\theta(a_i)x + \delta_\theta(a_i)\right)x^{i+j-1} & , \quad j \text{ tek ise} \end{cases} \tag{3.5}$$

dır. Eğer j tek ve $f_j \in S$ ise her $a \in R$ için $f_j\theta(a) = f_j a$ ve $f_j\delta_\theta(a) = 0$ olup (3.5) ten

$$\left(f_j x^j\right)\left(a_i x^i\right) = f_j\left(\theta(a_i)x + \delta_\theta(a_i)\right)x^{i+j-1} = f_j a_i x^{i+j} \tag{3.6}$$

elde edilir. (3.4), (3.5), (3.6) eşitliklerinden $f(x)$ in merkezi eleman olduğu görülür.

Örnek 3.2.6 $f(x) = x^4 + (2+2u)x^3 + (1+2u)x^2 + (2+2u)x + 3 + 2u$ elemanını düşünelim. x in tüm tek kuvvetlerinin katsayıları $2+2u$ olup S ye ait ve $1+2u,\ 3+2u \in R^\theta$ olduğundan $f(x)$ bir merkezi elemandır.

Lemma 3.2.7 Her $r \in$ R için $\delta_\theta\left(\theta(r)\right) + \theta(\delta_\theta(r)) = 0$ ve $x^2 r = rx^2$ dir.

İspat. $r = a' + ub' \in R$ olsun. O zaman

$$\delta_\theta\left(\theta(r)\right) = \delta_\theta(a' + (2+u)b') = 2b' + (2b')u$$

$$\theta\left(\delta_\theta(r)\right) = \theta(2b' + (2b')u) = 2b' + (2b')u = -(2b' + (2b')u) = -\delta_\theta\left(\theta(r)\right)$$

olduğundan $\delta_\theta\left(\theta(r)\right) + \theta(\delta_\theta(r)) = 0$ olur. $xr = \theta(r)x + \delta_\theta(r)$ eşitliğinin her iki tarafı da x ile çarpalım.

$$\begin{aligned} x^2 r &= x\theta(r)x + x\delta_\theta(r) \\ &= \left[\theta^2(r)x + \delta_\theta\left(\theta(r)\right)\right]x + \theta\left(\delta_\theta(r)\right)x + {\delta_\theta}^2(r) \\ &= rx^2 + \left[\delta_\theta\left(\theta(r)\right) + \theta\left(\delta_\theta(r)\right)\right]x + {\delta_\theta}^2(r) \\ &= rx^2 \end{aligned}$$

Sonuç 3.2.8 Herhangi bir $r \in R$ için

$$f(x) = \begin{cases} \big(\theta(r)x + \delta_\theta(r)\big)x^{n-1}, & n \text{ tek ise} \\ rx^n \quad , & n \text{ çift ise} \end{cases}$$

dir.

$R[x, \theta, \delta_\theta]$ halkası bir sol/sağ Öklid halkası olmadığı için bu halkada bölme algoritması sağlanmaz. Fakat $R[x, \theta, \delta_\theta]$ halkasının bazı özel elemanları için bölme algoritması uygulanabilir.

Teorem 3.2.9 *(Sağ Bölme Algoritması)* $f(x),\ g(x) \in R[x, \theta, \delta_\theta]$ ve $g(x)$ in baş katsayısı birimsel olsun. O zaman

$$f(x) = q(x)g(x) + r(x)$$

olacak şekilde $q(x),\ r(x) \in R[x, \theta, \delta_\theta]$ vardır. Burada $r(x) = 0$ ya da $\text{der}\big(r(x)\big) < \text{der}\big(g(x)\big)$ dir.

İspat. $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_rx^r$ ve g_s birimsel eleman olmak üzere $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_sx^s$ olsun. Eğer $r < s$ ise

$$f(x) = 0.g(x) + f(x)$$

ispat tamamlanır. $r \geq s$ olduğunu kabul edelim.

$$A(x) = \begin{cases} f_r\theta(g_s^{-1})x^{r-s}, & r-s \text{ tek ise} \\ f_rg_s^{-1}x^{r-s} \quad , & r-s \text{ çift ise} \end{cases}$$

olmak üzere $h(x) = f(x) - A(x)g(x)$ polinomunu tanımlayalım. $\text{der}(h(x)),\ \text{der}(f(x))$ ten en az 1 küçüktür. İspatı $f(x)$ polinomunun derecesi üzerinden tümevarım ile yapalım. Derecesi $f(x)$ den küçük olan her polinom için

iddianın doğru olduğunu kabul edelim. $\text{der}(f(x)) = 0$ ise iddianın doğru olduğu açıktır. Bu nedenle $\text{der}\, f(x) > 0$ olsun. $\text{der}\, h(x) < \deg f(x)$ olduğundan

$$h(x) = q_1(x)g(x) + r_1(x)$$

olacak şekilde $q_1(x)$, $r_1(x)$ elemanları vardır. Burada $r_1(x) = 0$ ya da $\text{der}\ r_1(x) < \text{der}\ g(x)$ dir. Buradan

$$f(x) = q_1(x)g(x) + r_1(x) + A(x)g(x) = \big(q_1(x) + A(x)\big)g(x) + r_1(x)$$

olup $q(x) = q_1(x) + A(x)$ ve $r(x) = r_1(x)$ olmak üzere

$$f(x) = q(x)g(x) + r(x)$$

elde edilir.

$R[x, \theta, \delta_\theta]$ halkasında sol bölme algoritması da benzer şekilde tanımlanır.

Örnek 3.2.10 $R[x, \theta, \delta_\theta]$ halkasındaki $f(x) = u + (2 + 2u)x + (1 + u)x^2$ ve $g(x) = (1 + u) + ux$ polinomlarını düşünelim. Burada $r = 2,\ s = 1$ ve $f_2 = 1 + u,\ g_1 = u$ dir. $r - s = 2 - 1 = 1$ tek olduğundan

$$A(x) = f_2\theta({g_1}^{-1})x^{2-1} = (1 + u)(u + 2)x = (3 + 3u)x$$

olup

$$\begin{aligned} A(x)g(x) &= (3 + 3u)x\big(ux + (1 + u)\big) \\ &= (3 + 3u)\big(\theta(u)x + \delta_\theta(u)\big)x + (3u + 3)\big(\theta(1 + u)x + \delta_\theta(1 + u)\big) \\ &= (3 + 3u)\big((u + 2)x + 2 + 2u\big)x + (3u + 3)\big((u + 3)x + 2 + 2u\big) \\ &= (u + 1)x^2 + 0.x + 0.x + 0 \\ &= (u + 1)x^2 \end{aligned}$$

bulunur. $h\ (x)\ =\ f(x) - A(x)g(x)\ =\ (2+2u)x + u$ polinomunu tanımlayalım. Yukarıdaki argümanı $h(x)$ üzerinde tekrarlarsak $h(x) = (2+2u)g(x) + u$ ve

$$f(x) = h(x) + A(x)g(x) = (2+2u)g(x) + u + (3u+3)xg(x)$$
$$= \big((2+2u) + (3u+3)x\big)g(x) + u$$

olur. O halde $q(x) = (2+2u) + (3u+3)x$ ve $r(x) = u$ olmak üzere $f(x) = q(x)g(x) + r(x)$ elde edilir.

3.3 $\boldsymbol{R = \mathbb{Z}_4 + u\mathbb{Z}_4}$ Halkası Üzerinde $\boldsymbol{\delta_\theta}$ −Devirli Kodlar

Bu kısımda $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ halkasındaki aykırı devirli kodlar tanımlanmıştır ve bunlar δ_θ −devirli kodlar olarak isimlendirilmiştir.

R halkası üzerindeki n uzunluklu bir lineer kod, R^n nin bir altmodülüdür. $a = (a_0, a_1, \dots, a_{n-1}) \in R^n$ elemanı, $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ olarak polinom şeklinde düşünülebilir. Bu nedenle $f(x)$, R deki n dereceli herhangi bir polinom olmak üzere R^n ile $R[x,\theta,\delta_\theta]/\langle f(x)\rangle$ bölüm halkasını özdeşleştirebiliriz. Üstelik

$$r(x)[a(x) + \langle f(x)\rangle] \ = \ r(x)a(x) \ + \langle f(x)\rangle$$

çarpması ile $R[x,\theta,\delta_\theta]/\langle f(x)\rangle$ bir sol $R[x,\theta,\delta_\theta]$ −modüldür.

Tanım 3.3.1. C, R üzerinde n uzunluklu bir kod ve $f(x)$, R üzerinde n dereceli herhangi bir polinom olsun. Eğer C, $R[x,\theta,\delta_\theta]/\langle f(x)\rangle$ in bir sol $R[x,\theta,\delta_\theta]$ −altmodülü ise C ye bir δ_θ −*lineer kod* denir. Eğer $f(x)$ merkezi polinom ise C ye bir *merkezi* δ_θ −*lineer kod* denir.

Tanım 3.3.2. C, R üzerinde bir δ_θ −lineer kod olsun. Eğer her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ için

$$T_{\delta_\theta}(c) = \left(\theta(c_{n-1}) + \delta_\theta(c_0), \theta(c_0) + \delta_\theta(c_1), \dots, \theta(c_{n-2}) + \delta_\theta(c_{n-1})\right) \in C$$

oluyorsa C ye bir δ_θ −devirli kod ve T_{δ_θ} dönüşümüne δ_θ −*devirsel öteleme* denir.

Lemma 3.3.3 $v = (v_0, v_1, \dots, v_{n-1}) \in R^n$ kelimesi,

$$v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1} \in R[x, \theta, \delta_\theta]/\langle x^n - 1\rangle$$

şeklinde yazılsın. O zaman $xv(x)$ polinomu da

$$\left(\theta(v_{n-1}) + \delta_\theta(v_0),\ \theta(v_0) + \delta_\theta(v_1),\ \theta(v_1) + \delta_\theta(v_2), \dots, \theta(v_{n-2}) + \delta_\theta(v_{n-1})\right)$$

şeklinde ifade edilir.

