T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KUATERNİYON HALKALARI ÜZERİNDE LİNEER KODLAR

SEDA AKBIYIK

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
PROF. DR. BAYRAM ALİ ERSOY

İSTANBUL, 2018

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KUATERNİYON HALKALARI ÜZERİNDE LİNEER KODLAR

Seda AKBIYIK tarafından hazırlanan tez çalışması 08/06/2018 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

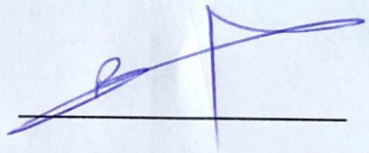
Prof. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi

Jüri Üyeleri

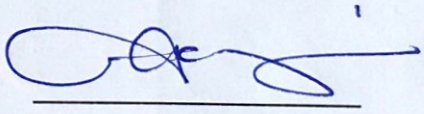
Prof. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi



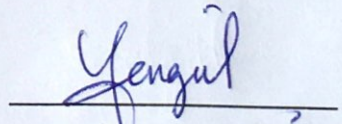
Prof. Dr. A. Göksel AĞARGÜN

Yıldız Teknik Üniversitesi



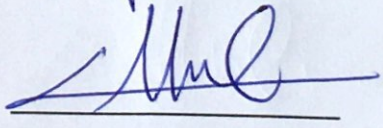
Doç. Dr. Uğur ŞENGÜL

Marmara Üniversitesi



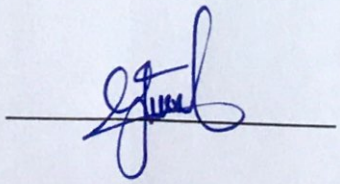
Prof. Dr. Mehmet ÖZEN

Sakarya Üniversitesi



Doç. Dr. Gürsel YEŞİLOT

Yıldız Teknik Üniversitesi



ÖNSÖZ

Doktora tez çalışmam sırasında verdiği desteklerinden dolayı danışman hocam sayın Prof. Dr. Bayram Ali Ersoy'a teşekkürlerimi sunarım.

Ayrıca, Tez İzleme Komitemdeki saygıdeğer hocalarım Prof. Dr. A. Göksel Ağargün'e ve Doç. Dr. Uğur Şengül'e; kıymetli hocam Prof. Dr. Ünsal Tekir'e verdikleri destek ve yönlendirmelerinden ötürü teşekkürlerimi sunarım.

Başta bu zorlu süreç olmak üzere hayatım boyunca her konuda maddi ve manevi desteklerini ve dualarını benden esirgemeyen, kıymetli annem Senem Yamaç'a ve babam Sıddık Yamaç'a, kardeşim ve ablama; varlığıyla yüksek motivasyon kaynağım olan eşim Arş. Gör. Mücahit Akbıyık'a ve biricik oğlum Yavuz Kaan Akbıyık'a sonsuz teşekkürlerimi sunarım.

Haziran, 2018

Seda AKBIYIK

İÇİNDEKİLER

SİMGE LİSTESİ

R	Halka
$\mathbb{Z}$	Tamsayılar Halkası
$\mathbb{R}$	Reel Sayılar Cismi
$\mathbb{C}$	Karmaşık Sayılar Cismi
F	Cisim
F_q	Sonlu Cisim
$\mathbb{Z}_n$	Tamsayıların n ile Bölümünden Kalanların Kümesi
$M_n(\mathbb{R})$	Girdileri Reel Sayılar Cismi Olan $n \times n$ lik Kare Matrislerin Halkası
$2\mathbb{Z}$	Çift Tamsayıların Halkası
0_R	R Halkasının Sıfır Elemanı
1_R	R Halkasının Birim Elemanı
$\varnothing$	Boş Küme
I	R Halkasının İdeali
(A)	A Kümesinin Ürettiği İdeal
R/I	Bölüm Halkası
R^n	R Halkasının Elemanlarının n lilerinden Oluşan Küme
$\mathbb{R}^+$	Pozitif Reel Sayılar
$kar(F)$	F Cisminin Karakteristiği
$\lvert F \rvert$	F Cisminin Eleman Sayısı
V	Vektör Uzayı
$F_q^{\,n}$	F Cisminin Elemanlarının n lilerinden Oluşan Küme
$boy(V)$	V Vektör Uzayının Boyutu
$\mathbb{R}^n$	$\mathbb{R}$ Cisminin Elemanlarının n lilerinden Oluşan Küme
$S^{\perp}$	S Kümesinin Dik Tümleyeni
$\langle \cdot, \cdot \rangle$	İki Vektörün İç Çarpımı

C	Kod
$d(\cdot,\cdot)$	İki Vektörün Arasındaki Minimum Hamming Uzaklık
$w(x)$	x Vektörünün Hamming Ağırlığı
$d(C)$	C Kodunun Minimum Hamming Uzaklığı
$w(C)$	C Kodunun Minimum Hamming Ağırlığı
(n,M,d)	Kodun Parametreleri
$[n,k,d]_q$	Lineer Kodun Parametreleri
G	Üreteç Matrisi
H	Kontrol Matrisi
π	H_3^n den $H_3[x]/(x^n-1)$ e Lineer Dönüşüm
π_λ	H_3^n den $H_3[x]/(x^n-\lambda)$ e Lineer Dönüşüm
π_v	H_3^n den $H_3[x]/(x^n-v(x))$ e Lineer Dönüşüm
$g(x)$	Üreteç Polinom
$h^R(x)$	$h(x)$ Polinomunun Ters Sıralı (Reciprocal) Polinomu
$der(g(x))$	$g(x)$ Polinomunun Derecesi
q	Kuaterniyon
q^{-1}	q Kuaterniyonunun Tersi
H_3	Sonlu Kuaterniyonlar Halkası
$\cdot_L$	Sonlu Kuaterniyonların Sol Çarpma İşlemi
$\overline{q}$	q Sonlu Kuaterniyonunun Eşleniği
$\|q\|$	q Sonlu Kuaterniyonunun Normu
$\{e_1,e_2\}$	H_3 Halkasının Merkezi İdempotent Çifti
F_9	9 Elemanlı Cisim
H_3^n	H_3 Halkasının Elemanlarının n lilerinden Oluşan Küme
$d_L(C)$	C Kodunun Minimum Lee Uzaklığı
$w_L(q)$	q Sonlu Kuaterniyonunun Lee Ağırlığı

ŞEKİL LİSTESİ

Sayfa

ÖZET

KUATERNİYON HALKALARI ÜZERİNDE LİNEER KODLAR

Seda AKBIYIK

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Prof. Dr. Bayram Ali ERSOY

Dijital bilgi transferi ve depolanmasının artmasıyla son yıllarda Cebirsel Kodlama Teorisi birçok araştırmacı tarafından ilgi görmektedir. Bu transfer ya da depolama esnasında kanalda meydana gelebilecek herhangi bir gürültü nedeniyle gönderilen mesaj değişikliğe uğrar. Bu nedenle hata meydana gelerek alınan mesaj gönderilenden farklı olana hatalı mesaj haline dönüşür. Kodlama Teorisi ya da Hata Düzelten Kodlar Teorisi bu hataları en aza indirmek, alınan sözü doğru bir şekilde hatalarını düzeltmekle ilgilenmektedir. Matematiğin birçok alt dalıyla ilişkili olan bu disiplinler arası alanda ilk çalışma 1948 yılında Shannon tarafından yapılmıştır. Bunu takip eden birçok çalışma ile kodlama teorisi cisimler, halkalar gibi farklı cebirsel yapılar üzerinde çalışılmıştır. Başlangıçta sonlu cisimler üzerinde yapılan çalışmalar ilk olarak Hammons ve arkadaşları tarafından halkalara taşınmıştır.

Kuaterniyonlar ilk olarak Hamilton tarafından 1847 yılında tanıtılmıştır. Vektörlerde bölme işlemi yapılmasını sağlayan bu yapı birçok matematikçi tarafından ilgi görmüştür. Son yıllarda kodlama teorisi alanında çalışma yapan araştırmacılar, Kuaterniyon tamsayıları adı verdikleri, katsayıları tamsayılardan oluşan halka üzerinde lineer kodların ve daha pek çok kod ailelerinin inşaalarını vermiş ve dekodlama teknikleri geliştirmişlerdir.

Bu tezde sonlu kuaterniyonlar halkası adı verilen, $\mathbb{Z}_3$ sonlu cisminden katsayılı halka incelenmiştir. Önce cebirsel özellikleri ele alınan halkanın sonlu, değişmeli olmayan ve

zincir halkası olmayan bir halka olduğu gösterilmiştir. Bu halkanın elemanlarının n lilerinin oluşturduğu H_3^n modülü üzerinde kodlar çalışılmıştır. Lineer kodlar bu yapı üzerinde inşaa edilmiş ve standart forma üreteç matris verilerek parametreleri belirlenmiştir. Öte yandan H_3^n üzerinde devirli kodlar, sabit devirli kodlar ve çoklu devirli kodlar çalışılmış ve bu kodlar için parametreler verilmiştir.

Anahtar Kelimeler: Kuaterniyonlar, değişmeli olmayan sonlu halka üzerinde lineer kodlar, devirli kodlar, sabit devirli kodlar, çoklu devirli kodlar.

ABSTRACT

LINEAR CODES OVER QUATERNION RINGS

Seda AKBIYIK

Department of Mathematics

PhD. Thesis

Advisor: Prof. Dr. Bayram Ali ERSOY

In recent years, Algebraic Coding Theory has attracted many researchers due to the increase of digital information transfer and storage. The message sent due to any noise that may occur in the channel during this transfer or storage is subject to change. For this reason, the error occurs and the received message becomes different from the one sent. The Coding Theory or the Error Correcting Codes Theory deals with correcting these errors to the best of their ability, correcting errors correctly. This interdisciplinary field study, which is associated with many subdivisions of mathematics, was first conducted by Shannon in 1948. In the following many studies, coding theory has been studied on different algebraic structures such as fields, rings. Initially, studies on finite fields were first generalized to rings by Hammons et al. [4].

Quaternions were first introduced by Hamilton in 1847. This structure, which allows dividing two vectors, has attracted many mathematicians. In recent years, researchers working in the field of coding theory have given the construction of linear codes and many more code families, called quaternion integers, coefficients on integers, and developed decoding techniques.

In this thesis, the ring of quaternions with coefficients from $\mathbb{Z}_3$ called finite quaternions ring has been studied. It has been shown that the ring, first of all algebraic properties, is a finite, non commutative and non chain ring. Codes have been worked on the module of the elements of this ring. Linear codes are constructed on this

structure and the parameters are determined by giving the generator matrix to the standard form. Moreover, cyclic codes, constacyclic codes and polycyclic codes have been studied and parameters have been given for these codes.

Keywords: Quaternions, linear codes on the non commutative finite ring, cyclic codes, constacyclic codes, polycyclic codes.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Kodlama teorisi, kodların özelliklerinin ve belirli uygulamalara yönelik uygunluklarının incelenmesidir. Kodlar, veri sıkıştırma, şifreleme, hata düzeltme ve ağ iletişimi için kullanılmaktadır. Kodlar, bilgi teorisi, elektrik mühendisliği, matematik, dilbilim ve bilgisayar bilimi gibi çeşitli bilimsel disiplinler tarafından, verimli ve güvenilir veri aktarım yöntemleri tasarlama amacıyla incelenmiştir. Temel amaç ise, iletilen verilerdeki hataların düzeltilmesi veya tespit edilmesidir. Dört tür kodlama vardır; veri sıkıştırma (veya kaynak kodlama), hata kontrolü (veya kanal kodlaması), kriptografik kodlama, satır kodlama. Veri sıkıştırma, verileri daha verimli bir şekilde iletmek için, bir kaynaktan sıkıştırmaya çalışmaktadır. Örneğin, Zip veri sıkıştırması, internet trafiğini azaltmak için veri dosyalarını küçültür. Veri sıkıştırma ve hata düzeltme birlikte çalışılabilmektedir. Hata düzeltme, veri aktarım kanalında mevcut olan gürütülere karşı kodun dayanıklı olabilmesi için koda ekstra veri bitleri eklemektedir. Sıradan bir kullanıcı hata düzeltme kodları kullanıldığında günlük hayatta birçok hatanın farkında olmayabilir. Örneğin, tipik bir müzik CD'si çizik ve tozu düzeltmek için Reed-Solomon kodunu kullanmaktadır. Bu uygulamada iletim kanalı CD'nin kendisidir. Cep telefonları, yüksek frekanslı radyo iletiminin hatalarını düzeltmek için kodlama tekniklerini kullanmaktadır. Veri modemleri, telefon aktarımları ve NASA, turbo kodu ve LDPC kodları gibi, verileri elde etmek için kanal kodlama tekniklerini kullanmaktadır.

Cebirsel kodlama teorisi alanında ilk çalışma 1948 yılında Claude Shannon [1] tarafından yapılmıştır. Shannon , “Bell System Technical Journal” adlı derginin Temmuz

ve Ekim aylarında iki bölümden oluşan bir makale olan "A Mathematical Theory of Communication" adlı çalışmasını yayınlanmıştır. Bu çalışma, bir gönderenin iletmek istediği bilgileri en iyi nasıl kodlayacağı problemine odaklanmaktadır. Bu temel çalışmada, Norbert Wiener tarafından geliştirilen ve o zamanın iletişim teorisine uygulanma aşamasında olan olasılık teorisindeki yöntemler kullanmıştır. Shannon, bilgi teorisi (information theory) alanını icat ederken bir mesajdaki belirsizlik için bir ölçü olarak bilgi entropisini geliştirmiştir. Sonrasında, 1949'da ikili Golay kodu geliştirilmiştir [2]. Bu kod, her 24 bitlik kelimede en fazla üç hatayı düzeltebilen ve dört hatayı tespit eden bir hata düzeltme kodudur. 1968'de Richard Hamming [3], Bell Labs'deki çalışmaları için sayısal yöntemler, otomatik kodlama sistemleri ve hata tespiti ve hata düzeltme kodları ile Turing Ödülü'nü kazandı. Hamming kodları , Hamming ağırlık ve Hamming mesafesi olarak bilinen kavramları icat etmiştir. Hata düzeltme kapasitesi yüksek kodlar arayışı, uzun yıllar boyunca cisimler üzerinde devam etmiştir. 1994 yılında Hammons ve arkadaşları [4], halkalar üzerinde kodları tanımlayarak kodlama teorisine yeni ve geniş bir çalışma alanı sunmuşlardır. Halkalar üzerinde, cisimler üzerindeki kodlara göre çok daha iyi parametrelere sahip kodlar bulunması bu bakış açısını kuvvetlendirmiştir. Bu çalışma dışında halkalar üzerinde birçok kodlama çalışması yapılmıştır [5-14].

1994 yılında Huber [7] tarafından Gauss tamsayılar halkası üzerinde yapılan çalışma sonrasında birçok çalışmaya ışık tutmuştur. Bu makalede Huber, Gauss tamsayıları üzerinde Manheimm metrik ve Manheimm ağırlık tanımlayarak lineer kodları çalışmıştır. Hemen arkasından bu çalışmasını Eistein-Jacobi tamsayıları halkasına genişletmesi [15], araştırmacıları farklı sayı halkaları üzerinde çalışmaya teşvik etmiştir. 2009 ve 2010 yıllarında Özen ve Güzeltepe [14, 16] yaptıkları çalışmalarda sonlu Gauss tamsayıları üzerinde devirli kodları ve Kuaterniyon tamsayıları halkası üzerinde devirli kodları tanımlamışlardır. 2010 ve 2013 yıllarında Ghaboussi ve arkadaşları [17, 18] yaptıkları çalışmalarında Gauss tamsayılar halkasındaki koldarı inceleyerek bu kodlar için dekodlama algoritması vermişlerdir. 2011 yılında Özen ve Güzeltepe [19], sonlu Kuaterniyon tamsayıları halkasında devirli kodları tanımlamışlardır. Bu çalışmadan esinlenerek Shah ve Rasool [20], 2013 yılında Kuaterniyon halkaları üzerinde kodları inceleyerek bu halkada MDS kodları inşaa etmişlerdir.

1.2 Tezin Amacı

Tezde, literatürde iyi bilinen devirli kodlar ve sabit devirli kodlar incelenerek bu kod ailelerinin sonlu, değişmeli olmayan, ideallerinin zincir yapısı olmayan bir halka üzerinde inşaası amaçlanmaktadır. Ayrıca devirli kodların en genel hali olan çoklu devirli kodların bu cebirsel yapı üzerinde inşa edilmesi ve tüm bu kodlar için parametreler belirlenmesi amaçlanmaktadır.

1.3 Hipotez

Bu tezde, literatürdeki çalışmalardan farklı olarak değişmeli olmayan sonlu kuaterniyon halkası üzerinde durulmuştur. Bu halka aynı zamanda zincir olmayan bir halkadır ve bu halkadan katsayılı polinomların oluşturduğu halka, elemanlarının tek türlü çarpanlarına ayrılamadığı bir halkadır. Bu halkada lineer kodların yapısı çalışılmış ve bu kodlar için standart formda üreteç matris verilmiştir. Ayrıca, bu cebirsel yapı üzerinde devirli kodlar ailesi inşaa edilerek bu kodlar için parametreler verilmiştir.

BÖLÜM 2

TEMEL BİLGİLER

Bu bölümde, tezde gerekli olan bilgiler ve kavramlar verilecek ve literatürde bilinen bazı önerme ve teoremler örneklerle açıklanacaktır. Bu temel bilgilerin cebirsel yapılar ile ilgili kısmı için [21-25] numaralı kaynaklara; hata düzelten kodlar ve lineer kodlar ile ilgili kısmı için ise [2, 26-38] numaralı kaynaklara başvurulmuştur.

2.1 Halkalar

Bu alt bölümde iki tane ikili işlemle tanımlanan cebirsel yapılar olan halkalar tanıtılacak ve bir halkanın sıfır bölen, birimsel, idempotent gibi özel elemanları incelenecektir. Bu bölümde Çallıalp'in Soyut Cebir kitabından [21] yararlanılmıştır.

Tanım 2.1 [21]

Boştan farklı bir R kümesi üzerinde tanımlı iki ikili işlem $+$ ve $\cdot$ olsun. Aşağıdaki özellikleri sağlayan $(R,+,\cdot)$ cebirsel yapısına bir **halka** denir.

- $(R,+)$ bir değişmeli (abel) grup,
- $\cdot$ işleminin R de birleşme özelliği vardır,
- $\cdot$ işleminin, $+$ işlemi üzerine sağdan ve soldan dağılma özelliği vardır.

Not 2.2

Kısalık açısından ikinci işlem olan $\cdot$, bazen iki elemanın yan yana yazılması şeklinde gösterilecektir.

Örnek 2.3

i. Tamsayılar kümesi $\mathbb{Z}$, bilinen toplama ve çarpma işlemleri ile bir halkadır.

ii. $M_n(\mathbb{R}) = \left\{ A = \left[a_{ij} \right]_{n\times n} \mid a_{ij} \in \mathbb{R}, \forall i, j = 1,2,...,n \right\}$ matrisler kümesi, matrislerin bilinen toplama ve çarpma işlemleri ile bir halkadır.

iii. Çift sayıların kümesi $2\mathbb{Z}$, tamsayıların toplama ve çarpma işlemleri ile bir halkadır.

Tanım 2.4 [21]

$(R,+,\cdot)$ halkasının $+$ işlemine göre etkisiz elemanına R nin **sıfır elemanı** denir ve 0_R ile gösterilir.

Örnek 2.5

i. $(\mathbb{Z},+,\cdot)$ halkasının sıfırı $0_{\mathbb{Z}} = 0$ tamsayısıdır.

ii. $(M_n(\mathbb{R}),+,\cdot)$ halkasının sıfırı $0_{M_n(\mathbb{R})} = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}_{n\times n}$ matrisidir.

iii. $(2\mathbb{Z},+,\cdot)$ halkasının sıfırı $0_{2\mathbb{Z}} = 0$ tamsayısıdır.

Tanım 2.6 [21]

$(R,+,\cdot)$ halkasının $\cdot$ işlemine göre etkisiz elemanına R nin **birim elemanı** denir ve 1_R ile gösterilir. Birim elemanı bulunan halkaya **birimli halka** denir.

Uyarı 2.7

Her halkanın bir birim elemanı bulunmak zorunda olmadığı gibi birden fazla birim elemanı da bulunabilir.

Örnek 2.8

i. $(M_n(\mathbb{R}),+,\cdot)$ halkasının birim elemanı $I = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}_{n\times n}$ birim matrisidir.

ii. $(2\mathbb{Z},+,\cdot)$ halkasının birim elemanı yoktur.

Tanım 2.9 [21]

$(R,+,\cdot)$ halkasında, halkanın sıfırından farklı bir $a \in R$ elemanı için $ar = ra = 1_R$ eşitliğini sağlayan $r \in R$ elemanına (ikinci işlem) $\cdot$ işlemine göre $a \in R$ nin **tersi** denir ve a^{-1} ile gösterilir.

Uyarı 2.10

Bir halkada sıfırdan farklı her elemanın tersi bulunamayabilir.

Tanım 2.11 [21]

$(R,+,\cdot)$ halkasında tersi mevcut olan elemanlara **birimsel (terslenebilir) elemanlar** denir.

Örnek 2.12

i. $(\mathbb{Z},+,\cdot)$ halkasında tüm birimsel elemanlar 1 ve -1 elemanlarıdır. $2 \in \mathbb{Z}$ elemanı için $2 \cdot \frac{1}{2} = \frac{1}{2} \cdot 2 = 1_{\mathbb{Z}}$ olup $\frac{1}{2} \notin \mathbb{Z}$ olduğu açıktır.

ii. Tamsayıların 5'e bölümünden kalanların oluşturduğu küme, $\mathbb{Z}_5 = \left\{ \overline{a} \mid a \equiv \overline{a} \bmod 5, a \in \mathbb{Z} \right\}$ ile gösterilmek üzere $(\mathbb{Z}_5,+,\cdot)$ halkasında sıfırdan farklı tüm elemanlar birimseldir.

Tanım 2.13 [21]

$(R,+,\cdot)$ halkasında, $a^2 = a \cdot a = a$ eşitliğini sağlayan elemanlara R nin **idempotent** elemanları denir.

Örnek 2.14

Her halkanın sıfırı ve birimi aşikâr olarak o halkanın idempotent elemanlarıdır.

Tanım 2.15 [21]

$(R,+,\cdot)$ halkası $\cdot$ işlemine göre değişmeli ise, yani her $r_1, r_2 \in R$ elemanları için $r_1 \cdot r_2 = r_2 \cdot r_1$ sağlanıyorsa R halkasına **değişmeli halka** denir.

Örnek 2.16

i. $(\mathbb{Z},+,\cdot)$ halkasında $a,b\in\mathbb{Z}$ için $a\cdot b=b\cdot a$ olduğundan $(\mathbb{Z},+,\cdot)$, değişmeli bir halkadır.

ii. $(M_n(\mathbb{R}),+,\cdot)$ halkası değişmeli olmayan bir halkadır.

Tanım 2.17 [21]

Bir $(R,+,\cdot)$ halkasında $a\in R$ elemanı ile değişmeli olan halkanın tüm elemanlarının oluşturduğu kümeye $a\in R$ **elemanının merkezi** denir ve $M(a)=\{r\in R\mid ar=ra\}$ şeklinde gösterilir. $(R,+,\cdot)$ nin tüm elemanları ile değişmeli olan elemanlarının kümesi ise R **halkasının merkezi** olarak tanımlanır ve $M(R)=\{r\in R\mid ra=ar,\forall a\in R\}$ şeklinde gösterilir.

Örnek 2.18

i. $(\mathbb{Z},+,\cdot)$ halkası değişmeli halka olduğundan tüm elemanları, diğer tüm elemanlarıyla değişmeli olup $M(\mathbb{Z})=\mathbb{Z}$ elde edilir.

ii. $M_n(\mathbb{R})$ halkasının merkezi $M(M_n(\mathbb{R}))$, köşegen matrisler kümesidir. Çünkü E_{ij}, $i-$nci ve $j-$nci girişleri 1, diğer girişleri 0 olan matris ve $A=(a_{ij})\in M_n(\mathbb{R})$ matrisi olmak üzere, $1\le i,j\le n$ için $E_{ij}A=AE_{ij}$ olması $a_{ii}=a_{jj}$ olmasını gerektirir.

Tanım 2.19

Bir $(R,+,\cdot)$ halkasının idempotent elemanları aynı zamanda halkanın merkezinde bulunuyorsa bu elemanlara **merkezi idempotent elemanlar** denir.

Tanım 2.20

Bir $(R,+,\cdot)$ halkasının idempotent elemanlarından $e_1,e_2\in R$ elemanları $e_1+e_2=1_R$ ve $e_1e_2=e_2e_1=0_R$ eşitliklerini sağlıyorsa $\{e_1,e_2\}$ çiftine **merkezi idempotent çifti** denir.

Tanım 2.21 [21]

R halkasında $0_R \neq a \in R$ elemanı için $a \cdot b = 0_R$ ya da $b \cdot a = 0_R$ olacak şekilde R nin sıfırından farklı bir $b \in R$ bulunabilirse a ve b elemanlarına **sıfır bölen** denir. Böyle elemanları mevcut olan halkaya **sıfır bölenli halka**, böyle elemanı bulunmayan halkaya ise **sıfır bölensiz halka** denir.

Not 2.22 [21]

R halkasının sıfırı 0_R ne sıfır bölendir ne de sıfır bölen olmayan elemandır.

Örnek 2.23

i. $(\mathbb{Z}, +, \cdot)$ halkası sıfır bölensiz bir halkadır.

ii. Tamsayıların 6 ile bölümünden kalanların oluşturduğu küme, $\mathbb{Z}_6 = \left\{ \bar{a} \mid a \equiv \bar{a} \bmod 6, a \in \mathbb{Z} \right\}$ ile gösterilmek üzere $(\mathbb{Z}_6, +, \cdot)$ halkasında $\bar{2} \cdot \bar{3} = \bar{0} = 0_{\mathbb{Z}_6}$ olduğundan $\bar{2}$ ve $\bar{3}$ elemanları, $\mathbb{Z}_6$ halkasının birer sıfır bölendir. Bu nedenle $(\mathbb{Z}_6, +, \cdot)$ sıfır bölenli bir halkadır.

Tanım 2.24 [21]

Sıfır böleni bulunmayan halkaya **tam halka** denir. Birimli, değişmeli, tam halkaya ise **tamlık bölgesi** denir.

Örnek 2.25

i. $(\mathbb{Z}, +, \cdot)$ halkası birimli, değişmeli ve sıfır bölensiz olduğundan bir tamlık bölgesidir.

ii. $(2\mathbb{Z}, +, \cdot)$ sıfır bölensiz olduğundan bir tam halka olup birimli olmadığından bir tamlık bölgesi değildir.

Önerme 2.26 [21]

$(R, +, \cdot)$ halkasının bir tam halka olması için gerek ve yeter koşul sıfırdan farklı herhangi bir $c \in R$ elemanı için sağdan ve soldan kısaltma özelliği sağlanmasıdır.

İspat

$(R, +, \cdot)$ halkası bir tam halka ve $0_R \neq c \in R$ olsun. Her $a, b \in R$ elemanları için

$ac = bc \Rightarrow (a-b)c = 0_R$ bulunur. $c \in R$ sıfırdan farklı ve R sıfır bölensiz olduğundan $a-b = 0_R$ olmalıdır. Bu ise $a = b$ demektir. Sağ kısaltma özelliğinin sağlandığı bu şekilde gösterilir.

Benzer şekilde $ca = cb$ iken $a = b$ olduğu ve sol kısaltma özelliğinin de sağlandığı kolaylıkla gösterilir.

Tersine, R halkasında sağ ve sol kısaltma özelliği sağlansın. Bu durumda sıfırdan farklı $a,b \in R$ elemanları için $0_R \neq a$ ve $ab = 0_R$ ise $b = 0_R$ olup R sıfır bölensiz yani tam halkadır.

Tanım 2.27 [21]

Bir $(R,+,\cdot)$ halkasının boştan farklı bir S alt kümesi, R halkasının iki ikili işlemi ile bir halka oluyorsa $(S,+,\cdot)$ halkasına $(R,+,\cdot)$ halkasının bir **alt halka**sı denir.

Örnek 2.28

i. $\{0_R\}$ ve R, $(R,+,\cdot)$ nin alt halkalarıdır.

ii. $(2\mathbb{Z},+,\cdot)$ halkasının, tamsayılardaki toplama ve çarpma işlemleri ile bir halka olduğu Örnek 2.3, iii de gösterildi. Bu nedenle $(\mathbb{Z},+,\cdot)$ halkasının bir alt halkasıdır.

