T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$\mathbb{F}_q[v]/(v^2-v)$ HALKASI ÜZERİNDE m–SEL KALAN KODLAR VE DNA KODLAR

FERHAT KÜRÜZ

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
PROF. DR. BAYRAM ALİ ERSOY

İSTANBUL, 2018

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

$\mathbb{F}_q[v]/(v^2-v)$ HALKASI ÜZERİNDE m-SEL KALAN KODLAR VE DNA KODLAR

Ferhat KÜRÜZ 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. Mehmet ÖZEN

Sakarya Üniversitesi _____

Doç. Dr. Murat ALAN

Yıldız Teknik Üniversitesi _____

Doç. Dr. Emre KOLOTOĞLU

Yıldız Teknik Üniversitesi _____

Doç. Dr. Uğur ŞENGÜL

Marmara Üniversitesi _____

ÖNSÖZ

Tez çalışmam esnasında benden yardımlarını esirgemeyen değerli hocam Prof. Dr. Bayram Ali ERSOY'a ve tez konumun belirlenip ilerlemesinde bana yol gösterici olan kıymetli hocam Prof. Dr. İrfan ŞİAP'a teşekkürü bir borç bilirim.

Doktora Tez sürecinde her 6 ayda bir tüm iş yoğunluklarına rağmen gelip beni dinleyen ve çalışmalarıma büyük katkılarda bulunan tez jüri üyelerime teşekkürlerimi sunarım.

Bu meşakkatli süreçte çeşitli konularda çıkan problemlerimin çözülmesinde yardımcı olan, bilgilerini benimle paylaşmakta çok cömert davranan arkadaşlarım Dr. Mehmet Emin KÖROĞLU, Dr. Elif Segâh ÖZTAŞ, Fatih TEMİZ ve Mustafa SARI'ya teşekkür ederim.

Doğduğum günden bu ana kadar bir an olsun maddi ve manevi desteklerini benden esirgemeyen, dualarıyla beni asla yalnız bırakmayan, varlıklarıyla huzur bulduğum, haklarını asla ödeyemeyeceğim canım annem, kıymetli babam ve değerli kardeşime minnet, şükran ve sevgilerimi iletmek isterim. Beni kendi çocuklarından ayırmayan, desteklerini sürekli yanımda hissettiğim değerli kayınpederim ve kayınvalideme şükranlarımı sunarım.

Hayatını benimle paylaşan, eğitim sürecimin sıkıntısız bir şekilde ilerlemesi için her an yanımda olan ve tüm yükümü hafifletmek için elinden gelen herşeyi yapan sevgili eşime ve dünyaya gelişiyle ailemize neşe getiren biricik oğluma sevgilerimi sunarım.

Haziran, 2018

Ferhat KÜRÜZ

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

$a \mid b$	a , b'yi böler
$a \equiv b \pmod{m}$	modülo m'ye göre a ile b denktir
$\mathbb{Z}_p$	0'dan $p-1$'e kadar olan tamsayıların kümesi
$\text{der}(f(x))$	$f(x)$ polinomunun derecesi
$\text{ebob}(f(x), g(x))$	$f(x)$ ile $g(x)$ polinomlarının en büyük ortak böleni
$\text{ekok}(f(x), g(x))$	$f(x)$ ile $g(x)$ polinomlarının en en küçük ortak katı
$(f(x))$	$f(x)$ polinomunun ürettiği ideal
$\lvert C \rvert$	C kodunun eleman sayısı
$C^{\perp}$	C kodunun duali
$boy(C)$	C kodunun boyutu
$w_H(a)$	a vektörünün Hamming ağırlığı
$d_H(a,b)$	a ile b vektörlerinin Hamming uzaklığı
$[n,k,d]_q$	uzunluğu n, boyutu k, minimum ağırlığı d olan $\mathbb{F}_q$ üzerindeki kodun parametreleri
$\lceil \cdot \rceil$	üst tam değer fonksiyonu
QR_p	modülo p'ye göre ikinci dereceden kalan olan tüm elemanların kümesi
NQR_p	modulo p'ye göre ikinci dereceden kalan olmayan tüm elemanların kümesi
Q_p	p uzunluklu ikinci dereceden kalan kod
$\chi(i)$	Legendre sembolü
$A_{q,p}$	$\left(\mathbb{F}_q[v]/(v^3-v)\right)[x]/(x^p-1)$ halkası

KISALTMA LİSTESİ

A	Adenine
C	Cytosine
DNA	Deoksiribo Nükleik Asit
G	Guanine
mod	modülo
T	Thymine
vd.	ve diğerleri
WCC	Watson-Crick Tamamlayıcı
YTÜ	Yıldız Teknik Üniversitesi

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖZET

$\mathbb{F}_q[v]/(v^2-v)$ HALKASI ÜZERİNDE m–SEL KALAN KODLAR VE DNA KODLAR

Ferhat KÜRÜZ

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Prof. Dr. Bayram Ali ERSOY

Bilgi depolama ve aktarmanın neredeyse tamamının dijital ortamlar yoluyla olduğu bir dönemde, veri aktarımındaki hataların belirlenmesi ve düzeltilmesi oldukça önem arz etmektedir. Tam olarak bu konuya matematiksel çözüm getiren cebirsel kodlama teorisi hızla gelişmektedir ve oldukça etkin yöntemler inşa edilmektedir. Bu alanda temel hedef optimal parametrelere sahip kodlar elde etmektir.

Hata belirleme ve düzeltme ihtiyacı sadece dijital ortamlarda değil aynı zamanda başka alanlarda da vardır. DNA da bu alanlardan biridir. DNA üzerinde oluşan hataların tespit edilmesi ve düzeltilmesi son zamanlarda popüler hale gelen bir problemdir. DNA kodlar yardımıyla bu probleme çözüm bulmak hedeflenmektedir. Cebirsel kodlama alanında bulunan optimal kodlarla DNA'lar arasında ilişki kurularak DNA üzerinde oluşan bozulmalar düzeltilmeye çalışılmaktadır.

Bu tez çalışmasında cisimler üzerinde tanımlanan m-sel kalan kodlar idempotent üreteçleri vasıtasıyla bazı zincir olmayan halkalar üzerinde tanımlandı ve optimal kodlar elde edildi. Ayrıca tanımlanan bu kodlar, DNA kodlarla ilişkilendirilerek daha önce tanımlanan DNA kod oluşturma yöntemlerinden daha basit ve kapsamlı bir yöntem inşa edildi.

Birinci bölümde konuyla ilgili literatür özeti, tezin amacı, tezin getirdiği yenilikler ve hipotez verilecektir. İkinci bölümde cisim teorisi, üçüncü bölümde cebirsel kodlama teorisi ile ilgili gerekli olan temel bilgiler verilecektir.

Dördüncü bölümde ikinci dereceden kalan kodların tanımı ve bazı örnekler verilecektir. Beşinci bölümde ikinci dereceden kalan kodların genel bir hali olan q. kuvvet kalan kodların tanımı verilecek, $\mathbb{F}_q[v]/(v^3-v)$ halkası üzerine taşınacak ve bu halka üzerinde idempotent üreteçlerin genel yapısı belirlenecektir.

Altıncı bölümde cisimler üzerinde m-sel kalan kodların tanımı ve bazı örnekler verilecektir. Yedinci bölümde $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde m-sel kalan kodlar, idempotent üreteçler yardımıyla verilecektir ve üreteç polinomların palindromik olması için gerekli koşullar belirlenecektir. Ayrıca bu bölümde halkalar üzerinde Griesmer sınırına göre bazı optimal kodlar verilecektir.

Sekizinci bölümde, yedinci bölümde elde ettiğimiz palindromik üreteç polinomları sayesinde $\mathbb{F}_{4^{2k}}[v]/(v^2-v)$ halkası üzerinde ters sıralı DNA kodlar inşa edilecek ve örnek verilecek. Son bölümde de elde edilen sonuçlar özetlenerek bazı öneriler verilecektir.

Anahtar Kelimeler: ikinci dereceden kalan kodlar, q. kuvvet kalan kodlar, m-sel kalan kodlar, DNA kodları, lineer kodlar, devirli kodlar

ABSTRACT

m-ADIC RESIDUE CODES OVER $\mathbb{F}_q[v]/(v^2-v)$ AND DNA CODES

Ferhat KÜRÜZ

Department of Mathematics

PhD. Thesis

Advisor: Prof. Dr. Bayram Ali ERSOY

At a time when almost all of the information storage and transmission is through digital media, it is very important to detect and correct the errors in data transmission. Algebraic coding theory, which provides a mathematical solution to this subject, develops rapidly and highly efficient methods are built. The basic goal of this area is to obtain codes with optimal parameters.

The need for error detection and correction is not only in digital media, but also in other areas. DNA is one of these areas. Detection and correction of errors on DNA is a problem that has become popular in recent times. Researchers are trying to solve this problem with the help of DNA codes. The relations that occur on DNAs are tried to be solved by using the correlation between DNAs and optimal codes over fields.

In this thesis, the m-adic residue codes over the fields are defined on some non-chain rings by means of idempotent generators and optimal codes are obtained. In addition, these codes are associated with DNA codes and a simpler and more comprehensive method than the previously described DNA code generation methods has been constructed.

In the first chapter, the relevant literature summary, the thesis purpose, the innovations brought by the thesis and the hypothesis will be given. In the second chapter, the field theory will be given. In the third chapter, basic informations about algebraic coding theory will be given.

In the fourth chapter, the definition of the quadratic codes and some examples will be given. In the fifth chapter, definition of the q^{th} power residue codes, which is a general form of quadratic codes, will be given, and the general structure of the idempotent generators on this ring will be determined.

In the sixth chapter, the definition of the m-adic residue codes and some examples of the code will be given. In the seventh chapter, the m-adic residue codes over the ring $\mathbb{F}_q[v]/(v^2-v)$ will be given by idempotent generators, and the necessary conditions for the generator polynomials to be palindromic will be determined. In addition, some optimal codes over the ring with respect to Griesmer bound will be given in this chapter.

In the eighth chapter, by means of the palindromic generator polynomials we obtained in the seventh chapter, reversable DNA codes over the ring $\mathbb{F}_{4^{2k}}[v]/(v^2-v)$ will be built and an example will be given. In the last chapter, the results obtained will be summarized and some suggestions will be given.

Keywords: quadratic residue codes, q^{th} power residue codes, m-adic residue codes, DNA codes, linear codes, cyclic codes

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

İkinci dereceden kalan kodlar önemli bir devirli kod ailesidir. Bu kodlar Andrew Gleason ve Cambridge Hava Kuvvetleri Araştırma Laboratuvarı araştırmacısı Eugene Prange tarafından bulunmuştur. Bu araştırma ilk olarak Mattson ve Assumus tarafından yayınlanmıştır [1]. Bu çalışmada ikinci dereceden kalan kodlar ve bu kodların devirli olması incelenmiştir. Bu kod ailesinde temel olarak, kosetlerden yararlanarak x^n-1 çarpanlarına ayrılıp bu çarpanlardan üreteç polinom elde etme amaçlanır. Bundan dolayı birçok araştırmacı bu kod ailesini çeşitli cebirsel yapılar üzerinde çalışmışlardır [2], [3], [4], [5] ve genelleştirilmesi üzerine çalışmalar yapmışlardır [6], [7], [8], [9].