İspat.

$$xv(x) = x\left(\sum_{i=0}^{n-1} v_i x^i\right) = \sum_{i=0}^{n-1} x\left(v_i x^i\right)$$

$$= \sum_{i=0}^{n-1} \left(\theta(v_i)x + \delta_\theta(v_i)\right)x^i$$

$$= \sum_{i=0}^{n-1} \theta(v_i)x^{i+1} + \sum_{i=0}^{n-1} \delta_\theta(v_i)x^i$$

$$= \sum_{i=1}^{n} \theta(v_{i-1})x^i + \sum_{i=0}^{n-1} \delta_\theta(v_i)x^i$$

$$= \sum_{i=1}^{n-1} \theta(v_{i-1})x^i + \sum_{i=1}^{n-1} \delta_\theta(v_i)x^i + \theta(v_{n-1})x^n + \delta_\theta(v_0)x^0$$

$$= \sum_{i=1}^{n} \left(\theta(v_{i-1}) + \delta_\theta(v_i)\right)x^i + \left(\theta(v_{n-1}) + \delta_\theta(v_0)\right) \qquad (x^n = 1)$$

$$= \sum_{i=0}^{n-1} \left(\theta(v_{i-1}) + \delta_\theta(v_i)\right)x^i$$

olup ispat tamamlanır.

Teorem 3.3.4 R halkasındaki n uzunluklu bir C kodunun bir δ_θ −devirli kod olması için gerek ve yeter koşul C nin $R_{n,\delta_\theta} = R[x,\theta,\delta_\theta]/\langle x^n - 1\rangle$ nin $R[x,\theta,\delta_\theta]$ −altmodülü olmasıdır.

İspat. C, R üzerinde n uzunluklu bir δ_θ −devirli kod olsun. O zaman herhangi bir $c(x) \in C$ için Lemma 3.3.3 ten $xc(x) \in C$ olup her $i \in \mathbb{N}$ için $x^i c(x) \in C$ olur. Her $a(x) \in R[x,\theta,\delta_\theta]$ için $a(x)c(x) \in C$ elde edilir.

Sonuç 3.3.5 n bir çift doğal sayı olmak üzere eğer C, n uzunluğunda bir δ_θ −devirli kod ise o zaman C, $R_{n,\delta_\theta} = R[x,\theta,\delta_\theta]/\langle x^n - 1\rangle$ in idealidir.

İspat. n bir çift doğal sayı olsun. O zaman $\langle x^n - 1\rangle$ çift taraflı bir ideal olup bu nedenle R_{n,δ_θ} bir halkadır.

Not 3.3.6 n bir çift doğal sayı olmak üzere R üzerindeki n uzunluklu bir δ_θ −devirli kod, bir merkezi δ_θ −devirli koddur. Fakat bunun tersinin doğru olmadığı aşağıdaki örnekte gösterilmiştir.

Örnek 3.3.7 C, R üzerinde 4 uzunluklu

$$f(x) = (1+2u)x^4 + (2+2u)x^2 + 1 = (x^2-1)\big((1+2u)x^2 - 1\big)$$

Polinomunun $g(x) = (1+2u)x^2 - 1$ sağ böleni tarafından üretilen bir kod olsun. $f(x)$, $R[x,\theta,\delta_\theta]$ in merkezi polinomu olduğundan C, bir merkezi δ_θ −lineer koddur. MAGMA kullanılarak $(1+3u,\ 2+3u,\ 1+3u,\ u) \in C$ elde edilir. Fakat bunun δ_θ −devirsel ötelemesi, yani $(3u,\ 1+u,\ 2+u,\ 1+u) \notin C$ olduğundan C, R üzerinde δ_θ −devirli kod değildir.

Teorem 3.3.8 C, R üzerinde n uzunluklu δ_θ −devirli kod olsun. O zaman

- **i.** Eğer n tek ise C, R üzerinde n uzunluklu bir devirli koddur.
- **ii.** Eğer n çift ise C, R üzerinde indeksi 2 olan n uzunluklu bir yarıdevirli koddur.

İspat.

i. Eğer n tek ise $(n, 2) = 1$ olur. Bu nedenle $na + 2b = 1$ ve böylece $2b = 1 - na = 1 + nl$ olacak şekilde a, b tamsayısı vardır. Burada $l \equiv -a \pmod{n}$ dir. $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$ bir kodsöz olsun. Lemma 3.2.7 den

$$\begin{aligned} x^{2b}c(x) &= x^{2b}(c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}) \\ &= c_0x^{2b} + c_1x^{2b+1} + \cdots + c_{n-1}x^{2b+n-1} \end{aligned}$$

olup bu nedenle

$$\begin{aligned} x^{2b}c(x) &= c_0x^{1+nl} + c_1x^{1+nl+1} + \cdots + c_{n-1}x^{(1+nl)+n-1} \\ &= c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}, \end{aligned}$$

$c(x)$ in bir devirsel ötelemesidir. Bu da ispatı tamamlar.

ii. C deki herhangi bir $c(x)$ kodsözü için $x^2c(x) \in C$ olup Lemma 3.2.7 den $c(x)x^2 \in C$ olur. Ayrıca genel olarak C devirli değildir. Yani 2, herhangi bir $c(x) \in C$ için $x^tc(x) \in C$ olacak şekildeki en küçük t tamsayısıdır. Bu nedenle C, indeksi 2 olan quasi-devirli koddur.

Teorem 3.3.9 C, R üzerinde n uzunluklu başkatsayısı birimsel olan minimum dereceli $g(x)$ polinomunu içerecek şekildeki bir δ_θ −devirli kod olsun. O zaman $C = \langle g(x) \rangle$ dir. Üstelik $g(x) | (x^n - 1)$ dir ve C için bir baz kümesi $\{g(x),\ xg(x),\ \ldots,\ x^{n-\mathrm{der}\, g(x)-1}g(x)\}$ dir.

İspat. C başkatsayısı birimsel olan bir minimum dereceli polinomu içerdiği için ispat [21] de verilen sonlu cisimlerdekine benzer şekilde yapılır.

Teorem 3.3.9 un tersi de doğrudur.

Teorem 3.3.10 C, R üzerinde n uzunluklu serbest δ_θ-devirli kod olsun. O zaman $C = \langle g(x) \rangle$ ve $g(x)|(x^n - 1)$ olacak şekilde minimum dereceli bir $g(x)$ polinomu vardır.

İspat. Açıktır.

Örnek 3.3.11 C, R üzerinde $x^6 - 1$ in $g(x) = (2+u)x^3 + 2x^2 + 3u$ sağ böleni tarafından üretilen 6 uzunluklu bir δ_θ −devirli kod olsun. O zaman

$$\{g(x),\ xg(x),\ x^2g(x)\} = \begin{Bmatrix} (2+u)x^3 + 2x^2 + 3u, \\ ux^4 + 2ux^3 + (2+3u)x + 2 + 2u, \\ (2+u)x^5 + 2x^4 + 3ux^2 \end{Bmatrix}$$

kümesi, C kodunun bir bazıdır. C nin kardinalitisi 16^3 tür.

Şimdi, aşağıda R halkası üzerinde n uzunluklu bir serbest δ_θ −devirli kodun üreteç matrisi verilmiştir.

C, R üzerinde $x^n - 1$ polinomunun $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$ sağ böleni tarafından üretilen n uzunluklu δ_θ −devirli kod olsun. $C = \langle g(x) \rangle$ kodunun üreteç matrisi, $(n-k)\ x\ n$ tipindeki

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{n-k-1}g(x) \end{bmatrix}_{(n-k)\times n}$$

matristir. Daha açık şekilde eğer $n-k$ çift ise

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) \end{bmatrix}$$

ve $n-k$ tek ise

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & 0 & g_0\cdots & g_{k-2} & g_{k-1} & g_k \end{bmatrix}$$

şeklindedir.

Örnek 3.3.12 Örnek 3.3.11 de verilen C δ_θ-devirsel kodunun üreteç matrisi;

$$\begin{bmatrix} 3u & 0 & 2 & u+2 & 0 & 0 \\ 2u+2 & 3u+2 & 0 & 2u & u & 0 \\ 0 & 0 & 3u & 0 & 2 & u+2 \end{bmatrix}$$

dir.

4. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ HALKASINDAKİ AYKIRI DEVİRLİ KODLAR

Bu bölümde bazı özel durumlarda $S = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ halkasının yapısı incelenmiş ve bu halka üzerindeki aykırı devirli kodlar tanımlanmış, bu kodların üreteç ve kontrol matrisleri verilmiştir.

4.1 $S_1 = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, $u^2 = u$, $v^2 = v$, $uv = vu = 0$ Halkası Üzerindeki Aykırı Devirli Kodlar

Bu kısımda $u^2 = u,\ v^2 = v,\ uv = vu = 0$ olmak üzere $S_1 = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ halkasının yapısı incelenmiş, S_1 halkası üzerindeki aykırı devirli kodlar tanımlanmış, bu kodların üreteç ve kontrol matrisleri verilmiştir. Bu kısımda Dertli ve Çengellenmiş'in [13] deki makalesinden yararlanılmıştır.

$a, b, c \in \mathbb{Z}_4$ olmak üzere S_1 halkasının bir s elemanı, $r = a + ub + vc$ şeklinde tek türlü yazılabilir. S_1 halkasının 64 tane elemanı olup S_1 halkası $\mathbb{Z}_4[u, v]/\langle u^2 - u,\ v^2 - u,\ uv = vu\rangle$ bölüm halkasına izomorftur.