Önerme 2.29 [21]

$(R,+,\cdot)$ bir halka ve $\varnothing \neq S \subset R$ alt kümesi olsun. S alt kümesinin R halkasının bir alt halkası olması için gerek ve yeter koşul her $a,b \in S$ elemanları için $a-b \in S$ ve $a \cdot b \in S$ olmasıdır.

İspat

S, $(R,+,\cdot)$ halkasının bir alt halkası olsun. Tanıma göre, $(S,+,\cdot)$ da bir halkadır. Dolayısıyla $(S,+)$ bir değişmeli gruptur. Bu nedenle her $a,b \in S$ elemanları için $a-b \in S$ elde edilir. Ayrıca S bir halka olduğundan ikinci işlemin kapalılık özelliği sağlanır ve $a \cdot b \in S$ elde edilir.

Tersine, her $a,b \in S$ elemanları için $a-b \in S$ ve $a \cdot b \in S$ sağlansın. Bu durumda $(S,+)$ toplamsal grubu, $(R,+)$ toplamsal grubunun bir alt grubu olup değişmelidir. İkinci işleme göre kapalılık sağlandığından ve sağdan ve soldan dağılma özellikleri de kolaylıkla gösterilebileceğinden $(S,+,\cdot)$ bir halkadır. Dolayısıyla $(R,+,\cdot)$ halkasının bir alt halkasıdır.

Tanım 2.30 [21]

$(R,+,\cdot)$ halkasının bir $\varnothing \neq I \subset R$ alt halkası aşağıdaki özellikleri sağlarsa, I alt halkasına $(R,+,\cdot)$ halkasının bir sol veya sağ **ideal**i denir:

- Her $a,b \in I$ elemanları için $a-b \in I$,
- Her $a \in I, r \in R$ elemanları için $ra \in I$ veya $ar \in I$.

Örnek 2.31

$\mathbb{Z}$ halkasının $(2\mathbb{Z},+,\cdot)$ alt halkasından alınan her $a,b \in 2\mathbb{Z}$ elemanı için $a-b \in 2\mathbb{Z}$ ve $ra \in 2\mathbb{Z}, r \in \mathbb{Z}$ olduğundan $2\mathbb{Z}$, $\mathbb{Z}$ nin bir idealidir. $(2\mathbb{Z},+,\cdot)$ değişmeli halka olduğundan aynı zamanda hem sağ hem sol idealidir.

Tanım 2.32 [21]

A, R halkasının bir alt kümesi olsun. R nin A kümesini kapsayan tüm ideallerinin arakesitine A **kümesinin ürettiği ideal** denir ve (A) ile gösterilir. Eğer A kümesi tek elemandan oluşuyorsa, diğer bir deyişle bir ideal tek $a \in A$ elemanı tarafından üretiliyorsa bu ideale **temel (esas) ideal** denir ve (a) ile gösterilir.

Örnek 2.33

$\mathbb{Z}$ halkasının $(2\mathbb{Z},+,\cdot)$ ideali 2 elemanı tarafından üretilen bir temel idealdir. $2\mathbb{Z}=(2)$ şeklinde ifade edilebilir.

Tanım 2.34 [21]

Tüm idealleri temel ideal olan bir tamlık bölgesine **temel ideal bölgesi** denir.

Örnek 2.35

$\mathbb{Z}$ halkasının tüm idealleri $(n)=n\mathbb{Z}, n\in\mathbb{Z}$ olduğundan $\mathbb{Z}$ bir temel ideal bölgesidir.

Tanım 2.36 [22]

Bir $(R,+,\cdot)$ halkasının idealleri arasında kümelerde kapsama sıralama bağıntısına göre bir zincir mevcutsa R ye **zincir halkası** denir.

Örnek 2.37

$(\mathbb{Z}_8,+,\cdot)$ halkasının tüm idealleri

$(\bar{1})=(\bar{3})=(\bar{5})=(\bar{7})=\mathbb{Z}_8,$
$(\bar{2})=\{\bar{0},\bar{2},\bar{4},\bar{6}\},$
$(\bar{4})=\{\bar{0},\bar{4}\},$
$(\bar{0})=\{\bar{0}\}$

olarak listelenebilir. Bu idealler arasında $(\bar{0})\subset(\bar{4})\subset(\bar{2})\subset(\bar{1})$ zinciri mevcut olduğundan $\mathbb{Z}_8$ bir zincir halkasıdır.

Tanım 2.38 [22]

$(R,+,\cdot)$ bir halka ve I bu halkanın bir ideali olsun. Her $a,b\in R$ elemanları için $a\equiv b \bmod I \Leftrightarrow a-b\in I$ şeklinde tanınmalan $\equiv$ denklik bağıntısına göre ayırdığı her $r\in R$ elemanı için $\bar{r}=r+I=\{r+a \mid a\in I\}$ denklik sınıflarının oluşturduğu kümeye R nin I ya göre **denklik kümesi** denir ve R/I ile gösterilir.

Örnek 2.39

$(\mathbb{Z},+,\cdot)$ halkasının bir ideali olan $I=(8)$ e göre ayırdığı denklik sınıfları $\bar{0},\bar{1},\bar{2},...,\bar{7}$ olduğundan $\mathbb{Z}/(8)$ denklik kümesi $\mathbb{Z}_8=\{\bar{0},\bar{1},\bar{2},...,\bar{7}\}$ olarak bulunur.

Tanım 2.40 [22]

Bir $(R,+,\cdot)$ halkasının bir I idealine göre tanımlanan denklik sınıflarının kümesi aşağıda tanımlanan iki ikili işlem ile oluşturduğu halkaya R halkasının I idealine göre **bölüm halkası** denir.

- Her $a,b \in R$ elemanları için $(a+I)\oplus(b+I)=(a+b)+I$,
- Her $a,b \in R$ elemanları için $(a+I)\odot(b+I)=(a\cdot b)+I$.

Örnek 2.41

$n \in \mathbb{Z}$ olmak üzere $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ olup $\mathbb{Z}$ halkasının (n) ideallerine göre bölüm halkalarıdır.

2.2 Modüller

Bu alt bölümde modül adı verilen cebirsel yapılar incelenecektir. Bunu yaparken halka ikinci işleme göre değişmeli olmadığından genelliği bozmadan sol çarpma işlemi alınacak ve tüm tanımlamalar buna göre yapılacaktır. Bu kısımda Çallıalp ve Tekir'in "Değişmeli Halkalar ve Modüller" [22] adlı kitabındaki temel bilgiler özetlenmiştir.

Tanım 2.42 [22]

$(G,+)$ bir değişmeli grup ve R bir halka olsun. $R\times G$ den G ye tanımlı skaler çarpma işlemi aşağıdaki özellikleri sağlıyorsa G ye bir $R-$ **modül** denir:

Her $r_1, r_2 \in R$ ve her $g_1, g_2 \in G$ için

- $r_1(g_1+g_2)=r_1g_1+r_1g_2$,
- $(r_1+r_2)g_1=r_1g_1+r_2g_1$,
- $(r_1r_2)g_1=r_1(r_2g_1)$.

Örnek 2.43

i. Bir R halkası, skaler çarpma işlemi halkanın ikinci işlemi olarak alınırsa kendi üzerinde bir $R-$ modüldür.

ii. Bir R halkasının herhangi bir I ideali bir $R-$modüldür.

iii. Her vektör uzayı, üzerinde tanımlı olduğu cisim üzerinde aynı zamanda bir modüldür.

iv. Bir R halkasının elemanlarının sıralı $n-$lileri ile oluşturulan $R^n=\{(r_1,r_2,...,r_n)\mid r_t\in R,t=1,2,...,n\}$ kümesi, bir $R-$modüldür.

v. I, bir R halkasının ideali olmak üzere

$$R\times R/I\to R/I$$
$$(r_1,r_2+I)\to r_1r_2+I$$

şeklinde tanımlı skaler çarpma işlemi ile R/I bölüm halkası bir $R-$modüldür.

Uyarı 2.44

Yukarıda tanımda sağ skaler çarpma işlemi tanımlanarak **sağ** $R-$ **modül** yapısı oluşturulur.

Tanım 2.45 [22]

R bir halka ve G bir $R-$modül olsun. Eğer R birimli bir halka ise, G ye **birimli modül**; eğer R değişmeli bir halka ise G ye bir **değişmeli modül** denir.

Örnek 2.46

i. R birimli bir halka olmak üzere $R^n=\{(r_1,r_2,...,r_n)\mid r_t\in R,t=1,2,...,n\}$ bir birimli $R-$modüldür ve birimi $(1_R,....,1_R)\in R^n$ sıralı $n-$lisidir.

ii. $\mathbb{Z}_n$ halkası bir değişmeli ve birimli $\mathbb{Z}-$modüldür.

Tanım 2.47 [22]

R bir halka, G bir $R-$modül ve $H\subseteq G$ boştan farklı bir alt küme olsun. H kümesi de skaler çarpma işlemi ile bir $R-$modülse H ye G nin bir alt modülü veya **alt** $R-$ **modülü** denir.

Örnek 2.48

i. Bir $R-$modül G kümesinin kendisi ve $\{0_G\}$, G modülünün aşikar alt modülleridir.

ii. $\mathbb{Z}_n$ halkası, $\mathbb{R}-$modül $\mathbb{Z}$ nin bir alt modülüdür.

Önerme 2.49 [22]

R bir halka, G bir $R-$modül olsun. $H \subseteq G$ bir alt $R-$ modül olması için gerek ve yeter koşul her $r_1, r_2 \in R$ ve $h_1, h_2 \in H$ için $r_1h_1 + r_2h_2 \in H$ olmasıdır.

İspat

H bir alt $R-$modül ise her $r_1, r_2 \in R$ ve $h_1, h_2 \in H$ için $r_1h_1 + r_2h_2 \in H$ sağlanır.

Tersine her $r_1, r_2 \in R$ ve $h_1, h_2 \in H$ için $r_1h_1 + r_2h_2 \in H$ olsun. Özel olarak $r_1 = 1, r_2 = -1$ için de $r_1h_1 + r_2h_2 \in H$ sağlanacağından $h_1, h_2 \in H$ elemanları için $h_1 - h_2 \in H$ olur. Böylece H, G nin bir alt grubudur. Ayrıca her $r \in R$ ve her $g \in G$ elemanları için $rg \in H$ dir. G nin tüm elemanları için skaler çarpma özellikleri sağlanacağından H alt kümesinin elemanları için de sağlanacaktır. Dolayısıyla H bir alt $R-$modüldür.

Örnek 2.50

Bir R halkasına $R-$modül gözüyle bakıldığında, alt $R-$modüller, R nin idealleridir.

Tanım 2.51 [22]

G bir $R-$modül ve $H \subseteq G$ boştan farklı bir alt küme olsun. Bu durumda H **kümesinin ürettiği alt** $R-$**modül**, H alt kümesini kapsayan $R-$modüllerin arakesitidir ve (H) ile gösterilir.

Buradan, G' ler birer $R-$modül olmak üzere $(H) = \bigcap_{H \subseteq G'} G'$, H yi kapsayan en küçük alt $R-$modüldür. H kümesine **üreteç sistemi** de denir.

Tanım 2.52 [22]

R birimli bir halka, G bir $R-$modül ve $g \in G$ olsun. $\{g\}$ nin ürettiği alt $R-$modül $(g) = Rg = \{rq \mid r \in R\}$ kümesidir. Bu kümeye g **ile üretilmiş alt** $R-$**modül** denir. Eğer

$R-$modül G, tek eleman tarafından üretiliyorsa, diğer bir ifadeyle $G=(g)$ olacak şekilde bir $g\in G$ bulunabiliyorsa G ye **devirli modül** denir.

Örnek 2.53

Bir birimli R halkası, $R-$modül gözüyle bakıldığında $R=R1_R$ olup 1_R elemanı tarafından üretilen bir devirli modüldür.

Tanım 2.54 [22]

G, H alt kümesi tarafından üretilmiş bir $R-$modül olsun. Eğer H sonlu bir küme ise G ye **sonlu üretilmiş** $R-$**modül** denir.

Örnek 2.55

$\mathbb{C}$ kompleks sayılar cismi $\mathbb{R}$ reel sayılar cismi üzerinde $\{1,i\}$ sonlu üreteç kümesiyle üretilir. Bu nedenle $\mathbb{C}$, bir sonlu üretilmiş $\mathbb{R}-$modüldür.

Tanım 2.56 [23]

$S=\{s_\alpha\}_{\alpha\in\Lambda}$ kümesi, bir R halkası ve bir $R-$modül G için bir üreteç kümesi olsun. Her $g\in G$ için $r_\alpha\in R, s_\alpha\in S$ olmak üzere $g=\sum_{\alpha\in\Lambda} r_\alpha s_\alpha$ şeklinde sonlu bir toplam olarak tek türlü ifade edilebiliyorsa S ye G nin bir **tabanı** denir. Bir tabanı bulunan modüle ise **serbest modül** denir.

Örnek 2.57

i. R bir halka ve $R^n=\{(r_1,r_2,...,r_n)\,|\,r_t\in R, t=1,2,...,n\}$ olsun. $e_s\in R^n$, $s-$nci bileşeni 1_R ve diğer bileşenleri 0_R olan $n-$li yani $e_s=\left(0,0,...,\underset{s-nci}{1},0,...,0\right)\in R^n$ olmak üzere $\{e_1,e_2,...,e_n\}$ üreteç sistemi R^n için bir taban olup R^n, R üzerinde bir serbest modüldür. $n-$liler $(r_1,r_2,...,r_n)$ şeklinde gösterileceği gibi $r_1r_2...r_n$ şeklinde yanyana yazılarak da gösterilebilir.

ii. $\mathbb{Z}_n$ halkası bir $\mathbb{Z}-$modül olarak serbest modül değildir. Ancak $\mathbb{Z}_n-$modül olarak $\{\bar{1}\}$ üreteç sistemini taban kabul eden bir serbest modüldür.

2.3 Cisimler ve Vektör Uzayları

Bu alt bölümde cisimler incelenecektir. Ayrıca sonlu cisimler üzerinde tanımlanan vektör uzaylarının yapısı incelenecektir. Vektör uzayları, sonlu cisimler üzerinde tanımlanacak olan lineer kodlarla yakından ilgilidir.

Tanım 2.58 [24]

Boştan farklı bir F kümesi üzerinde tanımlı iki ikili işlem $+,.$ aşağıdaki özellikleri sağlıyorsa F ye bir **cisim** denir:

Her $a,b,c \in F$ elemanları için,

- $(F,+)$ değişmeli grup,
- $ab \in F$ (kapalılık),
- $ab = ba$ (değişmelilik),
- $(ab)c = a(bc)$ (birleşmelilik),
- $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ (dağılma),
- $a1_F = 1_F a = a$ (etkisiz eleman),
- $a \in F - \{0\}$ olmak üzere $a^{-1}a = aa^{-1} = 1_F$ (ters eleman).

Örnek 2.59

i. $\mathbb{R}$ reel sayılar kümesi, bilinen toplama ve çarpma işlemleri ile bir cisimdir.

ii. $\mathbb{Z}$ tamsayılar kümesi, tamsayıların toplama ve çarpma işlemleri ile $2 \in \mathbb{Z}$ elemanı için $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$ olduğundan bir cisim değildir.

iii. $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ kümesi, bölüm halkası işlemleri ile bir cisimdir.

Tanım 2.60 [21]

Herhangi bir F cisminde sıfırdan farklı her $a \in F$ için $ka = 0_F$ sağlayan en küçük $k \in \mathbb{R}^+$ sayısına F cisminin **karakteristiği** denir ve $kar(F) = k$ ile gösterilir. Böyle bir $k \in \mathbb{R}^+$ bulunamıyorsa cismin **karakteristiği** 0 **dır** denir.

Örnek 2.61

i. Her sıfırdan farklı $a \in \mathbb{Z}_3$ elemanı için $3 \cdot \bar{1} \equiv \bar{0}$ ve $3 \cdot \bar{2} \equiv \bar{0}$ olduğundan ve bu eşitliği saylayan daha küçük bir reel sayı bulunmadığından $kar(F) = 3$ elde edilir.

ii. $\mathbb{R}$ reel sayılar cisminden alınan sıfırdan farklı $a \in \mathbb{R}$ elemanı için $ka = 0$ eşitliğini sağlayacak şekilde bir $k \in \mathbb{R}^+$ bulunamayacağı için $kar(\mathbb{R}) = 0$ bulunur.

Teorem 2.62 [21]

Bir cismin karakteristiği ya sıfırdır ya da asal bir sayıdır.

İspat

Bir F cisminde sıfırdan farklı her $a \in F$ elemanı için $na = 0$ eşitlşğini sağlayacak şekilde bir $n \in \mathbb{R}^+$ yoksa $kar(F) = 0$ elde edilir.

F bir cisim ve karakteristiği $0 \neq n \in \mathbb{R}$ olsun ve n sayısının bir asal sayı olmadığı kabul edilsin. Bu durumda her $a \in F$ sıfırdan farklı eleman için $na = 0$ eşitliğini sağlayan en küçük reel sayı n sayısıdır. Özel olarak $n1_F = 0_F$ sağlanır. n sayısı asal olmadığından $1 < n_1, n_2 < n$ olmak üzere $n = n_1 \cdot n_2$ şeklinde çarpanlarına ayrılabilir. Bu durumda

$n \cdot 1_F = (n_1 n_2)1_F = (n_1 1_F)(n_2 1_F) = 0_F$ elde edilir. F bir cisim dolayısıyla bir tamlık bölgesi olduğundan sıfır bölensizdir. Bu nedenle $(n_1 1_F) = 0_F$ veya $(n_2 1_F) = 0_F$ olmalıdır. Bu ise n reel sayısının $n1_F = 0_F$ özelliğini sağlayan en küçük reel sayı olması ile çelişir. Bu nedenle $n \in \mathbb{R}^+$ asal sayı olmalıdır.

Teorem 2.63 [24]

F bir sonlu cisim ve F nin karakteristiği p asal sayısı olsun. Bu durumda F cisminin eleman sayısı bir $n \in \mathbb{N}$ için $|F| = p^n$ dir.

Tanım 2.64 [24]

F_q sonlu cisminin boştan farklı bir V kümesi, F_q nun elemanları ile tanımlanan skaler çarpma işlemi ile aşağıdaki özellikleri sağlıyorsa V ye bir F_q-**vektör uzayı** denir ve V nin elemanlarının herbiri **vektör** adını alır:

Her $v_1,v_2 \in V, a,b \in F_q$ için,

- $(V,+)$ bir değişmeli grup,
- $(ab)v_1 = a(bv_1)$,
- $a(v_1+v_2) = av_1+av_2$, $(a+b)v_1 = av_1+bv_1$,
- $v_1 1_{F_q} = 1_{F_q} v_1 = v_1$ sağlanır.

Tanım 2.65 [24]

Tüm bileşenleri F_q sonlu cisminden alınarak oluşturulan **sıralı** $n-$**lilerin kümesi** $F_q{}^n = \{(u_1,u_2,...,u_n) \mid u_i \in F_q, i=1,2,...,n\}$ şeklinde tanımlanır.

Önerme 2.66

$F_q{}^n$ kümesi, aşağıdaki vektörel toplama ve skaler çarpma işlemleri ile bir F_q-vektör uzayıdır:

$u=(u_1,u_2,...,u_n), w=(w_1,w_2,...,w_n) \in F_q{}^n$ ve $a \in F_q$ için,

$u+w=(u_1+w_1,...,u_n+w_n)$ ve $au=(au_1,au_2,...,au_n)$ sağlanır.

İspat

F_q sonlu cisim ve $F_q{}^n = \{\mathbf{u}=(u_1,u_2,...,u_n) \mid u_i \in F_q, i=1,2,...,n\}$ olsun. $(F_q,+)$ bir değişmeli gruptur. Öte yandan her $a,b \in F_q$ ve $\mathbf{u} \in F_q{}^n$ elemanları için

$(ab)\mathbf{u} = ((ab)u_1,(ab)u_2,...,(ab)u_n) = (a(bu_1),a(bu_2),...,a(bu_n)) = a(bu_1,bu_2,...,bu_n)$
$= a(b(u_1,...,u_n)) = a(b\mathbf{u})$

sağlanır. Ayrıca her $a \in F$ ve $\mathbf{u}, \mathbf{v} \in F_q^{\,n}$ elemanları için

$$a(\mathbf{u}+\mathbf{v}) = a(u_1 v_1 + \ldots + u_n v_n) = (au_1 v_1 + \ldots + au_n v_n)$$
$$= a(u_1, \ldots, u_n) + a(v_1 + \ldots + v_n) = a\mathbf{u} + b\mathbf{v}$$

yazılabilir. Her $\mathbf{u} \in F_q^{\,n}$ vektörü için $\mathbf{u}1_F = 1_F \mathbf{u} = \mathbf{u}$ sağlandığından $F_q^{\,n}$ bir $F_q -$vektör uzayıdır.

Tanım 2.67 [21]

F_q bir sonlu cisim, V bir $F_q -$vektör uzayı ve $W \subseteq V$ boştan farklı bir alt küme olsun. W de skaler çarpma işlemi ile bir $F_q -$vektör uzayı ise W ye V nin bir **alt uzay** veya **alt** $F_q -$**vektör uzayı** denir.

Önerme 2.68 [24]

F_q bir sonlu cisim, V bir $F_q -$vektör uzayı olsun. $W \subseteq V$ bir alt $F_q -$vektör uzayı olması için gerek ve yeter koşul her $a \in F_q$ ve $w_1, w_2 \in W$ için $w_1 + w_2 \in W$ ve $aw_1 \in W$ olmasıdır.

İspat

F_q bir sonlu cisim, V bir $F_q -$vektör uzayı olsun. $W \subseteq V$ alt kümesi de bir $F_q -$vektör uzayı olsun. Bu durumda her $a \in F_q$ ve $w_1, w_2 \in W$ için $w_1 + w_2 \in W$ ve $aw_1 \in W$ açıkça sağlanır.

Tersine her $a \in F_q$ ve $w_1, w_2 \in W$ için $w_1 + w_2 \in W$ ve $aw_1 \in W$ sağlansın. Bu durumda $(W, +)$ bir değişmeli alt gruptur. Öte yandan birleşme ve dağılma özellikleri sağlanır. Bu nedenle W alt kümesi bir $F_q -$vektör uzayıdır.

Tanım 2.69 [24]

V bir $F_q -$vektör uzayı olsun. $a_1, a_2, \ldots, a_r \in F_q$ ve $v_1, v_2, \ldots, v_r \in V$ olmak üzere V vektör uzayının elemanlarının bir **lineer birleşimi (kombinasyonu)** $a_1 v_1 + \ldots + a_r v_r$ şeklinde tanımlanır.

Tanım 2.70 [24]

V bir F_q – vektör uzayı olsun. $a_1v_1 + ... + a_rv_r = 0$ olması, $a_1 = a_2 = ... = a_r = 0$ olmasını gerektiriyorsa $\{v_1, v_2, ..., v_r\}$ vektörleri **lineer bağımsızdır** denir.

Örnek 2.71

$\{000, 102, 110\}$ vektörler kümesi için $a_1, a_2, a_3 \in F_3$ olmak üzere

$a_1(000) + a_2(102) + a_3(110) = 0$
$a_2 + a_3 = 0$
$a_3 = 0$
$2a_2 = 0$

olduğundan F_3^3 üzerinde lineer bağımsızdır.

Tanım 2.72 [24]

$W = \{w_1, w_2, ..., w_n\}$, bir F_q – vektör uzayı olan V nin boştan farklı bir alt kümesi olsun. W kümesindeki vektörlerin tüm lineer kombinasyonlarının oluşturduğu kümeye W **nin ürettiği küme** denir ve (W) ile gösterilir. Üstelik bu küme V nin bir alt vektör uzayıdır. W kümesine de (W) alt uzayının bir **üreteç kümesi** denir.

Örnek 2.73

F_2 – vektör uzayı olarak

i. $W_1 = \{0001, 0010, 0100\}$ kümesinin ürettiği alt uzay

$(W_1) = \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\}$ dir.

ii. $W_2 = \{000, 111\}$ kümesinin kendisi bir F_2 – vektör uzayı olduğundan, ürettiği alt uzay W_2 dir.

Tanım 2.74 [24]

V bir F_q – vektör uzayı olsun. $W = \{w_1, w_2, ..., w_n\}$ kümesi lineer bağımsız ve $V = (W)$ ise W ye V vektör uzayının bir **tabanı (bazı)** denir. W nin eleman sayısına V vektör uzayının **boyutu** denir ve $boy(V)$ ile gösterilir.

Uyarı 2.75

Herhangi bir F_q −vektör uzayının birden fazla tabanı olabilir. Ancak, bu tabanların herbiri, eşit sayıda elemana sahiptir.

Örnek 2.76

$\mathbb{R}^3 = \{\mathbf{x} = (x_1, x_2, x_3) \mid x_1, x_2, x_3 \in \mathbb{R}\}$ kümesi bir $\mathbb{R}$ −vektör uzayıdır. Her bir (x_1, x_2, x_3) vektörü $x_1(1,0,0) + x_2(0,1,0) + x_3(0,0,1)$ şeklinde ifade edilebileceği için $W_1 = \{(1,0,0),(0,1,0),(0,0,1)\}$ kümesi $\mathbb{R}^3$ için bir tabandır. Ayrıca $W_2 = \{(1,0,0),(-1,1,0),(1,0,1)\}$ kümesi de $\mathbb{R}^3$ için bir tabandır. W_1 ile W_2 nin aynı sayıda vektör içerdiğine dikkat edilmelidir.

Önerme 2.77

V bir F_q −vektör uzayı olsun. Eğer V nin boyutu $boy(V) = k$ ise V alt uzayının eleman sayısı $|V| = q^k$ olarak bulunur.

İspat

V bir F_q −vektör uzayının boyutu k ise $W = \{w_1, ..., w_k\}$ üreteç sistemi, V için bir tabandır. Bu durumda her $v \in V$ elemanı, bu taban elemanlarının bazı skaler katlarının sonlu toplamları şeklinde ifade edilebilir. Bu nedenle $V = \{a_1 w_1 + ... + a_k w_k \mid a_i \in F_q\}$ yazılabilir. $|F_q| = q$ olduğundan her bir $a_1, ..., a_k \in F_q$ için tam olarak q farklı seçenek vardır. Böylece V deki vektör sayısı q^k olarak hesaplanır.

Örnek 2.78

$q = 2$, $S = \{0001, 0010, 0100\}$ ve $V = (S)$ olsun. Bu durumda $V = \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\}$ vektör uzayı olarak bulunur. Ayrıca $|V| = 2^{boy(V)} = 2^3 = 8$ olarak hesaplanır.

Tanım 2.79 [24]

$\alpha=(a_1,a_2,...,a_n),\beta=(b_1,b_2,...,b_n)\in F_q^{\,n}$ olsun. α ile β nin **iç çarpımı** $\langle\alpha,\beta\rangle=a_1b_1+...+a_nb_n\in F_q$ şeklinde tanımlanır. $\langle\alpha,\beta\rangle=0$ ise α ile β vektörleri birbirine **diktir** denir. S, $F_q^{\,n}$ vektör uzayının bir alt kümesi olmak üzere $S^{\perp}=\{v\in F_q^{\,n}\mid\langle v,s\rangle=0,s\in S\}$ kümesine S nin **diki (dik tümleyeni)** denir.

Örnek 2.80

$u=1012210121$, $v=0011002210$, $z=0101110020$ vektörlerinin F_3^{10} üzerinde iç çarpımları,

$$\langle u,v\rangle=1.0+0.0+1.1+2.1+2.0+1.0+0.2+1.2+2.1+1.0=1$$

$$\langle v,z\rangle=0.0+0.1+1.0+1.1+0.1+0.1+2.0+2.0+1.2+0.0=0$$

$$\langle u,z\rangle=1.0+0.1+1.0+2.1+2.1+1.1+0.0+1.0+2.2+1.0=0$$

olarak bulunur. Burada v ile z vektörleri ve u ile z vektörleri diktir.

Önerme 2.81 [30]

F_q bir cisim ve S bir F_q-alt vektör uzayı olmak üzere S nin dik tümleyeni $S^{\perp}$, bir F_q-alt vektör uzayıdır.

İspat

F_q bir cisim ve S bir F_q-alt vektör uzayı olmak üzere S nin dik tümleyeni $S^{\perp}$ olsun.