Pless ve Qian $\mathbb{Z}_4$ üzerinde ikinci dereceden kalan kodları ve devirli kodları çalışmışlardır [2]. Kaya vd. 68 uzunluklu yeni ve optimal bir kendine dual ikili ikinci dereceden kalan kod bulmuşlardır [3]. Taeri $\mathbb{Z}_4$ üzerinde ikinci dereceden kalan kodları incelemiştir [5]. Kaya vd. $v^2=v$ olacak şekilde $\mathbb{F}_p+v\mathbb{F}_p$ halkası üzerinde ikinci dereceden kalan kodları ve bu kodların Gray görüntüsünü çalışmışlardır [4].

Polyadic kodlar, q. kuvvet kalan kodlar ve m-sel kalan kodlar ikinci dereceden kalan kodların bazı genelleştirmeleridirler. Pless ve Brualdi polyadic kodları üreteç polinomlar, idempotent üreteçler ve idealler için gerekli şartları belirleyerek tanımladılar [6]. Daha sonra Job cisimler üzerinde m-sel kalan kodları üreteç polinomları ile tanımladı [10].

Diğer taraftan 1994'te Adleman bir NP problem olan Hamilton yolu(Hamiltonian path) problemini DNA molekülleri üzerinde yaptığı bir modelleme ile deney tüpünde çözmüştür [11]. Adleman'ın modellemesi DNA bazlarının WCC(Watson-Crick Complement) özelliğine dayanmaktadır. Bu özellik DNA'nın nükleotid denilen Adenine (A), Thymine (T), Guanine (G) ve Cytosine (C) isimli 4 adet yapısının bir sarmal üzerinde dizilimiyle oluştuğunu ve nükleotidlerin birbirlerini nasıl tamamladığını söyler; Adenine'in tamlayanı Thymine, Guanine'in tamlayanı Cytosine'dir [11].

DNA nükleotidleri ile cisim ve halka elemanlarını eşleştirerek cebirsel DNA kodlar oluşturulmuştur. $GF(4)$ üzerindeki lineer kodlar üzerinden DNA kod yapıları kurulmuştur [12]. Bu çalışmada $GF(4)$'ün elemanları $\{0,1,w,w^2\}$ ile DNA nükleotidleri $\{A,C,G,T\}$ eşleştirilmiştir. Bu çalışma lineer olmayan kodlara ve devirli kodlara da taşınarak bu yapılar üzerinden de DNA kodlar inşa edilmiştir [13]. Ayrıca $GF(4)$ üzerindeki BCH kodlardan yararlanarak DNA kodlar inşa edilmiştir [14]. Rocha vd. DNA yapısında hata düzelten kodların varlığını modelleyen bir biyolojik kodlama sistemi geliştirdiler [15] ve bu çalışmada $\mathbb{Z}_4$ üzerindeki $[n,k,3]$ parametreli BCH kodlar ile DNA kod oluşturdular. DNA kodlar inşa etmek için $\mathbb{Z}_4$ üzerindeki kendine dual kodlar kullanılmıştır [16], [17]. $\mathbb{F}_4$ üzerinde özel bir polinom ailesi olan yükseltilmiş polinomlarla $\mathbb{F}_{16}$ üzerinde tek uzunluklu ters sıralı kodlar inşa edilmiştir [18]. Bu çalışmada $\mathbb{F}_{16}$'nın elemanlarıyla DNA nükleotid çiftleri arasında bir eşleşme kurularak 4-yükseltilmiş polinomlar yardımıyla çift uzunluklu DNA kodlar üretilmiştir. $\mathbb{F}_2[u]/(u^4-1)$ halkasından devirli DNA kodlar elde edilmiştir [19]. Bu çalışmada elde edilen DNA kodlarda, DNA nükleotid çiftlerinin birbirlerini tamamlama ve ters sıralılık özellikleri korunmuştur. Liang ve Wang $u^2=0$ olacak şekilde $\mathbb{F}_2+u\mathbb{F}_2$ üzerinde, Pattanayak ve Singh $u^2=0$ olacak şekilde $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde DNA kodlar inşa ettiler, bu kodlar ters sıralı ve ters sıralı tamlayan DNA kodlardır [20], [21]. Ma vd. [22] $u^2=1$ olacak şekilde $\mathbb{F}_4[u]/(u^2+1)$ halkası üzerinde palindromik tamlayan devirli kodlar çalıştılar ve 6 uzunluklu DNA kodlar elde ettiler. Bennenni vd. $u^6=0$ olacak şekilde $\mathbb{F}_2[u]/(u^6)$ ve $u^2=u$ olacak şekilde $\mathbb{F}_2+u\mathbb{F}_2$ halkaları üzerinde yarı devirli (skew

cyclic) DNA kodlar inşa ettiler [23]. Bu çalışmada $\mathbb{F}_2[u]/(u^6)$ halkasının 64 elemanı ile 3'lü DNA nükleotidleri arasında bir eşleşme kurulmuştur.

1.2 Tezin Amacı

Bu tezde öncelikle cisimler üzerinde tanımlanmış ve halkalar üzerinde herhangi bir çalışma yapılmamış olan q. kuvvet kalan kodlar, q bir asal ve $v^3 = v$ olmak üzere $\mathbb{F}_q[v]/(v^3 - v)$ halkası üzerine taşınacaktır ve idempotent üreteçlerin yapısı belirlenerek halkalar üzerinde Griesmer sınırına göre optimale yakın kodlar elde edilecektir. Daha sonra ikinci dereceden kalan kodların genel hali olan ve yine sadece cisimler üzerinde inşa edilip herhangi bir halka üzerinde çalışılmayan m-sel kalan kodlar $v^2 = v$ olacak şekilde $\mathbb{F}_q[v]/(v^2 - v)$ halkası üzerine taşınacaktır. Bu halka üzerinde bu kodun idempotent üreteçlerinin yapısı belirlenecektir ve üreteç polinomlarının palindromik olması için gerekli şartlar verilecektir. Ayrıca halkalar üzerinde Griesmer sınırına göre optimal ve optimale yakın kod örnekleri verilecektir.

DNA kod üretmek için oldukça verimli olan palindromik üreteç polinomlar yardımıyla daha önce kurulan DNA kod yapılarından daha pratik olacak şekilde, $v^2 = v$ ve k pozitif bir tamsayı olmak üzere $\mathbb{F}_{4^{2k}}[v]/(v^2 - v)$ halkası üzerinde ters sıralı DNA kod yapısı belirlenecek ve bir örnek verilecektir.

1.3 Orijinal Katkı

Cisimler üzerinde tanımlanmış q. kuvvet kalan kodlar ve m-sel kalan kodlar halkalar üzerine taşınacak ve bazı optimal kodlar elde edilecektir. Daha önce DNA kod üretmek için gerekli olan ve birkaç işlem ile elde edilen palindromik üreteç polinomlar bazı şartlar altında doğrudan elde edilebilecek ve bunlar vasıtasıyla DNA kodlar daha pratik bir şekilde inşa edilebilecektir.

BÖLÜM 2

CİSİM TEORİSİ

Bu bölümde tezde kullanılacak olan cisimler ile ilgili gerekli ve temel cebirsel bilgiler verilecektir. Genel olarak *"Finite Fields"* (1997) [24] ve *"Coding Theory: A First Course"* (2004) [25] kaynakları referans alınmıştır.

2.1 Cisimler

Tanım 2.1 [24] Boştan farklı bir $\mathbb{F}$ kümesi üzerinde tanımlı '$+$' ve '$\cdot$' işlemleri aşağıdaki şartları sağlarsa $(\mathbb{F},+,\cdot)$ üçlüsüne bir ***cisim*** denir. Her $a,b,c\in\mathbb{F}$ için;

i. $+$ ve $\cdot$ işlemlerine göre kapalılık, $a+b\in\mathbb{F}$ ve $a\cdot b\in\mathbb{F}$,

ii. $+$ ve $\cdot$ işlemlerine göre değişme, $a+b=b+a$ ve $a\cdot b=b\cdot a$,

iii. $+$ ve $\cdot$ işlemlerine göre birleşme, $(a+b)+c=a+(b+c)$ ve $(a\cdot b)\cdot c=a\cdot(b\cdot c)$,

iv. $\cdot$ işleminin $+$ işlemi üzerine dağılma özelliği, $a\cdot(b+c)=a\cdot b+a\cdot c$,

v. $a+0=a$ olacak şekilde bir $0\in\mathbb{F}$ ($+$ işlemine göre birim eleman) elemanı olmalı,

vi. $a\cdot 1=a$ olacak şekilde bir $1\in\mathbb{F}$ ($\cdot$ işlemine göre birim eleman) elemanı olmalı,

vii. Her $a\in\mathbb{F}$ için $a+(-a)=0$ olacak şekilde $-a\in\mathbb{F}$ (a'nın $+$ işlemine göre tersi) elemanı olmalı,

viii. Her $a\neq 0\in\mathbb{F}$ elemanı için $a\cdot a^{-1}=1$ olacak şekilde $a^{-1}\in\mathbb{F}$ (a'nın $\cdot$ işlemine göre tersi) elemanı olmalı.

Örnek 2.2 $\mathbb{Z}_3 = \{0,1,2\}$ kümesi toplama ve çarpma işlemleri ile bir cisimdir.

Tanım 2.3 [24] $(\mathbb{F},+,\cdot)$ bir cisim olsun. E, $\mathbb{F}$'nin alt kümesi ve $(\mathrm{E},+,\cdot)$ bir cisim ise $(\mathrm{E},+,\cdot)$'ye $\mathbb{F}$'nin ***alt cismi*** denir. Ayrıca $\mathbb{F}$'ye de E cisminin bir ***cisim genişlemesi*** denir.

Örnek 2.4 $\mathbb{C}$, $\mathbb{R}$'nin bir cisim genişlemesidir.

Tanım 2.5 [24] a, b ve $m>1$ tamsayı olmak üzere $m|(a-b)$ ise modülo m'ye göre a ile b denktir denir ve

$$a \equiv b (\mathrm{mod}\, m) \tag{2.1}$$

şeklinde gösterilir.

Teorem 2.6 [25] p asal ise $\mathbb{Z}_p$ cisimdir.

Tanım 2.7 [25] R bir halka olmak üzere her $a \in R$ için $n \cdot a = 0$ olacak şekilde en küçük $n \in \mathbb{Z}^+$ tamsayısına R'nin ***karakteristiği*** denir. Eğer böyle bir pozitif tamsayı yoksa, R'nin karakteristiği sıfırdır denir.

Örnek 2.8 p bir asal sayı olmak üzere $\mathbb{Z}_p$ cisminin karakteristiği p'dir.

Teorem 2.9 [24] Karakteristiği p olan bir cismin eleman sayısı, $n \geq 1$ bir tamsayı olmak üzere, p^n'dir.

Tanım 2.10 [24] R bir halka olmak üzere $e \in R$ için, $e^2 = e$ ise e elemanına ***idempotent eleman*** denir.

2.2 Polinom Halkaları

Tanım 2.11 [25] R bir halka olmak üzere, $R[x] := \left\{ \sum_{i=0}^{n} a_i x_i : a_i \in \mathbb{F}, n \geq 0 \right\}$ kümesine R üzerindeki ***polinom halkası*** denir. $R[x]$'in bir $f(x) = \sum_{i=0}^{n} a_i x_i$ elemanı için $a_n \neq 0$ ise n tamsayısına $f(x)$ ***'in derecesi*** denir ve $\mathrm{der}(f(x))$ ile gösterilir. Ayrıca a_n'e ***başkatsayı*** denir.