S_1 halkasının birimsel elemanları

$$1,\ 3,\ 1 + 2u,\ 1 + 2v,\ 3 + 2u,\ 3 + 2v,\ 1 + 2u + 2v,\ 3 + 2u + 2v$$

olup birimsel elemanların kümesi

$$U(S_1) = \{a + ub + vc :\ a \in \{1,3\} \text{ ve } b, c \in \{0,2\}\}$$

şeklinde de ifade edilebilir. S_1 halkasının trivial idealleri; $\vartheta \in U(S_1)$ olmak üzere $\langle\vartheta\rangle = S_1$ ve $\langle 0\rangle = \{0\}$ dır. S_1 halkasının 2 elemanlı idealleri;

$$\langle 2u\rangle,\quad \langle 2v\rangle,\quad \langle 2 + 2u + 2v\rangle$$

4 elemanlı idealleri;

$$\langle u\rangle = \langle 3u\rangle,\ \langle v\rangle = \langle 3v\rangle,\ \langle 2+2u\rangle,\ \langle 2+2v\rangle,\ \langle 2u+2v\rangle,\ \langle 1+3u+3v\rangle$$

8 elemanlı idealleri;

$$\langle 2\rangle,\quad \langle 2u+v\rangle = \langle 2u+3v\rangle,\quad \langle u+2v\rangle = \langle 3u+2v\rangle,$$
$$\langle 2+2u+v\rangle = \langle 2+2u+3v\rangle,\quad \langle 1+3u+v\rangle = \langle 3+u+3v\rangle$$
$$\langle 3+3u+v\rangle = \langle 1+u+3v\rangle,\quad \langle 2+3u+2v\rangle = \langle 2+u+2v\rangle$$

16 elemanlı idealleri;

$$\langle 2+u\rangle = \langle 2+3u\rangle,\quad \langle 2+3v\rangle = \langle 2+v\rangle,\quad \langle 1+u+v\rangle = \langle 3+3u+3v\rangle$$
$$\langle 3+u\rangle = \langle 1+3u\rangle = \langle 3+u+2v\rangle = \langle 1+3u+2v\rangle,$$
$$\langle 3u+3v\rangle = \langle u+v\rangle = \langle 3u+v\rangle = \langle u+3v\rangle,$$
$$\langle 3+2u+v\rangle = \langle 1+3v\rangle = \langle 3+v\rangle = \langle 1+2u+3v\rangle$$

32 elemanlı idealleri;

$$\langle 3+3u\rangle = \langle 1+u\rangle = \langle 1+u+2v\rangle = \langle 3+3u+2v\rangle,$$
$$\langle 1+v\rangle = \langle 3+3v\rangle = \langle 1+2u+v\rangle = \langle 3+2u+3v\rangle,$$
$$\langle 2+3u+v\rangle = \langle 2+u+3v\rangle = \langle 2+3u+3v\rangle = \langle 2+u+v\rangle$$

dir. S_1 bir esas ideal halkasıdır, fakat bir sonlu zincir halkası değildir.

Tanım 4.1.1 S_1 halkası üzerindeki n uzunluklu bir kod, ${S_1}^n$ nin bir alt kümesidir. C lineer kodu, ${S_1}^n$ nin bir S_1- altmodülüdür.

C, S_1 üzerinde n uzunluklu bir lineer kod olsun.

$$\sigma:\quad {S_1}^n \to {S_1}^n,\qquad \sigma(\alpha_1,\alpha_2,\dots,\alpha_n) = (\alpha_n,\alpha_1,\alpha_2,\dots,\alpha_{n-1})$$

dönüşümü için eğer $\sigma(C) = C$ oluyorsa C bir devirli koddur.

Örnek 4.1.2 $C_1 = \{(2u, 0),\ (0,0)\}$, S_1 üzerinde 2 uzunluklu lineer koddur, fakat $(0,2u) \notin C$ olduğundan devirli kod değildir.

$C_2 = \{(0,0,0,0),\ (2v, 0,2v, 0),\ (0,2v, 0,2v),\ (2v, 2v, 2v, 2v)\}$, S_1 üzerinde 4 uzunluklu bir devirli koddur.

$s = a + ub + vc \in S_1$ elemanının Lee ağırlığı, $w_L(r) = (a, a + b, a + c)$ olarak tanımlanır. $c = (c_0, c_1, \dots, c_{n-1}) \in {S_1}^n$ vektörünün Lee ağırlığı; bileşenlerinin Lee ağırlıklarının toplamıdır. $c_1, c_2 \in {S_1}^n$ olmak üzere c_1 ve c_2 elemanlarının Lee uzaklığı; $d_L(c_1, c_2) = w_L(c_1 - c_2)$ olarak tanımlanır.

Örnek 4.1.3 $c = (1 + 2u + 2v,\ 3u + v,\ 2u + v)$ elemanının Lee ağırlığını bulalım.

$$w_L(1 + 2u + 2v) = (1, 1 + 2, 1 + 2) = (1, 3, 3)$$
$$w_L(3u + v) = (0, 0 + 3, 0 + 1) = (0, 3, 1)$$
$$w_L(2u + v) = (0, 0 + 2, 0 + 1) = (0, 2, 1)$$

olup

$$\begin{aligned} w_L(c) &= w_L(1 + 2u + 2v) + w_L(3u + v) + w_L(2u + v) \\ &= (1, 3, 3) + (0, 3, 1) + (0, 2, 1) \\ &= (1,0,1) \end{aligned}$$

bulunur.

Tanım 4.1.4 $\Phi : S_1 \to {\mathbb{Z}_4}^3$, $\Phi(a + ub + vc) = (a,\ a + b,\ a + c)$ olarak tanımlanan Gray dönüşümü,

$$\Phi: {S_1}^n \to {\mathbb{Z}_4}^{3n},\quad \Phi(\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_1 + b_1, \dots, a_n + b_n, a_1 + c_1, \dots, a_n + c_n)$$

dönüşümüne genişletilebilir. Bu dönüşüm bir $\mathbb{Z}_4$ −modül izomorfizmidir.

Teorem 4.1.5 Φ Gray dönüşümü Lee uzaklığını koruyan bir dönüşümdür.

İspat. $i = 0,1,2,\cdots,n-1$ için $z_{1,i} = a_{1,i}^0 + ua_{1,i}^1 + v_{1,i}^2$, $z_{2,i} = a_{2,i}^0 + ua_{2,i}^1 + v_{2,i}^2$ olmak üzere $z_1 = (z_{1,0}, \dots, z_{1,n-1})$, $z_2 = (z_{2,0}, \dots, z_{2,n-1}) \in {S_1}^n$ olsun. O zaman $z_1 - z_2 = (z_{1,0} - z_{2,0}, \dots, z_{1,n-1} - z_{2,n-1})$ ve $\Phi(z_1 - z_2) = \Phi(z_1) - \Phi(z_2)$ olup

$$\begin{aligned} d_L(z_1, z_2) &= w_L(z_1 - z_2) = w_L(\Phi(z_1 - z_2)) \\ &= w_L(\Phi(z_1) - \Phi(z_2) \\ &= d_L(\Phi(z_1), \Phi(z_2)) \end{aligned}$$

elde edilir.

Teorem 4.1.6 Eğer C self ortogonal ise $\Phi(C)$ de self ortogonaldir.

İspat. $a_1,\ b_1,\ c_1,\ a_2,\ b_2,\ c_2 \in \mathbb{Z}_4$ olmak üzere $x_1 = a_1 + ub_1 + vc_1$ ve $x_2 = a_2 + ub_2 + vc_2$ için

$$x_1x_2 = a_1a_2 + u(a_1b_2 + b_1a_2 + b_1b_2) + v(a_1c_2 + a_2c_1 + c_1c_2)$$

olup C self ortogonal olduğundan $a_1a_2 = 0$, $a_1b_2 + b_1a_2 + b_1b_2 = 0$, $a_1c_2 + a_2c_1 + c_1c_2 = 0$ dir. Buradan da

$$\begin{aligned} \Phi(x_1)\Phi(x_2) &= (a_1,\ a_1 + b_1,\ a_1 + c_1)(a_2,\ a_2 + b_2,\ a_2 + c_2) \\ &= (a_1a_2,\ b_2 + b_1a_2 + b_1b_2,\ a_1a_2 + a_1c_2 + a_2c_1 + c_1c_2) \\ &= 0 \end{aligned}$$

olduğundan $\Phi(C)$ de self ortogonaldir.

$a = (a_0, a_1, \dots, a_{3n-1}) = (a^{(0)}|a^{(1)}|a^{(2)}) \in {\mathbb{Z}_4}^{3n}$ olsun. $\sigma : {\mathbb{Z}_4}^n \to {\mathbb{Z}_4}^n$ dönüşümü her $a^{(i)} = (a^{(i,0)}, a^{(i,1)}, \cdots, a^{(i,n-1)})$ için

$$\sigma(a^{(i)}) = (a^{(i,n-1)},\ a^{(i,0)},\ a^{(i,1)}, \cdots, a^{(i,n-2)})$$

olarak tanımlanan devirsel öteleme olmak üzere

$$\varphi : {\mathbb{Z}_4}^{3n} \to {\mathbb{Z}_4}^{3n}, \quad \varphi(a) = \left(\sigma\left(a^{(0)}\right) \middle| \sigma\left(a^{(1)}\right) \middle| \sigma\left(a^{(2)}\right)\right)$$

dönüşümünü tanımlayalım. Eğer $\varphi(C) = C$ oluyorsa $\mathbb{Z}_4$ üzerindeki $3n$ uzunluklu bir koda indeksi 3 olan *yarı devirli kod* denir.

Önerme 4.1.7 $\Phi: {S_1}^n \to {\mathbb{Z}_4}^{3n}$ Gray dönüşümü, σ bir devirsel öteleme ve $\varphi: {\mathbb{Z}_4}^{3n} \to {\mathbb{Z}_4}^{3n}$ yukarıda tanımlanan dönüşüm olsun. O zaman $\Phi\sigma = \varphi\Phi$ dir.