$(S^{\perp},+)$ bir değişmeli gruptur. Ayrıca her $s\in S$ ve $s_1,s_2\in S^{\perp}$ vektörleri için $(s_1s_2)s=s_1(s_2s)=s_10=0$ olup kapalılık özelliği ve birleşme özelliği sağlanır. Her bir $a,b\in F_q$ ve $s_1,s_2\in S^{\perp}$ elemanları için $a(s_1+s_2)=as_1+as_2$ ve $(a+b)s_1=as_1+bs_1$ olup dağılma özelliği sağlanır. Bu nedenle $S^{\perp}$ bir F_q-vektör uzayıdır.

Teorem 2.81 [30]

$F_q^{\,n}$ vektör uzayının boştan farklı bir S alt uzayı ve dik tümleyeni için $boy(S)+boy(S^{\perp})=boy(F_q^{\,n})=n$ elde edilir.

İspat

$F_q^{\,n}$ bir vektör uzayı, S, $F_q^{\,n}$ nin boştan farklı bir alt uzayı ve $S^{\perp}$, S nin dik tümleyeni olsun. $\beta=\{w_1,...,w_k\}$ ve $\gamma=\{x_1,...,x_m\}$ kümeleri sırasıyla S ve $S^{\perp}$ için birer taban olduğunu kabul edelim. $\beta\cup\gamma=\{w_1,...,w_k,x_1,...,x_m\}$ nin $F_q^{\,n}$ için bir taban olduğunu göstermek yeterlidir.

Verilen bir $a\in F_q^{\,n}$ vektörü $s_1\in S$ ve $s_2\in S^{\perp}$ olmak üzere $a=s_1+s_2$ şeklinde yazılabilir. β ve γ birer taban olduklarından $a=\sum_{i=1}^{k}t_iw_i+\sum_{j=1}^{m}y_jx_j$ şeklinde ifade edilebilir. Verilen $c_1,...,c_k,d_1,...,d_m$ elemanları için

$0=\sum_{i=1}^{k}c_iw_i+\sum_{j=1}^{m}d_jx_j\Rightarrow\sum_{i=1}^{k}c_iw_i=-\sum_{j=1}^{m}d_jx_j$ elde edilir. Buradan $\sum_{i=1}^{k}c_iw_i\in S\cap S^{\perp}$ ve $\sum_{j=1}^{m}d_jx_j\in S\cap S^{\perp}$ bulunur. Bir $x\in S\cap S^{\perp}$ için $\langle x,x\rangle=0$ iken $x=0$ olacağından $\sum_{i=1}^{k}c_iw_i=\sum_{j=1}^{m}d_jx_j=0$ elde edilir. Bu ise c_i ve d_j lerin hepsinin birden sıfır olması yani $\beta\cup\gamma$ nin lineer bağımsız bir küme olması anlamına gelir. Bu nedenle $\beta\cup\gamma$, $F_q^{\,n}$ için bir taban olup $boy(F_q^{\,n})=n=k+m=boy(S)+boy(S^{\perp})$ bulunur.

Uyarı 2.82

- İki vektör birbirleriyle çarpılabilir fakat bölünemez.
- İç çarpım ve vektörel çarpım, çarpılan vektörlerin ürettiği vektör uzayında yer almaz.

2.4 Hata Düzelten Kodlar

Kodlama Teorisi alanında ilk çalışma 1948 yılında Claude Shannon tarafından yapılmış olan "A mathematical theory of communication" başlıklı çalışmadır. Bu çalışmada kanalın kapasitesi olarak adlandırılan bir sayı tanımlandı. Kanalın kapasitesi, verilen gürültülü bir iletişim kanalında, uygun kodlama ve kod çözme teknikleri kullanıldığında, o değerin altında herhangi bir oranda güvenilir iletişim sağlanacağı gösterildi. Bu, gürültülü kanallardaki verilerin iletilmesi ve bozuk mesajların kurtarılması ile ilgili bir çalışma alanı olan kodlama teorisinin doğuşu olarak kabul edilir.

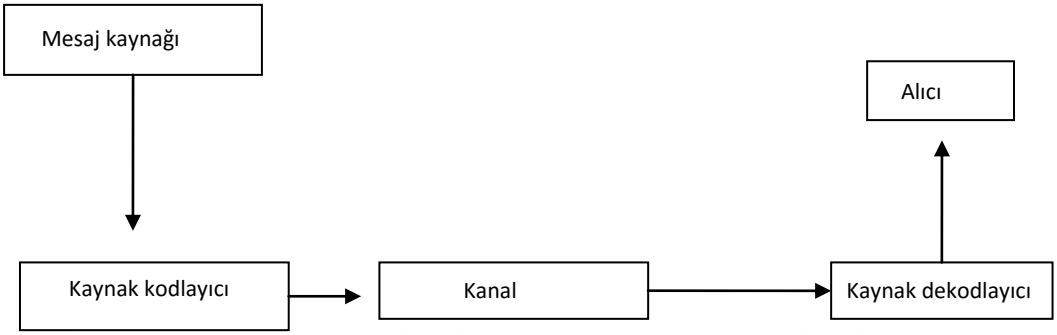
Yarım yüzyıldan az bir süre zarfında, kodlama teorisi olağanüstü bir büyüme gösterdi. İletişim sistemlerinden kompakt disk oynatıcılara, depolama teknolojisine kadar geniş alanlarda uygulama bulmuştur. Araştırmacılar, pratikte iyi kodlar bulmak için, blok kodların ötesine geçerek evrensel kodlar, turbo kodlar, uzay-zaman kodlar (space-time), düşük yoğunluklu parite kontrolü (LDPC) kodları ve hatta kuantum kodları çalışmaktadırlar. Kodlama teorisinde sıklıkla mühendislik uygulamalarından kaynaklanan sorunlar ortaya çıkarken, alanın geliştirilmesinde matematiğin oynadığı rolü çok büyüktür.

Cebir, kombinasyon ve geometrinin kodlama teorisinde önemi sıklıkla kabul gören bir gerçektir; kodlama teorisinin ilerlemesinde zarif yollarla kullanılan birçok derin matematiksel sonuçlar vardır. Kodlama teorisi, yalnızca mühendisler ve bilgisayar bilimcileri için değil aynı zamanda matematikçiler için de önem arz eder.

İyi kodların teorik ve pratik açıdan tasarımı, kodlama teorisinde çok önemli bir sorundur. Kodlama teorisinin başlangıcından beri, araştırmacılar bu yönlerde çok araştırmalar yapmış ve bu süreçte çok ilginç kod ailelerini inşa etmişlerdir. Hamming kodları, Golay kodları, Reed-Muller kodları, döngüsel kodlar, BCH kodları, Reed-Solomon kodları, alternatif kodlar, Goppa kodları vb. iyi bilinen kod ailelerinin çoğunun sistematik olarak sisteme sokulması için de bir çaba gösterilmektedir.

İletişim sistemleri ve veri saklama aygıtları gibi bilgi medyası, gürültüye veya girilen parazitlerin diğer biçimlerine bağlı olarak pratikte kesinlikle güvenilir değildir. Kodlama teorisinde görevlerden biri, hataları tespit etmek veya hatta düzeltmektir. Genellikle kodlama, kaynak kodlaması ve kanal kodlaması olarak tanımlanır. Kaynak kodlama, ileti

kaynağını kanal üzerinden iletilmek üzere uygun bir koda dönüştürmeyi içerir. Kaynak kodlamaya bir örnek, her bir karakteri 8 bitlik bir bayta çeviren ASCII kodudur. Basit bir iletişim modeli Şekil 2.1 ile gösterilebilir.



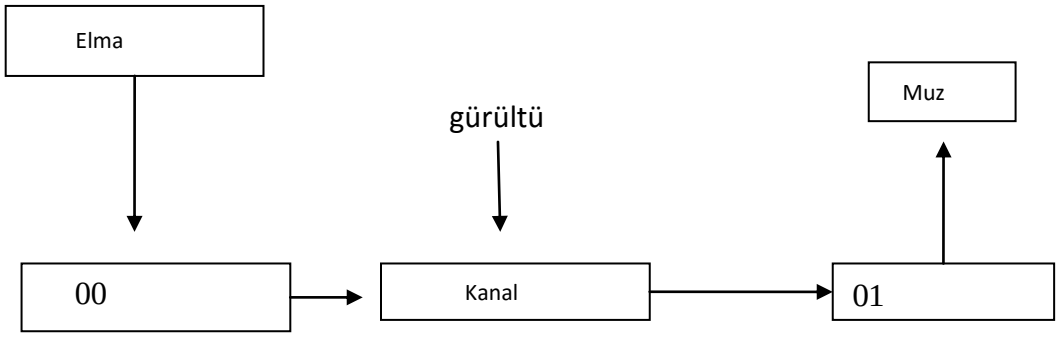
Şekil 2. 1 Kodlama şeması

Örnek 2.83 [30]

Elma, muz, kiraz, üzüm gibi keyfi dört meyvenin aşağıdaki şekilde kodlandığını düşünelim:

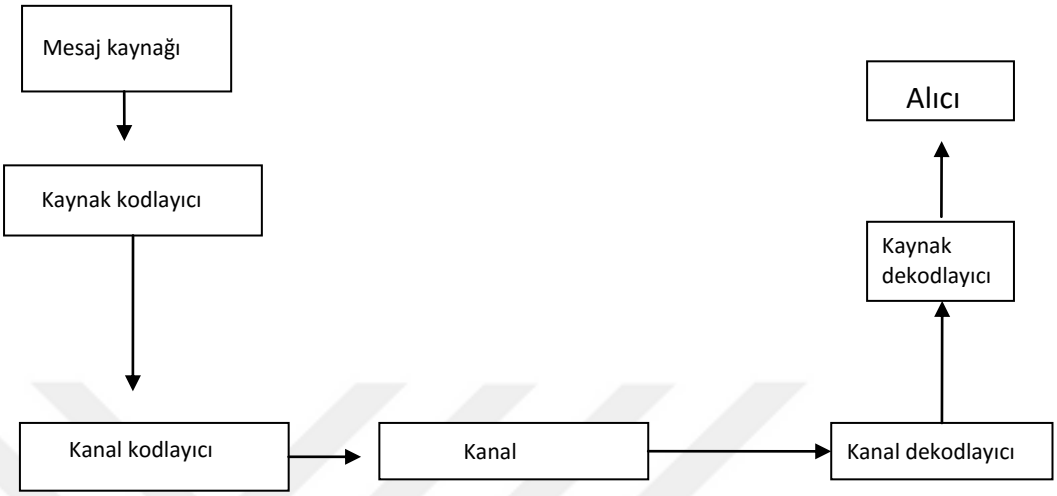
elma → 00, muz → 01, kiraz → 10, üzüm → 11.

Gönderilen mesaj elma yani 00 olsun ve gürültülü kanaldan geçerken karşılaşılan bir sorun nedeniyle 01 olarak alınsın. Bu durumda mesaj hatalı iletilmiş olur. Bu iletim için kodlama şeması Şekil 2.2 deki gibi olur.



Şekil 2. 2 Hatalı iletim

Kanal kodlaması fikri, hataları tespit edebilen veya düzeltilebilecek şekilde fazlalık özelliğini sunarak kaynak kodlamadan sonra mesajı tekrar kodlamaktır. Böylece, Şekil 2.1, Şekil 2.3'e dönüşür.



Şekil 2. 3 Geniş kodlama şeması

Örnek 2.84 [30]

Yukarıdaki örneği aşağıdaki gibi 1 bit fazladan ekleyerek kanal kodlaması yapalım:

$$00 \to 000,\ \ 01 \to 011,\ \ \ 10 \to 101,\ \ \ 11 \to 110$$

Kaynak ve kanal kodlamasından sonra 000 olarak kodlanan 'elma' mesajının gürültülü bir kanal üzerinden iletildiğini ve yalnızca bir bitte hata oluştuğunu varsayalım. Bu durumda alınan sözcük şu üçünden biri olmalıdır: $100, 010$ veya 001. Bu alınan kodların hiçbiri kodlanmış iletilerimizden değildir. Bu şekilde, hata tespit edilir.

Bu yöntemle 2 bitlik bir mesaj iletmek için 3 bitlik gönderim yapılır. Bu hatanın tespitini sağlar ancak hızı düşürür.

Yukarıdaki kanal kodlama düzeni 1 bitlik hatayı tespit eder ancak düzeltemez. Örneğin, alınan mesaj 100 olduğunda, 100 ün 000 da mı, 110 da mı yoksa 101 de mi hata yapılarak geldiğini gösteremez. Ancak, daha fazla bitlik ekleme yapılırsa hata düzeltilebilir. Örneğin, aşağıdaki kanal kodlama şemasını tasarlayabiliriz:

$00 \to 00000,\ \ 01 \to 01111,\ \ 10 \to 10110,\ \ 11 \to 11001.$

Kodlanan 'elma' mesajının gürültülü bir kanal üzerinden iletildiğini ve yalnızca bir bitte hata oluştuğunu varsayalım. Bu durumda alınan sözcük şu beş sözcükten biri olmalıdır: $10000, 01000, 00100, 00010, 00001$. Alınan mesajın 10000 olduğunu varsayalım. 10000 in 00000 den geldiği kesin olarak söyenebilir. Çünkü 10000 ile diğer üç kodlanmış mesajın $01111, 10110, 11001$ lerinin her biri arasında en az iki hata vardır. Bit ekleme işlemi yapılırken fazlalık bit eklendikçe kodun hızının düştüğü gerçeği göz ardı edilmemelidir.

Kanal kodlamanın amacı kodlayıcıları ve kod çözücüleri şu sonuçları verecek şekilde oluşturmaktır:

- mesajların hızlı kodlanması;
- kodlanmış mesajların kolay aktarımı;
- alınan mesajların hızlı bir şekilde dekodlanması;
- birim zamanda maksimum bilgi transferi;
- maksimum hata tespiti veya düzeltme kapasitesi.

Tanım 2.85 [30]

Keyfi q elemanlı bir küme $A = \{a_1, a_2, ..., a_q\}$ olsun. Bu kümeye **kod alfabesi**, elemanlarına ise **kod sembolleri** denir. Buna göre,

i. A üzerinde n uzunluklu bir q lu **söz**, tüm i ler için her $w_i \in A$ olan bir $w = w_1 w_2 ... w_n$ dizisidir. Diğer bir ifadeyle w bir $(w_1, w_2, ..., w_n)$ vektörü olarak da kabul edilebilir.

ii. A nın, boştan farklı, aynı n uzunluklu sözlerini içeren C alt kümesine A üzerinde n uzunluklu, q lu **blok kod** denir.

iii. C nin her bir elemanına C de bir **kodsöz** denir.

iv. C deki kodsöz sayısına C nin **eleman sayısı** denir ve $|C|$ ile gösterilir.

v. n uzunluklu bir C kodunun (bilgi) **hızı**, $\frac{\log_q |C|}{n}$ olarak tanımlanır.

vi. n uzunluklu ve M tane elemana sahip koda bir (n, M) **kodu** denir.

Tanım 2.86 [30]

Alfabesi $F_2 = \{0,1\}$ cismi olan koda **ikili (binary) kod**, $F_3 = \{0,1,2\}$ cismi üzerinde tanımlanan koda ise **üçlü (ternary) kod** denir.

Örnek 2.87

i. $C = \{000,101,111\}$ kodu, F_2 cismi üzerinde tanımlanmış bir $(3,3)$ ikili koddur.

ii. $C = \{0000,1010,0101,0011,1001,0110,1100,1111\}$ kodu, F_2 cismi üzerinde tanımlanmış bir $(4,8)$ ikili koddur.

Tanım 2.88 [30]

Herhangi bir A alfabesi üzerinde n uzunluklu iki söz x ve y olsun. x ile y arasındaki **Hamming uzaklık**, x ve y nin birbirinden farklı bileşen sayısıdır ve $d(x,y)$ ile gösterilir.

$x = x_1 x_2 ... x_n$ ve $y = y_1 y_2 ... y_n$ olsun. Bu durumda, $d(x,y) = d(x_1, y_1) + ... + d(x_n, y_n)$ dir. Burada x_i ve y_i, 1 uzunluklu söz olarak düşünülür ve

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

olarak tanımlanır.

Örnek 2.89

Alfabe F_2 cismi ve $x = 01010, y = 01101, z = 11101$ olsun. Bu durumda,

$d(x,y) = 3, d(y,z) = 1, d(z,x) = 4$ olarak hesaplanır.

Önerme 2.90 [30]

x, y ve z, A alfabesi üzerinde n uzunluklu sözler olsun. Bu durumda,

- $0 \le d(x,y) \le n$,
- $d(x,y) = 0 \Leftrightarrow x = y$,
- $d(x,y) = d(y,x)$,
- (Üçgen eşitsizliği) $d(x,z) \le d(x,y) + d(y,z)$ sağlanır.

Tanım 2.91 [30]

En az iki kodsöz içeren bir C **kodunun minimum uzaklığı** kodsözleri arasındaki en küçük Hamming uzaklıktır ve $d(C)$ ile gösterilir. Diğer bir deyişle,

$d(C) = \min\{d(x,y) \mid x, y \in C, x \neq y\}$ olarak ifade edilebilir.

Tanım 2.92 [30]

n uzunluklu, M kodsöze ve d uzaklığa sahip koda **bir** (n, M, d) **kod** denir. n, M, d sayılarına ise C kodunun **parametreler**i denir.

Örnek 2.93

F_3 cismi üzerinde $C = \{000000, 000111, 111222\}$ kodu, $(6,3,3)$ parametrelerine sahip bir koddur.

Tanım 2.94 [30]

Eğer bir C kodundaki her bir kodsözün en az 1 ve en fazla $t > 0$ bileşeninde hata oluşmasıyla elde edilen söz yine kodsöz değilse C ye $t-$ **hata tespit eden kod** denir. Eğer C kodu, $t-$ hatayı tespit edip $t+1$ hatayı tespit edemiyorsa C ye **tam** $t-$ **hata tespit eden kod** denir.

Teorem 2.95 [30]

Bir C kodunun $t-$ hata tespit eden bir kod olması için gerek ve yeter koşul $d(C) \ge t+1$ olmasıdır. $d(C) = t$ ise C kodu tam $(t-1)-$ hata tespit eder.

İspat

$d(C) \geq t+1$ olsun. Eğer $c \in C$ ve herhangi bir x vektörü için $1 \leq d(c,x) \leq t < d(C)$ eşitsizliği sağlanıyorsa $x \notin C$ elde edilir. Buradan, C kodunun $t-$ hata tespit eden kod olduğu söylenir.

Tersine, $d(C) < t+1$ yani, $d(C) \leq t$ eşitsizliği sağlanıyorsa, $1 \leq d(c_1,c_2) = d(C) \leq t$ olacak şekilde $c_1, c_2 \in C$ elemanları mevcuttur. Genelliği bozmadan c_1 kodsözünü ele alalım ve $d(C)$ tane bileşeninde hata oluşarak c_2 kodsözünün elde edildiğini kabul edelim. $c_2 \in C$ bir kodsöz olduğundan C kodu, $t-$hata tespit edemez.

Tanım 2.96 [30]

Eğer C kodundaki herhangi bir kodsözün en az 1, en fazla $t > 0$ bileşeninde hata oluşmasıyla elde edilen söz C nin başka bir kodsözünden en az 1, en fazla t bileşeninde hata meydana gelmesiyle elde edilemiyorsa C koduna $t-$ **hata düzelten bir kod** denir. Eğer C kodu $t-$ hata düzelten bir kod ve $(t+1)-$ hata düzeltemiyorsa C ye **tam** t **hata düzelten kod** denir.

Örnek 2.97

İkili $C = \{000, 111\}$ kodu verilsin.

- Eğer 000 mesajı gönderilirse ve gönderim esnasında bir bileşeninde hata meydana gelirse alınan söz, $100, 010, 001$ sözlerinden biri olacaktır. En küçük mesafeye sahip kodsöze dekodlama tekniği ile, kolaylıkla alınan bu hatalı söz 000 kodsözü olarak dekodlanır.
- Eğer 111 mesajı gönderilirse ve gönderim esnasında bir bileşeninde hata meydana gelirse alınan söz, $110, 011, 101$ sözlerinden biri olacaktır. En küçük mesafeye sahip kodsöze dekodlama tekniği ile, kolaylıkla alınan bu hatalı söz 111 kodsözü olarak dekodlanır.

Bu sebeple C kodu, $1-$hata tespit eden ve $1-$hata düzelten bir koddur.

- 000 mesajı gönderildiği ve gönderim esnasında iki bileşeninde hata meydana gelerek alınan sözün 011 olduğu kabul edilsin. Bu durumda en küçük mesafeye

sahip kodsöze dekodlama tekniği ile, C kodu alınan bu hatalı sözü 000 doğru mesajı yerine 111 kodsözü olarak dekodlar.

Bu ise C kodunun tam $2-$hata tesbit edebilen, tam $1-$hata düzelten bir kod olduğunu gösterir.

Teorem 2.98 [30]

Bir C kodunun t hata düzeltebilen kod olması için gerek ve yeter koşul $d(C) \geq 2t+1$ olmasıdır. $d(C) = 2t+1$ ise C kodu tam $t-$ hata düzeltebilen koddur.

İspat

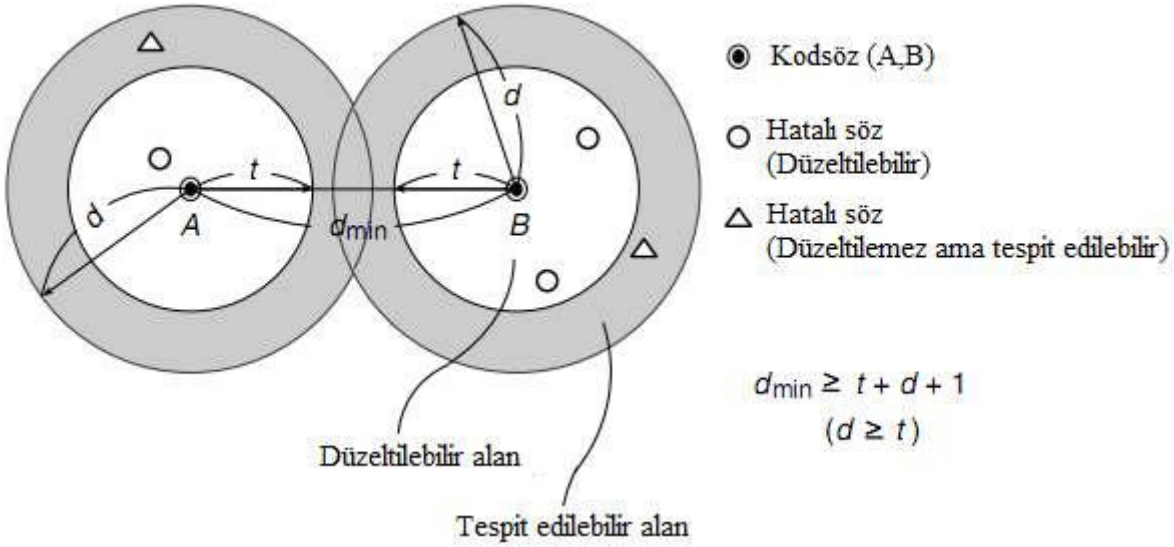
Önce ikinci tarafı ispatlanacaktır. $d(C) \geq 2t+1$ olsun. Gönderilen kodsöz c ve alınan söz x olsun. Gönderim sırasında t yada daha az bileşende hata meydana geldiyse $d(c,x) \leq t$ eşitsizliği yazılabilir. Buradan, her $c' \in C, c \neq c'$ kodsözü için $d(x,c') \geq d(c,c') - d(x,c) \geq 2t+1-t = t+1 > d(x,c)$ sağlanır. Bu ise x sözünün c kodsözüne dekodlanabileceğini gösterir. Bu nedenle, C kodu $t-$hata düzeltebilen koddur.

Tersine, C kodu $t-$hata düzeltebilen bir kod olsun. $d(C) < 2t+1$ eşitsizliği sağlanıyorsa $d(c,c') = d(C) \leq 2t$ olacak şekilde birbirinden farklı $c, c' \in C$ kodsözleri mevcuttur. Şimdi, c mesajının gönderildiğini ve hatalı olarak c' kodsözüne dekodlandığı varsayılarak, bunun C kodunun $t-$hata düzelten kod olması ile çeliştiği gösterilecektir. Böylece $d(C) \geq 2t+1$ eşitsizliği sağlanır.

Eğer $d(c,c') < t+1$ ise c kodsözü, en çok t bileşeninde hata meydana gelerek c' kodsözüne dönüşebilir. Bu durumda hatalı olarak c' kodsözüne dekodlar. Bu ise C kodunun $t-$hata düzeltebilen kod olması kabulü ile çelişir. Bu nedenle $d(C) \geq t+1$ olmalıdır. Genelliği bozmadan, $d = d(C)$ ve $t+1 \leq d \leq 2t$ olmak üzere c kodsözünün ilk d bileşeninde değişiklik yapılarak c' kodsözü elde edilsin. Eğer alınan söz

$$x = \underbrace{x_1 \ldots x_t}_{c' \text{ ile ortak}} \underbrace{x_{t+1} \ldots x_d}_{c \text{ ile ortak}} \underbrace{x_{d+1} \ldots x_n}_{\text{her ikisiyle de ortak}}$$

ise, $d(x,c') = d - t \le t = d(x,c)$ eşitliği sağlanır. Buradan, $d(x,c') < d(x,c)$ ya da $d(x,c) = d(x,c')$ sağlanır.



Şekil 2. 4 Hata tespit etme ve hata düzeltme prosedürü

Uyarı 2.99

Kodlama teorisinin temel problemi en iyi parametrelere sahip kodları bulmaktır. Bunu yaparken uzunluk, eleman sayısı, minimum uzaklık parametrelerinden ikisi sabit tutularak diğer parametre optimize edilir. Yani;

- n uzunluğa ve M eleman sayısına sahip kod için mümkün olan en büyük minimum Hamming uzaklığına,
- M elemana ve d minimum Hamming uzaklığa sahip bir kod için mümkün en küçük n uzunluğa,
- n uzunluğunda ve d minimum Hamming uzaklığa sahip bir kod için mümkün en büyük M elemana sahip olan kodlar optimaldir.

Tanım 2. 100 [30]

s elemana sahip bir A alfabesi üzerinde tanımlı n uzunluğunda d minimum uzaklığa sahip bir kodun eleman sayısının mümkün en büyük değeri $A_s(n,d) = \max\{M \mid C \subseteq A^n, C \text{ bir } (n,M,d) \text{ kod}\}$ ile tanımlanır.

2.5 Cisimler Üzerinde Lineer Kodlar

Bu alt bölümde bir q bir asal sayının kuvveti olmak üzere, F_q sonlu cismi üzerinde hata düzelten lineer kodlar ile ilgili temel kavramlar verilmektedir. Bu kavramlar arasında vektör uzayı ile lineer kod arasındaki ilişki, üreteç ve kontrol matrisleri, bir kodun minimum uzaklığı ve minimum uzaklığı sayesinde kodun hata tespit ve düzeltme kapasitesi yer almaktadır.

Tanım 2.101 [30]

F_q, q mertebeli bir sonlu cisim olsun. F_q^n vektör uzayının boştan farklı herhangi bir alt uzayına F_q^n üzerinde bir **lineer kod** denir.

Uyarı 2.102

Lineer kodların lineer olmayan kodlara göre sağladığı avantajlar şunlardır:

- Lineer kod, bir alt vektör uzayı olduğundan bir tabana sahiptir. Böylece tabanda bulunan az sayıda elemanla tüm elemanları ifade edilir.
- Lineer kodun minimum uzaklığı, sıfırdan farklı kodsözlerin Hamming ağırlığının minimumuna eşittir.
- Lineer kodların kodlama ve dekodlama prosedürleri ve algoritmaları daha hızlı ve daha kolaydır.

Tanım 2.103 [30]

F_q^n üzerinde bir C **lineer kodun boyutu**, bir vektör uzayı olarak boyutu olarak tanımlanır ve $boy(C) = k$ ile gösterilir. F_q^n üzerinde, n uzunluklu, k boyutlu C lineer kod, bir $[n,k]_q -$ kod olarak gösterilir.

Teorem 2.104 [30]

F_q^n üzerinde k boyutlu bir C lineer kodun kodsöz sayısı, $|C| = q^k$ olarak hesaplanır.