Tanım 2.12 [25] Başkatsayısı 1 olan polinoma ***monik polinom*** denir.

Tanım 2.13 [25] $\mathbb{F}$ cismi üzerinde bir $f(x)$ polinomu için, $\text{der}(g(x)), \text{der}(h(x)) \leq \text{der}(f(x))$ ve $f(x) = g(x)h(x)$ olacak şekilde $g(x), h(x) \in \mathbb{F}[x]$ elemanları varsa $f(x)$'e ***indirgenebilir polinom***, aksi takdirde ***indirgenemez polinom*** denir.

Örnek 2.14 $f(x) = 1 + 3x + 2x^2 + 4x^3 + 2x^4 + 3x^5 + x^6$ polinomu $\mathbb{F}_5[x]$'te indirgenemez polinomdur.

Tanım 2.15 [25] $f(x)$, $\mathbb{F}[x]$ polinom halkasının bir elemanı olsun. Herhangi bir $g(x) \in \mathbb{F}[x]$ için $g(x) = f(x)s(x) + r(x)$ olacak şekilde sadece birer tane $s(x)$ ve $r(x)$ polinomları vardır öyle ki $der(r(x)) < der(f(x))$ veya $r(x) = 0$'dır. Burada $r(x)$'e $g(x)$ ***'in*** $f(x)$ ***'e bölümünden kalanı*** denir.

Tanım 2.16 [24] $f(x)$ ve $g(x)$ $\mathbb{F}[x]$'te iki polinom olsun. Bu iki polinomu bölen en yüksek dereceli monik polinoma $f(x)$ ve $g(x)$'in ***en büyük ortak böleni*** denir ve $\text{ebob}(f(x), g(x))$ ile gösterilir. Eğer $\text{ebob}(f(x), g(x)) = 1$ ise bu iki polinom ***aralarında asaldır*** denir.

Tanım 2.17 [24] $f(x)$ ve $g(x)$ $\mathbb{F}[x]$'te iki polinom olsun. Bu iki polinomun ortak katlarından en küçük dereceli monik polinoma $f(x)$ ve $g(x)$'in ***en küçük ortak katı*** denir ve $\text{ekok}(f(x), g(x))$ ile gösterilir.

H bir halka ve I da H'nin bir ideali olsun. $a, b \in H$ için "$a \equiv b$ olması için gerek ve yeter koşul $a - b \in I$ olmasıdır" şeklinde tanımlanan bağıntı H üzerinde bir denklik bağıntısıdır. Bu bağıntı ile oluşan bütün denklik sınıflarının kümesini $H / I = \{a + I : a \in H\}$ ile gösteririz.

Tanım 2.18 [24] H bir halka ve I da H'nin bir ideali olsun. Her $a + I, b + I \in H / I$ için,

$(a + I) + (b + I) = (a + b) + I$ ve $(a + I) \cdot (b + I) = (a \cdot b) + I$ işlemleriyle $(H / I, +, \cdot)$ üçlüsü bir halkadır. Bu halkaya H'nin I'ya göre ***bölüm halkası*** denir.

Örnek 2.19 $f(x)$ $\mathbb{F}[x]$'in bir elemanı olsun. $g(x)+h(x)=(g(x)+h(x) \ (\mathrm{mod}(f(x))))$ ve $g(x)\cdot h(x)=(g(x)\cdot h(x) \ (\mathrm{mod}(f(x))))$ işlemleriyle $\left(\mathbb{F}[x]/\left(f(x)\right),+,\cdot\right)$ üçlüsü, $\mathbb{F}[x]$'in $f(x)$ polinomunun ürettiği $\left(f(x)\right)$ idealine göre bölüm halkasıdır.

Örnek 2.19'daki $\mathbb{F}$ bir cisim, $f(x)$ $\mathbb{F}[x]$'te indirgenemez bir polinom ise $\mathbb{F}[x]/\left(f(x)\right)$ bölüm halkası bir cisimdir. Ayrıca $\mathbb{F}[x]/\left(f(x)\right)$, $\mathbb{F}$'nin bir cisim genişlemesidir.

$f(x)$ polinomunun derecesi m olmak üzere $\mathbb{F}_q$'nun $\mathbb{F}_q[x]/\left(f(x)\right)$ cisim genişlemesini $\mathbb{F}_{q^m}$ ile gösterebiliriz.

Örnek 2.20 $1+x+x^2$ polinomu $\mathbb{F}_2[x]$ polinom halkasında indirgenemez bir polinomdur. Dolayısıyla $\mathbb{F}_2[x]/(1+x+x^2)$ cismi $\mathbb{F}_2$ cisminin bir cisim genişlemesidir.

2.3 Sonlu Cisimler

Herhangi bir $\mathbb{F}$ cismi sonsuz elemanlı değilse bu cisme ***sonlu cisim*** denir. Bu kısımda sonlu cisimler ile ilgili temel bilgiler verilecektir.

Lemma 2.21 [25] q elemanlı bir $\mathbb{F}$ cisminde herhangi bir α elemanı için $\alpha^q=\alpha$'dır.

Sonuç 2.22 [25] E $\mathbb{F}$ cisminin q elemanlı bir alt cismi olsun. $\alpha\in\mathbb{F}$ elemanının E'nin elemanı olması için gerek ve yeter koşul $\alpha^q=\alpha$ olmasıdır.

Tanım 2.23 [25] $\mathbb{F}_q$ bir sonlu cisim olsun. Bir $\alpha\in\mathbb{F}_q$ elemanı için, $\mathbb{F}_q=\left\{0,\alpha,\alpha^2,\ldots,\alpha^{q-1}=1\right\}$ şeklinde yazılabiliyorsa bu α elemanına $\mathbb{F}_q$'nun bir ***ilkel elemanı*** veya ***üreteci*** denir.

Örnek 2.24 2, $\mathbb{F}_5$'in bir ilkel elemanıdır.

Örnek 2.25 α, $\mathbb{F}_2[x]$ polinom halkasında $1+x+x^2$ polinomunun kökü olsun. Bu durumda α, $\mathbb{F}_2[x]/(1+x+x^2)$ cisminin bir ilkel elemanıdır.

Tanım 2.26 [25] Sıfırdan farklı bir $\alpha\in\mathbb{F}_q$ elemanı için $\alpha^k=1$ olacak şekilde en küçük pozitif k tamsayısına α'nın ***mertebesi*** denir.

Önerme 2.27 [25] $\mathbb{F}_q$'nun sıfırdan farklı bir elemanının ilkel eleman olması için gerek ve yeter koşul mertebesinin $q-1$ olmasıdır.

2.4 Minimal Polinomlar

Bu kısımda minimal polinomlarla ilgili sonraki konularda kullanacağımız temel bilgiler verilecektir.

Tanım 2.28 [25] $\mathbb{F}_q$'nun bir $\mathbb{F}_{q^m}$ cisim genişlemesindeki bir α elemanı için $f(\alpha)=0$ olacak şekilde sıfırdan farklı en küçük dereceli monik $f(x)\in\mathbb{F}_{q^m}$ polinomuna α'nın ***minimal polinomu*** denir.

Teorem 2.29 [25] $\mathbb{F}_q$'nun bir $\mathbb{F}_{q^m}$ cisim genişlemesindeki her elemanın bir minimal polinomu vardır ve tektir. Ayrıca bu polinom $\mathbb{F}_q$ üzerinde indirgenemezdir.

Tanım 2.30 [25] n ve q aralarında asal olmak üzere,

$$C_i=\{(i\cdot q^j \pmod n)\in\mathbb{Z}_n : j=0,1,\ldots\} \tag{2.2}$$

kümesine q'nun modülo n'e göre i'yi içeren ***siklotomik koseti(cyclotomic coset)*** denir.

Örnek 2.31 3'ün modülo 11'e göre siklotomik kosetleri $C_1=\{1,3,4,5,9\}$ ve $C_2=\{2,6,7,8,10\}$'dir.

Örnek 2.32 2'nin modülo 15'e göre siklotomik kosetleri $C_1=\{1,2,4,8\}$, $C_3=\{3,6,9,12\}$, $C_5=\{5,10\}$ ve $C_7=\{7,11,13,14\}$ şeklindedir.

Teorem 2.33 [25] α, bir $\mathbb{F}_{q^m}$ cisim genişlemesinde bir ilkel eleman olsun. C_i'ler q'nun modülo q^m-1 'e göre siklotomik kosetleri olmak üzere,

$$M^{(i)}(x):=\prod_{j\in C_i}(x-\alpha^j) \tag{2.3}$$

polinomları α^i'lerin $\mathbb{F}_q$ üzerindeki minimal polinomlarıdır.

Teorem 2.34 [25] n bir pozitif tamsayı ve n ile q aralarında asal olmak üzere m, $n|(q^m-1)$ olacak şekilde bir tamsayı olsun. α, $\mathbb{F}_q$'nun bir $\mathbb{F}_{q^m}$ cisim genişlemesinde bir ilkel eleman olsun. $M^{(i)}$'ler α^i'lerin $\mathbb{F}_q$ üzerindeki minimal polinomları ve $C_a, C_b, \ldots, C_t$'ler tüm siklotomik kosetler olmak üzere x^n-1,

$$x^n-1=M^{(a)}(x)M^{(b)}(x)\ldots M^{(t)}(x) \tag{2.4}$$

şeklinde çarpanlarına ayrılır.

Örnek 2.35 α, $\mathbb{F}_{3^3}=\mathbb{F}_3[x]/(x^3+2x+1)$ cisim genişlemesinde bir ilkel eleman olsun. 3'ün modülo 13'e göre siklotomik kosetleri $C_0=\{0\}$, $C_1=\{1,3,4,9,10,12\}$ ve $C_2=\{2,5,6,7,8,11\}$'dir. $\alpha^0=1$, α ve α^2'nin minimal polinomları

$M^{(0)}=(x-\alpha^0)=x-1$,

$M^{(1)}=(x-\alpha)(x-\alpha^3)(x-\alpha^4)(x-\alpha^9)(x-\alpha^{10})(x-\alpha^{12})=1+2x^2+2x^3+2x^4+x^6$ ve

$M^{(2)}=(x-\alpha^2)(x-\alpha^5)(x-\alpha^6)(x-\alpha^7)(x-\alpha^8)(x-\alpha^{11})=1+x+2x^2+2x^4+x^5+x^6$'dır.

Ayrıca $\mathbb{F}_3$ üzerinde $x^{13}-1$,

$$x^{13}-1=(x-1)(1+2x^2+2x^3+2x^4+x^6)(1+x+2x^2+2x^4+x^5+x^6) \tag{2.5}$$

şeklinde çarpanlarına ayrılır.

BÖLÜM 3

HATA DÜZELTEN KODLAR

Bu bölümde hata düzelten kodlar hakkında gerekli önbilgiler verilecektir. Hata düzelten kodlarla ilgili bilgiler *"The theory of error correcting codes"* (1977) [26], *"Coding Theory: A First Course"* (2004) [25], *"The Art of Error Correcting Coding*" (2006) [36] ve "*Quaternary codes*" (1997) [27] isimli kitaplardan yararlanılarak hazırlanmıştır.