İspat. $a = (a_0, \dots, a_{n-1}) \in R^n$ ve $i = 0,1, \dots, n-1$ için $a_1^0,\ a_1^1,\ a_1^2 \in \mathbb{Z}_4$ olmak üzere $a_1 = a_1^0 + ua_1^1 + va_1^2$ olsun. Φ nin tanımından

$$\Phi(a) = (a_0^0, a_1^0, \dots, a_{n-1}^0, a_0^0 + a_0^1, \dots, a_{n-1}^0 + a_{n-1}^1, a_0^0 + a_0^2, \dots, a_{n-1}^0 + a_{n-1}^2)$$

olup buna φ dönüşümü uygulanırsa

$$\varphi\left(\Phi(a)\right) = \begin{pmatrix} a_{n-1}^0,\ a_0^0, \dots,\ a_{n-2}^0,\ a_{n-1}^0 + a_{n-1}^1, \dots, a_{n-2}^0 + a_{n-2}^1, \\ a_{n-1}^0 + a_{n-1}^2, \dots, a_{n-2}^0 + a_{n-2}^2 \end{pmatrix}$$

elde edilir. Diğer taraftan $\sigma(a) = (a_{n-1}, a_0, \dots, a_{n-2})$ olup buna Φ uygulanırsa

$$\Phi\left(\sigma(a)\right) = \begin{pmatrix} a_{n-1}^0,\ a_0^0, \dots,\ a_{n-2}^0,\ a_{n-1}^0 + a_{n-1}^1, \dots, a_{n-2}^0 + a_{n-2}^1, \\ a_{n-1}^0 + a_{n-1}^2, \dots, a_{n-2}^0 + a_{n-2}^2 \end{pmatrix}$$

bulunur. Buradan da $\Phi\sigma = \varphi\Phi$ olduğu görülür.

Teorem 4.1.8 C nin S_1 üzerinde n uzunluklu bir devirli kod olması için gerek ve yeter koşul $\Phi(C)$ nin $3n$ uzunluklu $\mathbb{Z}_4$ deki 3 indeksli bir yarı devirli kod olmasıdır.

İspat. $\Rightarrow$: C, S_1 üzerinde bir devirli kod olsun. O zaman $\sigma(C) = C$ olup $\Phi\big(\sigma(C)\big) = \varphi\big(\Phi(C)\big) = \Phi(C)$ olduğundan $\Phi(C)$ 3 indeksli bir quasi-devirli koddur. $\Leftarrow$: $\Phi(C)$, indeksi 3 olan bir quasi-devirli kod olsun. O zaman $\varphi\big(\Phi(C)\big) = \Phi(C)$ dir. Önerme 4.1.7 den $\varphi\big(\Phi(C)\big) = \Phi\big(\sigma(c)\big) = \Phi(C)$ olup Φ birebir olduğundan $\sigma(C) = C$ olur. Böylece C bir devirli kod olur.

Şimdi S_1 halkası üzerindeki aykırı devirli kodları tanımlayalım. S_1 üzerindeki trivial olmayan bir θ dönüşümünü $a, b, c \in \mathbb{Z}_4$ olmak üzere

$$\theta: S_1 \to S_1, \qquad \theta(a + ub + vc) = a + uc + vb$$

olarak tanımlayalım. Her $x = a_1 + ub_1 + vc_1,\ y = a_2 + ub_2 + vc_2 \in S_1$ için

$$\begin{aligned}
\theta(x + y) &= \theta\big((a_1 + ub_1 + vc_1) + (a_2 + ub_2 + vc_2)\big) \\
&= \theta\big((a_1 + a_2) + u(b_1 + b_2) + v(c_1 + c_2)\big) \\
&= (a_1 + a_2) + u(c_1 + c_2) + v(b_1 + b_2) \\
&= (a_1 + uc_1 + vb_1) + (a_2 + uc_2 + vb_2) \\
&= \theta(a_1 + ub_1 + vc_1) + \theta(a_2 + ub_2 + vc_2) \\
&= \theta(x) + \theta(y)
\end{aligned}$$

ve

$$\begin{aligned}
\theta(x \cdot y) &= \theta\big((a_1 + ub_1 + vc_1) \cdot (a_2 + ub_2 + vc_2)\big) \\
&= \theta\big((a_1a_2) + u(a_1b_2 + b_1a_2 + b_1b_2) + v(a_2c_1 + c_1c_2 + a_1c_2)\big) \\
&= a_1a_2 + u(a_1c_2 + a_2c_1 + c_1c_2) + v(a_1b_2 + a_2b_1 + b_1b_2) \\
&= (a_1 + uc_1 + vb_1) \cdot (a_2 + uc_2 + vb_2) \\
&= \theta(x) \cdot \theta(y)
\end{aligned}$$

olduğundan θ bir homomorfizmdir.

$$\theta(a_1 + ub_1 + vc_1) = \theta(a_2 + ub_2 + vc_2) \quad \Rightarrow \quad a_1 + uc_1 + vb_1 = a_2 + uc_2 + vb_2$$

olup $a_1 = a_2,\ b_1 = b_2,\ c_1 = c_2$ olduğundan $a_1 + ub_1 + vc_1 = a_2 + ub_2 + vc_2$ elde edilir. Bu nedenle θ dönüşümü birebirdir. Her $a + uc + vb \in S_1$ için $\theta(a + ub + vc) = a + uc + vb$ olacak şekilde bir $a + ub + vc \in S_1$ var olduğundan θ dönüşümü örtendir. O halde θ dönüşümü bir otomorfizmdir.

$$\theta^2(a + ub + vc) = \theta\big(\theta(a + ub + vc)\big) = \theta(a + uc + vb) = a + ub + vc$$

olduğundan θ otomorfizminin derecesi 2 dir.

Lemma 4.1.9 s, S_1 halkasının birimsel elemanı ise $\theta(s)$ de S_1 halkasının bir birimsel elemanıdır.

İspat. $s = a + ub + vc$, S_1 halkasının bir birimsel elemanı olsun. O zaman $a \in \{1,3\}$ ve $b, c \in \{0,2\}$ olur. $\theta(s) = \theta(a + ub + vc) = a + uc + vb$ olup $a \in \{1,3\}$ ve $b, c \in \{0,2\}$ olduğundan $\theta(s)$ de S_1 in birimsel elemanı olur.

Lemma 4.1.10 ${S_1}^{\theta} = \{a + ub + vc : a, b, c \in \mathbb{Z}_4,\ \mathrm{b} = \mathrm{c}\}$, S_1 halkasının θ otomorfizmi tarafından sabit bırakılan bir alt halkasıdır.

İspat. ${S_1}^{\theta}$ nın S_1 halkasının bir alt halkası olduğu kolaylıkla gösterilir. $a + ub + vc \in {S_1}^{\theta}$ olsun. $\theta(a + ub + vc) = a + uc + vb$ olup $a + ub + vc$ nin θ otomorfizmi altında sabit kalması için gerek ve yeter koşul $b = c$ olmasıdır. Bu da ispatı tamamlar.

$S_1[x, \theta] = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} : a_i \in S_1,\ n \in \mathbb{N}\}$ kümesi üzerindeki toplama bilinen polinom toplaması olarak ve çarpma işlemi ise

$$\left(ax^i\right) \cdot \left(bx^j\right) = a\theta^i(b).x^{i+j} \tag{4.1}$$

şeklinde tanımlansın. (4.1) de tanımlanan çarpma işlemi, $S_1[x,\theta]$ kümesinin tüm elemanlarına lineer olarak genişletilebilir. $S_1[x,\theta]$ kümesi bu işlemlerle bir aykırı polinom halkasıdır.

$3x,\ (u+2v)x \in S_1[x,\theta]$ elemanları için

$$(3x).\big((u+2v)x\big) = 3\theta(u+2v)x^2 = 3(2u+v)x^2 = (2u+3v)x^2$$
$$\big((u+2v)x\big)(3x) = (u+2v)\theta(3)x^2 = (u+2v)3x^2 = (3u+2v)x^2$$

olup $(3x).\big((u+2v)x\big) \neq \big((u+2v)x\big)(3x)$ olduğundan $S_1[x,\theta]$, değişmeli olmayan bir halkadır.

Tanım 4.1.11 $C \subseteq {S_1}^n$ olsun. Eğer C, ${S_1}^n$ nin bir alt modülü ve her $c=(c_1,c_2,\dots,c_n)\in C$ için $\sigma(c)=\big(\theta(c_n),\theta(c_1),\dots,\theta(c_{n-1})\big)\in C$ oluyorsa C, n uzunluklu bir aykırı devirli kod (θ −devirli kod) dur.

Örnek 4.1.12 $C=\{(0,0),\ (0,2u),\ (2v,0),\ (2v,2u)\}$, bir aykırı devirli koddur.

Her $f(x)+\langle x^n-1\rangle \in S_1[x,\theta]/\langle x^n-1\rangle$ ve $s(x)\in S_1[x,\theta]$ için

$$s(x)(f(x)+\langle x^n-1\rangle) = s(x)f(x)\ +\ \langle x^n-1\rangle$$

Işlemiyle $S_1[x,\theta]/\langle x^n-1\rangle$, bir sol $S_1[x,\theta]-$modüldür.

Teorem 4.1.13 $S_1[x,\theta]/\langle x^n-1\rangle$ deki n uzunluklu bir C kodunun bir aykırı devirli kod olması için gerek ve yeter koşul C nin $S_1[x,\theta]/\langle x^n-1\rangle$ sol $S_1[x,\theta]$ −modülünün bir sol $S_1[x,\theta]$ −altmodülü olmasıdır.

İspat. $\Rightarrow$: C, $S_1[x,\theta]/\langle x^n-1\rangle$ de n uzunluklu aykırı devirli kod ve $c,c'\in C$ olsun. $c(x)=c_1+c_2x+\cdots+c_nx^{n-1}$ ve $c'(x)=c_1'+c_2'x+\cdots+c_n'x^{n-1}$ olup C lineer olduğundan $c+c'\in C$ ve C devirli olduğundan her i için $x^ic(x)\in C$ olur.

Böylece her $p(x) \in S_1[x,\theta]/\langle x^n-1\rangle$ için $p(x).c(x) \in C$ olduğundan C, $S_1[x,\theta]/\langle x^n-1\rangle$ sol $S_1[x,\theta]$ −modülünün bir sol $S_1[x,\theta]$ −altmodülü olur.