İspat

C lineer kodu bir alt F_q – vektör uzayı olduğundan ve $boy(V)=k$ olan bir alt uzay q^k sayıda vektör içerdiğinden $|C|=q^k$ olarak bulunur.

Tanım 2.105 [30]

${F_q}^n$, $\langle .,. \rangle$ iç çarpımı ile bir vektör uzayı ve ${F_q}^n$ üzerinde n uzunluklu bir lineer kod C olsun. Bu durumda, $C^{\perp}=\{v \in {F_q}^n \mid \langle c,v \rangle = 0, \forall c \in C\}$ kümesine C lineer kodun **dual**i denir.

Bu $\langle .,. \rangle : {F_q}^n \times {F_q}^n \to F_q$ tanımlanan bu iç çarpım işlemi $u,v,w \in {F_q}^n$ vektörleri olmak üzere aşağıdaki özellikleri sağlar:

i. $\langle u+v,w \rangle = \langle u,w \rangle + \langle v,w \rangle$,

ii. $\langle u,v+w \rangle = \langle u,v \rangle + \langle u,w \rangle$,

iii. Her $u \in {F_q}^n$ elemanı için $\langle u,v \rangle = 0$ olması için gerek ve yeter koşul $v=0$ olmasıdır,

iv. Her $v \in {F_q}^n$ elemanı için $\langle u,v \rangle = 0$ olması için gerek ve yeter koşul $u=0$ olmasıdır.

Teorem 2.106 [30]

${F_q}^n$ üzerinde n uzunluklu bir C lineer kod ve duali $C^{\perp}$ için;

i. $C^{\perp}$ bir lineer koddur.

ii. $boy(C)+boy(C^{\perp})=n$,

iii. $(C^{\perp})^{\perp}=C$ eşitlikleri sağlanır.

İspat

i. Bir alt uzayın dik tümleyeni de bir alt uzay olduğundan $C^{\perp}$ dual kodu bir lineer koddur.

ii. Vektör uzaylarında ispatlanan boyut teoreminden (Teorem 2.81) sonuç direkt görülür.

iii. (ii) de C yerine $C^{\perp}$ alındığında, $boy(C) = boy\left(\left(C^{\perp}\right)^{\perp}\right)$ eşitliği elde edilir. Bu nedenle $\left(C^{\perp}\right)^{\perp} = C$ olduğunu göstermek için $C \subseteq \left(C^{\perp}\right)^{\perp}$ olduğunu göstermek yeterlidir.

$c \in C$ olsun. Her $x \in C^{\perp}$ vektörü için, dual kodun tanımından $\langle x, c \rangle = 0$ sağlanır. Bu ise $c \in \left(C^{\perp}\right)^{\perp}$ olduğunu gösterir. Böylece $C \subseteq \left(C^{\perp}\right)^{\perp}$ sağlanır.

Tanım 2.107 [30]

$F_q^{\,n}$ üzerinde n uzunluklu bir C lineer kod ve duali $C^{\perp}$ için;

- $C \subseteq C^{\perp}$ ise C ye **kendine dik** (self orthogonal) kod denir,
- $C = C^{\perp}$ ise C ye **kendine dual** (self dual) kod denir.

Önerme 2.108 [30]

Kendine dik olan n uzunluğundaki bir lineer kodun boyutu $k \le \frac{n}{2}$ ve kendine dual olan n uzunluğundaki bir lineer kodun boyutu $k = \frac{n}{2}$ dir.

Tanım 2.109 [30]

$F_q^{\,n}$ vektör uzayında,

- Bir $x = (x_1, ..., x_n)$ sözünün sıfırdan farklı koordinat sayısına x in **Hamming ağırlığı** denir ve $wt(x) = \left|\{i \mid x_i \neq 0\}\right|$ ile gösterilir. 0 ile tüm bileşenleri sıfır olan vektör gösterilmek üzere $wt(x) = d(x, 0) = \left|\{x_l \mid x_l \neq 0\}\right|$ şeklinde de ifade edilir.
- Bir $x = (x_1, ..., x_n)$ ve $y = (y_1, ..., y_n)$ sözlerinin birbirlerinden farklı bileşen sayısı bu sözler arasındaki **Hamming uzaklık** olarak tanımlanır. Yani Hamming uzaklık, $d(x, y) = \left|\{i \mid x_i \neq y_i\}\right| = wt(x - y)$ olarak hesaplanır.

Önerme 2.110 [30]

$x, y \in F_q^{\,n}$ vektörleri için $d(x, y) = wt(x - y)$ dir.

İspat

$x, y \in F_q^{\,n}$ vektörleri için $d(x, y) = 0$ eşitliği ancak $x = y$ olması durumunda sağlanır. Bu ise $x - y = 0$ olması demektir. Buradan $wt(x - y) = 0$ eşitliği elde edilir. Ayrıca $wt(x - y) = wt(x_1 - y_1) + ... + wt(x_n - y_n)$ olduğundan istenen eşitlik elde edilir.

Sonuç 2.111

q çift sayı ise $x, y \in F_q^{\,n}$ için $d(x, y) = wt(x + y)$ eşitliği sağlanır.

Teorem 2.112

F_q üzerinde bir C lineer kodu için $d(C) = wt(C)$ olarak bulunur.

İspat

Her x, y sözü için $d(x, y) = wt(x - y)$ eşitliği ile ispatlandı. Hamming ağırlık tanımından, $d(x', y') = d(C)$ olacak şekilde $x', y' \in C$ kodsözleri vardır. Bu nedenle, $x' - y' \in C$ olduğundan $d(C) = d(x', y') = wt(x' - y') \geq wt(C)$ elde edilir.

Tersine, $wt(C) = wt(z)$ olacak şekilde sıfırdan farklı $z \in C$ kodsözü için, $wt(C) = wt(z) = d(z, 0) \geq d(C)$ elde edilir. Bu iki eşitsizlikten $d(C) = wt(C)$ eşitliği elde edilir.

Örnek 2.113

F_3 cismi üzerinde

$C = \{0000, 1200, 0010, 2100, 0020, 1210, 1220, 2110, 2120\}$

üçlü lineer kodu bir $(4, 2)-$ koddur. $d(C) = wt(C) = 1$ dir.

Tanım 2.114 [30]

q asalın kuvveti olmak üzere F_q üzerinde n uzunluklu d minimum uzaklığına sahip bir lineer kodun eleman sayısının mümkün en büyük değeri $B_q(n,d) = \max\{q^k \mid C \subseteq F_q^{\,n} \text{ ve } C \text{ bir } [n,k,d]-kod\}$ ile tanımlanır. Bu durumda C, $F_q^{\,n}$ üzerinde bir $[n,k,d]-$kod ve $q^k = B_q(n,d)$ ise C lineer koduna **optimal kod** denir.

Tanım 2.115 [30]

$F_q^{\,n}$ üzerinde n uzunluklu bir C lineer kod ve duali $C^{\perp}$ için;

- C lineer kodun alt vektör uzayı olarak tabanını oluşturan elemanlarını satır kabul eden matrise C lineer kodun **üreteç matrisi** denir. G ile gösterilir.
- Her $c \in C$ için $Hc^T = 0$ eşitliğini sağlayan H matrisine $C^{\perp}$ dual kodun üreteç matrisi veya C lineer kodun **kontrol matrisi** denir.

Uyarı 2.116

$F_q^{\,n}$ üzerinde n uzunluklu bir C lineer kodu için bir üreteç matris G, kontrol matrisi H olsun. Bu durumda,

- C nin parametreleri $[n,k]_q$ ise G matrisi $k \times n$ ve H matrisi $(n-k) \times n$ formundadır.
- G ve H matrislerinin satırları lineer bağımsızdır.
- $C = \{x \in F_q^{\,n} \mid Hx^T = 0\}$ dir.

Tanım 2.117

i. Bir üreteç matris $(I_k \mid X)$ formundaysa bu üreteç matrise **standart formda üreteç matris** denir.

ii. Bir kontrol matrisi $(-X^T \mid I_{n-k})$ formundaysa bu kontrol matrisine **standart formda kontrol matrisi** denir.

Önerme 2.118 [30]

C, $F_q^{\,n}$ üzerinde bir $[n,k]-$lineer kod ve üreteç matrisi G olsun. Bu durumda,

- $v \in F_q^{\,n}$ nin $C^{\perp}$ dual kodun bir elemanı olması için gerek ve yeter koşul v vektörünün G üreteç matrisinin her bir satırına dik olması, diğer bir ifadeyle, $vG^T = 0$ olmasıdır.
- Verilen bir $(n-k)\times n$ tipindeki H matrisinin, C lineer kodu için kontrol matrisi olması için gerek ve yeter koşul H matrisinin satırlarının lineer bağımsız olması ve $HG^T = 0$ olmasıdır.

İspat

- G üreteç matrisinin $i-$nci satırı r_i vektörü olarak gösterilsin. $r_i \in C$ olduğundan $1 \le i \le k$ için her bir $c \in C$ kodsözü, $a_1,...,a_k \in F_q$ olmak üzere $c = a_1 r_1 + ... + a_k r_k$ olarak ifade edilebilir. $v \in C^{\perp}$ ise her $c \in C$ kodsözü için $\langle v, c \rangle = 0$ olacaktır. Özel olarak, her $1 \le i \le k$ için $\langle v, r_i \rangle = 0$ olup $vG^T = 0$ eşitliği sağlanır.

  Tersine, her $1 \le i \le k$ için $\langle v, r_i \rangle = 0$ olsun. Her $c = a_1 r_1 + ... + a_k r_k \in C$ kodsözü için $\langle v, c \rangle = a_1 \langle v, r_1 \rangle + ... + a_k \langle v, r_k \rangle = 0$ eşitliği yazılabilir.

- Eğer H matrisi, C kodu için bir kontrol matrisi ise H nın satırları lineer bağımsızdır. H matrisinin satır vektörleri $C^{\perp}$ dual kodun kodsözleri olduğundan $HG^T = 0$ eşitliği sağlanır.

  Tersine, eğer $HG^T = 0$ eşitliği sağlanıyorsa H matrisinin satır uzayı (satırlarını oluşturan vektörlerin ürettiği vektör uzayı) $C^{\perp}$ tarafından içerilir. H matrisinin satırları lineer bağımsız ve $boy(H) = n-k$ olduğundan H nın satır uzayı tam olarak $C^{\perp}$ dual koduna eşittir. Yani, H matrisi $C^{\perp}$ dual kodu için bir üreteç matris olup C lineer kodu için bir kontrol matrisidir.

Teorem 2.119 [30]

C, $F_q^{\,n}$ üzerinde bir $[n,k]-$lineer kod ve kontrol matrisi H olsun. Bu durumda aşağıdaki ifadeler geçerlidir:

- $d(C)\geq d$ olması için gerek ve yeter koşul H matrisinin herhangi $d-1$ tane sütununun lineer bağımsız olmasıdır.
- $d(C)\leq d$ olması için gerek ve yeter koşul H matrisinin en az d tane sütununun lineer bağımlı olmasıdır.

İspat

$v=(v_1,...,v_n)\in C$ kodsözünün ağırlığı $e>0$ olsun. v vektörünün $i_1,...,i_e$ pozisyonlarında sıfırdan farklı bileşenler olduğu ve $j\notin\{i_1,...,i_e\}$ için $v_j=0$ olduğu kabul edilsin. c_i, H matrisinin $i-$nci sütununu göstermek üzere, $0=vH^T=v_{i_1}c_{i_1}{}^T+...+v_{i_e}c_{i_e}{}^T$ eşitliği sağlanır. Buradan, H matrisinin $\{c_{i_1},...,c_{i_e}\}$ olarak etiketlenen e tane sütunu lineer bağımlıdır.

- $d(C)\geq d$ olduğunu söylemek, C kodunun, ağırlığı $\leq d-1$ olan sıfırdan hiçbir kodsöz içermediğini söylemek demektir. Bu ise H matrisinin herhangi $\leq d-1$ tane sütununun lineer bağımsız olması demektir.
- Benzer şekilde, $d(C)\leq d$ olduğunu söylemek, C kodunun, ağırlığı $\leq d$ olan sıfırdan en az bir kodsöz içerdiğini söylemek demektir. Bu ise H matrisinin en az d tane sütununun lineer bağımlı olması demektir.

Sonuç 2.120

C, $F_q^{\,n}$ vektör uzayı üzerinde bir $[n,k]-$lineer kod ve kontrol matrisi H olsun. Aşağıdakiler denktir:

- $d(C)=d$,
- H matrisinin herhangi $d-1$ tane sütunu lineer bağımsızdır ve H matrisinin d tane sütunu lineer bağımlıdır.

Örnek 2.121

F_2^5 üzerinde C lineer kodu için bir kontrol matrisi

$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$ olsun. H matrisinin $3.$ ve $4.$ sütunları toplandığında $1.$ sütunu elde edildiğinden 3 sütunu lineer bağımlıdır. Herhangi 2 sütunu da lineer bağımsız olduğundan C nin minimum uzaklığı $d(C) = 3$ dir.

2.6 Cisimler Üzerinde Devirli Kodlar

Devirli kodlar ilk olarak Eugene Prange tarafından 1957 yılında tanımlanmıştır [34]. Bu alt bölümde q bir asal sayının kuvveti olmak üzere F_q sonlu cismi üzerinde devirli koldarın yapısı anlatılacaktır.

Tanım 2.122

F_q^n vektör uzayının bir S alt kümesinden alınan her bir $(a_0, a_1, ..., a_{n-1})$ vektörü için $(a_{n-1}, a_0, ..., a_{n-2}) \in S$ vektörüne, $(a_0, a_1, ..., a_{n-1})$ vektörünün bir $1-$**devirli ötelemesi** denir. $(a_{n-1}, a_0, ..., a_{n-2})$ de S kümesinin bir elemanı ise S kümesine **devirli küme** denir. F_q üzerinde C lineer kodu, bir devirli küme ise C ye **devirli kod** denir.

Örnek 2.123

- F_q^n ve $\{000...0\}$ aşikar devirli kodlardır.
- F_2^7 üzerinde

  $C = \{0000000, 1011100, 0101110, 0010111, 1110010, 0111001, 1001011, 1100101\}$

  ikili kodu devirli bir koddur.

Aşağıdaki lineer dönüşüm yardımıyla devirli kodların cebirsel yapısı oluşturulmaktadır:

$$\pi: \quad F_q^n \quad \rightarrow \quad F_q[x] \Big/ (x^n - 1)$$
$$(a_0, a_1, ..., a_{n-1}) \mapsto a_0 + ... + a_{n-1}x^{n-1}$$

şeklinde tanımlansın. Bu durumda, π, F_q-lineer dönüşümü $u=(u_0,u_1,...,u_{n-1})$ vektörünü $u(x)=\sum_{i=0}^{n-1}u_i x_i$ polinomuna dönüştürür. $F_q[x]/(x^n-1)$, $F_q{}^n$ deki toplama ve çarpma ile bir halkadır. Böylece, $F_q{}^n$ deki bir vektörün devirli ötelemesi, $F_q[x]/(x^n-1)$ deki o vektöre karşılık gelen polinomun x ile çarpılmasına karşılık gelir.

Örnek 2.124

F_2 cismi üzerinde $C=\{000,110,101,011\}$ lineer kodu devirli bir koddur. π lineer dönüşümü altında $\pi(C)=\{0,1+x,1+x^2,x+x^2\}\subset F_2[x]/(x^3-1)$ elde edilir. Burada $\{0,1+x,1+x^2,x+x^2\}$ kümesinin $F_2[x]/(x^3-1)$ halkasının bir ideali olduğuna dikkat edilmelidir.

Teorem 2.125

F_q bir cisim olmak üzere $F_q[x]/(x^n-1)$ bölüm halkası temel (esas) ideal halkasıdır.

İspat

$F_q[x]/(x^n-1)$ bölüm halkasının sıfırdan farklı bir I idealinin bir en küçük dereceli $g(x)\neq 0$ polinomu verilsin. Her $f(x)\in I$ polinomu için, $f(x)=s(x)g(x)+r(x)$ olacak şekilde $s(x),r(x)\in F_q[x]$ vardır ve $der(r(x))<der(g(x))$ eşitsizliği geçerlidir. $r(x)=f(x)-s(x)g(x)\in I$ ve $g(x)\in I$ en küçük dereceli polinom olduğundan $r(x)=0$ olmak zorundadır. Bu nedenle $I=(g(x))$ olup $F_q[x]/(x^n-1)$ bölüm halkası temel (esas) ideal halkasıdır.

Teorem 2.126 [30]

π, yukarıda tanımlanan F_q −lineer dönüşümü olmak üzere $F_q^{\,n}$ vektör uzayının boştan farklı bir C alt kümesi bir devirli koddur ancak ve ancak $\pi(C)$, $F_q[x]/(x^n-1)$ nin bir idealidir.

İspat

$\pi(C)$, $F_q[x]/(x^n-1)$ bölüm halkasının bir ideali olsun. Bu durumda her $a,b \in F_q \subset F_q[x]/(x^n-1)$ ve $c_1,c_2 \in C$ kodsözleri için $a\pi(c_1), b\pi(c_2) \in \pi(C)$ elde edilir. Buradan $a\pi(c_1)+b\pi(c_2) \in \pi(C)$ olup $\pi(ac_1+bc_2) \in \pi(C)$ bulunur. Bu ise $ac_1+bc_2 \in C$ demektir. Böylece C kodu bir lineer koddur. $c=(c_0,...,c_{n-1}) \in C$ kodsözü için $\pi(c)=c_0+c_1x+...+c_{n-1}x^{n-1}$ polinomu $\pi(C)$ nin bir elemanıdır. $\pi(C)$, $F_q[x]/(x^n-1)$ halkasının bir ideali olduğundan,

$$\begin{aligned} x\pi(c) &= c_0x+...+c_{n-1}x^n \\ &= c_{n-1}+c_0x+...+c_{n-1}(x^n-1) \\ &= c_{n-1}+c_0x+...+c_{n-2}x^{n-1} \\ &\in \pi(C) \end{aligned}$$

bulunur. Bu nedenle C lineer kodu bir devirli koddur.

Tersine, C bir devirli kod olsun. Bu durumda $\pi(C)$ den alınan herhangi bir $f(x)$ polinomu için $(f_0,...,f_{n-1}) \in C$ olmak üzere $f(x)=f_0+f_1x+...+f_{n-1}x^{n-1}=\pi(f_0,...,f_{n-1})$ olup C devirli kod olduğundan $xf(x)=f_{n-1}+f_0x+...+f_{n-2}x^{n-1} \in \pi(C)$ sağlanır. Böylece $x^2f(x)=x(xf(x)) \in \pi(C)$ sağlanır. Tümevarımla, her $i \geq 0$ için $x^if(x) \in \pi(C)$ sağlanır. C bir lineer kod ve π bir

lineer dönüşüm olduğundan $\pi(C)$, F_q üzerinde bir lineer uzaydır. Buradan, her $g(x)=g_0+\ldots+g_{n-1}x^{n-1}\in F_q[x]/(x^n-1)$ polinomu için $g(x)\,f(x)=\sum_{i=1}^{n} g_i\left(x^i f(x)\right)\in\pi(C)$ sağlanır. Bu ise $\pi(C)$ nin $F_q[x]/(x^n-1)$ halkasının bir ideali olduğunu gösterir.

Örnek 2.127

$C=\{000,111,222\}$ üçlü devirli kodu verilsin. $\pi(C)=\{0,1+x+x^2,2+2x+2x^2\}$, $F_3[x]/(x^3-1)$ halkasının bir idealidir.

Teorem 2.128 [30]

I, $F_q[x]/(x^n-1)$ nin sıfırdan farklı bir ideali ve $g(x)$, I daki sıfırdan farklı, en küçük dereceli, monik (baş katsayısı 1), indirgenemez polinom olsun. Bu durumda, $g(x)$, I idealinin bir üretecidir ve x^n-1 i böler.

İspat

$x^n-1=s(x)g(x)+r(x)$ ve $der(r(x))<der(g(x))$ olsun. Bu durumda $r(x)=(x^n-1)-s(x)g(x)\in I$ sağlanır. x^n-1 polinomunun, $F_q[x]/(x^n-1)$ halkasının sıfırı olduğu göz önünde bulundurulursa, $g(x)$ polinomunun en küçük dereceli olmasından dolayı $r(x)=0$ olmalıdır. Böylece $g(x)\,|\,x^n-1$ elde edilir.

Sonuç 2.129

I idealinde x^n-1 i bölen, monik, indirgenemez, en küçük dereceli polinom tektir.

Tanım 2.130

$F_q[x]/(x^n-1)$ nin sıfırdan farklı bir I idealinin en küçük dereceli, monik, indirgenemez polinomuna I nin **üreteç polinom**u denir. C bir devirli kod olmak üzere, $\pi(C)$ nin üreteç polinomuna C **nin üreteç polinomu** denir.

Teorem 2.131

x^n-1 polinomunun her bir monik böleni $F_q^{\,n}$ de bazı devirli kodlar için üreteç polinomdur.

İspat

$g(x)$ polinomu, x^n-1 polinomunun bir monik böleni ve I, $F_q[x]/(x^n-1)$ halkasının $g(x)$ tarafından üretilen ideali olsun. C, $h(x)$ polinomuna karşılık gelen devirli kod olmak üzere $h(x)\equiv g(x)b(x)\bmod(x^n-1)$ olacak şekilde bir $b(x)$ polinomu mevcuttur. Bu durumda $g(x)$ polinomu, $h(x)$ polinomunun bir bölenidir. $h(x)$ en küçük dereceli ve monik polinom olduğundan $g(x)$, $h(x)$ polinomunun kendisi olmalıdır.

Sonuç 2.132

$F_q^{\,n}$ deki devirli kodlarla $x^n-1\in F_q[x]$ nin monik bölenleri arasında birebir bir eşeleme vardır.

Örnek 2.133

$1\in F_q[x]$, $F_q^{\,n}$ vektör uzayına ve $x^n-1\in F_q[x]$, $\{0\ldots0\}$ devirli koduna karşılık gelir.

Örnek 2.134

6 uzunluklu tüm ikili devirli kodları bulmak için, $x^6-1\in F_2[x]$ nin monik çarpanları incelenmelidir:

$x^6-1=(1+x)^2(1+x+x^2)^2$ olduğundan tüm monik bölenler:

$1, 1+x, 1+x+x^2, (1+x)^2, (1+x)(1+x+x^2), (1+x)^2(1+x+x^2), (1+x+x^2)^2, (1+x)^2(1+x+x^2)^2,$
$1+x^6$.

Buradan 6 uzunluklu ikili devirli kodların sayısı 9 dur. Örneğin, $(1+x)(1+x+x^2)$ polinomunun ürettiği devirli kod,

$C = \{000000, 100100, 010010, 001001, 110110, 011011, 101101, 111111\}$ dir.

Teorem 2.135

$g(x)$ polinomu, $F_q[x] / (x^n - 1)$ bölüm halkasının bir idealinin üreteç polinomu olsun. Bu durumda $der(g(x)) = n-k$ ise $g(x)$ polinomunun ürettiği ideale karşılık geldiği devirli kodun boyutu k olarak hesaplanır.

İspat

$c_1(x) \neq c_2(x)$ polinomları dereceleri $\leq k-1$ olan polinomlar olmak üzere $g(x)c_1(x) \not\equiv g(x)c_2(x) \bmod (x^n - 1)$ yazılabilir. Bu nedenle

$A = \left\{ g(x)c(x) \mid c(x) \in F_q[x] / (x^n - 1), der(c(x)) \leq k-1 \right\}$ kümesinin q^k elemanı vardır ve $g(x)$ tarafından üretilen idealin bir alt kümesidir. Diğer taraftan, her $a(x)g(x)$ kodsözü aşağıdaki şekilde yazılabilir:

$a(x)g(x) = u(x)(x^n - 1) + v(x), der(v(x)) < n.$

$v(x) = a(x)g(x) - u(x)(x^n - 1)$ olduğundan $g(x)$, $v(x)$ in bir bölenidir. O halde $v(x) = b(x)g(x)$ yazılabilir. $der(b(x)) < k$ olduğundan $v(x) \in A$ elde edilir. Buradan $A = (g(x))$ olup kodun boyutu $\log_q |A| = k$ olarak hesaplanır.

Örnek 2.136

F_3 cismi üzerinde 4 uzunluklu üçlü devirli kodları bulmak için, $x^4 - 2 \in F_3[x]$ polinomunun monik çarpanları incelenmelidir:

$x^4 - 2 = (x^2 + x + 2)(x^2 + 2x + 2)$ olduğundan tüm monik bölenler:

$1, x^2+x+2, x^2+2x+2, 1+x^4$. Buradan 4 uzunluklu üçlü devirli kodların sayısı 4 tür. Örneğin, $2+x+x^2$ polinomunun ürettiği devirli kod,

$C=\{0000, 2110, 0211, 1220, 2021, 0122, 2202, 1101, 1012\}$ dir. Devirli kodlara benzer şekilde $|C|=3^{4-2}=9$ dir.

Teorem 2.137

C, $F_q^{\,n}$ üzerinde bir devirli kod ve $g(x)=g_0+g_1x+\ldots+g_{n-k}x^{n-k}\in F_q^{\,n}[x]$ polinomu x^n-1 in bir böleni olsun. $g(x)$, C nin bir üreteci ise,

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}=\begin{pmatrix} g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} \end{pmatrix}$$ matrisi C kodunun üreteç matrisidir.

İspat

$g(x), xg(x), \ldots, x^{k-1}g(x)$ polinomları C için bir taban olduğu gösterilmelidir. F_q üzerinde $g(x), xg(x), \ldots, x^{k-1}g(x)$ polinomları lineer bağımsızdır. $boy(C)=k$ eşitliği bilindiğinden sonuç görülür.

Tanım 2.138 [30]

Herhangi bir $k-$dereceli $h_R(x)=x^k h\left(\frac{1}{x}\right)=\sum_{i=0}^{k}a_{k-i}x^i$ polinomuna, $h(x)=\sum_{i=0}^{k}a_i x^i$ polinomunun **ters sıralı (reciprocal) polinomu** denir.

Teorem 2.139 [30]

$F_q^{\,n}$ deki C, $[n,k]-$devirli kodun üreteç polinomu $g(x)$ ve $h(x)=\frac{x^n-1}{g(x)}=h_0+h_1x+h_2x^2+\ldots+h_kx^k$ olsun. Bu durumda $h_0^{-1}h_R(x)$ polinomu C kodun kontrol polinomudur ve kontrol matrisi

$$H=\begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{n-k-1}h_R(x) \end{pmatrix}=\begin{pmatrix} h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{pmatrix}$$ dir.

İspat

Üreteç matris için yapılan ispata benzer şekilde kolaylıkla yapılabilir.

Örnek 2.140

$x^4-2=\left(x^2+x+2\right)\left(x^2+2x+2\right)\in F_3{}^4$ olduğundan x^2+x+2 böleni tarafından üretilen devirli kod için üreteç matris

$G=\begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 \end{pmatrix}$ dir ve $h_R(x)=2x^2+2x+1$ olduğundan kontrol matrisi $H=\begin{pmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 2 \end{pmatrix}$ dir.

Tanım 2.141

C, $F_q{}^n$ üzerinde bir devirli kod ve $e^2(x)\equiv e(x)\bmod\left(x^n-1\right)$ denkliğini sağlayan $e(x)$ polinomu olsun. C için bir üreteç polinomsa, $e(x)$ polinomuna C nin **idempotent üreteci** denir.

Teorem 2.142

$F_q{}^n$ deki C, $[n,k]-$devirli kod ve $(n,q)=1$ olsun. Bu durumda $C=\left(e(x)\right)$ olacak şekilde bir tek $e(x)$ idempotent polinomu vardır.

Önerme 2.143

$F_q{}^n$ deki C, $[n,k]-$devirli kod, $(n,q)=1$ ve $g(x)$ üreteç polinomu olsun. Bu durumda,

- x^n-1 polinomunun $F_q[x]$ de katlı kökü yoktur. Böylece, $x^n-1=h(x)g(x)$ ise $OBEB\left(g(x),h(x)\right)=1$ dir.

- $1 = a(x)g(x) + b(x)h(x)$ olacak şekilde $a(x), b(x) \in F_q[x]$ vardır.
- $e(x) \equiv a(x)g(x) \bmod (x^n - 1)$ polinomu C nin idempotent üretecidir.

Teorem 2.144

C, F_q^n üzerinde bir devirli kod ve $e(x)$, C kodunun idempotent üreteci olsun. Bu durumda $g(x) \equiv OBEB(e(x), x^n - 1) \in F_q[x]$ polinomu C için bir üreteç polinomudur.