3.1 Hata Düzelten Kodlar ile İlgili Temel Bilgiler

Tanım 3.1 [25] $A=\{a_1,a_2,\ldots,a_q\}$ kümesine bir ***kod alfabesi***, $a_i \in A$ elemanlarına da ***kod sembolleri*** denir.

i) Her i için $w_i \in A$ olacak şekilde $\mathrm{w}=w_1w_2\ldots w_n$ kod sembolleri dizisine A üzerinde n uzunluklu bir ***söz*** denir ve w $(w_1,w_2,\ldots,w_n)$ vektörü şeklinde de gösterilebilir.

ii) A kümesi üzerindeki n uzunluklu sözlerden oluşan boştan farklı bir C kümesine A üzerinde n ***uzunluklu bir kod*** denir.

iii) C kodunun her bir elemanına ***kodsöz*** denir.

iv) C'deki kodsözlerin sayısı $|C|$ ile gösterilir ve C kodunun ***eleman sayısı*** denir.

v) q elemanlı bir alfabenin üzerinde tanımlanan n uzunluklu bir C kodunun ***hızı*** $\dfrac{\log_q|C|}{n}$ şeklinde tanımlanır.

vi) M elemanlı n uzunluklu bir koda (n, M) - kod denir.

Genellikle alfabe olarak q bir asalın kuvveti olacak şekilde $\mathbb{F}_q$ cismi seçilir. $q=2$ olduğunda bu koda ***ikili kod*** (binary code), $q=3$ olduğunda ***üçlü kod*** (ternary code), $q=4$ olduğunda ***dörtlü kod*** (quaternary code) denir.

Tanım 3.2 [36] $\mathbb{F}_q^n$ vektör uzayının k boyutlu bir alt uzayına $\mathbb{F}_q$ üzerinde n-uzunluklu, k boyutlu bir ***lineer kod*** denir ve $[n,k]_q$ parametreleriyle gösterilir.

Tanım 3.3 [25] C, $\mathbb{F}_q$ üzerinde bir lineer kod olsun.

i) $\{x \in \mathbb{F}_q^n : \langle x, c \rangle = 0, \forall c \in C\}$ kümesi C lineer kodunun ***dual kodudur*** ve $C^{\perp}$ ile gösterilir.

ii) C'nin vektör uzayı olarak boyutuna C lineer kodunun ***boyutu*** denir ve $boy(C)$ ile gösterilir.

Teorem 3.4 [25] C, $\mathbb{F}_q$ üzerinde n-uzunluklu, k boyutlu bir lineer kod olsun. Bu durumda;

i) $|C| = q^{boy(C)}$ yani $M = q^k$ dır.

ii) $C^{\perp}$ bir lineer koddur ve $boy(C) + boy(C^{\perp}) = n$ dir.

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

3.2 Üreteç ve Kontrol Matrisleri

Tanım 3.5 [25] C, $[n,k]_q$ parametreli bir lineer kodun, alt vektör uzayı olarak tabanı $\{c_1, c_2, \ldots, c_k\}$ olsun. Bu durumda C lineer kodun ***üreteç matrisi***,

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}_{k \times n} \tag{3.1}$$

şeklindedir. Bu matris yardımıyla C lineer kodunun tüm elemanları elde edilebilir.

Tanım 3.6 [25] Bir C lineer kodu için $C^{\perp}$ dual kodunun üreteç matrisi, C lineer kodunun ***parite kontrol matrisidir***, genellikle H ile gösterilir ve C'yi $\left\{x \in \mathbb{F}_q^n \middle| Hx^T = 0\right\}$ şeklinde ifade edebiliriz.

Tanım 3.7 [25] $[n,k]_q$ parametreli C lineer kodun üreteç matrisi, I_k, $k \times k$ tipinde birim matris ve A $k \times (n-k)$ tipinde bir matris olmak üzere $G = \left[I_k \middle| A\right]$ şeklinde ise G üreteç matrisi ***standart formdadır*** denir.

Teorem 3.8 [25] Bir $[n,k]_q$ parametreli C lineer kodunun üreteç matrisi $G = \left[I_k \middle| A\right]$ şeklinde standart formda verildiyse, C'nin parite kontrol matrisi $H = \left[-A^T \mid I_{n-k}\right]$ şeklindedir.

3.3 Hamming Uzaklık ve Hamming Ağırlık

Tanım 3.9 [36] Bir $x \in \mathbb{F}_q^n$ vektörünün sıfırdan farklı koordinatlarının sayısına bu vektörün ***Hamming ağırlığı*** denir ve $w_H(x)$ ile gösterilir. Ayrıca bir C kodunun ***minimum Hamming ağırlığı*** $w(x) = \min\left|\left\{i : x_i \neq 0, x = (x_1, x_2, \ldots, x_n) \in C, x \neq 0\right\}\right|$'dir.

Tanım 3.10 [36] $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$ olmak üzere, $d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$, $d_H(a,b) = \left|\{i : a_i \neq b_i, i = 1,2,\ldots n\}\right|$ şeklinde tanımlanan fonksiyona a ve b vektörlerinin ***Hamming uzaklığı*** denir.

Teorem 3.11 [25] $d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$, $d_H(a,b) = \left|\{i : a_i \neq b_i, i = 1,2,\ldots n\}\right|$ şeklinde tanımlanan fonksiyon olsun. Bu durumda aşağıdaki ifadeler sağlanır:

i. $0 \leq d_H(a,b) \leq n$,

ii. $d_H(a,b) = 0$ olması için gerek ve yeter koşul $a = b$ olmasıdır,

iii. $d_H(a,b) = d_H(b,a)$,

iv. $d_H(a,c) \leq d_H(a,b) + d_H(b,c)$.

Bu şartların sağlanması d_H'nin $\mathbb{F}_q^n$ vektör uzayı üzerinde bir metrik olduğunu gösterir.

Tanım 3.12 [36] Bir C kodunun birbirinden farklı tüm kodsöz çiftlerinin arasındaki en küçük Hamming uzaklığa bu C kodunun minimum ***Hamming uzaklığı*** denir, $d(C)$ ile gösterilir ve $d(C)=\min\{d_H(x,y): x\neq y, x,y\in C\}$ şeklinde ifade edilebilir. Bu durumda, minimum uzaklığı d olan bir $[n,k]_q$ lineer kod $[n,k,d]_q$ parametreleri ile gösterilir.

Teorem 3.13 [25] $a,b\in\mathbb{F}_q^n$ için $d_H(a,b)=w_H(a-b)$'dir.

Teorem 3.14 [25] Eğer C bir lineer kod ise $d(C)=w(C)$.

Tanım 3.15 [25] Bir C kodunun herhangi bir kodsözünde, k bir pozitif tamsayı olmak üzere, en az 1 en çok k adet hata oluştuğunda yeni oluşan söz C'nin bir kodsözü değilse C'ye k ***- hata tespit eden kod*** denir. Eğer bir C kodu k hata tespit edebiliyor fakat $k+1$ hata tespit edemiyorsa bu koda ***tam olarak*** k ***- hata tespit eden kod*** denir.

Teorem 3.16 [25] Bir C kodunun k - hata tespit edebiliyor olması için gerek ve yeter koşul $d(C)\geq k+1$ olmasıdır.

Çeşitli yöntemler inşa edilerek, kodlanarak gönderilen veri tekrar asıl haline dönüştürülür. Bu işleme ***dekodlama*** denir. Dekodlama ile inşa edilen yönteme bağlı olarak belli oranlarda hata düzeltilebilir.

Tanım 3.17 [25] Bir C kodunun herhangi bir kodsözünde, v bir pozitif tamsayı olmak üzere, v veya v'den daha az hata düzeltilebiliyorsa fakat $v+1$ hata ve daha fazla hata düzeltilemiyorsa C koduna ***tam olarak*** v ***- hata düzelten kod*** denir.

Teorem 3.18 [36] Bir C kodunun v - hata düzeltebiliyor olması için gerek ve yeter koşul $d(C)\geq 2v+1$ olmasıdır.

3.4 Lineer Kodlarda Kodlama

Bir bilgi gönderilmeden önce kullanılan yapıya göre özel bir işlemden geçirilip, iletişim kanalında oluşabilecek hatalar belli sınırlarda kontrol ve düzeltme yapılabilecek bir hale getirilir. Bu işleme ***kodlama*** denir [25] ve aşağıdaki şekilde tanımlayabiliriz.

Tanım 3.19 [25] C, parametreleri $[n,k,d]_q$ ve üreteç matrisi $G=\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$ olan bir lineer kod olsun. Bu durumda bir $x=(x_1,x_2,\ldots,x_k)\in\mathbb{F}_q^k$ elemanı $xG=c\in C\subseteq\mathbb{F}_q^n$ şeklinde kodlanır ve $c\in C$ vektörüne de bir ***kodsöz*** denir.

3.5 Devirli Kodlar

Tanım 3.20 [27] Bir C lineer kodunun her $(c_0,c_1,c_2,\ldots,c_{n-1})\in C$ elemanı için $(c_{n-1},c_0,c_1,\ldots,c_{n-2})\in C$ oluyorsa C'ye bir ***devirli kod*** denir.

3.5.1 Devirli Kodun Polinom ile Gösterimi

$C\subseteq\mathbb{F}_q^n$ bir devirli kod olsun. $\mathbb{F}_q[x]/\langle x^n-1\rangle=R_n$ bölüm halkası ve $\langle x^n-1\rangle$ $\mathbb{F}_q[x]$ polinom halkasının bir ideali olmak üzere,

$$\varphi: C\to \mathbb{F}_q[x]/\langle x^n-1\rangle = R_n,\quad \varphi(c)=\varphi(c_0,c_1,\ldots,c_{n-1})=c_0+c_1x+\ldots+c_{n-1}x^{n-1} \tag{3.2}$$

şeklindeki dönüşüm bu devirli kodun her bir kodsözüne bir polinom karşılık getirir [25]. Her devirli kodun φ altındaki görüntüsü bir ideal oluşturur ve her ideale karşılık bir devirli kod gelir [25].

Teorem 3.21 [25] $\varphi(C)$, $\mathbb{F}_q[x]/\langle x^n-1\rangle=R_n$ bölüm halkasının sıfırdan farklı bir ideali olsun. Bu durumda en küçük dereceli bir monik $g(x)\in\varphi(C)$ polinomu vardır ve $g(x)\,|\,(x^n-1)$ dir.

Tanım 3.22 [25] Teorem 3.21'de verilen $g(x)\in\varphi(C)$ polinomuna $\varphi(C)$'nin ve dolayısıyla C devirli kodunun ***üreteç polinomu*** denir ve $C=\langle g(x)\rangle$ şeklinde gösterilir. Ayrıca $der(g(x))=r$ olmak üzere C devirli kodunun boyutu $n-r$'dir.

Tanım 3.23 [25] Bir C devirli kodunu üreten idempotent polinoma ***idempotent üreteç*** denir.

İdempotent üreteçler cisimler üzerindeki devirli kodları çeşitli halkalar üzerine taşırken kullanılırlar ve bunlar sayesinde halkalar üzerindeki üreteç polinomlara geçiş sağlanabilir.

Tanım 3.24 [36] $\varphi(C)$, $\mathbb{F}_q[x]/\langle x^n-1\rangle = R_n$ bölüm halkasının sıfırdan farklı bir ideali ve $C=\langle g(x)\rangle$, $der(g(x))=r$ olmak üzere, $G=\begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-r-1}g(x) \end{pmatrix}_{(n-r)\times n}$ ile verilen matrise C devirli kodunun ***üreteç matrisi*** denir.

3.6 Griesmer Sınırı

Tanım 3.25 [28] C, $\mathbb{F}_q$ cismi üzerinde $[n,k,d]_q$ parametreli bir lineer bir kod olsun. Bu durumda $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$ eşitsizliği sağlanır. Bu eşitsizliğe lineer kodlar için ***Griesmer sınırı*** denir. Bu eşitsizliği sağlayan koda da Griesmer sınırına göre optimal denir.