$\Leftarrow$: C, $S_1[x,\theta]/\langle x^n-1\rangle$ sol $S_1[x,\theta]$ −modülünün bir sol $S_1[x,\theta]$ −altmodülü ve $c, c' \in C$ olsun. C bir $S_1[x,\theta]$ −altmodül olduğundan $c+c' \in C$ ve $x^i c(x) \in C$ olur. Böylece C, $S_1[x,\theta]/\langle x^n-1\rangle$ de n uzunluklu aykırı devirli kod olur.

Sonuç 4.1.14 n bir çift doğal sayı olmak üzere eğer C, $S_1[x,\theta]/\langle x^n-1\rangle$ de n uzunluklu aykırı devirli kod ise o zaman C, $S_1[x,\theta]/\langle x^n-1\rangle$ nin bir idealidir.

İspat. n bir çift doğal sayı olsun. O zaman $\langle x^n-1\rangle$ iki taraflı ideal olup $S_1[x,\theta]/\langle x^n-1\rangle$ bir halkadır.

Teorem 4.1.15 C, $S_1[x,\theta]/\langle x^n-1\rangle$ de n uzunluklu aykırı devirli kod ve $f(x)$ de C de başkatsayısı birimsel eleman olan minimal dereceli polinom olsun. Eğer $f(x)$, x^n-1 polinomunun bir sağ böleni ise $C=\langle f(x)\rangle$ dir ve $\{f(x),\ xf(x),\ x^2f(x),\ \dots,\ x^{n-\mathrm{der}(f(x))-1}f(x)\}$ kümesi C için bir bazdır.

İspat. Sharma, Bhaintwal [11] deki Teorem 14 ün ispatına benzer şekilde yapılır.

$C=\langle f(x)\rangle$, x^n-1 polinomunun bir sağ böleni tarafından üretilen S_1 üzerinde bir n - uzunluklu aykırı devirli kod olsun. $f(x)=f_0+f_1x+f_2x^2+\cdots+f_kx^k$ olmak üzere C kodunun üreteç matrisi

$$\begin{bmatrix} f(x) \\ xf(x) \\ x^2f(x) \\ \vdots \\ x^{n-k-1}f(x) \end{bmatrix}_{(n-k)\times n}$$

şeklindedir. Daha açık şekilde ifade edilirse eğer $n-k$ çift ise

$$G=\begin{bmatrix} f_0 & f_1 & f_2 & \cdots & f_k & 0 & 0 & \cdots & 0 \\ 0 & \theta(f_0) & \theta(f_1) & \cdots & \theta(f_{k-1}) & \theta(f_k) & 0 & \cdots & 0 \\ 0 & 0 & f_0 & \cdots & f_{k-2} & f_{k-1} & f_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \theta(f_0) & \theta(f_1) & \theta(f_2) & \cdots & \theta(f_k) \end{bmatrix}$$

ve eğer $n-k$ tek ise

$$G=\begin{bmatrix} f_0 & f_1 & f_2 & \cdots & f_k & 0 & 0 & \cdots & 0 \\ 0 & \theta(f_0) & \theta(f_1) & \cdots & \theta(f_{k-1}) & \theta(f_k) & 0 & \cdots & 0 \\ 0 & 0 & f_0 & \cdots & f_{k-2} & f_{k-1} & f_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & f_0 & f_1 & f_2 & \cdots & f_k \end{bmatrix}$$

şeklindedir.

Örnek 4.1.15 $f_0 = f_4 = 1+2u+2v$, $f_1 = f_2 = f_3 = 2+2u+2v$ olmak üzere $f(x) = f_0 + f_1x + f_2x^2 + f_3x^3 + f_4x^4$ ve $h_0 = 3+2u+2v$, $h_4 = 1+2u+2v$, $h_1 = h_2 = h_3 = 2+2u+2v$ olmak üzere $h(x) = h_0 + h_1x + hx^2 + h_3x^3 + h_4x^4$ olsun. O zaman $x^8-1 = h(x)\cdot f(x)$ olur. C, x^8-1 polinomunun sağ böleni olan $f(x)$ tarafından üretilen 8 uzunluklu bir aykırı devirli kod ise $\{f(x),\ xf(x),\ x^2f(x),\ x^3f(x)\}$ kümesi C kodu için bir bazdır. Bu durumda C kodunun üreteç matrisi;

$$G=\begin{bmatrix} f_0 & f_1 & f_2 & f_3 & f_4 & 0 & 0 & 0 \\ 0 & \theta(f_0) & \theta(f_1) & \theta(f_2) & \theta(f_3) & \theta(f_4) & 0 & 0 \\ 0 & 0 & f_0 & f_1 & f_2 & f_3 & f_4 & 0 \\ 0 & 0 & 0 & \theta(f_0) & \theta(f_1) & \theta(f_2) & \theta(f_3) & \theta(f_4) \end{bmatrix}$$

$$=\begin{bmatrix} 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 1+2u+2v & 0 & 0 & 0 \\ 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 1+2u+2v & 0 & 0 \\ 0 & 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 1+2u+2v & 0 \\ 0 & 0 & 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 1+2u+2v \end{bmatrix}$$

dir.

Lemma 4.1.16 n çift doğal sayı ise x^n-1, $S_1[x,\theta]$ nın merkezi elemanıdır, yani $f(x),\ h(x)\in S_1[x,\theta]$ için $x^n-1=h(x).f(x)=f(x).h(x)$ dir.

Lemma 4.1.17 $f(x)$, x^n-1 polinomunun monik sağ böleni ve n çift pozitif tamsayı olmak üzere C, $f(x)$ tarafından üretilen n uzunluklu bir aykırı devirli kod olsun. O zaman $c(x)\in S_1[x,\theta]/\langle x^n-1\rangle$ elemanının C de olması için gerek ve yeter koşul $x^n-1=h(x)f(x)$ olmak üzere $S_1[x,\theta]/\langle x^n-1\rangle$ de $c(x)h(x)=0$ olmasıdır.

İspat. $c(x)\in C$ olsun. O zaman $c(x)=k(x)f(x)$ olacak şekilde bir $k(x)\in S_1[x,\theta]/\langle x^n-1\rangle$ vardır. Böylece Lemma 4.1.16 dan $S_1[x,\theta]/\langle x^n-1\rangle$ de $c(x)h(x)=k(x)f(x)h(x)=0$ elde edilir. Tersine bir $c(x)\in S_1[x,\theta]/\langle x^n-1\rangle$ için $S_1[x,\theta]/\langle x^n-1\rangle$ de $c(x).h(x)=0$ olduğunu kabul edelim. O zaman

$$c(x)h(x)=p(x)(x^n-1)=p(x)h(x)f(x)=p(x)f(x)h(x)$$

olacak şekilde bir $p(x)\in S_1[x,\theta]$ elemanı vardır. Böylece $c(x)=p(x)f(x)$ olup $c(x)\in C$ elde edilir.

Teorem 4.1.18 n bir çift pozitif tamsayı olmak üzere S_1 üzerindeki n uzunluklu bir C aykırı devirli kodu, $h(x)=h_0+h_1x+h_2x^2+\cdots+h_kx^k\in S_1[x,\theta]$ için $x^n-1=h(x)f(x)$ olacak şekildeki $f(x)$ tarafından üretilsin. O zaman $C^\perp$ dual kodunun üreteç matrisi, k tek pozitif tamsayı ise

$$H=\begin{bmatrix} h_k & \theta(h_{k-1}) & \cdots & h_3 & \theta(h_2) & \cdots & 0 \\ 0 & \theta(h_k) & \cdots & h_4 & \theta(h_3) & \cdots & 0 \\ 0 & 0 & \cdots & h_5 & \theta(h_4) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \theta(h_0) \end{bmatrix}_{(n-k)\times n}$$

ve k çift pozitif tamsayı ise

$$H=\begin{bmatrix} h_k & \theta(h_{k-1}) & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & \theta(h_k) & \cdots & h_1 & \theta(h_0) & \cdots & 0 \\ 0 & 0 & \cdots & h_2 & \theta(h_1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \theta(h_k) & \cdots & h_0 \end{bmatrix}_{(n-k)\times n}$$

şeklindedir.

İspat. k tek pozitif tam sayı olsun. $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in C$ alalım. Lemma 4.1.17 den $S_1[x,\theta]/\langle x^n-1\rangle$ halkasında $c(x)h(x)=0$ olduğundan $(c_0+c_1x+\cdots+c_{n-1}x^{n-1})(h_0+h_1x+\cdots+h_kx^k)$ polinomundaki $x^k, x^{k+1}, \ldots, x^{n-1}$ terimlerinin katsayıları sıfır olur. Böylece

$$c_0h_k+c_1\theta(h_{k-1})+c_2h_{k-2}+\cdots+c_k\theta(h_0)=0$$
$$c_1\theta(h_k)+c_2h_{k-1}+c_3\theta(h_{k-1})+\cdots+c_{k+1}h_0=0$$
$$c_2h_k+c_3\theta(h_{k-1})+c_4h_{k-2}+\cdots+c_{k+2}\theta(h_0)=0$$
$$\vdots$$
$$c_{n-k-1}h_k+c_{n-k}\theta(h_{k-1})+c_{n-k-1}h_{k-2}+\cdots+c_{n+2}\theta(h_0)=0$$

bulunur. $c\in C$ için $cH^T=0$ olup $GH^T=0$ elde edilir. H nin satırları her bir $c\in C$ ye ortogonal olduğundan span $H\subseteq C^\perp$ olur. Lemma 4.1.9 dan H tüm köşegen bileşenleri birimsel olan alt üçgensel matris olduğundan H determinantı sıfır olmayan $(n-k)\times(n-k)$ tipindeki alt matrisi içerir. Bu nedenle H nin tüm satırları lineer bağımsız olup $|\text{span } H|=|S_1|^{n-k}$ olur. $|C|.|C^\perp|=|S_1|^n$ ve $|C^\perp|=|S_1|^{n-k}$ olup span $H=C^\perp$ olur. Böylece H, $C^\perp$ için bir üreteç matrisidir. k nın çift pozitif tam sayı olması durumu da benzer şekilde gösterilir.