Örnek 2.145

F_2^7 üzerinde devirli bir C kodu, $x^7 - 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + 1)$ in monik bölenlerinden biri olan $g(x) = x^3 + x^2 + 1$ polinomu tarafından üretilen devirli kod olsun. $1 = x^3(x^3 + x^2 + 1) + (x^2 + 1)(x^4 + x^3 + x^2 + 1)$ elde edilir. Böylece

$e(x) \equiv x^3(x^3 + x^2 + 1) \bmod (x^7 - 1) = x^6 + x^5 + x^3$ polinomu C için idempotent üreteçtir.

2.7 Cisimler Üzerinde Sabit Devirli (Constacyclic) Kodlar

F_q bir sonlu cisim $\lambda \in F_q$ sıfırdan farklı bir eleman olmak üzere $\lambda -$ sabit devirli kodlar ilk olarak Berlekamp tarafından 1968 yılında tanımlanmıştır [39]. Bir çok uygulama alanı bulunan bu kod ailesi, bir önceki alt bölümde tanıtılan devirli kodların bir genelleştirilmesidir. Bu alt bölümde sonlu cisimler üzerinde sabit devirli (constacylic) kodların yapısı incelenecektir.

Tanım 2.146 [39]

F_q vektör uzayının $S \subset F_q^n$ boştan farklı bir küme olsun. Alınan bir $(s_0, s_1, ..., s_{n-1}) \in S$ vektörünün $\lambda \in F_q - \{0\}$ olmak üzere bir $\lambda -$ **sabit devirli ötelemesi**, $(\lambda s_{n-1}, s_0, ..., s_{n-2})$ vektörü olarak tanımlanır. Eğer her $(s_0, s_1, ..., s_{n-1}) \in S$ vektörü için $(\lambda s_{n-1}, s_0, ..., s_{n-2})$ vektörü yine S kümesinin bir elemanı oluyorsa S kümesine $\lambda -$ **sabit devirli küme** denir. Eğer bir C lineer kodu bir $\lambda -$ sabit devirli küme ise C koduna bir $\lambda -$ **sabit devirli kod** denir.

Örnek 2.147

F_3 cismi alfabe olmak üzere $(2,1,2,0,1,1,0,1)$ vektörünün $2-$sabit devirli ötelemesi $(2,2,1,2,0,1,1,0)$ vektörüdür.

Aşağıdaki lineer dönüşüm yardımıyla $\lambda-$sabit devirli kodların cebirsel yapısı oluşturulmaktadır:

$$\pi_\lambda : \ F_q{}^n \rightarrow F_q[x]\Big/\left(x^n-\lambda\right)$$
$$(a_0,a_1,...,a_{n-1}) \mapsto a_0+...+a_{n-1}x^{n-1} \bmod\left(x^n-\lambda\right)$$

şeklinde tanımlansın. Bu durumda π_λ, F_q-lineer dönüşümü $u=(u_0,...,u_{n-1})$ vektörünü $u(x)=\sum_{i=0}^{n-1}u_i x_i$ polinomuna dönüştürür. $F_q[x]\Big/\left(x^n-\lambda\right)$, $F_q{}^n$ deki toplama ve çarpma ile bir halkadır. Böylece, $F_q{}^n$ deki bir vektörün $\lambda-$sabit devirli ötelemesi, $F_q[x]\Big/\left(x^n-\lambda\right)$ deki o vektöre karşılık gelen polinomun x ile çarpılmasına karşılık gelir.

Teorem 2.148 [39]

F_q bir cisim olmak üzere $F_q[x]\Big/\left(x^n-\lambda\right)$ bölüm halkası temel (esas) ideal halkasıdır.

İspat

Devirli kodlar için yapılan ispata benzer şekilde, $F_q[x]\Big/\left(x^n-\lambda\right)$ bölüm halkasının sıfırdan farklı bir I idealinin bir en küçük dereceli $g(x)\neq 0$ polinomu alınsın. Her $f(x)\in I$ polinomu için, $f(x)=s(x)g(x)+r(x)$ olacak şekilde $s(x),r(x)\in F_q[x]$ vardır ve $der(r(x))<der(g(x))$ eşitsizliği geçerlidir. $r(x)=f(x)-s(x)g(x)\in I$ ve $g(x)\in I$ en küçük dereceli polinom olduğundan $r(x)=0$ olmak zorundadır. Bu nedenle $I=(g(x))$ olup $F_q[x]\Big/\left(x^n-\lambda\right)$ bölüm halkası temel (esas) ideal halkasıdır.

Teorem 2.149 [39]

$$\pi_\lambda : \ F_q^{\,n} \ \rightarrow \ F_q[x]\Big/\left(x^n-\lambda\right)$$
$$\left(a_0,a_1,...,a_{n-1}\right)\mapsto a_0+...+a_{n-1}x^{n-1}\bmod\left(x^n-\lambda\right)$$

Lineer dönüşümü ile $F_q^{\,n}$ nin boştan farklı bir C alt kümesinin bir $\lambda-$sabit devirli kod olması için gerek ve yeter koşul $\pi_\lambda(C)$ nin, $F_q[x]\Big/\left(x^n-\lambda\right)$ bölüm halkasının bir ideali olmasıdır.

İspat

$\pi_\lambda(C)$, $F_q[x]\Big/\left(x^n-\lambda\right)$ bölüm halkasının bir ideali olsun. Bu durumda her $a,b\in F_q\subset F_q[x]\Big/\left(x^n-\lambda\right)$ ve $c_1,c_2\in C$ kodsözleri için $a\pi_\lambda(c_1),b\pi_\lambda(c_2)\in\pi_\lambda(C)$ elde edilir. Buradan $a\pi_\lambda(c_1)+b\pi_\lambda(c_2)\in\pi_\lambda(C)$ olup $\pi_\lambda(ac_1+bc_2)\in\pi_\lambda(C)$ bulunur. Bu ise $ac_1+bc_2\in C$ demektir. Böylece C kodu bir lineer koddur. $c=(c_0,...,c_{n-1})\in C$ kodsözü için $\pi_\lambda(c)=c_0+c_1x+...+c_{n-1}x^{n-1}$ polinomu $\pi_\lambda(C)$ nin bir elemanıdır. $\pi_\lambda(C)$, $F_q[x]\Big/\left(x^n-\lambda\right)$ halkasının bir ideali olduğundan,

$$\begin{aligned}&x\pi_\lambda(c)=c_0x+...+c_{n-1}x^n\\&=\lambda c_{n-1}+c_0x+...+c_{n-1}\left(x^n-\lambda\right)\\&=\lambda c_{n-1}+c_0x+...+c_{n-2}x^{n-1}\\&\in\pi_\lambda(C)\end{aligned}$$

bulunur. Bu nedenle C lineer kodu bir $\lambda-$sabit devirli koddur.

Tersine, C bir $\lambda-$sabit devirli kod olsun. Bu durumda $\pi_\lambda(C)$ den alınan herhangi bir $f(x)$ polinomu için $(f_0,...,f_{n-1})\in C$ olmak üzere $f(x)=f_0+f_1x+...+f_{n-1}x^{n-1}=\pi_\lambda(f_0,...,f_{n-1})$ olup C $\lambda-$sabit devirli kod olduğundan $xf(x)=\lambda f_{n-1}+f_0x+...+f_{n-2}x^{n-1}\in\pi_\lambda(C)$ ve $x^2f(x)=x\left(xf(x)\right)\in\pi_\lambda(C)$ sağlanır.

Tümevarımla, her $i \geq 0$ için $x^i f(x) \in \pi_\lambda(C)$ sağlanır. C bir lineer kod ve π_λ bir lineer dönüşüm olduğundan $\pi_\lambda(C)$, F_q üzerinde bir lineer uzaydır. Buradan, her $g(x) = g_0 + \ldots + g_{n-1}x^{n-1} \in F_q[x]/(x^n - \lambda)$ polinomu için $g(x) f(x) = \sum_{i=1}^{n} g_i \left(x^i f(x)\right) \in \pi_\lambda(C)$ sağlanır. Bu ise $\pi_\lambda(C)$ nin $F_q[x]/(x^n - \lambda)$ halkasının bir ideali olduğunu gösterir.

Örnek 2.150

F_3 cismi üzerinde $C = \{000, 101, 210, 011, 202, 120, 221, 112, 022\}$ lineer kodu $2-$sabit devirli bir koddur. π_2 lineer dönüşümü altında $\pi_2(C) = \{0, 1+x^2, 2+x^2, x+x^2, 2+2x^2, 1+2x, 2+2x+x^2, 1+x+2x^2, 2x+2x^2\} \subset F_3[x]/(x^3 - 2)$ dir. Burada $\{0, 1+x^2, 2+x^2, x+x^2, 2+2x^2, 1+2x, 2+2x+x^2, 1+x+2x^2, 2x+2x^2\}$ kümesinin $F_3[x]/(x^3 - 2)$ halkasının bir ideali olduğuna dikkat edilmelidir.

Teorem 2.151 [39]

I, $F_q[x]/(x^n - \lambda)$ nin sıfırdan farklı bir ideali ve $g(x)$, I daki sıfırdan farklı, en küçük dereceli, monik (baş katsayısı 1), indirgenemez polinom olsun. Bu durumda, $g(x)$, I idealinin bir üretecidir ve $x^n - \lambda$ polinomunu böler.

İspat

$x^n - \lambda = s(x) g(x) + r(x)$ ve $der(r(x)) < der(g(x))$ olsun. Bu durumda $r(x) = (x^n - \lambda) - s(x) g(x) \in I$ sağlanır. $x^n - \lambda$ polinomunun, $F_q[x]/(x^n - \lambda)$ halkasının sıfırı olduğu göz önünde bulundurulursa, $g(x)$ polinomunun en küçük dereceli olmasından dolayı $r(x) = 0$ olmalıdır. Böylece $g(x) \mid x^n - \lambda$ elde edilir.

Sonuç 2.152

I idealinde $x^n-\lambda$ polinomunu bölen, monik, indirgenemez, en küçük dereceli polinom tektir.

Tanım 2.153 [39]

$F_q[x]/(x^n-\lambda)$ nin sıfırdan farklı bir I idealinin en küçük dereceli, monik, indirgenemez polinomuna I nin **üreteç polinom**u denir. C bir $\lambda-$sabit devirli kod olmak üzere, $\pi_\lambda(C)$ nin üreteç polinomuna C **nin üreteç polinomu** denir.

Teorem 2.154 [39]

$x^n-\lambda$ polinomunun her bir monik böleni $F_q^{\,n}$ de bazı $\lambda-$sabit devirli kodlar için üreteç polinomdur.

İspat

$g(x)$ polinomu, $x^n-\lambda$ polinomunun bir monik böleni ve I, $F_q[x]/(x^n-\lambda)$ halkasının $g(x)$ tarafından üretilen ideali olsun. C, $h(x)$ polinomuna karşılık gelen $\lambda-$sabit devirli kod olmak üzere $h(x)\equiv g(x)b(x)\bmod(x^n-\lambda)$ olacak şekilde bir $b(x)$ polinomu mevcuttur. Bu durumda $g(x)$ polinomu, $h(x)$ polinomunun bir bölenidir. $h(x)$ en küçük dereceli ve monik polinom olduğundan $g(x)$, $h(x)$ polinomunun kendisi olmalıdır.

Sonuç 2.155

$F_q^{\,n}$ deki $\lambda-$sabit devirli kodlarla $x^n-\lambda\in F_q[x]$ nin monik bölenleri arasında birebir bir eşeleme vardır.

Örnek 2.156

4 uzunluklu tüm üçlü $2-$sabit devirli kodları bulmak için, $x^6-2\in F_3[x]$ nin monik çarpanları incelenmelidir:

$x^4-2=\left(x^2+x+2\right)\left(x^2+2x+2\right)$ olduğundan tüm monik bölenler:

$1, 2+x+x^2, 2+2x+x^2, 2+x^4$.

Buradan 4 uzunluklu üçlü $2-$sabit devirli kodları sayısı 4 dur. Örneğin, $2+x+x^2$ polinomunun ürettiği $2-$sabit devirli kod,

$C=\{0000, 2110, 0211, 2021, 1220, 0122, 1012, 2202, 1101\}$ dir.

Teorem 2.157 [39]

$g(x)$ polinomu, $F_q[x]/\left(x^n-\lambda\right)$ bölüm halkasının bir idealinin üreteç polinomu olsun. Bu durumda $der\left(g(x)\right)=n-k$ ise $g(x)$ polinomunun ürettiği ideale karşılık geldiği $\lambda-$sabit devirli kodun boyutu k bulunur.

İspat

$c_1(x)\neq c_2(x)$ polinomları dereceleri $\leq k-1$ olan polinomlar olmak üzere $g(x)c_1(x)\not\equiv g(x)c_2(x)\bmod\left(x^n-\lambda\right)$ dir. Bu nedenle $A=\left\{g(x)c(x)\,|\,c(x)\in F_q[x]/\left(x^n-\lambda\right), der\left(c(x)\right)\leq k-1\right\}$ kümesinin q^k elemanı vardır ve $g(x)$ tarafından üretilen idealin bir alt kümesidir. Diğer taraftan, her $a(x)g(x)$ kodsözü aşağıdaki şekilde yazılabilir:

$a(x)g(x)=u(x)\left(x^n-\lambda\right)+v(x), der\left(v(x)\right)<n$.

$v(x)=a(x)g(x)-u(x)\left(x^n-\lambda\right)$ olduğundan $g(x)$, $v(x)$ in bir bölenidir. O halde $v(x)=b(x)g(x)$ yazılabilir. $der\left(b(x)\right)<k$ olduğundan $v(x)\in A$ elde edilir. Buradan $A=\left(g(x)\right)$ olup kodun boyutu $\log_q|A|=k$ olarak hesaplanır.

Örnek 2.158

F_3 cismi üzerinde 4 uzunluklu $2+x+x^2$ polinomunun ürettiği üçlü $2-$sabit devirli kod, $C=\{0000,2110,0211,2021,1220,0122,1012,2202,1101\}$ olarak bulunur. $der\left(2+x+x^2\right)=2$ olduğundan $boy(C)=4-2=2$ ve $|C|=3^{4-2}=9$ elde edilir.

Uyarı 2.159

$\lambda-$devirli kodlar için standart formda bir üreteç ve kontrol matrisi verilememektedir.

2.8 Cisimler Üzerinde Çoklu Devirli (Polycyclic) Kodlar

Çoklu devirli kodlar ilk olarak Sergio Lopez ve arkadaşları tarafından 2009 yılında tanımlanmıştır [40]. Devirli kodlar ailesinin en geniş halidir. Bu alt bölümde sonlu cisimler üzerinde çoklu devirli (polycylic) kodların yapısı incelenecektir.

Tanım 2.160 [40]

F_q vektör uzayının $S\subset {F_q}^n$ boştan farklı bir küme olsun. Alınan bir $s=(s_0,s_1,...,s_{n-1})\in S$ vektörünün $v=(v_0,...,v_{n-1})\in {F_q}^n$ olmak üzere saat yönünde bir $v-$**çoklu devirli ötelenmesi**, $(0,s_0,s_1,...,s_{n-2})+s_{n-1}(v_0,...,v_{n-1})$ vektörü olarak tanımlanır. Eğer her $(s_0,s_1,...,s_{n-1})\in S$ vektörü için $(0,s_0,s_1,...,s_{n-2})+s_{n-1}(v_0,...,v_{n-1})$ vektörü yine S kümesinin bir elemanı oluyorsa S kümesine $v-$**çoklu devirli küme** denir. Eğer bir C lineer kodu bir $v-$çoklu devirli küme ise C koduna bir $v-$**çoklu devirli kod** denir.

Aşağıdaki lineer dönüşüm yardımıyla $v=(v_0,...,v_{n-1})\in {F_q}^n$ ve $v(x)=v_0+v_1x+...+v_{n-1}x^{n-1}$ olmak üzere $v-$çoklu devirli kodların cebirsel yapısı oluşturulmaktadır:

$$\pi_v:\ {F_q}^n \rightarrow {F_q[x]}\Big/{\left(x^n-v(x)\right)}$$

$$(a_0,a_1,...,a_{n-1})\mapsto a_0+...+a_{n-1}x^{n-1} \bmod\left(x^n-v(x)\right)$$

lineer dönüşümü tanımlansın. Bu durumda, $F_q^{\,n}$ deki bir vektörün $v-$çoklu devirli ötelemesi, $F_q[x]/\left(x^n-v(x)\right)$ deki o vektöre karşılık gelen polinomun x ile çarpılmasına karşılık gelir.

Teorem 2.161 [40]

F_q bir cisim olmak üzere $F_q[x]/\left(x^n-v(x)\right)$ bölüm halkası temel (esas) ideal halkasıdır.

İspat

Devirli kodlar için yapılan ispata benzer şekilde, $F_q[x]/\left(x^n-v(x)\right)$ bölüm halkasının sıfırdan farklı bir I idealinin bir en küçük dereceli $g(x)\neq 0$ polinomu alınsın. Her $f(x)\in I$ polinomu için, $f(x)=s(x)g(x)+r(x)$ olacak şekilde $s(x),r(x)\in F_q[x]$ vardır ve $der\left(r(x)\right)<der\left(g(x)\right)$ eşitsizliği geçerlidir. $r(x)=f(x)-s(x)g(x)\in I$ ve $g(x)\in I$ en küçük dereceli polinom olduğundan $r(x)=0$ olmak zorundadır. Bu nedenle $I=\left(g(x)\right)$ olup $F_q[x]/\left(x^n-v(x)\right)$ bölüm halkası temel (esas) ideal halkasıdır.

Teorem 2.162 [40]

π_v, yukarıda tanımlanan F_q-lineer dönüşümü olmak üzere $F_q^{\,n}$ nin boştan farklı bir C alt kümesi bir $v-$çoklu devirli koddur ancak ve ancak $\pi_v(C)$, $F_q[x]/\left(x^n-v(x)\right)$ bölüm halkasının bir idealidir.

İspat

$\pi_v(C)$, $F_q[x]/\left(x^n-v(x)\right)$ bölüm halkasının bir ideali olsun. Bu durumda her $a,b\in F_q\subset F_q[x]/\left(x^n-v(x)\right)$ ve $c_1,c_2\in C$ kodsözleri için $a\pi_v(c_1),b\pi_v(c_2)\in\pi_v(C)$ elde edilir. Buradan $a\pi_v(c_1)+b\pi_v(c_2)\in\pi_v(C)$ olup $\pi_v(ac_1+bc_2)\in\pi_v(C)$ bulunur. Bu

ise $ac_1 + bc_2 \in C$ demektir. Böylece C kodu bir lineer koddur. $c = (c_0, ..., c_{n-1}) \in C$ kodsözü için $\pi_v(c) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$ polinomu $\pi_v(C)$ nin bir elemanıdır. $\pi_v(C)$, $F_q[x] \Big/ \left(x^n - v(x)\right)$ halkasının bir ideali olduğundan, C lineer kodu bir $v-$çoklu devirli koddur.

Tersine, devirli ve $\lambda-$sabit devirli kodlar için yapılan ispatlara benzer şekilde $\pi_v(C)$ nin $F_q[x] \Big/ \left(x^n - v(x)\right)$ halkasının bir ideali olduğu görülür.

Tanım 2.163 [40]

$F_q[x] \Big/ \left(x^n - v(x)\right)$ nin sıfırdan farklı bir I idealinin en küçük dereceli, monik, indirgenemez polinomuna I nin **üreteç polinom**u denir. C bir $v-$çoklu devirli kod olmak üzere, $\pi_v(C)$ nin üreteç polinomuna C **nin üreteç polinomu** denir.

Teorem 2.164 [40]

$F_q[x]$ de $x^n - v(x)$ formundaki polinomunun her bir monik böleni $F_q{}^n$ de bazı $v-$çoklu devirli kodlar için üreteç polinomdur.

İspat

$g(x)$ polinomu, $x^n - v(x)$ polinomunun bir monik böleni ve I, $F_q[x] \Big/ \left(x^n - v(x)\right)$ halkasının $g(x)$ tarafından üretilen ideali olsun. C, $h(x)$ polinomuna karşılık gelen $v-$çoklu devirli kod olmak üzere $h(x) \equiv g(x) b(x) \bmod \left(x^n - v(x)\right)$ olacak şekilde bir $b(x)$ polinomu mevcuttur. Bu durumda $g(x)$ polinomu, $h(x)$ polinomunun bir bölenidir. $h(x)$ en küçük dereceli ve monik polinom olduğundan $g(x)$, $h(x)$ polinomunun kendisi olmalıdır.

Sonuç 2.165

$F_q[x]$ de $x^n - v(x)$ formundaki polinomunun her bir monik bölenine bir çoklu devirli kod karşılık gelir.

Teorem 2.166 [40]

$g(x)$ polinomu, bir C, $v-$çoklu devirli kodun üreteç polinomu olması için gerek ve yeter koşul $g(x) = g_0 + g_1 x + ... + g_{n-1} x^{n-1}$ polinomu için $g_0 \neq 0$ olmasıdır.

İspat

$g_0 = 0$ olsun. Bu durumda C kodunun tüm kodsözlerinin ilk bileşeni 0 dır ve $1 \leq i \leq n-k$ için $g_i \neq 0$ olmak üzere $(0...0 g_i ...10...0) \in C$ dir. C bir $v-$çoklu devirli kod olduğundan $(g_i ...10...0) \in C$ olmalıdır. Bu ise $g_i = 0$ olmasını gerektirir. Bu çelişkiden dolayı $g_0 \neq 0$ olmalıdır.

Teorem 2.167 [40]

$g(x)$ polinomu, $F_q[x] \Big/ \left(x^n - v(x)\right)$ bölüm halkasının bir idealinin üreteç polinomu olsun. Bu durumda $der(g(x)) = n-k$ ise karşılık geldiği $v-$çoklu devirli kodun boyutu k bulunur.

İspat

Devirli ve $\lambda-$sabit devirli kodlar için yapılan ispatlara benzer şekilde yapılır.

Örnek 2.168

F_3 cismi üzerinde 4 uzunluklu $v(x) = 2 + x$ vektörüne göre çoklu devirli kodları bulmak için, $x^4 - x - 2 \in F_3[x]$ polinomunun monik çarpanları incelenmelidir:

$x^4 - x - 2 = (x+1)(x^3 + 2x^2 + x + 1)$ olduğundan tüm monik bölenler:

$1, 1+x, 1+x+2x^2+x^3, 1+2x+x^4$ olarak bulunur. Buradan 4 uzunluklu $v(x) = 2 + x$ vektörüne göre devirli kodların sayısı 4 tür. Örneğin, $x^3 + 2x^2 + x + 1$ polinomunun

ürettiği devirli kod, $C = \{0000, 1121, 2212\}$ bulunur. Devirli kodlara benzer şekilde $|C| = 3^{4-3} = 3$ olarak hesaplanır.

BÖLÜM 3

KUATERNİYONLAR

Sir William Rowan Hamilton'un [41] 1843 yılı Kasım ayında akademiye sunduğu teoride kuaterniyon adını verdiği dörtlü yapı ilk kez tanıtıldı. Bu terimin bir parçası reel (gerçek) kısımdır; diğer parçası ise, kuaterniyonun sanal kısmı (imaginary part) olarak adlandırılan bir üçlü terimdir. Reel kısmın karesi daima pozitif iken ikinci bölüm olan sanal kısmın (veya üç köşeli) karesi her zaman negatiftir.

Özel olarak, $x, y, z \in \mathbb{R}$ olmak üzere sanal kısım $ix + jy + kz$ formundadır ve kuaterniyonlar teorisinin bazı uygulamalarında üç köşeli olarak temsil edilir ya da inşaa edilir.

Kürenin geometrisi başta olmak üzere birçok yapı ve sonuçlar bu ilkelerden hareketle oluşturulmuştur. Kuaterniyonların kalkülüsü de denen kuaterniyonların cebirsel özelliklerinin uygulamalarının geliştirilmesiyle birçok problem daha açık şekilde ifade edilebilmiştir.

Bu nedenle, pek çok uygulamada, $ix + jy + kz$ sanal kısımının üç reel bileşeni olan x, y, z nin ayrı ayrı değerlendirilmesi yerine bu üçlüyü tek bir harfle temsil etmek işlem kolaylığı sağlamıştır. Buradaki bu üçlü yapıya **vektör** denir. Dolayısıyla, bir kuaterniyonun genellikle gerçek bir kısım ve bir vektörden oluştuğu söylenebilir. Bununla birlikte, sanal parçanın bileşenlerini koordinat olarak ele alma fikri Hamilton'un ilk araştırmalarında ortaya çıkmıştı.

Bu bölümde kuaterniyonların cebirsel yapısı incelenecektir.

Tanım 3.1 [41]

Bir q **kuaterniyon**u, $1, i, j, k$ baz elemanları için $i^2 = j^2 = k^2 = ijk = -1$ ve $a_0, a_1, a_2, a_3 \in \mathbb{R}$ olmak üzere $q = a_0 + a_1 i + a_2 j + a_3 k$ olarak tanımlanır.

Tanım 3.2 [41]

Bir q kuaterniyonunda $a_0 = 0$ ise q kuaterniyonuna **pür (pure) kuaterniyon** denir.

Tanım 3.3 [41]

$\mathbb{R}^4$ uzayının standart baz (taban) elemanları olan $(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)$ vektörleri sırasıyla, $1, i, j, k$ sembolleri ile temsil edilmek üzere

$$\cdot : \mathbb{R}^4 \times \mathbb{R}^4 \to \mathbb{R}^4$$
$$(a, b) \mapsto ab$$

işlemi

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, jk = i, ki = j,$$

$$ji = -k, kj = -i, ik = -j$$

denklemleri yardımıyla tanımlansın. Bu birimli (bilineer) çarpıma $\mathbb{R}^4$ üzerinde **kuaterniyon çarpımı** denir.

Uyarı 3.4

Böylece $\mathbb{R}^4$ teki bir vektöre, bir kuaterniyon gözüyle bakılabilir.

Tanım 3.5 [41]

p ve q iki kuaterniyon, $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{R}$ olmak üzere $p = a_0 + a_1 i + a_2 j + a_3 k$ ve $q = b_0 + b_1 i + b_2 j + b_3 k$ olsun. Bu durumda iki kuaterniyonun **toplamı ve çarpımı** sırasıyla aşağıdaki gibi tanımlanır:

$$p+q=(a_0+b_0)+i(a_1+b_1)+j(a_2+b_2)+k(a_3+b_3),$$
$$pq=(a_0b_0-a_1b_1-a_2b_2-a_3b_3)+i(a_0b_1+a_1b_0+a_2b_3-a_3b_2)$$
$$+j(a_0b_2+a_2b_0+a_3b_1-a_1b_3)+k(a_0b_3+a_3b_0+a_1b_2-a_2b_1)$$

şeklindedir.

Uyarı 3.6

$ij=-ji$ olduğundan kuaterniyonlarda çarpma işlemi değişme özelliğini sağlamaz.

Örnek 3.7

$p=2+5i-j+15k$ ve $q=i+2j-k$ rastgele seçilmiş iki kuaterniyon olmak üzere,

$(2+5i-j+15k)+(i+2j-k)=2+6i+j+14k$,

$(2+5i-j+15k)(i+2j-k)=8-27i+24j+9k$,

ancak

$(i+2j-k)(2+5i-j+15k)=-20-31i-21j-13k$ elde edilir.

Uyarı 3.8

Reel ve kompleks sayılardaki çarpmanın aksine kuaterniyonların çarpımı değişmeli olmadığından, kuaterniyon katsayılı polinomlardan oluşan denklemlerin, polinomun derecesinden fazla çözümü olabilir. Örneğin, $q^2+1=0$ denkleminin kökleri yalnız $\pm i$ değildir. $a_0^{\,2}+a_1^{\,2}+a_2^{\,2}=1$ olmak üzere $q=a_0+a_1i+a_2j$ kuaterniyonları da bu denklemin birer köküdür.

Tanım 3.9 [41]

p ve q iki kuaterniyon, $a_0,a_1,a_2,a_3,b_0,b_1,b_2,b_3\in\mathbb{R}$ olmak üzere $p=a_0+a_1i+a_2j+a_3k$ ve $q=b_0+b_1i+b_2j+b_3k$ olsun. $a_0=b_0,a_1=b_1,a_2=b_2,a_3=b_3$ eşitlikleri sağlanıyorsa p ve q kuaterniyonlarına **eşit kuaterniyonlar** denir.