BÖLÜM 4

İKİNCİ DERECEDEN KALAN KODLAR

Bu bölümde ikinci dereceden kalan kodlar ile ilgili bilgiler verilecektir. Bu bilgiler "*Coding Theory; A First Course"* [25] ve *"Fundamentals of Error Correcting Codes"* [29] isimli kitaplar esas alınarak oluşturulmuştur.

4.1 İkinci Dereceden Kalan Kodların Tanımı

Tanım 4.1 [29] $p > 2$ olmak üzere p bir asal olsun. $g^2 \equiv a(\mathrm{mod}\ p)$ denkliğinin çözümü varsa a'ya modulo p'ye göre ***ikinci dereceden kalan*** denir. Genellikle modulo p'ye göre ikinci dereceden kalan olan tüm elemanların kümesi QR_p, ikinci dereceden kalan olmayan tüm elemanların kümesi de NQR_p ile gösterilir.

Tanım 4.2 [29] $p > 2$ olmak üzere p bir asal, $q \in QR_p$ olmak üzere bir asalın kuvveti olsun. α, $\mathbb{F}_q$'nun bir cisim genişlemesinde bir ilkel eleman olmak üzere, $g(x) = \prod_{i \in QR_p} (x - \alpha^i)$ ve $r(x) = \prod_{i \in NQR_p} (x - \alpha^i)$ olsun. $g(x)$, $r(x)$, $(x-1)g(x)$ ve $(x-1)r(x)$ üreteç polinomları ile üretilen devirli kodlara $\mathbb{F}_q$ üzerinde p uzunluklu (ya da p'li) ***ikinci dereceden kalan kodlar*** denir ve sırasıyla Q_p, Q_p', N_p ve N_p' ile gösterilir.

Teorem 4.3 [29] Q_p ile Q_p' sırasıyla N_p ile N_p''ye denk kodlardır (parametreleri aynıdır). Ayrıca $|Q_p| = |N_p| = q^{(p+1)/2}$ ve $|Q_p'| = |N_p'| = q^{(p-1)/2}$'dir.

Teorem 4.4 [29] Q_p'nin(veya N_p) minimum uzaklığı d olmak üzere $d^2 \geq p$'dir. Ayrıca kodun boyutu k olmak üzere, eğer $p = 4k-1$ ise $d^2 - d + 1 \geq p$'dir.

Örnek 4.5 13 uzunluklu üçlü ikinci dereceden kalan kodun üreteç polinomlarını bulalım. Öncelikle $\mathbb{F}_{13}$'ün kosetleri $QR_{13} = \{1,3,4,9,10,12\}$ ve $NQR_{13} = \{2,5,6,7,8,11\}$ şeklindedir. $\mathbb{F}_3$'ün bir cisim genişlemesinde birimin 13. ilkel kökü olacak şekilde bir α elemanı bulmalıyız. Bunun için $\mathbb{F}_3[x]/(x^3+2x+1)$ genişlemesi uygundur. a, x^3+2x+1 polinomunun kökü ise birimin 26. ilkel kökü olur. $\alpha = a^2$ olarak seçersek α birimin 13. ilkel kökü olur. Bu durumda Q_{13} ve Q_{13}' kodlarının üreteç polinomları,

$g(x) = (x-\alpha)(x-\alpha^3)(x-\alpha^4)(x-\alpha^9)(x-\alpha^{10})(x-\alpha^{12}) = 1+2x^2+2x^3+2x^4+x^6$,

$r(x) = (x-\alpha^2)(x-\alpha^5)(x-\alpha^6)(x-\alpha^7)(x-\alpha^8)(x-\alpha^{11}) = 1+x+2x^2+2x^4+x^5+x^6$'dır, parametreleri $[13,7,5]_3$'tür ve optimaldir.

N_{13} ve N_{13}' kodlarının üreteç polinomları da, $(x-1)g(x) = 2+x+x^2+2x^5+2x^6+x^7$, $(x-1)r(x) = 2+2x^2+2x^3+x^4+x^5+x^7$'dir, parametreleri $[13,6,6]_3$'tür ve optimaldir.

4.2 İkinci Dereceden Kalan Kodların İdempotent Üreteçleri

Bu kısımda $l_1(\mathrm{x}) = \sum_{i \in QR_p} x^i$, $l_2(\mathrm{x}) = \sum_{i \in NQR_p} x^i$ ve polinomlarını kullanacağız.

Teorem 4.6 [25] Eğer $p = 4k-1$ ise, ikili ikinci dereceden kalan kodların Q_p, N_p, Q_p', N_p' idempotent üreteçleri sırasıyla $E_Q(x) = l_1(x)$, $E_N(x) = l_2(x)$, $F_Q(x) = 1+l_2(x)$, $F_N(x) = 1+l_1(x)$ şeklindedir.

Teorem 4.7 [25] Eğer $p = 4k+1$ ise, ikili ikinci dereceden kalan kodların Q_p, N_p, Q_p', N_p' idempotent üreteçleri sırasıyla $E_Q(x) = 1+l_1(x)$, $E_N(x) = 1+l_2(x)$, $F_Q(x) = l_2(x)$, $F_N(x) = l_1(x)$ şeklindedir.

Teorem 4.8 [25] Eğer $p = 4k \pm 1$ ise, $q > 2$ olmak üzere $\mathbb{F}_q$ üzerindeki ikinci dereceden kalan kodların Q_p, N_p, Q_p', N_p' idempotent üreteçleri sırasıyla

$$E_Q = \frac{1}{2}\left(1+\frac{1}{p}\right)+\frac{1}{2}\left(\frac{1}{p}-\frac{1}{\theta}\right)l_1+\frac{1}{2}\left(\frac{1}{p}+\frac{1}{\theta}\right)l_2 \quad (4.1)$$

$$E_N = \frac{1}{2}\left(1+\frac{1}{p}\right)+\frac{1}{2}\left(\frac{1}{p}+\frac{1}{\theta}\right)l_1+\frac{1}{2}\left(\frac{1}{p}-\frac{1}{\theta}\right)l_2 \quad (4.2)$$

$$F_Q = \frac{1}{2}\left(1-\frac{1}{p}\right)-\frac{1}{2}\left(\frac{1}{p}+\frac{1}{\theta}\right)l_1-\frac{1}{2}\left(\frac{1}{p}-\frac{1}{\theta}\right)l_2 \quad (4.3)$$

$$F_N = \frac{1}{2}\left(1-\frac{1}{p}\right)-\frac{1}{2}\left(\frac{1}{p}-\frac{1}{\theta}\right)l_1-\frac{1}{2}\left(\frac{1}{p}+\frac{1}{\theta}\right)l_2 \quad (4.4)$$

şeklindedir. Burada θ Gauss toplamıdır. $\chi(i)$ Legendre sembolü olmak üzere $\theta = \sum_{i=1}^{q-1} \chi(i)\alpha^i$ ve $\chi(\mathrm{i}) = \begin{cases} 0, & p \mid i \\ 1, & i \in QR_p \\ -1, & i \in NQR_p \end{cases}$ 'dir. Ayrıca $p = 4k-1$ ise $\theta^2 = -p$ ve $p = 4k+1$ ise $\theta^2 = p$ olduğunu biliyoruz.

Örnek 4.9 Örnek 4.5'deki ikinci dereceden kalan kodların idempotent üreteçleri,

$E_Q(x) = 1+x^2+x^5+x^6+x^7+x^8+x^{11}$, $E_N(x) = 1+x+x^3+x^4+x^9+x^{10}+x^{12}$,

$F_Q(x) = 2x+2x^3+2x^4+2x^9+2x^{10}+2x^{12}$ ve

$F_N(x) = 2x^2+2x^5+2x^6+2x^7+2x^8+2x^{11}$'dir.

BÖLÜM 5

q. KUVVET KALAN KODLAR

q. kuvvet kalan kodlar 1968'de Berlekamp tarafından tanımlanmıştır [30]. Daha sonra Charters bu kodların idempotent üreteçlerini çalışmıştır ve yeni bir idempotent tanımlamıştır [31]. q. kuvveti kendine eşit olan ve q. kuvvet kalan kodları üreten polinomlara q***-idempotent*** ismini vermiştir ve bu idempotent üreteçlerin yapısını çalışmıştır. Bu bölümdeki temel bilgiler *"Algebraic coding theory"* (1968) [30] ve Charters'ın "*Generalizing binary quadratic residue codes to higher power residues over larger fields*" isimli makalesinden derlenmiştir [31].

Bu kodlar ikinci dereceden kalan kodların bir genelleştirilmesidir. İkinci dereceden kalan kodların tanımlanmasında kullanılan koset sayısını q bir asal olmak üzere, 2'den q'ya çıkarmıştır.

Bu bölümde öncelikle cisimler üzerinde q. kuvvet kalan kodların tanımı verilecektir, daha sonra bu kodlar $\mathbb{F}_q[v]/(v^3-v)$ halkası üzerinde tanımlanacaktır.

5.1 Cisimler Üzerinde q. Kuvvet Kalan Kodlar

Tanım 5.1 [30] p ve q birbirinden farklı asallar olsun. $\beta^q \equiv \alpha (\mathrm{mod}\, p)$ olacak şekilde $\beta \in \mathbb{F}_p$ varsa α'ya ***modülo*** p ***'ye göre*** q***. kuvvet kalan*** denir.

p ve q birbirinden farklı asallar, $q|(p-1)$ ve q modülo p'ye göre q. kuvvet kalan olsun. Bu durumda $\mathbb{F}_p$'yi aşağıdaki şekilde, eşit sayıda elemana sahip q kosete ayırabiliriz:

$\mathbb{F}_p - \{0\}$'da birimin q. ilkel kökü olan bir ζ elemanı seçelim ve $j^{(p-1)/q} \equiv \zeta^i \pmod p$ olacak şekilde,

$$\begin{aligned} \psi_q : \quad & \mathbb{F}_p - \{0\} \to (\mathbb{F}_p, +) \\ & j \to i \end{aligned} \tag{5.1}$$

bir homomorfizma tanımlayalım. Her i'ye karşılık gelen elamanları A_i kümesinde toplarsak, $\mathbb{F}_p$'yi $A_0, A_1, \ldots A_{q-1}$ şeklinde q kosete ayırmış oluruz.

Örnek 5.2 $p = 31$, $q = 5$ olarak şeçelim. $\mathbb{F}_{31}$'i 5 kosete ayırabiliriz: $A_0 = \{1, 5, 6, 25, 26, 30\}$, $A_1 = \{2, 10, 12, 19, 21, 29\}$, $A_2 = \{4, 7, 11, 20, 24, 27\}$, $A_3 = \{8, 9, 14, 17, 22, 23\}$, $A_4 = \{3, 13, 15, 16, 18, 28\}$.

Tanım 5.3 [30] α, $\mathbb{F}_q$'nun n. dereceden bir cisim genişlemesinde birimin p. ilkel kökü olsun. Yukarıda tanımladığımız A_i kosetlerine karşılık gelen,

$$a_i(x) = \prod_{s \in A_i} (x - \alpha^s) \tag{5.2}$$

polinomları ve $(x-1)a_i(x)$ polinomları ile $\mathbb{F}_q$ cismi üzerinde üretilen p uzunluklu devirli kodlara q***. kuvvet kalan kodlar*** denir. Özel olarak $a_i(x)$ ile üretilen kodlara ***artırılmış(augmented)*** q***. kuvvet kalan kodlar***, $(x-1)a_i(x)$ ile üretilen kodlara ***azaltılmış(expurgated)*** q***. kuvvet kalan kodlar*** denir. Ayrıca,

$$x^p - 1 = (x-1) \prod_{i=0}^{q-1} a_i(x) \tag{5.3}$$

olduğu görülür.