Örnek 4.1.19 Örnek 4.1.15 te verilen C kodunun kontrol matrisi;

$$H=\begin{bmatrix} h_4 & \theta(h_3) & h_2 & \theta(h_1) & h_0 & 0 & 0 & 0 \\ 0 & \theta(h_4) & h_3 & \theta(h_2) & h_1 & \theta(h_0) & 0 & 0 \\ 0 & 0 & h_4 & \theta(h_3) & h_2 & \theta(h_1) & h_0 & 0 \\ 0 & 0 & 0 & \theta(h_4) & h_3 & \theta(h_2) & h_1 & \theta(h_0) \end{bmatrix}$$

$$= \begin{bmatrix} 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 3+2u+2v & 0 & 0 & 0 \\ 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 3+2u+2v & 0 & 0 \\ 0 & 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 3+2u+2v & 0 \\ 0 & 0 & 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 2+2u+2v & 3+2u+2v \end{bmatrix}$$

dir.

4.2 $S_2 = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, $u^2 = 1$, $v^2 = 1$, $uv = vu = 0$ Halkası Üzerindeki Aykırı Devirli Kodlar

Bu kısımda $u^2 = 1,\ v^2 = 1,\ uv = vu = 0$ olmak üzere $S_2 = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ halkasının yapısı incelenmiş, S_2 halkası üzerindeki aykırı devirli kodlar tanımlanmış, bu kodların üreteç ve kontrol matrisleri verilmiştir.

$a, b, c \in \mathbb{Z}_4$ olmak üzere S_2 halkasının bir s elemanı, $r = a + ub + vc$ şeklinde tek türlü yazılabilir. S_2 halkasının 64 tane elemanı olup S_2 halkası $\mathbb{Z}_4[u, v]/\langle u^2 - 1,\ v^2 - 1,\ uv = vu\rangle$ bölüm halkasına izomorftur.
S_2 halkasının birimsel elemanları;

$$1,3,u,v,3u,3v,2+u,1+2u,3+2u,2+3u,2+v,1+2v,3+2v,2+3v,u+v,$$

$$u+2v,u+3v,2u+v,2u+3v,3u+2v,3u+v,3u+3v,1+u+v,1+u+3v$$

$$1+2u+2v,1+3u+v,1+3u+3v,2+u+2v,2+2u+v,2+2u+3v,$$

$$2+3u+2v,3+u+v,3+u+3v,3+2u+2v,3+3u+v,3+3u+3v$$

dir. .S_2 halkasının trivial idealleri; S_2 ve $\langle 0\rangle = \{0\}$ dır. S_2 halkasının trivial olmayan tek ideali 8 elemanlı olup

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

dir.

S_2 üzerindeki trivial olmayan bir φ dönüşümünü $a,b,c \in \mathbb{Z}_4$olmak $\varphi: S_2 \to S_2$, $\varphi(a+ub+vc) = a+u(3b)+v(3c)$

olarak tanımlayalım. Her $x = a_1+ub_1+vc_1,\ y = a_2+ub_2+vc_2 \in S_2$ için

$$\begin{aligned}\varphi(x+y) &= \varphi\big((a_1+ub_1+vc_1)+(a_2+ub_2+vc_2)\big)\\ &= \theta\big((a_1+a_2)+u(b_1+b_2)+v(c_1+c_2)\big)\\ &= (a_1+a_2)+u3(b_1+b)+v3(c_1+c_2)\\ &= \big(a_1+u(3b_1)+v(3c_1)\big)+\big(a_2+u(3b_2)+v(3c_2)\big)\\ &= \theta(a_1+ub_1+vc_1)+\theta(a_2+ub_2+vc_2)\\ &= \varphi(x)+\varphi(y)\end{aligned}$$

ve

$$\begin{aligned}\varphi(x\cdot y) &= \varphi\big((a_1+ub_1+vc_1)\cdot(a_2+ub_2+vc_2)\big)\\ &= \varphi\big((a_1a_2+b_1b_2+c_1c_2)+u(a_1b_2+b_1a_2)+v(a_1c_2+c_1a_2)\big)\\ &= a_1a_2+b_1b_2+c_1c_2+u3(a_1b_2+b_1a_2)+v3(a_1c_2+c_1a_2)\\ &= \big(a_1+u(3b_1)+v(3c_1)\big)\cdot(a_2+u(3b_2)+v(3c_2))\\ &= \varphi(x)\cdot\varphi(y)\end{aligned}$$

olduğundan φ bir homomorfizmdir.

$$\begin{aligned}\text{Çek}\varphi &= \{a+ub+vc \in S_2 :\ \varphi(a+ub+vc)=0\}\\ &= \{a+ub+vc \in S_2 :\ a+u(3b)+v(3c)=0\}\\ &= \{a+ub+vc \in S_2 :\ a=0,\ b=0,\ c=0\}\\ &= \{0\}\end{aligned}$$

olduğundan φ birebirdir.

Her $a+u(3b)+v(3c) \in S_2$ için $\varphi(a+ub+vc)=a+u(3b)+v(3c)$ olacak şekilde bir $a+ub+vc \in S_2$ var olduğundan φ örtendir.

O halde φ dönüşümü bir otomorfizmdir. Her $x=a+ub+vc \in S_2$ için

$$\begin{aligned}\varphi^2(a+ub+vc) &= \varphi(\varphi(a+ub+vc)) \\ &= \varphi(a+u(3b)+u(3c)) \\ &= a+u3(3b)+u3(3c) \\ &= a+ub+vc\end{aligned}$$

olduğundan $\varphi^2(x)=x$ dir. Dolayısıyla φ nin derecesi 2 dir.

Lemma 4.2.1 s, S_2 halkasında birimsel eleman ise $\varphi(s)$ de S_2 halkasında birimsel elemandır.

Lemma 4.2.2 $S_2{}^{\varphi}=\{a+ub+vc : b,c \in \{0,2\}\}$, S_2 nin φ otomorfizmi tarafından sabit bırakılan bir alt halkasıdır.

İspat. $x=a_1+ub_1+vc_1$, $y=a_2+ub_2+vc_2 \in S_2{}^{\varphi}$ alalım. O zaman $a_1,a_2 \in \mathbb{Z}_4$ ve $b_1,b_2,c_1,c_2 \in \{0,2\}$ olur. $(a_1+a_2) \in \mathbb{Z}_4$, $(b_1+b_2) \in \{0,2\}$, $(c_1+c_2) \in \{0,2\}$ olup $x+y=(a_1+a_2)+u(b_1+b_2)+v(c_1+c_2) \in S_2{}^{\varphi}$ bulunur. $a_1a_2+b_1b_2+c_1c_2 \in \mathbb{Z}_4$, $a_1b_2+b_1a_2 \in \{0,2\}$, $a_1c_2+c_1a_2 \in \{0,2\}$ olup

$$\begin{aligned}x.y &= (a_1+ub_1+vc_1)(a_2+ub_2+vc_2) \\ &= a_1a_2+ua_1b_2+va_1c_2+ub_1a_2+b_1b_2+vc_1a_2+c_1c_2 \\ &= (a_1a_2+b_1b_2+c_1c_2)+u(a_1b_2+b_1a_2)+v(a_1c_2+c_1a_2) \in S_2{}^{\varphi}\end{aligned}$$

olduğundan $S_2{}^{\varphi}$, S_2 nin bir alt halkasıdır. $a+ub+vc \in S^{\varphi}$ ise $b,c \in \{0,2\}$ olup $3b,3c \in \{0,2\}$ dir. $\varphi(a+ub+vc)=a+u(3b)+v(3c)$ olup $a+ub+vc$ nin φ altında sabit kalması için $b,c \in \{0,2\}$ olmasıdır.

$S_2[x,\varphi] = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} : \ a_i \in S_2, \ n \in \mathbb{N}\}$ kümesi üzerindeki toplama bilinen polinom toplaması olarak ve çarpma işlemi ise

$$\left(ax^i\right) \cdot \left(bx^j\right) = a\varphi^i(b).x^{i+j}$$

şeklinde tanımlansın. Bu çarpma işlemi $S_2[x,\varphi]$ kümesinin tüm elemanlarına lineer olarak genişletilebilir. $S_2[x,\varphi]$ kümesi bu işlemlerle bir aykırı polinom halkasıdır.

Teorem 4.2.3 $Z(S_2) = \left\{\sum_{i=0}^{m} \alpha_i x^{2i} : \ \alpha_i \in {S_2}^{\varphi}\right\}$ dir.

İspat. $D = \left\{\sum_{i=0}^{l} d_i x^{2i} \mid d_i \in {S_2}^{\varphi}\right\}$ ve $p = \sum_{i=0}^{l} d_i x^{2i} | d_i \in D$ olsun. Negatif olmayan herhangi bir i ve her $d_i \in S_2$ için φ otomorfizminin derecesi 2 olduğundan $x^{2i}d_i = (\varphi^2)^i(d_i)x^{2i} = d_i x^{2i}$ olduğu elde edilir. Bu $x^{2i} \in Z(S_2)$ olmasını gerektirir. Dolayısıyla $p = d_0 + d_1x^2 + \cdots + d_lx^{2l}$ formundaki tüm polinomların $Z(S_2)$ olduğunu gösterir. Tersine, $p = p_0 + p_1x + \cdots + p_kx^k \in Z(S_2)$ olsun. Bu durumda $xp = px$ dir. Dolayısıyla, tüm p_i ler φ tarafından sabit bırakılır ve $p_i \in {S_2}^{\varphi}$ dir. Ayrıca, $\varphi(d_i) \neq d_i$ olacak şekilde bir $d_i \in S$ olarak seçilirse, $d_ip = pd_i$ bağıntısından 2 ile bölünemeyen tüm i indisleri için $p_i = 0$ olur. Dolayısıyla, $p = p_0 + p_2x^2 + p_4x^4 + \cdots + p_lx^{2l} \in D$ elde edilir. Buradan $Z(S_2) \subseteq D$ olduğundan, ispat tamamlanır.