Tanım 3.10 [41]

Bir $q=a_0+a_1i+a_2j+a_3k$ kuaterniyonu için $\bar{q}=a_0-a_1i-a_2j-a_3k$ kuaterniyonuna q nun **eşleniği** denir.

Eşlenik ile ilgili bazı özellikler

p ve q keyfi kuaterniyonlar olmak üzere aşağıdakiler özellikler sağlanır:

- $\overline{(p+q)} = \overline{p} + \overline{q}$,
- $\overline{(pq)} = \overline{p}\,\overline{q}$,
- $\overline{(\overline{q})} = q$,
- $\alpha \in \mathbb{R}$ olmak üzere $\overline{\alpha q} = \alpha \overline{q}$,
- $\overline{q} = \begin{cases} q, q \in \mathbb{R} \\ -q, q \in \mathbb{R}^3 \end{cases}$,
- $q_1, \ldots, q_n$ birer kuaterniyon olmak üzere $\overline{(q_1 + \ldots + q_n)} = \overline{q_1} + \ldots + \overline{q_n}$,
- $q_1, \ldots, q_n$ birer kuaterniyon olmak üzere $\overline{(q_1 \ldots q_n)} = \overline{q_1} \ldots \overline{q_n}$ elde edilir.

Tanım 3.11 [41]

Bir $q = a_0 + a_1 i + a_2 j + a_3 k$ kuaterniyonu için $\sqrt{q\overline{q}} = \sqrt{\overline{q}q} = \sqrt{{a_0}^2 + {a_1}^2 + {a_2}^2 + {a_3}^2} \in \mathbb{R}^+$ reel sayısına q kuaterniyonunun **normu** denir ve $\|q\|$ ile gösterilir.

Örnek 3.12

$p = 2 - 2i + 2k$ ve $q = 1 + i - 3j + k$ kuaterniyonlarının normu $2\sqrt{3}$ dir.

Tanım 3.13 [41]

q kuaterniyonunun normu 1 ise q kuaterniyonuna **birim kuaterniyon** denir.

Norm ile ilgili bazı özellikler

p ve q iki kuaterniyon olmak üzere aşağıdaki özellikler sağlanır:

- $\|qp\| = \|q\|\|p\| = \|pq\|$,
- $\|q + p\| \le \|q\| + \|p\|$,
- $\|q\|^2 + \|p\|^2 = \frac{1}{2}\left(\|q + p\|^2 + \|q - p\|^2\right)$,

- $\|q\| = \|\bar{q}\|$,
- $\|q\| = 0 \Leftrightarrow q = 0$,
- $q_1, \ldots, q_n$ birer Kuaterniyon olmak üzere $\|q_1 \ldots q_n\| = \|q_1\| \ldots \|q_n\|$ elde edilir.

Tanım 3.14 [41]

Bir q sıfırdan farklı kuaterniyonunun **tersi** $\frac{\bar{q}}{\|q\|^2}$ olarak tanımlanır ve q^{-1} ile gösterilir.

Örnek 3.15

$q = 1 + i - 3j + k$ kuaterniyonunun normu $\|1 + i - 3j + k\| = \sqrt{1+1+9+1} = \sqrt{12}$ olduğundan, tersi $q^{-1} = \frac{1}{12} - \frac{1}{12} i + \frac{1}{4} j - \frac{1}{12} k$ kuaterniyonudur.

Ters eleman ile ilgili bazı özellikler

- $\|q^{-1}\| = \|q\|^{-1}$,
- $qq^{-1} = q^{-1}q = 1$,
- $q_1, \ldots, q_n$ birer kuaterniyon olmak üzere $(q_1 \ldots q_n)^{-1} = q_1^{-1} \ldots q_n^{-1}$ sağlanır.

Tanım 3.16 [41]

Herhangi p ve q iki kuaterniyonu için **sağ (sol) bölme** $q \neq 0$ olmak üzere $r_{sağ} = pq^{-1}$ ($r_{sol} = q^{-1}p$) olarak tanımlanır.

Gösterim 3.17

Reel kuaterniyonların kümesi

$$H = \{q = a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$$

ile gösterilecektir.

Önerme 3.18

Reel kuaterniyonların kümesi H ile gösterilmek üzere, yukarıda tanımlanan kuaterniyon toplaması ve kuaterniyon çarpması işlemleri ile H kümesi bir halkadır.

Önerme 3.19

H reel kuaterniyonlar halkası değişmeli olmayan bir halkadır.

Önerme 3.20

H reel kuaterniyonlar halkasında sıfırdan farklı her eleman terslenebilir olduğundan H bir bölenler halkası (division ring) dır.

Önerme 3.21

H reel kuaterniyonlar halkası, tabanı $\{1, i, j, k\}$ olmak üzere 4 boyutlu bir $\mathbb{R}-$vektör uzayıdır.

Sonuç 3.22

Her bir reel kuaterniyona $\mathbb{R}^4$ te bir vektör gözüyle bakılarak $\mathbb{R}^4$ teki iki vektörün birbirine bölme işlemi yapılmaktadır. Bu, kuaterniyonların literatüre kattığı çok önemli bir özelliktir.

Örnek 3.23

$(1,1,2,-1)$, $(2,-1,0,3) \in \mathbb{R}^4$ vektörlerinin birbirine bölümü, $1+i+2j-k$, $2-i+3k \in H$ kuaterniyonlarının birbirine bölümüdür.

$(2-i+3k)^{-1} = \frac{2}{\sqrt{14}} - \frac{1}{\sqrt{14}}i + \frac{6}{\sqrt{14}}k$ olduğundan

$$\frac{(1,1,2,-1)}{(2,-1,0,3)} = \frac{1+i+2j-k}{2-i+3k} = (1+i+2j-k)(2-i+3k)^{-1} = (1+i+2j-k)\left(\frac{2}{\sqrt{14}} - \frac{1}{\sqrt{14}}i + \frac{6}{\sqrt{14}}k\right)$$

$$= \frac{9}{\sqrt{14}} + \frac{13}{\sqrt{14}}i - \frac{1}{\sqrt{14}}j + \frac{6}{\sqrt{14}}k = \left(\frac{9}{\sqrt{14}}, \frac{13}{\sqrt{14}}, \frac{-1}{\sqrt{14}}, \frac{6}{\sqrt{14}}\right) \in \mathbb{R}^4$$

BÖLÜM 4

SONLU KUATERNİYONLAR HALKASI H_3

Bu bölümde katsayıları $\mathbb{Z}_3 = \{0,1,2\}$ sonlu cisminden alınan katsayılarla oluşturulan kuaterniyonların sonlu $H_3 = \{q = a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}_3, i^2 = j^2 = k^2 = ijk = 2\}$ kümesinin cebirsel yapısı incelenecektir.

Tanım 4.1

Bir $\mathbb{Z}_3 -$ katsayılı q **kuaterniyonu** $1, i, j, k$ baz elemanları ve $a_0, a_1, a_2, a_3 \in \mathbb{Z}_3$ olmak üzere $q = a_0 + a_1 i + a_2 j + a_3 k$ olarak tanımlanır.

Tanım 4.2

Bir $\mathbb{Z}_3 -$ katsayılı q kuaterniyonunda $a_0 = 0$ ise q kuaterniyonuna **pür (pure) kuaterniyon** denir.

Tanım 4.3

H_3 uzayının standart baz (taban) elemanları olan $(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)$ vektörleri $1, i, j, k$ sembolleri ile temsil edilmek üzere

$$\cdot_L : H_3 \times H_3 \to H_3$$
$$(q_1, q_2) \mapsto q_1 \cdot_L q_2$$

işlemi

$i^2 = j^2 = k^2 = 2$,

$ij = k, jk = i, ki = j$,

$ji = 2k, kj = 2i, ik = 2j$

denklemleri yardımıyla tanımlansın. Bu birimli (bilineer) çarpıma H_3 üzerinde **kuaterniyon çarpımı** denir.

Gösterim 4.4

Tez çalışmamızın devamında sol çarpma işlemi alınacak ve kısalık için $\cdot_L$ yerine iki kuaterniyonun yan yana yazılmasıyla gösterilecektir. Elde edilen sonuçların tamamı sağ çarpma işlemine göre de elde edilmiştir.

Tanım 4.5

$\mathbb{Z}_3 = \{0,1,2\}$ sonlu cismi olmak üzere p ve q iki kuaterniyon, $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{Z}_3$ olmak üzere $p = a_0 + a_1 i + a_2 j + a_3 k$ ve $q = b_0 + b_1 i + b_2 j + b_3 k$ olsun. Bu durumda iki kuaterniyonun **toplamı ve çarpımı** sırasıyla aşağıdaki gibi tanımlanır:

$$p + q = (a_0 + b_0) + i(a_1 + b_1) + j(a_2 + b_2) + k(a_3 + b_3),$$
$$pq = (a_0 b_0 + 2a_1 b_1 + 2a_2 b_2 + 2a_3 b_3) + i(a_0 b_1 + a_1 b_0 + a_2 b_3 + 2a_3 b_2)$$
$$+ j(a_0 b_2 + a_2 b_0 + a_3 b_1 + 2a_1 b_3) + k(a_0 b_3 + a_3 b_0 + a_1 b_2 + 2a_2 b_1)$$

şeklindedir.

Uyarı 4.6

$ij = 2ji$ olduğundan sonlu kuaterniyonlarda çarpma işlemi değişme özelliğini sağlamaz.

Örnek 4.7

$p = 2 + i + 2j$ ve $q = 2 + i + 2j + 2k$ rastgele seçilmiş iki sonlu kuaterniyon olmak üzere,

$(2 + i + 2j) + (2 + i + 2j + 2k) = 1 + 2i + j + 2k$,

$(2 + i + 2j)(2 + i + 2j + 2k) = 2 + 2i + k$,

ancak

$(2+i+2j)(2+i+2j+2k)=2+j+k$ elde edilir.

Tanım 4.8

p ve q iki kuaterniyon, $a_0,a_1,a_2,a_3,b_0,b_1,b_2,b_3\in\mathbb{Z}_3$ olmak üzere $p=a_0+a_1i+a_2j+a_3k$ ve $q=b_0+b_1i+b_2j+b_3k$ olsun. $a_0=b_0, a_1=b_1, a_2=b_2, a_3=b_3$ eşitlikleri sağlanıyorsa p ve q kuaterniyonlarına **eşit kuaterniyonlar** denir.

Tanım 4.9

Bir $q=a_0+a_1i+a_2j+a_3k$ kuaterniyonu için $\bar{q}=a_0+2a_1i+2a_2j+2a_3k$ kuaterniyonuna q nun **eşleniği** denir.

Eşlenik ile ilgili bazı özellikler

p ve q iki kuaterniyon olmak üzere aşağıdakiler özellikler sağlanır:

- $\overline{(p+q)}=\bar{p}+\bar{q}$,
- $\overline{(pq)}=\bar{p}\bar{q}$,
- $\overline{(\bar{q})}=q$,
- $\alpha\in\mathbb{R}$ olmak üzere $\overline{\alpha q}=\alpha\bar{q}$,
- $\bar{q}=\begin{cases}q, q\in\mathbb{R}\\ 2q, q\in\mathbb{R}^3\end{cases}$,
- $q_1,\ldots,q_n$ birer kuaterniyon olmak üzere $\overline{(q_1+\ldots+q_n)}=\overline{q_1}+\ldots+\overline{q_n}$,
- $q_1,\ldots,q_n$ birer kuaterniyon olmak üzere $\overline{(q_1\ldots q_n)}=\overline{q_1}\ldots\overline{q_n}$ elde edilir.

Tanım 4.10

Bir $q=a_0+a_1i+a_2j+a_3k$ kuaterniyonu için $q\bar{q}=\bar{q}q={a_0}^2+{a_1}^2+{a_2}^2+{a_3}^2\in\mathbb{Z}_3$ reel sayısına q kuaterniyonunun **normu** denir ve $\|q\|$ ile gösterilir.

Örnek 4.11

$p = 2 + 2i + 2k$ kuaterniyonunun normu $2^2 + 2^2 + 2^2 = 1+1+1 \equiv 0 \bmod 3$ ve $q = 1 + i + 2j + k$ kuaterniyonlarının normu $1+1+2^2+1 = 1 \in \mathbb{Z}_3$ olarak bulunur.

Tanım 4.12

q kuaterniyonunun normu 1 ise q kuaterniyonuna **birim kuaterniyon** denir.

Önerme 4.13

Sonlu kuaterniyonların kümesi H_3, yukarıda tanımlanan kuaterniyon toplaması ve kuaterniyon çarpması işlemleri ile değişmeli olmayan, birimli, sıfır bölenli bir halkadır ve 81 elemana sahiptir.

İspat

Kuaterniyon çarpma işlemi değişmeli olmadığından H_3 açıkça değişmeli değildir. $1 + 0i + 0j + 0k \in H_3$ birim eleman olup H_3 birimli bir halkadır. H_3 halkasının eleman sayısı $3^4 = 81$ elemanlıdır. H_3 halkasının bazı elemanları,

$$(1+\mathrm{i}+\mathrm{j})\ (2+\mathrm{i}+\mathrm{j}) = 0, (1+\mathrm{i}+\mathrm{j})\ (1+2\mathrm{i}+2\mathrm{j}) = 0, (2+\mathrm{i}+\mathrm{j}\ )(2+2\mathrm{i}+2\mathrm{j}) = 0,$$
$$(1+2\mathrm{i}+\mathrm{j}\ )(2+2\mathrm{i}+\mathrm{j}) = 0, (1+2\mathrm{i}+\mathrm{j})\ (1+\mathrm{i}+2\mathrm{j}) = 0, (2+2\mathrm{i}+\mathrm{j})\ (1+2\mathrm{i}+\mathrm{j}) = 0,$$
$$(2+2\mathrm{i}+\mathrm{j})(2+\mathrm{i}+2\mathrm{j}) = 0, (1+\mathrm{i}+2\mathrm{j}\ )(1+2\mathrm{i}+\mathrm{j}) = 0, (1+\mathrm{i}+2\mathrm{j})(\ 2+\mathrm{i}+2\mathrm{j}) = 0,$$
$$(2+\mathrm{i}+2\mathrm{j}\ )(2+2\mathrm{i}+\mathrm{j}) = 0, (2+\mathrm{i}+2\mathrm{j}\ )(1+\mathrm{i}+2\mathrm{j}) = 0, (1+2\mathrm{i}+2\mathrm{j})(2+2\mathrm{i}+2\mathrm{j}) = 0,$$
$$(1+\mathrm{i}+\mathrm{k})(\ 2+\mathrm{i}+\mathrm{k}) = 0, (1+\mathrm{i}+\mathrm{k}\ )(1+2\mathrm{i}+2\mathrm{k}) = 0, (2+\mathrm{i}+\mathrm{k})(\ 2+2\mathrm{i}+2\mathrm{k}) = 0$$

sağladığından sıfır bölenli bir halkadır. Halkanın bu elemanlar dışında da sıfır bölenleri mevcuttur.

Önerme 4.14

$H_3^{\,n}$ sıralı $n-$lilerin kümesi bir tabanı $\{1, i, j, k\}$ olan serbest H_3-modüldür.

4.1 H_3 Halkasının İdealleri

Bu alt bölümde H_3 halkasının tüm ideallerini belirleyeceğiz. Sol çarpma işlemi kullanılarak bulunacak tüm sonuçlar sağ çarpma için de bulunabilir.

Önerme 4.15

H_3, merkezi $\mathbb{Z}_3 = \{0,1,2\}$ olan bir temel (esas) ideal halkasıdır.

İspat

$(0) = \{0\}$

$(1+i+j) = \{0, 1+i+j, \text{i + 2j + 2k, 2 + i + k, 1 + 2j + k, 2 + j + 2k, 1 + 2i +2k, 2 + 2i + 2j, 2i + j + k}\}$

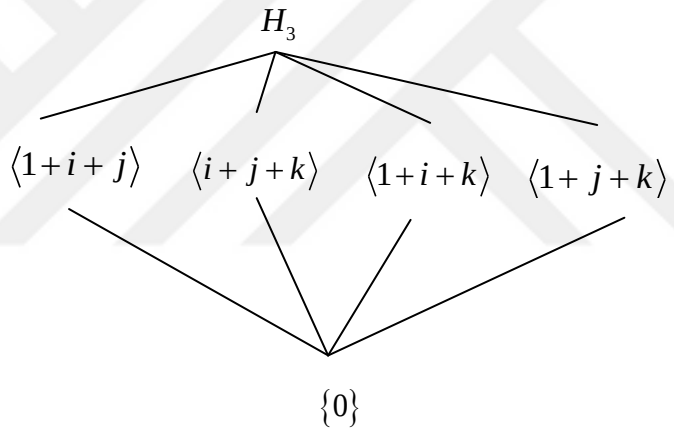
$(i+j+k) = \{0, i+j+k, \text{2 + i + 2k, 2i + 2j + 2k, 2 + 2i + j, 1 + 2i + k, 1 + j +2k, 2 + 2j + k, 1 + i + 2j}\}$

$(1+i+k) = \{0, 1+i+k, \text{2 + 2i + 2k, 1 + 2j + 2k, 2i + 2j + k, 2 + j + k, i + j +2k, 2 + i + 2j, 1 + 2i + j}\}$

$(1+j+k) = \{0, 1+j+k, \text{ i + 2j + k, 2 + i + j, 1 + 2i + 2j, 2 + 2i + k, 1 + i + 2k, 2i + j +2k,2 + 2j + 2k}\}$

$(1) = (i) = (j) = (k) = (1+i) = \ldots = H_3$

olduğundan H_3 halkası bir temel ideal halkasıdır. İdeallerin şeması şekildeki gibidir.



Şekil 4. 1 H_3 halkasının idealleri

Şekilden açıkça H_3 halkasının bir zincir halkası olmadığı (non chain) görülmektedir.

4.2 H_3 Halkasının İdempotent ve Birimsel Elemanları

Tanım 4.17

$q \in H_3$ keyfi elemanı için $qs = sq = 1$ sağlayan bir $s \in H_3$ varsa $q \in H_3$ kuaterniyonuna **terslenebilir kuaterniyon** denir. $s \in H_3$ kuaterniyonuna q kuaterniyonunun **tersi** denir ve $q^{-1} = s$ ile gösterilir.

Sonuç 4.18

H_3 halkasının sıfırdan farklı her elemanının çarpımsal tersi yoktur. 48 adet terslenebilir kuaterniyon vardır ve aşağıda listelenmiştir:

$(1)^{-1} = 1,(2)^{-1} = 2,(i)^{-1} = 2i,(1+i)^{-1} = 2+i,(2+i)^{-1} = 1+i,(1+2i)^{-1} = 2+2i,$
$(j)^{-1} = 2j,(1+j)^{-1} = 2+j,(i+j)^{-1} = i+j,(2i+j)^{-1} = 2i+j,(1+2j)^{-1} = 2+2j,$
$(i+2j)^{-1} = i+2j,(2i+2j)^{-1} = 2i+2j,(k)^{-1} = 2k,(1+k)^{-1} = 2+k,(i+k)^{-1} = i+k,$
$(2i+k)^{-1} = 2i+k,(j+k)^{-1} = j+k,(1+i+j+k)^{-1} = 1+2i+2j+2k,$
$(2+i+j+k)^{-1} = 2+2i+2j+2k,(1+2i+j+k)^{-1} = 1+i+2j+2k,$
$(2+2i+j+k)^{-1} = 2+i+2j+2k,(2j+k)^{-1} = 2j+k,(1+i+2j+k)^{-1} = 1+2i+j+2k,$
$(2+i+2j+k)^{-1} = 2+2i+j+2k,(1+2i+2j+k)^{-1} = 1+i+j+2k,(1+2k)^{-1} = 2+2k,$
$(i+2k)^{-1} = i+2k,(2i+2k)^{-1} = 2i+2k,(j+2k)^{-1} = j+2k,(2+i+j+2k)^{-1} = 2+2i+2j+k,$
$(1+2i+j+2k)^{-1} = 1+i+2j+k,(2j+2k)^{-1} = 2j+2k.$

Bu terslenebilir kuaterniyonlar aşağıdaki eşlenik sınıfları ile temsil edilir:

$$[1],[2],[i],[1+i],[2+i],[i+j],[1+i+j+k],[2+i+j+k].$$

Sonuç 4.19

H_3 teki her bir kuaterniyona $\mathbb{Z}_3^4$ te bir vektör gözüyle bakılırsa, terslenebilir kuaterniyonlara karşılık gelen vektörlerin birbirine bölünme işlemi yapılabilir. Bu, $\mathbb{Z}_3^4$ te bazı vektörlerin kuaterniyon temsilleri yardımıyla bölünebilmesi demektir. Böylece $\mathbb{Z}_3$ üzerinde 4 uzunluklu bir kodun kodsözlerinin birbirine bölünmesi işlemi yapılabilir.

Tanım 4.19

$q \in H_3$ keyfi elemanı için $q^2 = q$ sağlayan bir $q \in H_3$ kuaterniyonuna **idempotent kuaterniyon** denir.

Sonuç 4.19

14 adet idempotent kuaterniyon vardır ve aşağıda listelenmiştir:

$1,2,i+j,2i+j,i+2j,2i+2j,i+k,2i+k,j+k,2j+k,i+2k,2i+2k,j+2k,2j+2k.$

eleman vardır ve $[1],[2],[i+j]$ eşlenik sınıfları ile temsil edilir.

Tanım 4.20

$q_1, q_2 \in H_3$ keyfi elemanı için $q_1^{\,2} = q^1, q_2^{\,2} = q_2$, $q_1 q_2 = q_2 q_1 = 0$ ve $q_1 + q_2 = 1$ özelliklerini sağlayan bir $\{q_1, q_2\} \in H_3$ kuaterniyon çiftine **merkezi idempotent kuaterniyon çifti** denir.

Sonuç 4.21

6 adet merkezi (central) idempotent çifti bulunur ve aşağıda listelenmiştir:

$$\{2+i+2k, 2+2i+2k\}, \{2+2i+j, 2+i+2j\}, \{2+j+k, 2+2j+2k\},$$
$$\{2+2i+2j, 2+i+j\}, \{2+j+2k, 2+2j+k\}, \{2+2i+2k, 2+i+k\}.$$

Uyarı 4.22

Herhangi bir merkezi idempotent çifti bir diğeri kullanılarak elde edilemiyor. Bu nedenle tezin bu kısmında özel bir çift için elde edilecek olan tüm sonuçlar diğer çiftler için de elde edilebilmektedir.

Tanım 4.23

F_9 cismi**,** $F_3 = \{0,1,2\}$ sonlu cisim olmak üzere, $F_3[x]$ halkasında indirgenemez $x^2 + x + 2$ polinomunun ilkel (primitif) kökü olan w ile aşağıdaki gibi çarpımsal olarak oluşturulan cisimdir.

$$F_9 = \{0,1,w,w^2,w^3,w^4,w^5,w^6,w^7\} = \{0,1,2,w,1+w,2w,2+w,1+2w,2+2w\}$$

Önerme 4.24

F_9 cismi $\mathbb{Z}_3 + i\mathbb{Z}_3 \cong {\mathbb{Z}_3[x]}\big/{\langle x^2+1 \rangle}$ cismine izomorftur.

İspat

Aşağıdaki izomorfizma ile ispat açıkça görülür:

$$\theta : \mathbb{Z}_3 + i\mathbb{Z}_3 \to F_9$$
$$0 \mapsto 0$$
$$1 \mapsto 1$$
$$2 \mapsto w^4$$
$$i \mapsto w^6$$
$$1+i \mapsto w$$
$$2i \mapsto w^2$$
$$1+2i \mapsto w^3$$
$$2+2i \mapsto w^5$$

4.3 H_3 Halkasının Bir Ayrışımı

Bu alt bölümde merkezi idempotent elemanlar sayesinde değişmeli olmayan H_3 halkası, F_9 cismine izomorf olan $\mathbb{Z}_3 + i\mathbb{Z}_3$ cisminde bulunan iki parçaya ayrıştırılacaktır.

Önerme 4.25

Her $q \in H_3$ elemanı, H_3 halkasının idempotent çiftlerinden biri $\{e_1, e_2\}$ ve $z_1, z_2 \in \mathbb{Z}_3 + i\mathbb{Z}_3$ olmak üzere $q = e_1 z_1 + e_2 z_2$ şeklinde yazılabilir.

İspat

H_3 halkasının idempotent çiflerinden biri $\{2+i+2k, 2+2i+k\}$ olarak seçilsin. Buna göre

$$0 = (2+i+2k)0 + (2+2i+k)0$$
$$1 = (2+i+2k)1 + (2+2i+k)1$$
$$i = (2+i+2k)i + (2+2i+k)i$$
$$j = (2+i+2k)(2+2i) + (2+2i+k)(2+i)$$
$$k = (2+i+2k)(1+i) + (2+2i+k)(2+i)$$

şeklinde yazılabildiğinden ve her $q \in H_3$, $1, i, j, k$ elemanlarının lineer birleşimi olduğundan istenen görülür.

Örnek 4.26

$\{2+i+2k, 2+2i+2k\}$ merkezi idempotent çiftini kullanarak $1+i+j+2k \in H_3$ elemanı,

$1+i+j+2k=(2+i+2k)(2+i)+(2+2i+k)(1+2i)$

şeklinde yazılır.

Önerme 4.27

Her $q \in H_3$ elemanı, H_3 halkasının idempotent çiftlerinden biri $\{e_1, e_2\}$ ve $z_1, z_2 \in \mathbb{Z}_3 + i\mathbb{Z}_3$ olmak üzere $q = e_1 z_1 + e_2 z_2$ şeklinde yazılışı tek türlüdür.

İspat

$q \in H_3$ ve $\{e_1, e_2\}$ idempotent çifti için $z_1, z_2, z_1', z_2' \in \mathbb{Z}_3 + i\mathbb{Z}_3$ olmak üzere $q = e_1 z_1 + e_2 z_2 = e_1 z_1' + e_2 z_2'$ şeklinde iki farklı yazılışa sahip olsun. Bu durumda, $e_1(z_1 + 2z_1') = e_2(2z_2 + z_2')$ elde edilir. Her iki eşitlik soldan e_1 ile çarpıldığında $e_1 e_1 = e_2 e_2 = 1$ ve $e_1 e_2 = e_2 e_1 = 0$ olduğundan $z_1 = z_1'$ elde edilir. Benzer şekilde her iki eşitlik soldan e_2 ile çarpıldığında, $z_2 = z_2'$ elde edilir. Bu nedenle yazılış tek türlüdür.

Sonuç 4.28

H_3 halkası merkezi idempotent elemanlar sayesinde $(\mathbb{Z}_3 + i\mathbb{Z}_3) \times (\mathbb{Z}_3 + i\mathbb{Z}_3)$ direk çarpımına parçalanabilir. Bu ayrışım ile değişmeli olmayan H_3 halkasında kodları incelerken, $\mathbb{Z}_3 + i\mathbb{Z}_3 \cong F_9$ cismi üzerindeki bilinen kodlardan yararlanılacaktır.

BÖLÜM 5

H_3 ÜZERİNDE KODLAR

Bu bölümde, bir önceki bölümde tanıtılan ve cebirsel yapısı incelenen H_3-modül H_3^n üzerinde hata düzelten kodlar tanıtılacaktır. Ayrıca H_3^n üzerinde lineer kodlar, devirli kodlar, $\lambda-$sabit devirli kodlar ve çoklu devirli kodlar inşaa edilerek bu kodlar için parametreler verilecektir.

5.1 H_3 Halkası Üzerinde Hata Düzelten Kodlar

Bu alt bölümde H_3^n ile gösterilen H_3 halkasının elemanlarının sıralı $n-$lilerinin oluşturduğu küme üzerinde kodları tanıtarak temel tanım ve teroemler verilecektir.

Tanım 5.1

Alfabe, $H_3=\left\{q=a_0+a_1i+a_2j+a_3k \mid a_0,a_1,a_2,a_3\in\mathbb{Z}_3, i^2=j^2=k^2=ijk=2\right\}$ sonlu kuaternyonlar kümesi olsun.

i. H_3 üzerinde n uzunluklu bir **söz**, $t=1,2,...,n$ için $w_t\in H_3$ olmak üzere $w=w_1w_2...w_n$ dizisi olarak tanımlanır. Diğer bir ifadeyle, w, bir $\left(w_1,...,w_n\right)\in H_3^n$ vektörü olarak da kabul edilir.

ii. H_3 kümesinin boştan farklı, aynı n uzunluklu sözlerini içeren C alt kümesine H_3 üzerinde n uzunluklu bir **kod** denir.

iii. C kodunun her bir elemanına C de bir kodsöz denir.

vii. C deki kodsöz sayısına C nin **eleman sayısı** denir ve $|C|$ ile gösterilir.

viii. n uzunluklu ve M tane elemana sahip koda bir (n, M) **kodu** denir.