Örnek 5.4 $\mathbb{F}_5$ üzerinde 31 uzunluklu q. kuvvet kalan kodları bulalım. Burada kosetler $A_0 = \{1, 5, 6, 25, 26, 30\}$, $A_1 = \{2, 10, 12, 19, 21, 29\}$, $A_2 = \{4, 7, 11, 20, 24, 27\}$, $A_3 = \{8, 9, 14, 17, 22, 23\}$ ve $A_4 = \{3, 13, 15, 16, 18, 28\}$ şeklindedir. Bu kosetlere karşılık gelen üreteç polinomlar da $a_0(x) = 1 + 3x + 2x^2 + 4x^3 + 2x^4 + 3x^5 + x^6$, $a_1(x) = 1 + 4x^2 + x^3 + 4x^4 + x^6$, $a_2(x) = 1 + 3x + 4x^2 + 3x^3 + 4x^4 + 3x^5 + x^6$,

$a_3(x)=1+4x+x^2+2x^3+x^4+4x^5+x^6$, $a_4(x)=1+x+2x^2+3x^3+2x^4+x^5+x^6$ olur. Artırılmış 5. kuvvet kalan kodların parametreleri $[31,25,4]_5$, azaltılmış 5. kuvvet kalan kodların parametreleri $[31,24,5]_5$'tir ve bu kodlar optimale yakındır(nearly optimal).

Teorem 5.5 [30] $j^{(p-1)/q}\equiv\zeta^i \pmod p$ olmak üzere,

$$\begin{aligned}\psi_q:\ \ \mathbb{F}_p-\{0\}&\to(\mathbb{F}_p,+)\\ j&\to i\end{aligned} \tag{5.4}$$

dönüşümünü tanımlayalım. $E_q(x)=\sum_{m=1}^{p-1}\psi_q(m)x^m$ polinomu ile $\mathbb{F}_q$ üzerinde üretilen devirli kod, $\mathbb{F}_q$ üzerinde p uzunluklu azaltılmış q. kuvvet kalan kodlara denk koddur. Ayrıca $\mathbb{F}_q[x]/(x^p-1)$ halkası üzerinde $(E_q(x))^q=E_q(x)$'dir. $E_q(x)$'e azaltılmış q. kuvvet kalan kodların q-idempotenti diyeceğiz.

Örnek 5.6 Bir önceki örnekteki azaltılmış 5. kuvvet kalan kodların 5-idempotent'i,

$$\begin{aligned}E_5(x)=\ \ & x^2+4x^3+2x^4+2x^7+3x^8+3x^9+x^{10}+2x^{11}+x^{12}++4x^{13}+3x^{14}+4x^{15}\\ &+4x^{16}+3x^{17}+4x^{18}+x^{19}+2x^{20}+x^{21}+3x^{22}+3x^{23}+2x^{24}+4x^{28}+x^{29}\end{aligned}$$

polinomudur.

5.2 $\mathbb{F}_q[v]/(v^3-v)$ Halkası Üzerinde q. Kuvvet Kalan Kodlar

$\mathbb{F}_q[v]/(v^3-v)$ halkası üzerinde q. kuvvet kalan kodlar, bu kodların cisimler üzerindeki idempotent üreteçleri yardımıyla tanımlanacaktır. Öncelikle $\mathbb{F}_q[v]/(v^3-v)$ halkasının yapısına göz atalım.

q bir asal olmak üzere $\mathbb{F}_q[v]/(v^3-v)$ halkası q^3 mertebeli, karakteristiği q olan bir halkadır. Minimal idealleri $\langle v(v-1)\rangle$, $\langle v(v+1)\rangle$ ve $\langle (v\text{-}1)(v+1)\rangle$'dir. Dolayısıyla $\mathbb{F}_q[v]/(v^3-v)=\langle v(v-1)\rangle+\langle v(v+1)\rangle+\langle (v-1)(v+1)\rangle$ şeklinde yazabiliriz.

p ve q birbirinden farklı asallar, $q\mid(p-1)$ ve q modülo p'ye göre q. kuvvet kalan olsun. $\left(\mathbb{F}_q[v]/(v^3-v)\right)[x]/(x^p-1)$ halkasını $A_{q,p}$ ile gösterelim. $\hat{v}=(v-1)(v+1)$, $v+1=(v)(v-1)$ ve $v-1=(v)(v+1)$ olmak üzere $A_{q,p}$'nin elamanlarını,

$$
\begin{aligned}
A_{q,p} &= \left\{a_1 + a_2 x + \cdots a_p x^{p-1} : a_i \in \mathbb{F}_q[v]/(v^3 - v)\right\} \\
&= \Big\{(a_{11}(\hat{v}) + a_{12}(v+1) + a_{13}(v-1) + \\
&\quad (a_{21}(\hat{v}) + a_{22}(v+1) + a_{23}(v-1))x + \\
&\quad \cdots \\
&\quad (a_{q1}(\hat{v}) + a_{q2}(v+1) + a_{q3}(v-1))x^{p-1} : a_{ij} \in \mathbb{F}_q\Big\} \\
&= \Big\{(a_{11} + a_{21}x + \cdots a_{p1}x^{p-1})(\hat{v}) + \\
&\quad (a_{12} + a_{22}x + \cdots a_{p2}x^{p-1})(v+1) + \\
&\quad (a_{13} + a_{23}x + \cdots a_{p3}x^{p-1})\widehat{(v-1) : a_{ij}} \in \mathbb{F}_q\Big\} \\
&= \left\{A_1(\hat{v}) + A_2\widehat{(v+1)} + A_3\widehat{(v-1) : A_i} \in \mathbb{F}_q[x]/(x^p - 1)\right\}
\end{aligned}
\tag{5.5}
$$

şeklinde düzenleyebiliriz.

Teorem 5.7 $q > 2$ olacak şekilde $A_{q,p}$'nin bir $\alpha = A_1(\hat{v}) + A_2(v+1) + A_3(v-1)$ elemanının q-idempotent olması için gerek ve yeter koşul A_1, $2A_2$ ve $2A_3$'ün $\mathbb{F}_q[x]/(x^p - 1)$'de q-idempotent olmalarıdır.

İspat Öncelikle $\hat{v}$, $v+1$ ve $v-1$'in q. kuvvetlerini hesaplayalım.

$$\left(\hat{v}\right)^2 = \left((v+1)(v-1)\right)^2 = \left(v^2-1\right)^2 = v^4 - 2v^2 + 1 = v^2 - 2v^2 + 1 = -\left(v^2 - 1\right) \tag{5.6}$$

$$\left(\hat{v}\right)^3 = \left(\hat{v}\right)^2\left(\hat{v}\right) = -\left(\hat{v}\right)\left(\hat{v}\right) = -\left(\hat{v}\right)^2 = \left(\hat{v}\right) \tag{5.7}$$

$$\left(\hat{v}\right)^4 = \left(\hat{v}\right)^2\left(\hat{v}\right)^2 = \left(-\left(\hat{v}\right)\right)\left(-\left(\hat{v}\right)\right) = \left(\hat{v}\right)^2 = -\left(\hat{v}\right) \tag{5.8}$$

$$\left(\hat{v}\right)^5 = \left(\hat{v}\right)^3\left(\hat{v}\right)^2 = \left(\hat{v}\right)\left(-\left(\hat{v}\right)\right) = -\left(\hat{v}\right)^2 = \left(\hat{v}\right) \tag{5.9}$$

Bu şekilde devam edildiğinde, q tek olduğunda $\left(\hat{v}\right)^q = \hat{v}$ olduğu görülür.

$$\left(v+1\right)^2 = \left(v(v-1)\right)^2 = \left(v^2 - v\right)^2 = v^4 - 2v^3 + v^2 = -2v^3 + 2v^2 = 2v^2 - 2v = 2\left(v+1\right) \tag{5.10}$$

$$(v+1)^3=(v+1)^2(v+1)=2(v+1)(v+1)=2(v+1)^2=4(v+1)=2^2(v+1) \quad (5.11)$$

$$(v+1)^4=(v+1)^2(v+1)^2=4(v+1)^2=8(v+1)=2^3(v+1) \quad (5.12)$$

Bu şekilde devam edildiğinde, $(v+1)^q=2^{q-1}(v+1)$ olduğu görülür.

$$(v-1)^2=(v(v+1))^2=(v^2+v)^2=v^4+2v^3+v^2=2v^3+2v^2=2v^2+2v=2(v-1) \quad (5.13)$$

$$(v-1)^3=(v-1)^2(v-1)=2(v-1)(v-1)=2(v-1)^2=4(v-1)=2^2(v-1) \quad (5.14)$$

$$(v-1)^4=(v-1)^2(v-1)^2=2(v-1)2(v-1)=4(v-1)^2=8(v-1)=2^3(v-1) \quad (5.15)$$

Bu şekilde devam edildiğinde, $(v-1)^q=2^{q-1}(v-1)$ olduğu görülür.

$\alpha \in A_{q,p}$ elemanı için $\alpha^q=\alpha$ olsun. Bu durumda,

$$\begin{aligned}\alpha^q &= \left(A_1(\hat{v})+A_2(v+1)+A_3(v-1)\right)^q \\ &= \left(A_1(\hat{v})\right)^q+\left(A_2(v+1)\right)^q+\left(A_3(v-1)\right)^q \\ &= A_1{}^q(\hat{v})+2^{q-1}A_2{}^q(v+1)+2^{q-1}A_3{}^q(v-1)\end{aligned} \quad (5.16)$$

olur. α^q'nun α'ya eşit olması için, $A_1=A_1^q$, $A_2=2^{q-1}A_2^q$ ve $A_3=2^{q-1}A_3^q$ olması gerekir. $A_2=2^{q-1}A_2^q$ eşitliğini $2A_2=2^qA_2^q=(2A_2)^q$ şeklinde düzenleyebiliriz. Benzer şekilde $2A_3=2^qA_3^q=(2A_3)^q$ olur. Dolayısıyla A_1, $2A_2$ ve $2A_3$ q-idempotenttir.

Diğer taraftan A_1, $2A_2$ ve $2A_3$ q-idempotent olduğunda $\alpha^q=\alpha$ olduğu açıktır.

Tanım 5.8 A_1, $2A_2$ ve $2A_3$ $\mathbb{F}_q$ üzerinde p uzunluklu q-idempotent kodun idempotent üreteçleri olsun. $\mathbb{F}_q[v]/(v^3-v)$ halkası üzerinde $A_1(\hat{v})+A_2(v+1)+A_3(v-1)$ q-idempotenti ile üretilen p uzunluklu devirli koda $\mathbb{F}_q[v]/(v^3-v)$ ***halkası üzerinde*** q***. kuvvet kalan kod*** denir.