Sonuç 4.2.4 $x^m - 1 \in Z(S_2)$ olması için gerek ve yeter koşul $2|m$ olmasıdır.

Örnek 4.2.5 $p(x) = (1 + 3u + 3v)x^2 + u, \quad q(x) = (1 + u + v)x$ için $p(x) = xq(x) + u$ ve $p(x) = (1 + 2u + 2v)x + q(x) + u$ olduğundan $S_2[x,\varphi]$ halkası, öklidyen halka değildir.

Tanım 4.2.6 $C \subseteq {S_2}^n$ olsun. Eğer C, ${S_2}^n$ nin bir altmodülü ve her $c = (c_1, c_2, \ldots, c_n) \in C$ için $\sigma(c) = \left(\varphi(c_n), \varphi(c_1), \ldots, \varphi(c_{n-1})\right) \in C$ oluyorsa C, n uzunluklu bir aykırı devirli kod (φ −devirli kod) dur.

Örnek 4.2.7

$$C=\left\{\begin{array}{c}(0,0),(0,2),(2,0),(2,2),(0,2u),(2u,0),(2u,2u),(0,2v),(2v,0),(2v,2v)\\(2,2u),(2u,2),(2,2v),(2v,2),(2u,2v),(2v,2u),(0,2+2u),(2+2u,0)\\(2+2u,2+2u),(0,2+2v),(2+2v,0),(2+2v,2+2v),(2,2+2u),\\(2+2u,2),(2,2+2v),(2+2v,2),(2u+2v,0),(0,2u+2v),\\(2u,2+2v),(2+2v,2u),(2v,2+2v),(2+2v,2v),(2u,2u+2v),\\(2u+2v,2u),(2u+2v,2+2u),(2+2u,2u+2v),(2u+2v,2+2v)\\(2+2v,2u+2v),(2+2u,2+2v),(2+2v,2+2u),(2u+2v,2u+2v)\\(0,2+2u+2v),(2+2u+2v,0),(2,2+2u+2v),(2+2u+2v,2),\\(2u,2+2u+2v),(2+2u+2v,2u),(2v,2+2u+2v),(2+2u+2v,2v),\\(2+2u,2+2u+2v),(2+2u+2v,2+2u),(2+2v,2+2u+2v)\\(2+2u+2v,2+2v),(2u+2v,2+2u+2v),\\(2+2u+2v,2+2u+2v)\end{array}\right\},$$

S_2 halkası üzerinde 2 uzunluklu bir aykırı devirli koddur.

$f(x),g(x)\in S_2[x,\varphi]$ ve $g(x)$ in başkatsayısı birimsel olsun. O zaman $r(x)=0$ veya $\text{der}(r(x))<der\big(g(x)\big)$ olmak üzere $f(x)=q(x)g(x)+r(x)$ olacak şekilde $q(x),r(x)\in S_2[x,\varphi]$ vardır.

$p(x)$, S_2 üzerinde derecesi n olan bir polinom olmak üzere ${S_2}^n=S_2[x,\varphi]/\langle p(x)\rangle$ olsun. ${S_2}^n$, $r(x)(c(x)+\langle p(x)\rangle)=r(x)c(x)+\langle p(x)\rangle$ işlemiyle bir sol $S_2[x,\varphi]$ −modüldür.

Teorem 4.2.8 $S_2[x,\varphi]/\langle x^n-1\rangle$ de n uzunluklu bir C kodunun bir $\varphi-$ devirli kod olması için gerek ve yeter koşul C nin ${S_2}^n$ $S_2[x,\varphi]$ −modülünün bir sol $S_2[x,\varphi]$ −altmodülü olmasıdır.

İspat. Teorem 4.1.13 ün ispatına benzer şekilde yapılır.

Sonuç 4.2.9 n bir çift doğal sayı olmak üzere eğer C, $S_2[x,\varphi]/\langle x^n-1\rangle$ de n uzunluklu aykırı devirli kod ise o zaman C, $S_1[x,\varphi]/\langle x^n-1\rangle$ nin bir idealidir.

İspat. Sonuç 4.1.14 ün ispatına benzer şekilde yapılır.

Teorem 4.2.10 C, $S_2[x,\varphi]/\langle x^n-1\rangle$ de n uzunluklu aykırı devirli kod ve $f(x)$ de C de başkatsayısı birimsel eleman olan minimal dereceli polinom olsun. Eğer $f(x), x^n-1$ polinomunun bir sağ böleni ise $C=\langle f(x)\rangle$ dir ve $\{f(x),\ xf(x),\ x^2f(x),\ \dots,\ x^{n-\mathrm{der}(f(x))-1}f(x)\}$ kümesi C için bir bazdır.

$C=\langle f(x)\rangle$, x^n-1 polinomunun bir sağ böleni tarafından üretilen S_2 üzerinde bir n - uzunluklu $\varphi-$ devirli kod olsun. $f(x)=f_0+f_1x+f_2x^2+\cdots+f_kx^k$ olmak üzere C kodunun üreteç matrisi

$$\begin{bmatrix} f(x) \\ xf(x) \\ x^2f(x) \\ \vdots \\ x^{n-k-1}f(x) \end{bmatrix}_{(n-k)\times n}$$

şeklindedir. Daha açık şekilde ifade edilirse eğer $n-k$ çift ise

$$G=\begin{bmatrix} f_0 & f_1 & f_2 & \cdots & f_k & 0 & 0 & \cdots & 0 \\ 0 & \varphi(f_0) & \varphi(f_1) & \cdots & \varphi(f_{k-1}) & \varphi(f_k) & 0 & \cdots & 0 \\ 0 & 0 & f_0 & \cdots & f_{k-2} & f_{k-1} & f_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \varphi(f_0) & \varphi(f_1) & \varphi(f_2) & \cdots & \varphi(f_k) \end{bmatrix}$$

ve eğer $n-k$ tek ise

$$G=\begin{bmatrix} f_0 & f_1 & f_2 & \cdots & f_k & 0 & 0 & \cdots & 0 \\ 0 & \varphi(f_0) & \varphi(f_1) & \cdots & \varphi(f_{k-1}) & \varphi(f_k) & 0 & \cdots & 0 \\ 0 & 0 & f_0 & \cdots & f_{k-2} & f_{k-1} & f_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & f_0 & f_1 & f_2 & \cdots & f_k \end{bmatrix}$$

şeklindedir.

Örnek 4.2.11 C, $x^{10}-1$ in sağ böleni olan

$$f(x) = (2+u+2v)x^5+(2+2v)x^4+(2+2v)x^3+(2+2v)x^2+ (2+2v)x+(2+3u+2v)$$

tarafından üretilen S_2 üzerindeki 10 uzunluklu bir $\varphi-$devirli kod olsun. $k=5$ olduğundan C kodunun baz kümesi $\{g(x), xg(x), x^2g(x), x^3g(x), x^4g(x)\}$ dir.

$$xg(x) = x.(2+u+2v)x^5+x.(2+2v)x^4+x.(2+2v)x^3+x.(2+2v)x^2 + x.(2+2v)x+x.(2+3u+2v)$$

$$= \varphi(2+u+2v)x^6+\varphi(2+2v)x^5+\varphi(2+2v)x^4+\varphi(2+2v)x^3 + \varphi(2+2v)x^2+\varphi(2+3u+2v)x$$

$$= (2+3u+2v)x^6+(2+2v)x^5+(2+2v)x^4+(2+2v)x^3 + (2+2v)x^2+(2+u+2v)x$$

$$x^2g(x) = x^2(2+u+2v)x^5+x^2(2+2v)x^4+x^2(2+2v)x^3+x^2(2+2v)x^2 +x^2(2+2v)x+x^2(2+3u+2v)$$

$$= \varphi^2(2+u+2v)x^7+\varphi^2(2+2v)x^6+\varphi^2(2+2v)x^5 + \varphi^2(2+2v)x^4+\varphi^2(2+2v)x^3+\varphi^2(2+3u+2v)x^2$$

$$= (2+u+2v)x^7+(2+2v)x^6+(2+2v)x^5+(2+2v)x^4 + (2+2v)x^3+(2+3u+2v)x^2$$

$$x^3g(x) = x^3(2+u+2v)x^5+x^3(2+2v)x^4+x^3(2+2v)x^3+x^3(2+2v)x^2 +x^3(2+2v)x+x^3(2+3u+2v)$$

$$= \varphi^3(2+u+2v)x^8+\varphi^3(2+2v)x^7+\varphi^3(2+2v)x^6 +\varphi^3(2+2v)x^5+\varphi^3(2+2v)x^4+\varphi^3(2+3u+2v)x^3$$

$$= (2+3u+2v)x^8+(2+2v)x^7+(2+2v)x^6+(2+2v)x^5 +(2+2v)x^4+(2+u+2v)x^3$$

$$x^4 g(x) = x^4(2+u+2v)x^5 + x^4(2+2v)x^4 + x^4(2+2v)x^3 + x^4(2+2v)x^2$$
$$+x^4(2+2v)x + x^4(2+3u+2v)$$
$$= \varphi^4(2+u+2v)x^9 + \varphi^4(2+2v)x^8 + \varphi^4(2+2v)x^7$$
$$+ \varphi^4(2+2v)x^6 + \varphi^4(2+2v)x^5 + \varphi^4(2+3u+2v)x^4$$
$$= (2+u+2v)x^9 + (2+2v)x^8 + (2+2v)x^7 + (2+2v)x^6$$
$$+(2+2v)x^5 + (2+3u+2v)x^4$$

olduğundan $C = \langle g(x) \rangle$ kodu için üreteç matrisi,

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \\ x^4 g(x) \end{bmatrix}$$

$$= \begin{bmatrix} 2+3u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+u+2v & 0 & 0 & 0 & 0 \\ 0 & 2+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+3u+2v & 0 & 0 & 0 \\ 0 & 0 & 2+3u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+u+2v & 0 & 0 \\ 0 & 0 & 0 & 2+u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+3u+2v & 0 \\ 0 & 0 & 0 & 0 & 2+3u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+u+2v \end{bmatrix}$$

dir. Üreteç matrisinin Gray dönüşümü;

$$\begin{bmatrix} 220 & 220 & 220 & 220 & 220 & 220 & 000 & 000 & 000 & 000 \\ 000 & 230 & 220 & 220 & 220 & 220 & 210 & 000 & 000 & 000 \\ 000 & 000 & 210 & 220 & 220 & 220 & 220 & 210 & 000 & 000 \\ 000 & 000 & 000 & 220 & 220 & 220 & 220 & 220 & 210 & 000 \\ 000 & 000 & 000 & 000 & 210 & 220 & 220 & 220 & 220 & 230 \end{bmatrix}$$

dir.