Örnek 5.2

$C = \{(0,0,0), (1+i, 2i+j, k), (0,0,1+i+j+k)\}$ kodu, H_3 halkası üzerinde tanımlanmış bir $(3,3)$ koddur.

Tanım 5.3

H_3 üzerinde n uzunluklu iki söz x ve y olsun. x ile y arasındaki **Hamming uzaklık**, x ve y nin birbirinden farklı bileşen sayısıdır ve $d(x, y)$ ile gösterilir.

$x = x_1 x_2 ... x_n$ ve $y = y_1 y_2 ... y_n$ olsun. Bu durumda, $d(x, y) = d(x_1, y_1) + ... + d(x_n, y_n)$ dir. Burada x_i ve y_i, 1 uzunluklu söz olarak düşünülebilir ve

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

Örnek 5.4

H_3^4 den alınmış vektörler, $x = (1, 0, i+j, 2k)$, $y = (2+2k, 1+j, 2i, 0)$ ve $z = (0, 1, 2i, j)$ olsun. Bu durumda, $d(x, y) = 4, d(y, z) = 3, d(z, x) = 4$ olarak bulunur.

Önerme 5.5

x, y ve z, H_3 üzerinde n uzunluklu sözler olsun. Bu durumda,

- $0 \leq d(x, y) \leq n$,
- $d(x, y) = 0 \Leftrightarrow x = y$,
- $d(x, y) = d(y, x)$,
- (Üçgen eşitsizliği) $d(x, z) \leq d(x, y) + d(y, z)$ sağlanır.

Tanım 5.6

En az iki kodsöz içeren bir C **kodunun minimum uzaklığı** kodsözleri arasındaki en küçük Hamming uzaklıktır ve $d(C)$ ile gösterilir. Diğer bir deyişle,

$d(C) = \min\{d(x,y) \mid x, y \in C, x \neq y\}$ olarak ifade edilebilir.

Tanım 5.7

n uzunluklu, M kodsöze ve d uzaklığa sahip koda **bir** (n, M, d) **kod** denir. n, M, d sayılarına ise C kodunun **parametreler**i denir.

Örnek5.8

H_3 halkası üzerinde verilen $C = \{(0,0,0),(1+i,2i+j,k),(0,0,1+i+j+k)\}$ kodu, $(3,3,1)$ parametrelerine sahip bir koddur.

Tanım 5.9

Eğer bir C kodundaki her bir kodsözün en az 1 ve en fazla $t > 0$ bileşeninde hata oluşmasıyla elde edilen söz yine kodsöz değilse C ye $t-$ **hata tespit eden kod** denir. Eğer C kodu, $t-$ hatayı tespit edip $t+1$ hatayı tespit edemiyorsa C **ye tam** $t-$ **hata tespit eden kod** denir.

Teorem 5.10

Bir C kodunun $t-$ hata tespit eden bir kod olması için gerek ve yeter koşul $d(C) \geq t+1$ olmasıdır. $d(C) = t$ ise C kodu tam $(t-1)-$ hata tespit eder.

Tanım 5.11

Eğer C kodundaki herhangi bir kodsözün en az 1, en fazla $t > 0$ bileşeninde hata oluşmasıyla elde edilen söz C nin başka bir kodsözünden en az 1, en fazla t bileşeninde hata meydana gelmesiyle elde edilemiyorsa C koduna $t-$ **hata düzelten bir kod** denir. Eğer C kodu $t-$ hata düzelten bir kod ve $(t+1)-$ hata düzeltemiyorsa C ye **tam** t **hata düzelten kod** denir.

Teorem 5.12

Bir C kodunun t hata düzeltebilen kod olması için gerek ve yeter koşul $d(C) \geq 2t+1$ olmasıdır. $d(C) = 2t+1$ ise C kodu tam $t-$ hata düzeltebilen koddur.

İspat

Hata düzelten kodlar için verilen ispata benzer şekilde kolaylıkla yapılabilir.

Tanım 5.13

s elemana sahip bir A alfabesi üzerinde tanımlı n uzunluğunda d minimum uzaklığa sahip bir kodun eleman sayısının mümkün en büyük değeri $A_s(n,d) = \max\{M \mid C \subseteq A^n, C \text{ bir } (n,M,d) \text{ kod}\}$ ile tanımlanır.

5.2 H_3 Halkası Üzerinde Lineer Kodlar

Bu alt bölümde H_3^n ile gösterilen H_3 halkasının elemanlarının sıralı $n-$lilerinin oluşturduğu kümenin, bir H_3-modül olması kullanılarak, H_3^n üzerinde lineer kodlar tanıtılacaktır. Ayrıca lineer kodlar için standart formda üreteç matris verilecek ve bu kodların parametreleri belirlenecektir. Tüm bunlar yapılırken bir önceki bölümde açıklanan ayrışımdan yararlanılacaktır.

Bir önceki bölümde yapıldığı gibi, kısalık açısından sol çarpma kullanılacak ve buna bağlı olarak sol modüllerden sözedilecektir. Bulunan tüm teorem ve sonuçlar sağ çarpma işlemi için de benzer şekilde elde edilmektedir.

Tanım 5.15

Boştan farklı $C \subseteq H_3^n$ alt kümesi, H_3 üzerinde bir modülse C koduna, H_3 üzerinde $n-$uzunluklu bir **lineer kod** denir.

Tanım 5.16

H_3^n üzerinde bir C lineer kodun boyutu, bir modül olarak boyutu olarak tanımlanır ve $boy(C) = k$ ile gösterilir.

Önerme 5.17

$H_3^{\,n}$ üzerinde bir C lineer kodun eleman sayısı $|C| = 81^k$ olarak hesaplanır.

İspat

H_3 halkasının $3^4 = 81$ elemanı olduğundan, $H_3^{\,n}$ üzerinde tanımlı bir lineer kodun eleman sayısı bir $k \in \mathbb{R}^+$ için $|C| = 81^k$ olarak bulunur.

Tanım 5.18

$H_3^{\,n}$ üzerinde bir C lineer kodu için C nin alt $H_3 -$ modül olarak tabanını oluşturan elemanlarını satır kabul eden matrise C lineer kodun **üreteç matrisi** denir ve G ile gösterilir.

Önerme 5.19

H_3 üzerinde $n-$uzunluklu bir C lineer kodu için standart formda üreteç matris aşağıdaki şekilde elde edilir.

$$\begin{pmatrix} I_{m_0} & a_1+b_1k & a_2+b_2k & a_3+b_3k & a_4+b_4k \\ 0 & (1+i+j)I_{m_1} & 0 & 0 & 0 \\ 0 & 0 & (1+j+k)I_{m_2} & 0 & 0 \\ 0 & 0 & 0 & (1+i+k)I_{m_3} & 0 \\ 0 & 0 & 0 & 0 & (i+j+k)I_{m_4} \end{pmatrix}$$

Burada, $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Z}_3$ dir. Ek olarak, $|C| = 9^{2m_0+m_1+m_2+m_3+m_4}$ olarak hesaplanır.

İspat

H_3 halkasının maksimal ideallerinin üreteçleri $1+i+j, 1+j+k, 1+i+k, i+j+k$ dir. Ürettikleri idealler ise,

$(1+i+j) = \{0, 1+i+j, \text{i} + 2\text{j} + 2\text{k},\ 2 + \text{i} + \text{k},\ 1 + 2\text{j} + \text{k},\ 2 + \text{j} + 2\text{k},\ 1 + 2\text{i} + 2\text{k},\ 2 + 2\text{i} + 2\text{j},\ 2\text{i} + \text{j} + \text{k}\}$

$(1+j+k) = \{0, 1+j+k,\ \text{i} + 2\text{j} + \text{k},\ 2 + \text{i} + \text{j},\ 1 + 2\text{i} + 2\text{j},\ 2 + 2\text{i} + \text{k},\ 1 + \text{i} + 2\text{k},\ 2\text{i} + \text{j} + 2\text{k},\ 2 + 2\text{j} + 2\text{k}\}$

$(1+i+k) = \{0, 1+i+k,\ 2 + 2\text{i} + 2\text{k},\ 1 + 2\text{j} + 2\text{k},\ 2\text{i} + 2\text{j} + \text{k},\ 2 + \text{j} + \text{k},\ \text{i} + \text{j} + 2\text{k},\ 2 + \text{i} + 2\text{j},\ 1 + 2\text{i} + \text{j}\}$

$(i+j+k) = \{0, i+j+k,\ 2 + \text{i} + 2\text{k},\ 2\text{i} + 2\text{j} + 2\text{k},\ 2 + 2\text{i} + \text{j},\ 1 + 2\text{i} + \text{k},\ 1 + \text{j} + 2\text{k},\ 2 + 2\text{j} + \text{k},\ 1 + \text{i} + 2\text{j}\}$

şeklindedir. H_3 halkasının herhangi bir q elemanı, $q_1 \in H_3$ ve $a,b \in \mathbb{Z}_3$ olmak üzere $qq_1 + (a+bk)$ şeklinde yazılabilir. Ayrıca matrisin satırları lineer bağımsız olduğundan matris H_3 üzerinde lineer kodlar için standart formda üreteç matristir.

Tanım 5.20

H_3 ten $\mathbb{Z}_3 + i\mathbb{Z}_3$ e bir ϕ dönüşümü, her $q \in H_3$ ve $\{e_1, e_2\}$ merkezi idempotent çiflerinden biri için $q = e_1 z_1 + e_2 z_2 \in H_3$, $z_1, z_2 \in \mathbb{Z}_3 + i\mathbb{Z}_3$ olmak üzere;

$$\phi : H_3 \to (\mathbb{Z}_3 + i\mathbb{Z}_3) \times (\mathbb{Z}_3 + i\mathbb{Z}_3)$$
$$q \mapsto (z_1, z_2)$$

şeklinde tanımlansın. H_3^n üzerinde bir vektörün **Lee ağırlığı**, bu ϕ dönüşümü yardımıyla, $w_L(q) = d_L(q,0) = d_H(\phi(q), \phi(0))$ şeklinde tanımlanır.

Önerme 5.21

H_3 ten $\mathbb{Z}_3 + i\mathbb{Z}_3$ e bir ϕ dönüşümü $\mathbb{Z}_3$ – lineer bir dönüşümdür.

İspat

Her $q_1 = e_1 z_1 + e_2 z_2, q_2 = e_1 w_1 + e_2 w_2 \in H_3$ ve $\{e_1, e_2\}$ merkezi idempotent çiflerinden biri için $z_1, z_2, w_1, w_2 \in \mathbb{Z}_3 + i\mathbb{Z}_3$ ve $\alpha, \beta \in \mathbb{Z}_3$ olmak üzere

$$\begin{aligned}
&\phi(\alpha q_1 + \beta q_2) = \phi(\alpha(e_1 z_1 + e_2 z_2) + \beta(e_1 w_1 + e_2 w_2)) \\
&= \phi(\alpha e_1 z_1 + \alpha e_2 z_2 + \beta e_1 w_1 + \beta e_2 w_2) \\
&= \phi(e_1(\alpha z_1 + \beta w_1) + e_2(\alpha z_2 + \beta w_2)) \\
&= (\alpha z_1 + \beta w_1, \alpha z_2 + \beta w_2) \\
&= \alpha\phi(z_1, z_2) + \beta\phi(w_1, w_2) \\
&= \alpha\phi(q_1) + \beta\phi(q_2)
\end{aligned}$$

bulunur. Böylece ϕ dönüşümü, H_3 ten $(\mathbb{Z}_3 + i\mathbb{Z}_3) \times (\mathbb{Z}_3 + i\mathbb{Z}_3)$ e bir lineer dönüşümdür.

H_3 ten $(\mathbb{Z}_3 + i\mathbb{Z}_3) \times (\mathbb{Z}_3 + i\mathbb{Z}_3)$ e bir ϕ dönüşümü, H_3^n den $(\mathbb{Z}_3 + i\mathbb{Z}_3)^{2n}$ e $q_t \in H_3$, $z_{t1}, z_{t2} \in \mathbb{Z}_3 + i\mathbb{Z}_3$, $i = 1, 2, \ldots, n$ olmak üzere aşağıdaki şekilde genişletilebilir:

$$\phi^n : {H_3}^n \to \left(\mathbb{Z}_3 + i\mathbb{Z}_3\right)^{2n} = \underbrace{\left(\mathbb{Z}_3 + i\mathbb{Z}_3\right) \times \ldots \times \left(\mathbb{Z}_3 + i\mathbb{Z}_3\right)}_{2n \text{ tane}}$$

$$\left(q_1, q_2, \ldots, q_n\right) \mapsto \left(z_{11}, z_{12}, z_{21}, z_{22}, \ldots, z_{n1}, z_{n2}\right)$$

Örnek 5.22

$w_L\left(1+i+j, 2i, j+2k\right) = w_H\left(\phi\left(1+i+j\right), \phi\left(2i\right), \phi\left(j+2k\right)\right)$. Merkezi idempotent çifti olarak $\left\{2+2i+j, 2+i+2j\right\}$ seçilirse;

$$\phi\left(1+i+j\right) = \phi\left(\left(2+2i+j\right)\left(2i\right) + \left(2+i+2j\right)\left(2+2i\right)\right) = \left(2i, 2+2i\right)$$
$$\phi\left(2i\right) = \phi\left(\left(2+2i+j\right)\left(2i\right) + \left(2+i+2j\right)\left(2i\right)\right) = \left(2i, 2i\right)$$
$$\phi\left(j+2k\right) = \phi\left(\left(2+2i+j\right)1 + \left(2+i+2j\right)\left(2i\right)\right) = \left(1, 2i\right)$$

Buradan, $w_L\left(1+i+j, 2i, j+2k\right) = 6$ dir.

Tanım 5.23

$q = a_0 + a_1 i + a_2 j + a_3 k$, H_3 halkasında keyfi bir sonlu Kuaterniyonun Mannheim ağırlığı $w_M\left(q\right) = \left|a_0\right| + \left|a_1\right| + \left|a_2\right| + \left|a_3\right|$ şeklinde tanımlanır.

$q_1, q_2 \in H_3$ arasındaki Mannheim mesafe $d_M\left(q_1, q_2\right) = w_M\left(q_2 - q_1\right)$ şeklinde tanımlanır.

$w_M\left(q_1, q_2, \ldots, q_n\right) = \sum_{l=1}^{n} w_M\left(q_l\right)$ ile hesaplanır.

Örnek 5.24

$w_M\left(1+i+j, 2i, j+2k\right) = w_M\left(1+i+j\right) + w_M\left(2i\right) + w_M\left(j+2k\right) = 3+2+3 = 8$ olarak hesaplanır.

5.3 H_3 Halkası Üzerinde Devirli Kodlar

Bu alt bölümde H_3 halkası üzerinde $n-$uzunluklu devirli kodlar inşaa edilecek ve bu kodlar için parametreler verilecektir. İnşaa yapılırken H_3 halkasının ayrışımdan faydalanarak, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerindeki devirli kodlar kullanılacaktır.

Tanım 5.25

H_3-modül H_3^n bir S alt kümesinden alınan her bir $(q_0,q_1,...,q_{n-1})$ vektörü için $(q_{n-1},q_0,...,q_{n-2})\in S$ vektörüne, $(q_0,q_1,...,q_{n-1})$ vektörünün bir $1-$**devirli ötelemesi** denir. S kümesinin bir elemanının $1-$devirli ötelemesi yine S kümesinde bir vektör ise S kümesine **devirli küme** denir. H_3 üzerinde $n-$uzunluklu bir C lineer kodu, bir devirli küme ise C ye **devirli kod** denir.

Örnek 5.26

F_3^n ve $\{000...0\}$ aşikar devirli kodlardır.

Aşağıdaki $\mathbb{Z}_3-$lineer dönüşüm yardımıyla devirli kodların cebirsel yapısı oluşturulmaktadır:

$$\pi:\ H_3^n \rightarrow H_3[x]/(x^n-1)$$

$$(q_0,q_1,...,q_{n-1})\mapsto q_0+...+q_{n-1}x^{n-1}.$$

$H_3[x]/(x^n-1)$ bir halka olduğuna dikkat edilmelidir. Üstelik, H_3^n deki bir vektörün $1-$devirli ötelemesi, $H_3[x]/(x^n-1)$ deki o vektöre karşılık gelen polinomun x ile çarpılmasına karşılık gelir.

Teorem 5.27

H_3 bir temel ideal halkası olduğundan $H_3[x]/(x^n-1)$ bölüm halkası temel (esas) ideal halkasıdır.

İspat

$H_3[x]/(x^n-1)$ bölüm halkasının sıfırdan farklı bir I idealinin bir en küçük dereceli $g(x)\neq 0$ monik polinomu alınsın. Her $f(x)\in I$ monik polinomu için, $f(x)=s(x)g(x)+r(x)$ olacak şekilde $s(x),r(x)\in H_3[x]$ monik polinomları vardır

ve $der\left(r\left(x\right)\right)<der\left(g\left(x\right)\right)$ eşitsizliği geçerlidir. $r\left(x\right)=f\left(x\right)-s\left(x\right)g\left(x\right)\in I$ ve $g\left(x\right)\in I$ en küçük dereceli polinom olduğundan $r\left(x\right)=0$ olmak zorundadır. Bu nedenle $I=\left(g\left(x\right)\right)$ olup $H_3\left[x\right]/\left(x^n-1\right)$ bölüm halkası temel (esas) ideal halkasıdır.

Teorem 5.28

π, yukarıda tanımlanan $\mathbb{Z}_3-$lineer dönüşümü olmak üzere $H_3{}^n$ nin boştan farklı bir C alt kümesi bir devirli koddur ancak ve ancak $\pi\left(C\right)$, $H_3\left[x\right]/\left(x^n-1\right)$ nin bir idealidir.

İspat

$\pi\left(C\right)$, $H_3\left[x\right]/\left(x^n-1\right)$ bölüm halkasının bir ideali olsun. Bu durumda her $a,b\in H_3\subset H_3\left[x\right]/\left(x^n-1\right)$ ve $c_1,c_2\in C$ kodsözleri için $a\pi\left(c_1\right),b\pi\left(c_2\right)\in\pi\left(C\right)$ elde edilir. Buradan $a\pi\left(c_1\right)+b\pi\left(c_2\right)\in\pi\left(C\right)$ olup $\pi\left(ac_1+bc_2\right)\in\pi\left(C\right)$ bulunur. Bu ise $ac_1+bc_2\in C$ demektir. Böylece C kodu bir lineer koddur. $c=\left(c_0,...,c_{n-1}\right)\in C$ kodsözü için $\pi\left(c\right)=c_0+c_1x+...+c_{n-1}x^{n-1}$ polinomu $\pi\left(C\right)$ nin bir elemanıdır. $\pi\left(C\right)$, $H_3\left[x\right]/\left(x^n-1\right)$ halkasının bir ideali olduğundan,

$$\begin{aligned}&x\pi\left(c\right)=c_0x+...+c_{n-1}x^n\\&=c_{n-1}+c_0x+...+c_{n-1}\left(x^n-1\right)\\&=c_{n-1}+c_0x+...+c_{n-2}x^{n-1}\\&\in\pi\left(C\right)\end{aligned}$$

bulunur. Bu nedenle C lineer kodu bir devirli koddur.

Tersine, C bir devirli kod olsun. Bu durumda $\pi\left(C\right)$ den alınan herhangi bir $f\left(x\right)$ polinomu için $\left(f_0,...,f_{n-1}\right)\in C$ olmak üzere $f\left(x\right)=f_0+f_1x+...+f_{n-1}x^{n-1}=\pi\left(f_0,...,f_{n-1}\right)$ olup C devirli kod olduğundan $xf\left(x\right)=f_{n-1}+f_0x+...+f_{n-2}x^{n-1}\in\pi\left(C\right)$ sağlanır. Böylece $x^2f\left(x\right)=x\left(xf\left(x\right)\right)\in\pi\left(C\right)$

sağlanır. Tümevarımla, her $i \geq 0$ için $x^i f(x) \in \pi(C)$ sağlanır. C bir lineer kod ve π bir lineer dönüşüm olduğundan $\pi(C)$, H_3 üzerinde bir lineer uzaydır. Buradan, her $g(x) = g_0 + \ldots + g_{n-1}x^{n-1} \in H_3[x]/(x^n - 1)$ polinomu için $g(x) f(x) = \sum_{i=1}^{n} g_i (x^i f(x)) \in \pi(C)$ sağlanır. Bu ise $\pi(C)$ nin $H_3[x]/(x^n - 1)$ halkasının bir ideali olduğunu gösterir.

Teorem 5.29

I, $H_3[x]/(x^n - 1)$ nin sıfırdan farklı bir ideali ve $g(x)$, I daki sıfırdan farklı, en küçük dereceli, monik (baş katsayısı 1), indirgenemez polinom olsun. Bu durumda, $g(x)$, I idealinin bir üretecidir ve $x^n - 1$ i böler.

Tanım 5.30

$H_3[x]/(x^n - 1)$ nin sıfırdan farklı bir I idealinin en küçük dereceli, monik, indirgenemez polinomuna I nin **üreteç polinom**u denir. C bir devirli kod olmak üzere, $\pi(C)$ nin üreteç polinomuna C **nin üreteç polinomu** denir.

Sonuç 5.31

$H_3[x]$, tek türlü çarpanlara ayrılabilir halka olmadığından $x^n - 1$ polinomunun çarpanlara ayrılışı birden fazladır. Bu nedenle $x^n - 1$ bu halkadaki herbir monik böleni ile, halkadaki devirli kodlar arasında eşleme yapmak olanaksızdır. Bunu aşmak için H_3 halkasının idempotent elemanlar yardımıyla yapılan ayrışımı kullanılacaktır.

Teorem 5.32

C, H_3 üzerinde $n-$uzunluklu bir devirli kod, C_1, C_2, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde $n-$uzunluklu birer devirli kod ve $\{e_1, e_2\}$, H_3 ün merkezi idempotent çiftlerinden biri olsun. Bu durumda $C = e_1 C_1 + e_2 C_2$ dir.

İspat

$\{e_1, e_2\}$, H_3 ün merkezi idempotent çiftlerinden biri C_1, C_2, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde $n-$uzunluklu birer devirli kod ise $C = e_1C_1 + e_2C_2 = \{(e_1c_0 + e_2d_0, ..., e_1c_{n-1} + e_2d_{n-1}) \in H_3^{\,n} \mid c_t \in C_1, d_t \in C_2, t = 0,1,...,n-1\}$ şeklinde tanımlanan C kodunun devirli olduğunu göstermek için alınan $(e_1c_0 + e_2d_0, ..., e_1c_{n-1} + e_2d_{n-1}) \in C$ kodsözü için $(e_1c_{n-1} + e_2d_{n-1}, e_1c_0 + e_2d_0, ..., e_1c_{n-2} + e_2d_{n-2}) \in C$ olduğu gösterilmelidir. $(e_1c_0 + e_2d_0, ..., e_1c_{n-1} + e_2d_{n-1}) = e_1\underbrace{(c_0, ..., c_{n-1})}_{\in C_1} + e_2\underbrace{(d_0, ..., d_{n-1})}_{\in C_2}$ olduğundan ve C_1 ile C_2 birer devirli kod olduğundan $(c_{n-1}, c_0, ..., c_{n-2}) \in C_1$ ve $(d_{n-1}, d_0, ..., d_{n-2}) \in C_2$ olup $e_1(c_{n-1}, c_0, ..., c_{n-2}) + e_2(d_{n-1}, d_0, ..., d_{n-2}) = (e_1c_{n-1} + e_2d_{n-1}, e_1c_0 + e_2d_0, ..., e_1c_{n-2} + e_2d_{n-2}) \in C$ sağlanır.

Sonuç 5.33

$C = \langle g(x) \rangle$, H_3 üzerinde $n-$uzunluklu bir devirli koddur ancak ve ancak $C_1 = \langle g_1(x) \rangle$, $C_2 = \langle g_2(x) \rangle$, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde $n-$uzunluklu birer devirli kod ve $g_1, g_2 \mid x^n - 1$ olmak üzere, $g(x) = e_1g_1(x) + e_2g_2(x)$ dir. Üstelik, $g(x) \in H_3[x]$ için $g \mid x^n - 1$ dir.

Önerme 5.34

$C_1 = \langle g_1 \rangle$, $C_2 = \langle g_2 \rangle$, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde $n-$uzunluklu birer devirli kod ve $d_L(C_1) = d_1$, $d_L(C_2) = d_2$ olsun. Bu durumda, $C = \langle g \rangle$, H_3 üzerinde $n-$uzunluklu bir devirli kodun eleman sayısı, $|C| = M = |C_1|.|C_2|$ dir. Ayrıca, C nin minimum uzaklığı, $d_L(C) = \min\{d_1, d_2\}$ olarak bulunur. Diğer bir deyişle, C kodu bir $[n, M, d_L]$ koddur.

İspat

$C = e_1C_1 + e_2C_2$ olduğundan $|C| = M = |C_1|.|C_2|$ açıkça görülür. $d_L(C_1) = d_L(e_1C_1) = d_1$ ve $d_L(C_2) = d_L(e_2C_2) = d_2$ olduğundan $d_L(C) = \min\{d_1, d_2\}$ olarak bulunur.

Örnek 5.35

$\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde $C_1 = \langle g_1 \rangle = \langle x^3 + 2ix^2 + 2x + i \rangle$, $C_2 = \langle x^2 + (2+i)x + 2i \rangle$ devirli kodları verilsin. Merkezi idempotent çifti olarak $\{2 + i + 2k, 2 + 2i + 2k\}$ çifti alındığında $C = \langle g \rangle = \langle (2+i+2k)x^3 + (j+2k)x^2 + (2i+2j+2k)x + 1 \rangle$ olup H_3 üzerinde Lee metriğine göre bir $[4, 9^3, 6]$ ve Mannheim metriğine göre $[4, 9^3, 14]$ devirli koddur.

Uyarı 5.36

Mannheim metrik ile kodun 4 olan hata düzeltme kapasitesinin 6 ya yükseldiğine dikkat edilmelidir.

5.4 H_3 Halkası Üzerinde Sabit Devirli (Constacyclic) Kodlar

Bu alt bölümde H_3 halkası üzerinde $\lambda \in H_3$ sıfırdan farklı bir eleman olmak üzere $n-$uzunluklu $\lambda-$sabit devirli kodlar inşaa edilecek ve bu kodlar için parametreler verilecektir. İnşaa yapılırken H_3 halkasının ayrışımdan faydalanarak, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerindeki $\lambda-$sabit devirli kodlar kullanılacaktır.

Tanım 5.37

H_3-modül H_3^n bir S alt kümesinden alınan her bir $(q_0, q_1, ..., q_{n-1})$ vektörü için $(\lambda q_{n-1}, q_0, ..., q_{n-2}) \in S$ vektörüne, $(q_0, q_1, ..., q_{n-1})$ vektörünün bir $\lambda-$**sabit devirli ötelemesi** denir. S kümesinin bir elemanının $\lambda-$sabit devirli ötelemesi yine S kümesinde bir vektör ise S kümesine $\lambda-$**sabit devirli küme** denir. H_3 üzerinde $n-$uzunluklu bir C lineer kodu, bir $\lambda-$sabit devirli küme ise C ye $\lambda-$**sabit devirli kod** denir.

Örnek 5.38

$\lambda = 1$ alındığında tüm $1-$sabit devirli kodlar, devirli kodlardır.

Aşağıdaki $\mathbb{Z}_3-$lineer dönüşüm yardımıyla devirli kodların cebirsel yapısı oluşturulmaktadır:

$\pi_\lambda : \ H_3^{\,n} \rightarrow \dfrac{H_3[x]}{\left(x^n-\lambda\right)}$

$\left(q_0,q_1,...,q_{n-1}\right)\mapsto q_0+...+q_{n-1}x^{n-1}.$

$\dfrac{H_3[x]}{\left(x^n-\lambda\right)}$ bir halka olduğuna dikkat edilmelidir. Üstelik, $H_3^{\,n}$ deki bir vektörün $\lambda-$sabit devirli ötelemesi, $\dfrac{H_3[x]}{\left(x^n-\lambda\right)}$ deki o vektöre karşılık gelen polinomun x ile çarpılmasına karşılık gelir.