Örnek 5.9 $\mathbb{F}_5$ üzerinde 31 uzunluklu 5. kuvvet kalan kodun 5- idempotentini bir önceki örnekte vermiştik. $A_1 = E_5(x)$, $A_2 = E_5(x)/2$ ve $A_3 = E_5(x)/2$ olarak seçersek, $\mathbb{F}_5[v]/(v^3 - v)$ halkası üzerinde 5- idempotent üreteç,

$$\begin{aligned} E_5(x) = \quad & (4+2v^2)x^2 + (1+3v^2)x^3 + (3+4v^2)x^4 + (3+4v^2)x^7 + (2+v^2)x^8 \\ & + (2+v^2)x^9 + (4+2v^2)x^{10} + (3+4v^2)x^{11} + (4+2v^2)x^{12} + (1+3v^2)x^{13} \\ & + (2+v^2)x^{14} + (1+3v^2)x^{15} + (1+3v^2)x^{16} + (2+v^2)x^{17} + (1+3v^2)x^{18} \\ & + (4+2v^2)x^{19} + (3+4v^2)x^{20} + (4+2v^2)x^{21} + (2+v^2)x^{22} + (2+v^2)x^{23} \\ & + (3+4v^2)x^{24} + (3+4v^2)x^{24} + (3+4v^2)x^{27} + (1+3v^2)x^{28} + (4+2v^2)x^{29} \end{aligned}$$

şeklindedir. Bu idempotent üretecin ürettiği kodun, aynı zamanda $\mathbb{F}_5[v]/(v^3 - v)$ halkası üzerinde azaltılmış 5. kuvvet kalan kodların parametreleri $[31, 24, 5]_5$'tir. Bu kod halkalar üzerinde Griesmer sınırına göre neredeyse optimaldir.

BÖLÜM 6

m-SEL KALAN KODLAR

Bu bölümde cisimler üzerinde m-sel kalan kodların tanımını vereceğiz.

6.1 Cisimler Üzerinde m-sel Kalan Kodlar

Tanım 6.1 [10] p bir asal, q bir asalın kuvveti ve $ebob(p,q)=1$ olsun. b, $\mathbb{Z}_p^*$'ın bir ilkel elemanı ve γ, $\mathbb{F}_q$'nun bazı cisim genişlemelerinde birimin p. ilkel kökü olsun. $m \geq 2$, $m \in \mathbb{Z}$ ve $m|(p-1)$ olmak üzere modulo p'ye göre sıfırdan farklı m-***sel kalanların kümesi***,

$$Q_0 = \{\alpha^m : \alpha \in \mathbb{Z}_p\} \tag{6.1}$$

şeklinde tanımlanır. Ayrıca, diğer kosetler de,

$$Q_i = b^i Q_0 \tag{6.2}$$

şeklinde tanımlanır. $a \in Q_1$ olmak üzere

$$\mu_a : i \to a.i \tag{6.3}$$

şeklinde tanımlanan fonksiyona da ***koordinat permütasyon fonksiyonu*** denir. Bu fonksiyon Q_i'leri devirli olarak permüte eder.

Örnek 6.2 $p=19$ ve $q=5$ alalım. 2, $\mathbb{Z}_{19}^*$'ın bir ilkel elemanı olduğundan $b=2$ alabiliriz. $6|19-1$ olduğundan $m=6$ seçebiliriz. Bu durumda,

$Q_0 = \{1,7,11\}$, $Q_1 = \{2,3,14\}$, $Q_2 = \{4,6,9\}$, $Q_3 = \{8,12,18\}$, $Q_4 = \{5,16,17\}$, $Q_5 = \{10,13,15\}$ olur.

Tanım 6.3 [10] q, m-sel kalan olsun, yani, $q \in Q_0$ olsun.

$$g_i(x) = \frac{x^p - 1}{\prod_{k \in Q_i} x - \gamma^k} \qquad (i = 0,1,\ldots,m-1) \tag{6.4}$$

olacak şekilde $C_i = \langle g_i(x) \rangle$ kodunu tanımlayalım. Bu durumda $\{C_0, C_1, \ldots, C_{m-1}\}$ kümesine $\mathbb{F}_q$ üzerinde p uzunluklu ***sınıf(class) I*** m***-sel kalan kodlarının çiftsel(even-like) ailesi*** denir. C_i'lerin boyutları $(p-1)/m$ şeklindedir.

Benzer şekilde $\overline{C_i}$'ler, C_i'lerin komplementleri olmak üzere $\{\overline{C_0}, \overline{C_1}, \ldots, \overline{C_{m-1}}\}$ kod ailesine $\mathbb{F}_q$ üzerinde p uzunluklu ***sınıf I*** m***-sel kalan kodlarının teksel(odd-like) ailesi*** denir, üreteç polinomu,

$$\overline{g_i}(x) = \prod_{k \in Q_i} x - \gamma^k \qquad (i = 0,1,\ldots,m-1) \tag{6.5}$$

şeklindedir ve boyutları $p - (p-1)/m$'dir.

Tanım 6.4 [10] D_i'ler, C_i'lerin komplement kodları olmak üzere $\{D_0, D_1, \ldots, D_{m-1}\}$ kod ailesine $\mathbb{F}_q$ üzerinde p uzunluklu ***sınıf II*** m***-sel kalan kodlarının çiftsel ailesi*** denir, üreteç polinomu,

$$h_i(x) = (x-1)\overline{g_i}(x) \tag{6.6}$$

şeklindedir ve boyutları $p - 1 - (p-1)/m$'dir.

Benzer şekilde $\overline{D_i}$'ler, D_i'lerin komplementleri olmak üzere $\{\overline{D_0}, \overline{D_1}, \ldots, \overline{D_{m-1}}\}$ kod ailesine $\mathbb{F}_q$ üzerinde p uzunluklu ***sınıf II*** m***-sel kalan kodlarının teksel ailesi*** denir, üreteç polinomu,

$$\overline{h_i}(x) = \frac{g_i(x)}{x-1} \tag{6.7}$$

şeklindedir ve boyutları $(p-1)/m + 1$'dir.

Örnek 6.5 $\mathbb{F}_4$ üzerinde 17 uzunluklu 4-sel kalan kodları belirleyelim. $\mathbb{Z}_{17}^{*}$'ın kosetleri, $Q_0=\{1,4,13,16\}$, $Q_1=\{3,5,12,14\}$, $Q_2=\{2,8,9,15\}$ ve $Q_3=\{6,7,10,11\}$'dir.

α, $\mathbb{F}_4[x]/(x^4+x^3+x+w)$ genişlemesinde birimin 17. ilkel kökü olsun. Bu durumda $\mathbb{F}_4$ üzerinde 17 uzunluklu sınıf I 4-sel kalan kodların çiftsel ailesi,

$C_0=\langle g_0(x)=1+x+w^2x^2+x^4+w^2x^5+wx^6+wx^7+w^2x^8+x^9+w^2x^{11}+x^{12}+x^{13}\rangle$,

$C_1=\langle g_1(x)=1+wx+wx^2+w^2x^3+x^4+wx^6+wx^7+x^9+w^2x^{10}+wx^{11}+wx^{12}+x^{13}\rangle$,

$C_2=\langle g_2(x)=1+x+wx^2+x^4+wx^5+w^2x^6+w^2x^7+wx^8+x^9+wx^{11}+x^{12}+x^{13}\rangle$,

$C_3=\langle g_3(x)=1+w^2x+w^2x^2+wx^3+x^4+w^2x^6+w^2x^7+x^9+wx^{10}+w^2x^{11}+w^2x^{12}+x^{13}\rangle$

polinomlarının ürettikleri kodlardan oluşur. Bu kodların parametreleri $[17,4,12]$'dir.

$\mathbb{F}_4$ üzerinde 17 uzunluklu sınıf I 4-sel kalan kodların teksel ailesi,

$\overline{C_0}=\langle \overline{g_0}(x)=1+x+wx^2+x^3+x^4\rangle$, $\overline{C_1}=\langle \overline{g_1}(x)=1+wx+x^2+wx^3+x^4\rangle$,

$\overline{C_2}=\langle \overline{g_2}(x)=1+x+w^2x^2+x^3+x^4\rangle$ ve $\overline{C_3}=\langle \overline{g_3}(x)=1+w^2x+x^2+w^2x^3+x^4\rangle$

polinomlarının ürettikleri kodlardan oluşur. Bu kodların parametreleri $[17,13,4]$'tür.

$\mathbb{F}_4$ üzerinde 17 uzunluklu sınıf II 4-sel kalan kodların çiftsel ailesi,

$D_0=\langle h_0(x)=1+w^2x^2+w^2x^3+x^5\rangle$, $D_1=\langle h_1(x)=1+w^2x+w^2x^2+w^2x^3+w^2x^4+x^5\rangle$,

$D_2=\langle h_2(x)=1+wx^2+wx^3+x^5\rangle$ ve $D_3=\langle h_3(x)=1+wx+wx^2+wx^3+wx^4+x^5\rangle$

polinomlarının ürettikleri kodlardan oluşur. Bu kodların parametreleri $[17,12,4]$'tür.

$\mathbb{F}_4$ üzerinde 17 uzunluklu sınıf II 4-sel kalan kodların teksel ailesi,

$\overline{D_0}=\langle \overline{h_0}(x)=1+w^2x^2+w^2x^3+wx^4+x^5+w^2x^6+x^7+wx^8+w^2x^9+w^2x^{10}+x^{12}\rangle$,

$\overline{D_1}=\langle \overline{h_1}(x)=1+w^2x+x^2+wx^3+w^2x^4+w^2x^5+x^6+w^2x^7+w^2x^8+wx^9+x^{10}+w^2x^{11}+x^{12}\rangle$,

$\overline{D_2}=\langle \overline{h_2}(x)=1+w^2x^2+wx^3+w^2x^4+x^5+wx^6+x^7+w^2x^8+wx^9+wx^{10}+x^{12}\rangle$ ve

$\overline{D_3}=\langle \overline{h_3}(x)=1+wx+x^2+w^2x^3+wx^4+wx^5+x^6+wx^7+wx^8+w^2x^9+x^{10}+wx^{11}+x^{12}\rangle$

polinomlarının ürettikleri kodlardır. Bu kodların parametreleri $[17,5,9]$'dur.

6.2 m -sel Kalan Kodların İdempotent Üreteçleri

Önerme 6.6 [10] e, C m-sel kalan kodunun idempotent üreteci olsun. Bu durumda, $l_i(x) = \sum_{k \in Q_i} x^k$ olmak üzere, e, $\mathbb{F}_q$ üzerindeki $l_0(x), l_1(x), \ldots, l_{m-1}(x)$ ve 1 polinomlarının bir lineer kombinasyonudur.

Örnek 6.7 $\mathbb{F}_4$ üzerinde 17 uzunluklu 4-sel kalan kodlar için $l_0(x) = x + x^4 + x^{13} + x^{16}$, $l_1(x) = x^3 + x^5 + x^{12} + x^{14}$, $l_2(x) = x^2 + x^8 + x^9 + x^{15}$ ve $l_3(x) = x^6 + x^7 + x^{10} + x^{11}$ olmak üzere idempotent üreteçler;

$id(C_0) = id(\overline{C_0}) = l_0 + wl_1 + l_2 + w^2 l_3$, $id(C_1) = id(\overline{C_1}) = wl_0 + l_1 + w^2 l_2 + l_3$,

$id(C_2) = id(\overline{C_2}) = l_0 + w^2 l_1 + l_2 + wl_3$, $id(C_3) = id(\overline{C_3}) = w^2 l_0 + l_1 + wl_2 + l_3$,

$id(D_0) = id(\overline{D_0}) = w^2 l_1 + wl_3$, $id(D_1) = id(\overline{D_1}) = w^2 l_0 + wl_2$, $id(D_2) = id(\overline{D_2}) = wl_1 + w^2 l_3$

ve $id(D_3) = id(\overline{D_3}) = wl_0 + w^2 l_2$

şeklindedir.