Örnek 4.2.12 C, $x^{10}-1$ in sağ böleni olan

$$h(x)=(2+u+2v)x^5+(2+2v)x^4+(2+2v)x^3+(2+2v)x^2+(2+2v)x+(2+u+2v)$$

tarafından üretilen S_2 üzerindeki 10 uzunluklu bir $\varphi-$ devirli kod olsun.

$k=5\ (\mathrm{der}(h(x))=5),\quad n=10$ olup $(x^{n-k-1}=x^{10-5-1}=x^4)$

$\{h(x),xh(x),x^2h(x),x^3h(x),x^4h(x)\}$ olan bir devirli kod üretir. $C=\langle h(x)\rangle$ kodu için kontrol matrisi,

$$H=\begin{bmatrix}h(x)\\xh(x)\\x^2h(x)\\x^3h(x)\\x^4h(x)\end{bmatrix}$$

$$=\begin{bmatrix}2+u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+u+2v & 0 & 0 & 0 & 0\\ 0 & 2+3u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+3u+2v & 0 & 0 & 0\\ 0 & 0 & 2+u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+u+2v & 0 & 0\\ 0 & 0 & 0 & 2+3u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+3u+2v & 0\\ 0 & 0 & 0 & 0 & 2+u+2v & 2+2v & 2+2v & 2+2v & 2+2v & 2+u+2v\end{bmatrix}$$

şeklindedir.

5. SONUÇLAR VE ÖNERİLER

Bu tezde öncelikle bir otomorfizm kullanılarak tanımlanan aykırı polinom halkalarının cebirsel özellikleri incelenerek bu halkalar üzerindeki aykırı devirli kodlar araştırılmıştır.

Bu tezin üçüncü bölümünde $u^2 = 1$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerindeki $\theta(a + ub) = a + (u + 2)b$ otomorfizmi ve δ_θ türetimi kullanılarak tanımlanan aykırı polinom halkasının cebirsel özellikleri incelenmiş, bu halka üzerindeki aykırı devirli kodların üreteç ve kontrol matrisleri verilmiştir [11].

Bu tezin dördüncü bölümünde $u^2 = u, \quad v^2 = v, \quad uv = vu = 0$ olmak üzere $\theta(a + ub + vc) = a + uc + vb$ otomorfizmi kullanılarak $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki aykırı polinom halkası tanımlanmış, bu halka üzerindeki aykırı devirli kodlar çalışılmış ve bu kodların üreteç ve kontrol matrisleri verilmiştir [13]. Ayrıca $u^2 = 1, \ v^2 = 1, \ uv = vu = 0$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki aykırı polinom halkası $\theta(a + ub + vc) = a + u(3b) + v(3c)$ otomorfizmi kullanılarak tanımlanmış ve bu halkanın özellikleri incelenmiş, bu halka üzerindeki aykırı devirli kodlar çalışılmış ve bu kodların üreteç ve kontrol matrisleri verilmiştir.

Bu tezdeki çalışmalar $\mathbb{Z}_{2^s} + u\mathbb{Z}_{2^s} + v\mathbb{Z}_{2^s}$ halkasına genellenebilir. Ayrıca başka halkalar üzerindeki aykırı devirli kodlar çalışılabilir, bu kodların üreteç ve kontrol matrislerinin yapısı araştırılabilir.

KAYNAKLAR

[1] Shannon, C.E., A mathematical theory of communication, The Bell System Technical Journal, 27, 379-423, 1948.

[2] Haming, R.W., error detecting and error-correcting codes, The Bell System Technical Journal, 29, 147-160, 1950.

[3] Gilbert, E.N., A comparision of signalling alphabets, The Bell System Technical Journal, 31, 504-522, 1952.

[4] Varshanov, R.R., Estimate of the number of signals in error-correcting codes, Doklady Akademii Nauk SSSR, 117, 739-741, 1957.

[5] Prange, E., Cyclic error-correcting codes in two symbols, Technical Notes AFCRL, TN 57-103, 1957.

[6] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J., Sole, P., The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethalsand related codes, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 40, 301-319, 1994.

[7] Özen, M., Uzekmek, F.Z., Aydın, N., Özzaim, N. T., Cyclic and some constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$, Finite Fields and Their Applications, 38, 27-39, 2016.

[8] Yıldız, B., Aydın, N., On codes over $\mathbb{Z}_4+u\mathbb{Z}_4$ and their $\mathbb{Z}_4$ −images, Int. Journal Inf. Coding Theory, 2, 226-237, 2014.

[9] Yıldız, B., Karadeniz, S., Linear codes over $\mathbb{Z}_4+u\mathbb{Z}_4$: MacWilliams identities and formally self dual codes, Finite Fields Appl., 27, 24–40, 2014.

[10] Boucher, D., Geiselmann, W., Ulmer, F., Skew cyclic codes, Applicable Algebra in Engineering, Communication and Computing, 18(4), 379–389, 2007.

[11] Sharma, A., Bhaintwal, M., A class of skew-cyclic codes over Z4 + uZ4 with derivation, Advanced in Mathematics of Communications, 12(4), 723-739, 2018.

[12] Çalışkan, B., Türetim ile $\mathbb{Z}_{2^s} + u\mathbb{Z}_{2^s}$ halkası üzerindeki, aykırı devirli kodlar, Çanakkale Onsekiz Mart Üniversity Journal of Afvanced Researc in Natural and Applied Science s Open Access, 2020.

[13] Dertli, A., Çengellenmiş, Y., On the codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ cyclic, constacylic, quasi-cyclic, codes, their skew codes, cyclic DNA&skew cyclic DNA codes, Prespacetime Journal, 10(2), 196-213, 2019.

[14] Mohammadi, R., Rahimi, S., Mousavi, H., On skew cyclic codes over a finite ring, Iranian Journal of Mathematical Sciences an Informatics, 14(1), 135-145, 2019.

[15] Roman, S., Coding and Information Theory, Springer-Verlag, New York, 1992.

[16] Ore, O., Theory of non-commutative polynomials, Annals of Mathematics, 34, 480-508, 1933.

[17] Jacobson, N., The Theory of Rings, American Mathematical Society, Newyork, 1943.

[18] Mcdonald, B.R., Finite Rings with İdentity, Marcel Dekker Inc, NewYork, 1974.

[19] Şiap, İ., Abualrub, T., Aydın, N., Seneviratne, P., Skew cyclic codes of arbitrary length, International Journal of Information and Coding Theory, 2, 10-20, 2011.

[20] Boucher, D., Ulmer, F., A note on the dual codes of module skew codes, Lecture Notes in Computer Science. 7089, 230–243, 2011.

[21] Gürsoy, F., Değişmeli olmayan aykırı polinom halkaları üzerinde tanımlı DNA kodlar, , Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi,. İstanbul, 67, 2019.

[22] Boucher, D., Ulmer, F., Coding with skew polynomial rings, Journal of Symbolic Computation. 44, 1644–1656, 2009.

[23] Gürsoy, F., Şiap, İ., Yldız, B., Construction of skewcyclic codes over $F_q + vF_q$, Advanced in Mathematics of Communications. 8(3), 313–322, 2014.

ÖZGEÇMİŞ

1. Adı Soyadı **:** Nesibe YILMAZ

2. Doğum Tarihi **:**

3. Ünvanı **:** Matematik Öğretmeni

4. Öğrenim Durumu **:** Lisans

Derece	**Bölüm/Program**	**Üniversite**	**Bitirme Yılı**
Lisans	Matematik	Mustafa Kemal Üniversitesi	2015

6.İş Tecrübesi:

Görev Unvanı	**Görev Yeri**	**Yıl**
Matematik Öğretmeni		2015
Matematik Öğretmeni		2018
Matematik Öğretmeni		2021

OSMANİYE KORKUT ATA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

FORM YL11

OSMANİYE KORKUT ATA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 31/08/2022

Tez Başlığı / Konusu: BAZI HALKALAR ÜZERİNDEKİ AYKIRI DEVİRLİ KODLAR

Yukarıda başlığı/konusu belirlenen tez çalışmamın a) Kapak sayfası, b) Özet ve Abstract, c) Giriş, d) Ana bölümler ve e) Sonuç, f) Kaynakça kısımlarından oluşan toplam 68 sayfalık kısmına ilişkin, 31/08/2022 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtreleme tiplerinden biri uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % **29** 'tür.

Filtreleme Tip 1 (maksimum %30) ☒	**Filtreleme Tip 2 (maksimum %10)** ☐
1- Kabul/Onay ve Bildirim sayfaları hariç, 2- Kaynakça hariç, 3- Alıntılar dahil, 4- 5 kelimeden daha az örtüşme içeren metin kısımları hariç.	1- Kabul/Onay ve Bildirim sayfaları hariç, 2- Kaynakça hariç, 3- Alıntılar hariç, 4- 5 Kelimeden daha az örtüşme içeren metin kısımları hariç.

Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Tez Çalışması Orjinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

Adı Soyadı: Nesibe YILMAZ
Öğrenci No:
Anabilim Dalı: Matematik
Programı: Matematik
Statüsü: ☒ Y.Lisans ☐ Doktora

DANIŞMAN ONAYI

UYGUNDUR.

(Unvan, Ad Soyad, İmza)

RAPORU DÜZENLEYEN

(Unvan, Ad Soyad, İmza)