Teorem 5.39

H_3 bir temel ideal halkası olduğundan $\dfrac{H_3[x]}{\left(x^n-\lambda\right)}$ bölüm halkası temel (esas) ideal halkasıdır.

İspat

$\dfrac{H_3[x]}{\left(x^n-\lambda\right)}$ bölüm halkasının sıfırdan farklı bir I idealinin bir en küçük dereceli $g(x)\neq 0$ monik polinomu alınsın. Her $f(x)\in I$ monik polinomu için, $f(x)=s(x)g(x)+r(x)$ olacak şekilde $s(x),r(x)\in H_3[x]$ monik polinomları vardır ve $der\left(r(x)\right)<der\left(g(x)\right)$ eşitsizliği geçerlidir. $r(x)=f(x)-s(x)g(x)\in I$ ve $g(x)\in I$ en küçük dereceli polinom olduğundan $r(x)=0$ olmak zorundadır. Bu nedenle $I=\left(g(x)\right)$ olup $\dfrac{H_3[x]}{\left(x^n-\lambda\right)}$ bölüm halkası temel (esas) ideal halkasıdır.

Teorem 5.40

π_λ, yukarıda tanımlanan $\mathbb{Z}_3-$lineer dönüşümü olmak üzere $H_3^{\,n}$ nin boştan farklı bir C alt kümesi bir $\lambda-$sabit devirli koddur ancak ve ancak $\pi_\lambda(C)$, $\dfrac{H_3[x]}{\left(x^n-\lambda\right)}$ nin bir idealidir.

İspat

$\pi_\lambda(C)$, $H_3[x]/(x^n-\lambda)$ bölüm halkasının bir ideali olsun. Bu durumda her $a,b \in H_3 \subset H_3[x]/(x^n-\lambda)$ ve $c_1, c_2 \in C$ kodsözleri için $a\pi_\lambda(c_1), b\pi_\lambda(c_2) \in \pi_\lambda(C)$ elde edilir. Buradan $a\pi_\lambda(c_1)+b\pi_\lambda(c_2) \in \pi_\lambda(C)$ olup $\pi_\lambda(ac_1+bc_2) \in \pi_\lambda(C)$ bulunur. Bu ise $ac_1+bc_2 \in C$ demektir. Böylece C kodu bir lineer koddur. $c=(c_0,...,c_{n-1}) \in C$ kodsözü için $\pi_\lambda(c)=c_0+c_1x+...+c_{n-1}x^{n-1}$ polinomu $\pi_\lambda(C)$ nin bir elemanıdır. $\pi_\lambda(C)$, $H_3[x]/(x^n-\lambda)$ halkasının bir ideali olduğundan,

$$\begin{aligned} &x\pi_\lambda(c)=c_0x+...+c_{n-1}x^n \\ &=\lambda c_{n-1}+c_0x+...+c_{n-1}(x^n-\lambda) \\ &=c_{n-1}+c_0x+...+c_{n-2}x^{n-1} \\ &\in \pi_\lambda(C) \end{aligned}$$

bulunur. Bu nedenle C lineer kodu bir $\lambda-$sabit devirli koddur.

Tersine, C bir $\lambda-$sabit devirli kod olsun. Bu durumda $\pi_\lambda(C)$ den alınan herhangi bir $f(x)$ polinomu için $(f_0,...,f_{n-1}) \in C$ olmak üzere $f(x)=f_0+f_1x+...+f_{n-1}x^{n-1}=\pi_\lambda(f_0,...,f_{n-1})$ olup C $\lambda-$sabit devirli kod olduğundan $xf(x)=f_{n-1}+f_0x+...+f_{n-2}x^{n-1} \in \pi_\lambda(C)$ sağlanır. Böylece $x^2f(x)=x(xf(x)) \in \pi_\lambda(C)$ sağlanır. Tümevarımla, her $i \geq 0$ için $x^if(x) \in \pi_\lambda(C)$ sağlanır. C bir lineer kod ve π_λ bir lineer dönüşüm olduğundan $\pi_\lambda(C)$, H_3 üzerinde bir lineer uzaydır. Buradan, her $g(x)=g_0+...+g_{n-1}x^{n-1} \in H_3[x]/(x^n-\lambda)$ polinomu için $g(x)f(x)=\sum_{i=1}^{n} g_i(x^if(x)) \in \pi_\lambda(C)$ sağlanır. Bu ise $\pi_\lambda(C)$ nin $H_3[x]/(x^n-\lambda)$ halkasının bir ideali olduğunu gösterir.

Teorem 5.41

I , $H_3[x]/(x^n-\lambda)$ nin sıfırdan farklı bir ideali ve $g(x)$, I daki sıfırdan farklı, en küçük dereceli, monik (baş katsayısı 1), indirgenemez polinom olsun. Bu durumda, $g(x)$, I idealinin bir üretecidir ve $x^n-\lambda$ i böler.

Tanım 5.42

$H_3[x]/(x^n-\lambda)$ nin sıfırdan farklı bir I idealinin en küçük dereceli, monik, indirgenemez polinomuna I nin **üreteç polinom**u denir. C bir devirli kod olmak üzere, $\pi_\lambda(C)$ nin üreteç polinomuna C **nin üreteç polinomu** denir.

Sonuç 5.43

$H_3[x]$, tek türlü çarpanlara ayrılabilir halka olmadığından $x^n-\lambda$ polinomunun çarpanlara ayrılışı birden fazladır. Bu nedenle $x^n-\lambda$ bu halkadaki herbir monik böleni ile, halkadaki devirli kodlar arasında eşleme yapmak olanaksızdır. Bunu aşmak için H_3 halkasının idempotent elemanlar yardımıyla yapılan ayrışımı kullanılacaktır.

Teorem 5.44

C_1, C_2 , $\mathbb{Z}_3+i\mathbb{Z}_3$ üzerinde, sırasıyla, $n-$uzunluklu λ_1-, λ_2-sabit devirli kodlar ve $\{e_1, e_2\}$ idempotent çifti, H_3 ün merkezi idempotent çiftlerinden biri olsun. Bu durumda, $\lambda=\lambda_1 e_1+\lambda_2 e_2$ olmak üzere, $C=e_1C_1+e_2C_2$, H_3 üzerinde $n-$uzunluklu bir $\lambda-$sabit devirli koddur.

İspat

$\{e_1, e_2\}$, H_3 ün merkezi idempotent çiftlerinden biri C_1, C_2 , $\mathbb{Z}_3+i\mathbb{Z}_3$ üzerinde sırasıyla, $n-$uzunluklu λ_1-, λ_2-sabit devirli kodlar ise $C=e_1C_1+e_2C_2=\{(e_1c_0+e_2d_0,...,e_1c_{n-1}+e_2d_{n-1})\in {H_3}^n \mid c_t\in C_1, d_t\in C_2, t=0,1,...,n-1\}$ şeklinde tanımlanan C kodunun $\lambda=\lambda_1 e_1+\lambda_2 e_2-$sabit devirli kod olduğunu göstermek için alınan $(e_1c_0+e_2d_0,...,e_1c_{n-1}+e_2d_{n-1})\in C$ kodsözü için

$\left((\lambda_1 e_1 + \lambda_2 e_2)e_1 c_{n-1} + e_2 d_{n-1}, e_1 c_0 + e_2 d_0, ..., e_1 c_{n-2} + e_2 d_{n-2}\right) \in C$ olduğu gösterilmelidir. ${e_1}^2 = e_1, e^2 = e_2$, $e_1 e_2 = e_2 e_1 = 0$ ve C_1 ile C_2, sırasıyla birer $\lambda_1 -, \lambda_2 -$sabit devirli kod olduğundan $\left(\lambda_1 c_{n-1}, c_0, ..., c_{n-2}\right) \in C_1$ ve $\left(\lambda_2 d_{n-1}, d_0, ..., d_{n-2}\right) \in C_2$ olup

$e_1\left(\lambda_1 c_{n-1}, c_0, ..., c_{n-2}\right) + e_2\left(\lambda_2 d_{n-1}, d_0, ..., d_{n-2}\right) \in C$ sağlanır. Böylece C kodu, $\lambda -$sabit devirli koddur.

Sonuç 5.45

$C_1 = \langle g_1(x) \rangle$, $C_2 = \langle g_2(x) \rangle$, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde sırasıyla, $n -$uzunluklu $\lambda_1 -, \lambda_2 -$sabit devirli kodlar ve $g_1(x)h(x) = x^n - \lambda_1$, $g_2(x)h(x) = x^n - \lambda_2$ olsun. $C = \langle g(x) \rangle$, H_3 üzerinde $n -$uzunluklu bir $\lambda -$sabit devirli koddur ve $g(x) = e_1 g_1(x) + e_2 g_2(x)$ dir. Üstelik, $\lambda = \lambda_1 e_1 + \lambda_2 e_2$ olmak üzere, $g(x)h(x) = x^n - \lambda$ dir.

Önerme 5.46

$C_1 = \langle g_1 \rangle$, $C_2 = \langle g_2 \rangle$, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde sırasıyla, $n -$uzunluklu $\lambda_1 -, \lambda_2 -$sabit devirli kodlar, $g_1(x)h(x) = x^n - \lambda_1$, $g_2(x)h(x) = x^n - \lambda_2$ ve $d_H(C_1) = d_1$, $d_H(C_2) = d_2$ olsun. Bu durumda, $C = \langle g \rangle$, $\lambda = \lambda_1 e_1 + \lambda_2 e_2$, H_3 üzerinde $n -$uzunluklu bir $\lambda -$sabit devirli kodun eleman sayısı, $|C| = M = |C_1|.|C_2|$ dir. Ayrıca, C nin minimum uzaklığı, $d_L(C) = \min\{d_1, d_2\}$ ve parametreleri, (n, M, d_L) şeklinde gösterilir.

5.5 H_3 Halkası Üzerinde Çoklu Devirli (Polycyclic) Kodlar

Bu alt bölümde, H_3 halkası üzerinde $n -$uzunluklu çoklu devirli kodların yapısı incelenecektir. Özel durumlarda devirli kodlara ve $\lambda -$sabit devirli kodlara karşılık geldiği gösterilecektir.

Tanım 5.47

$H_3 -$modül ${H_3}^n$ nin boştan farklı bir $S \subset {H_3}^n$ altkümesi olsun. Alınan bir $s = (s_0, s_1, ..., s_{n-1}) \in S$ vektörünün $v = (v_0, ..., v_{n-1}) \in {H_3}^n$ olmak üzere saat yönünde bir $v -$**çoklu devirli ötelenmesi**, $(0, s_0, s_1, ..., s_{n-2}) + s_{n-1}(v_0, ..., v_{n-1})$ vektörü olarak

tanımlanır. Eğer her $(s_0, s_1, ..., s_{n-1}) \in S$ vektörü için $(0, s_0, s_1, ..., s_{n-2}) + s_{n-1}(v_0, ..., v_{n-1})$ vektörü yine S kümesinin bir elemanı oluyorsa S kümesine $v-$**çoklu devirli küme** denir. Eğer bir C lineer kodu bir $v-$çoklu devirli küme ise C koduna bir $v-$**çoklu devirli kod** denir.

Örnek 5.48

i. $v(x)=1$ alındığında tüm devirli kodlar, $v-$çoklu devirli kodlardır.

ii. $v(x)=\lambda$ alındığında tüm $\lambda-$sabit devirli kodlar, $v-$çoklu devirli kodlardır.

Aşağıdaki lineer dönüşüm yardımıyla $v=(v_0, ..., v_{n-1}) \in H_3^{\,n}$ ve $v(x)=v_0+v_1x+...+v_{n-1}x^{n-1}$ olmak üzere $v-$çoklu devirli kodların cebirsel yapısı oluşturulmaktadır:

$$\pi_v : \ H_3^{\,n} \ \rightarrow \ H_3[x] \Big/ \left(x^n - v(x)\right)$$
$$(a_0, a_1, ..., a_{n-1}) \mapsto a_0 + ... + a_{n-1}x^{n-1} \bmod \left(x^n - v(x)\right).$$

Dikkat edilmelidir ki, $H_3^{\,n}$ deki bir vektörün $v-$çoklu devirli ötelemesi, $H_3[x] \Big/ \left(x^n - v(x)\right)$ deki o vektöre karşılık gelen polinomun x ile çarpılmasına karşılık gelir.

Teorem 5.49

$H_3^{\,n}$ bir temel ideal halkası olduğundan $H_3[x] \Big/ \left(x^n - v(x)\right)$ bölüm halkası temel (esas) ideal halkasıdır.

Teorem 5.50

π_v, yukarıda tanımlanan $\mathbb{Z}_3-$lineer dönüşümü olmak üzere $H_3^{\,n}$ nin boştan farklı bir C alt kümesi bir $v-$çoklu devirli koddur ancak ve ancak $\pi_v(C)$, $H_3[x] \Big/ \left(x^n - v(x)\right)$ bölüm halkasının bir idealidir.

İspat

$\pi_v(C)$, $H_3[x]/(x^n - v(x))$ bölüm halkasının bir ideali olsun. Bu durumda her $a,b \in \mathbb{Z}_3 \subset H_3[x]/(x^n - v(x))$ ve $c_1, c_2 \in C$ kodsözleri için $a\pi_v(c_1), b\pi_v(c_2) \in \pi_v(C)$ elde edilir. Buradan $a\pi_v(c_1) + b\pi_v(c_2) \in \pi_v(C)$ olup $\pi_v(ac_1 + bc_2) \in \pi_v(C)$ bulunur. Bu ise $ac_1 + bc_2 \in C$ demektir. Böylece C kodu bir lineer koddur. $c = (c_0, ..., c_{n-1}) \in C$ kodsözü için $\pi_v(c) = c_0 + c_1 x + ... + c_{n-1}x^{n-1}$ polinomu $\pi_v(C)$ nin bir elemanıdır. $\pi_v(C)$, $H_3[x]/(x^n - v(x))$ halkasının bir ideali olduğundan, C lineer kodu bir $v-$çoklu devirli koddur.

Tersine, devirli ve $\lambda-$sabit devirli koldar için yapılan ispatlara benzer şekilde $\pi_v(C)$ nin $H_3[x]/(x^n - v(x))$ halkasının bir ideali olduğu görülür.

Tanım 5.51

$H_3{}^n[x]/(x^n - v(x))$ nin sıfırdan farklı bir I idealinin en küçük dereceli, monik, indirgenemez polinomuna I nin **üreteç polinom**u denir. C bir $v-$çoklu devirli kod olmak üzere, $\pi_v(C)$ nin üreteç polinomuna C **nin üreteç polinomu** denir.

Sonuç 5.52

$H_3[x]$, tek türlü çarpanlara ayrılabilir halka olmadığından $x^n - v(x)$ polinomunun çarpanlara ayrılışı birden fazladır. Bu nedenle $x^n - v(x)$ bu halkadaki her bir monik böleni ile, halkadaki devirli kodlar arasında eşleme yapmak olanaksızdır. Bunu aşmak için H_3 halkasının idempotent elemanlar yardımıyla yapılan ayrışımı kullanılacaktır.

Teorem 5.53

C_1, C_2, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde, sırasıyla, $n-$uzunluklu v_1-, v_2-çoklu devirli kodlar ve $\{e_1, e_2\}$ idempotent çifti, H_3 ün merkezi idempotent çiftlerinden biri olsun. Bu

durumda, $v(x)=v_1(x)e_1+v_2(x)e_2$ olmak üzere, $C=e_1C_1+e_2C_2$, H_3 üzerinde $n-$uzunluklu bir $v-$sabit devirli koddur.

İspat

$\{e_1,e_2\}$, H_3 ün merkezi idempotent çiftlerinden biri C_1,C_2, $\mathbb{Z}_3+i\mathbb{Z}_3$ üzerinde sırasıyla, $n-$uzunluklu v_1-,v_2-çoklu devirli kodlar ise $C=e_1C_1+e_2C_2=\{(e_1c_0+e_2d_0,...,e_1c_{n-1}+e_2d_{n-1})\in {H_3}^n \mid c_t\in C_1,d_t\in C_2,t=0,1,...,n-1\}$ şeklinde tanımlanan C kodunun $v(x)=v_1(x)e_1+v_2(x)e_2-$çoklu devirli kod olduğunu göstermek için alınan $(e_1c_0+e_2d_0,...,e_1c_{n-1}+e_2d_{n-1})\in C$ kodsözü için $((v_1(x)e_1+v_2(x)e_2)e_1c_{n-1}+e_2d_{n-1},e_1c_0+e_2d_0,...,e_1c_{n-2}+e_2d_{n-2})\in C$ olduğu gösterilmelidir.

Sonuç 5.54

$C_1=\langle g_1(x)\rangle$, $C_2=\langle g_2(x)\rangle$, $\mathbb{Z}_3+i\mathbb{Z}_3$ üzerinde sırasıyla, $n-$uzunluklu v_1-,v_2-çoklu devirli kodlar ve $g_1(x)h(x)=x^n-v_1$, $g_2(x)h(x)=x^n-v_2$ olsun. $C=\langle g(x)\rangle$, H_3 üzerinde $n-$uzunluklu bir $v-$çoklu devirli koddur ve $g(x)=e_1g_1(x)+e_2g_2(x)$ dir. Üstelik, $v=v_1e_1+v_2e_2$ olmak üzere, $g(x)h(x)=x^n-v$ dir.

Önerme 5.55

$C_1=\langle g_1\rangle$, $C_2=\langle g_2\rangle$, $\mathbb{Z}_3+i\mathbb{Z}_3$ üzerinde sırasıyla, $n-$uzunluklu v_1-,v_2-çoklu devirli kodlar, $g_1(x)h(x)=x^n-v_1$, $g_2(x)h(x)=x^n-v_2$ ve $d_H(C_1)=d_1$, $d_H(C_2)=d_2$ olsun. Bu durumda, $C=\langle g\rangle$, $v=v_1e_1+v_2e_2$, H_3 üzerinde $n-$uzunluklu bir v_1-,v_2-çoklu devirli kodun eleman sayısı, $|C|=M=|C_1|.|C_2|$ dir. Ayrıca, C nin minimum uzaklığı, $d_L(C)=\min\{d_1,d_2\}$ ve parametreleri, (n,M,d_L) şeklinde gösterilir.

Örnek 5.56

$v_1(x)=(2+i)x^2+i$, $v_2(x)=x^3+ix^2+(1+2i)x+(1+i)$ olmak üzere, $C_1=\langle g_1(x)=x^3+(2+i)x^2+i\rangle$, $C_2=\langle g_2(x)=x^3+ix^2+(1+2i)x+(1+i)\rangle$ olsun.

$g_1 \mid x^3 - v_1(x)$ ve $g_2 \mid x^3 - v_2(x)$ olduğundan C_1 ve C_2, $\mathbb{Z}_3 + i\mathbb{Z}_3$ üzerinde 3 uzunluklu birer çoklu devirli koddur. Bu durumda, $e_1 = 2 + i + 2k$ ve $e_2 = 2 + 2i + k$ alınırsa, $g(x) = (2 + i + 2k)g_1(x) + (2 + 2i + k)g_2(x)$ ve $v(x) = (2 + i + 2k)v_1(x) + (2 + 2i + k)v_2(x)$ olmak üzere, $g(x) \mid x^3 - v(x)$ olduğundan $C = \langle g(x) \rangle$, H_3 üzerinde 3 uzunluklu bir çoklu devirli koddur.

BÖLÜM 6

SONUÇ VE ÖNERİLER

Bu tez çalışmasında literatürden farklı olarak değişmeli olmayan ve zincir halkası olmayan bir sonlu halka incelenmiş ve bu cebirsel yapı üzerinde lineer kodların inşaası yapılmıştır.

Öte yandan devirli kodlar incelenerek bu kodlar için parametreler verilmiştir. Lee metrik ve Mannheim metrik kullanılarak kodun minimum medafesi hesaplanarak metrikler karşılaştırılmıştır. Halkanın herhangi bir elemanına bağlı sabit devirli kodlara genişletimiştir.

Son olarak lineer kodların en geniş ailesi olan çoklu devirli kodların yapısı verilmiştir.

Bu çalışma ilerleyen zamanlarda, keyfi bir p asal sayısı için H_p halkasına genişletilebilir. Ayrıca dual kodlar çalışılarak kendine dik (self-dual) kodlar incelenebilir. Lineer kodlar için iyi bilinen sınırlar çalışılarak iyi parametrelere sahip yeni kodlar araştırılabilir.

KAYNAKLAR

[1] Shannon C. E., (1948). “A mathematical theory of communication”, The Bell System Technical Journal, 27: 379–423.

[2] Golay M. J. E., (1949). “Notes on digital coding”, Proc. IRE, 37: 657.

[3] Hamming R. W., (1950). “Error detecting and error correcting codes”, Nokia Bell Labs, The Bell System Technical Journal, 29(2):147-160.

[4] Hammons A. R., Kumar P. V., Calderbank A. R., Slaone N. J. A. ve Sole P., (1994). “The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes”, IEEE Transactions on Information Theory, 40(2):301-319.

[5] Blake I., (1972). “Codes over certain rings”, Information and Control, 20(4):396-404.

[6] Speiegel E., (1977). “Codes over $\mathbb{Z}_m$”, Information and Control, 35(1):48-51.

[7] Huber K., (1994). “Cyclic codes over Gaussian integers”, IEEE Transactions On Information Theory, 40(1):207-220.

[8] Vinck A. J. H. ve Morita H., (1998). “Cyclic codes over the ring of integers modulo m”, IEICE Transactions, E81-A, 10:2013-2018.

[9] Wood J., (1999). “Duality for Modules over Finite Rings and Applications to Coding Theory”, The Johns Hopkins University Press, American Journal of Mathematics, 121(3):555-575.

[10] Bini G. ve Flamini F., (2002). “Finite commutative rings and their applications”, Kluwer Academic Publisher.

[11] Andrade A. A. ve Palazzo R., (2005). “Linear cyclic codes over finite rings”, TEMA Tend. Mat. Apl. Comput., 6(2):207-217.

[12] Dinh H. Q. ve Lopez- Permouth S. R., (2004). “On the equivalence of codes over rings and modules”, Finite Fields and Their Application, 10(4):615-625.

[13] Dougherty S. T., Kim J., Kulosman H. ve Liu H., (2010). “Self-dual codes over commutative Frobenius rings”, Finite Fields and Their Applications, 16(1):14-26.

[14] Özen M. ve Güzeltepe M., (2009). “Cyclic codes over some finite rings”, Selçuk J. Appl. Math., 11(2):71-76.

[15] Huber K., (1994). “Cyclic codes over Eisenstein- Jacobi integers”, Contemprory Mathematics, 168:165-179.

[16] Özen M. ve Güzeltepe M., (2010). “Cyclic codes over quaternions integers”, European Journal of Pure And Applied Mathematics, 3(4):670-677.

[17] Ghaboussi F. ve Freudenberger J., (2010). “Codes over Gaussian integer rings”, IEEE Transactions On Communications, 61(8):3114-3124.

[18] Freudenberger J., Ghaboussi F. ve Shavguldze S., (2013). “New coding techniques for codes over Gaussian integers”, IEEE Transactions on Communications, 61(8):3114 – 3124.

[19] Özen M. ve Güzeltepe M., (2011). “Cyclic codes over some finite quaternion integers rings”, Journal of the Franklin Institute, 348(7):1312-1317.

[20] Shah T. ve Rasool S. S., (2013). “On codes over quaternion integers”, Applicable Algebra in Engineering, Communication and Computing, 24(6):477–496.

[21] Çallıalp F., (2011), Örneklerle Soyut Cebir, Birsen Yayınevi.

[22] Çallıalp F. ve Tekir Ü., (2009), Değişmeli Halkalar ve Modüller, Birsen Yayınevi.

[23] Dummit D. S. ve Foote R. M., (1991). Abstract Algebra, John Wiley Press.

[24] Fraleigh J. B., (2003). A First Course in Abstract Algebra, Pearson Education Inc.

[25] Gary L. M. ve Mummert C., (2007). Finite Fields and Applications, American Mathematical Society Student Mathematical Library.

[26] Blahut R. E., (1983). ”Theory and Practice of Error Control Codes”, Addison-Wesley Press.

[27] Fujiwara E., (2005). Code Design for Dependable Systems: Theory and Practical Applications, Wiley-Interscience Press.

[28] Huffman W. C. ve Pless V., (2003). Fundamentals of Error-Correcting Codes, Cambridge University Press.

[29] Lin S. ve Costello J. R., (1983). Error Control Coding: Fundamentals and Applications, Pearson Education India.

[30] Ling S. ve Xing C., (2004). Coding Theory A First Course, National University of Singapore, Cambridge University Press.

[31] MacWilliams F. J. ve Sloane N. J. A., (1992). The Theory of Error-Correcting Codes, North-Holland Mathematical Library.

[32] Peter S., (2002). Error Control Coding, Wiley Press.

[33] Peterson W. W. ve Weldon E. J., (1961). Error-Correcting Codes, MIT Press.

[34] Prange E., (1957). “Cyclic error-correcting codes in two symbols”, AFCRC-TN, 57:103.

[35] Raymond H., (1986). A First Course in Coding Theory, Clarendon Press.

[36] Roman S., (1996). Introduction to Coding and Information Theory, Springer Press.

[37] Trappe W. ve Washington L., (2006). Introduction to Cryptography with Coding Theory, Prentice Hall.

[38] Wan Z., (1997). Quaternary Codes, World Scientific Press.

[39] BerlekampE., (1968). Algebraic Coding Theory, World Scientific Publishing.

[40] Lopez- Permouth S. R., Parra- Avila B. ve Szabo S., (2009). “Dual generalizations of the concept of cyclicity of codes”, Advances in Mathematics of Communications, 3:3.

[41] Hamilton W. R., (1847). “On Quaternions”, Proccedings of the Royal Irish academy, 3:1-16.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı :Seda AKBIYIK

Doğum Tarihi ve Yeri :10/09/1989, İstanbul

Yabancı Dili: :İngilizce

E-posta: :akbiyiks@yildiz.edu.tr

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Yüksek Lisans	Matematik	Yıldız Teknik Üniversitesi	2012
Lisans	Matematik	Zonguldak Karaelmas Üniversitesi	2009
Lise	Fen Bilimleri	Şişli Ahmet Buhan Lisesi	2005

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2010- 2011	Karamanoğlu Mehmetbey Üniversitesi	Araştırma Görevlisi
2011- …	Yıldız Teknik Üniversitesi	Araştırma Görevlisi

YAYINLARI

Makale

Uluslararası Hakemli Dergilerde Yayınlanmış Makaleler:

1. **Akbiyik S.**,Siap I., "MACWILLIAMS IDENTITIES OVER SOME SPECIAL POSETS", Commun.Fac.Sci.Univ.Ank.Series A1, Volume 62, Number 1,61-71,2013. http://dergiler.ankara.edu.tr/dergiler/29/1889/19822.pdf (ESCI)
2. **Akbiyik S.**, "MacWilliams identities for poset level weight enumerators of linear codes", Sigma Journal of Engineering and Natural Sciences, (In Press), 2018. (ESCI)
3. **Akbiyik S.**, "Codes over Multiplicative Hyperrings", (Submitted).
4. **Akbiyik S.**, Akbiyik M., Yüce S., " On Metallic Ratios in Zp", (Submitted).

Bildiriler:

1. **Akbiyik S.**,, Siap I., "MacWilliams identitiy for codes over trees", ICAAA2012, ISTANBUL, TURKEY. (Kısa Özet)
2. **Akbiyik S.**, Siap I., "MacWilliams Identity for Codes Over Forests", The Algerian-Turkish International days on Mathematics, ATIM2012, Annaba, ALGERIA. (Kısa Özet)
3. **Akbiyik S.**, Siap V., Siap I., "A Macwıllıams Type Identıty For Poset Level Weight And M-Spotty Poset Level Weight Enumerators", IWBCMS-2013, Elbasan, ALBANIA. (Kısa Özet)
4. Siap V., **Akbiyik S.**, Siap I., "Complete and byte m-spotty poset level weight enumerators of linear codes over finite fields", CMMSE-2013, Almeria, SPAIN. (Kısa Özet)
5. **Akbiyik S.**, Ersoy B. A., "Cyclic Codes Over A Non-Commutative Ring", Seventh International Conference on Modeling, Simulation and Applied Optimization, ICMSAO'17, Sharjah, DUBAI. (Tam Metin)
6. **Akbiyik S.**, Ersoy B. A., "Polycyclic Codes Over A Finite Non Commutative Ring" , International Conference on Mathematics and Engineering, ICOME-2017, Istanbul, Turkey. (Kısa Özet)