BÖLÜM 7

$\mathbb{F}_q[v]/(v^2-v)$ HALKASI ÜZERİNDE m-SEL KALAN KODLAR

Bu bölümde cisimler üzerinde inşa edilen m-sel kalan kodları idempotent üreteçler vasıtasıyla, q bir asalın kuvveti olacak şekilde $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerine taşıyacağız. İdempotentlerin belirlenmesinde Brualdi ve Pless'in belirlediği idempotentlerin birbiri ile olan bağıntıları kullanılmıştır [6]. Ayrıca Kaya vd. halkalar üzerinde ikinci dereceden kalan kodlar için idempotent belirleme yöntemi kullanılmıştır [4].

7.1 $\mathbb{F}_q[v]/(v^2-v)$ Halkası Üzerinde İdempotentlerin Yapısı

Önerme 7.1 p bir asal ve q bir asalın kuvveti olsun. $m|(p-1)$ olacak şekilde bir $m \in Z^+$ seçelim ve $a, q \in Q_0$ olsun. e_i ile e_j $\mathbb{F}_q$ üzerinde p uzunluklu m-sel kalan kodların idempotent üreteçleri ise $v.e_i+(1-v).e_j$'ler de $\mathbb{F}_q[v]/(v^2-v)$ halkasında idempotentlerdir.

İspat: e_i ve e_j $\mathbb{F}_q$ üzerinde idempotent olsun. $v.e_i+(1-v).e_j \in \mathbb{F}_q[v]/(v^2-v)$ elemanı için,

$$(v.e_i+(1-v).e_j)^2 = v.e_1^{\,2}+(1-v).e_j^{\,2} = v.e_i+(1-v).e_j \qquad (7.1)$$

olur ve $v.e_i+(1-v).e_j$ elemanının da idempotent olduğu görülür.

7.2 $\mathbb{F}_q[v]/(v^2-v)$ Üzerinde m-sel Kalan Kodların İdempotent Üreteçleri

Önerme 7.2 $i, j \in \{0,1,...,m-1\}$ olmak üzere, $e_i, e_j \in \mathbb{F}_q[x]/(x^p-1)$ $\mathbb{F}_q$ üzerinde sınıf I çiftsel m-sel kalan kodların idempotent üreteçleri,

$E_k = v.e_i + (1-v).e_j \in (\mathbb{F}_q[v]/(v^2-v))[x]/(x^p-1)$ ve $h = 1+x+x^2+\cdots+x^{p-1}$ olsun.

i. $\mu_a(E_k)$ da idempotenttir.

ii. $a \neq c, b \neq d \in \mathbb{Z}^+ \cup \{0\}$ olmak üzere $E_i = v.e_a + (1-v).e_b$, $E_j = v.e_c + (1-v).e_d$ olsun. Bu durumda $E_i E_j = 0$ 'dır.

iii. $E_k = E_0$ olarak alırsak ve $\mu_a(E_i) = E_{i+1}$ dersek $E_0 + E_1 + \cdots E_{m-1} = 1-h$ olur

İspat:

i. $E_k = v.e_i + (1-v).e_j$ ise,

$\mu_a(v.e_i + (1-v).e_j) = v\mu_a(e_i) + (1-v)\mu_a(e_j)$ olur ve $\mu_a(e_i)$ ile $\mu_a(e_j)$ idempotent olduğundan,

$$\begin{aligned}(\mu_a(E_k))^2 = \quad & (v.\mu(e_i) + (1-v).\mu(e_2))^2 = v^2(\mu(e_i))^2 + (1-v)^2(\mu(e_j))^2 \\ & = v\mu(e_i) + (1-v)\mu(e_j) = \mu_a(E_k)\end{aligned} \tag{7.2}$$

ii. $a \neq c, b \neq d \in \mathbb{Z}^+ \cup \{0\}$ olmak üzere $E_i = v.e_a + (1-v).e_b$, $E_j = v.e_c + (1-v).e_d$ olsun.

$$\begin{aligned}E_i E_j = \quad & (v.e_a + (1-v).e_b)(v.e_c + (1-v).e_d) \\ & = v^2 e_a e_c + (1-v)^2 e_b e_d = v^2.0 + (1-v)^2.0 = 0\end{aligned} \tag{7.3}$$

iii. $E_0 = v.e_0 + (1-v).e_{0'}$, $E_1 = v.e_1 + (1-v).e_{1'}$,..., $E_{m-1} = v.e_{m-1} + (1-v).e_{m-1'}$ olsun.

$\mu_a(E_i) = E_{i+1}$ olduğundan $\mu_a(e_i) = e_{i+1}$ ve $\mu_a(e_{i'}) = e_{i+1'}$ olur. O halde,

$$\begin{aligned}E_0 + E_1 + \cdots E_{m+1} = \quad & v(e_0 + e_1 + \cdots e_{m-1}) + (1-v)(e_{0'} + e_{1'} + \cdots e_{m-1'}) \\ & = v.(1-h) + (1-v)(1-h) = 1-h\end{aligned} \tag{7.4}$$

eşitliği elde edilir.

$E_k = v.e_i + (1-v).e_j$ idempotent elemanı Önerme 7.2'deki özellikleri sağladığından dolayı m-sel kalan kodlar için idempotent üreteç olarak alınabilir.

Tanım 7.3 e_i'ler $\mathbb{F}_q$ cismi üzerinde sınıf I çiftsel m-sel kalan kodların idempotent üreteçleri olmak üzere $(\mathbb{F}_q[v]/(v^2-v))[x]/(x^p-1)$ halkasında $E_k = v.e_i + (1-v).e_j$ idempotent elemanının ürettiği koda $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde p uzunluklu sınıf I çiftsel m-sel kalan kod denir.

Önerme 7.4 E_i, $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde p uzunluklu sınıf I çiftsel m-sel kalan kodun idempotent üreteci olsun ve $i, j \in \{0,1,\ldots,m-1\}$ olmak üzere, $E_i' = 1-E_i$ olarak alalım. O halde E_i' aşağıdaki özellikleri sağlar:

i. $\mu_a(E_i) = E_j$ olmak üzere, $\mu_a(E_i') = E_j'$ olur.

ii. $a \neq c, b \neq d \in \mathbb{Z}^+ \cup \{0\}$ olmak üzere $E_i' = v.e_a + (1-v).e_b$, $E_j' = v.e_c + (1-v).e_d$ olsun. Bu durumda $E_i' + E_j' - E_i'E_j' = 1$'dir.

iii. $E_k' = E_0'$ olarak alırsak ve $\mu_a(E_i') = E_{i+1}'$ dersek $E_0'E_1'\ldots E_{m-1}' = h$ olur.

İspat:

i. $$\mu_a(E_i') = \mu_a(1-E_i) = 1-\mu_a(E_i) = 1-E_j = E_j' \,. \tag{7.5}$$

ii. $$\begin{aligned} E_i' + E_j' - E_i'E_j' &= 1-E_i+1-E_j-(1-E_i)(1-E_j) \\ &= 2-E_i-E_j-(1-E_i-E_j+E_iE_j) = 1-E_iE_j = 1-0 = 1. \end{aligned} \tag{7.6}$$

iii. $$\begin{aligned} E_0'E_1'\ldots E_{m-1}' &= (1-E_0)(1-E_1)\ldots(1-E_{m-1}) \\ &= 1-(E_0+E_1+\cdots E_{m-1}) + (E_0E_1+E_0E_2+\cdots E_{m-2}E_{m-1}) \\ &\quad -(E_0E_1E_2+E_0E_1E_3+\cdots E_{m-3}E_{m-2}E_{m-1})+\cdots+E_0E_1\ldots E_{m-1} \\ &= 1-(1-h) = 1-1+h = h. \end{aligned} \tag{7.7}$$

Tanım 7.5 $i \in \{0,1,\ldots,m-$ için $E_i' = 1-E_i$ olmak üzere E_i' idempotent elemanının ürettiği koda $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde p uzunluklu sınıf I teksel m-sel kalan kod denir.

Önerme 7.6 E_i, $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde p uzunluklu sınıf I çiftsel m-sel kalan kodun idempotent üreteci olsun ve $i, j \in \{0,1,...,m-1\}$ olmak üzere, $F_i = 1-h-E_i$ olarak alalım. O halde F_i aşağıdaki özellikleri sağlar:

i. $\mu_a(E_i) = E_j$ olmak üzere, $\mu_a(F_i) = F_j$'dir.

ii. $a \neq c, b \neq d \in \mathbb{Z}^+ \cup \{0\}$ olmak üzere $F_i = v.e_a + (1-v).e_b$, $F_j = v.e_c + (1-v).e_d$ olsun.

$F_i + F_j - F_iF_j = 1-h$'dir.

iii. $F_k = F_0$ olarak alırsak ve $\mu_a(F_i) = F_{i+1}$ dersek $F_0F_1 \ldots F_{m-1} = 0$.

İspat:

i. $\mu_a(F_i) = \mu_a(1-h-E_i) = 1-\mu_a(h)-\mu_a(E_i) = 1-h-E_j = F_j$. (7.8)

ii. $F_i + F_j - F_iF_j = (1-h-E_i)+(1-h-E_j)-(1-h-E_i)(1-h-E_j)$

$$= 2-2h-E_i-E_j-(1-h-E_j-h+h^2-hE_j-E_i+hE_i+E_iE_j) = 1-h\,. \quad (7.9)$$

iii. $F_0F_1 \ldots F_{m-1} = (1-h-E_0)(1-h-E_1)\ldots(1-h-E_{m-1})$

$$= 1-h(m-(m-1)(E_0+E_1+\cdots E_{m-1})+(m-2)(E_0E_1+E_0E_2+\cdots E_{m-2}E_{m-1})$$

$$+\cdots+(E_0E_1\ldots E_{m-2}+\cdots+E_1E_2\ldots E_{m-1}))-(E_0+E_1+\cdots E_{m-1}) \quad (7.10)$$

$$= 1-h(m-(m-1)(1-h)+(m-2).0+\cdots+2.0+0)-(1-h) = 0\,.$$

Tanım 7.7 $i \in \{0,1,...,m-1\}$ için $F_i = 1-h-E_i$ olmak üzere F_i idempotent elemanının ürettiği koda $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde p uzunluklu sınıf II çiftsel m-sel kalan kod denir.

Önerme 7.8 E_i ve F_i, $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde sırasıyla, p uzunluklu sınıf I çiftsel m-sel kalan kodun idempotent üreteci ve p uzunluklu sınıf II çiftsel m-sel kalan kodun idempotent üreteci olsun. $i, j \in \{0,1,...,m-1\}$ olmak üzere, $F_i' = 1-F_i = h+E_i$ olarak alalım. O halde F_i' aşağıdaki özellikleri sağlar:

i. $\mu_a(E_i) = E_j$ olmak üzere, $\mu_a(F_i') = F_j'$.

ii. $a \neq c, b \neq d \in \mathbb{Z}^+ \cup \{0\}$ olmak üzere $F_i' = v.e_a + (1-v).e_b$, $F_j' = v.e_c + (1-v).e_d$ olsun.

$F_i'F_j' = h$'dır.

iii. $F_k' = F_0'$ olarak alırsak ve $\mu_a(F_i') = F_{i+1}'$ dersek

$F_0' + F_1' + \cdots + F_{m-1}' = 1-(m-1)h$ 'dır.

İspat:

i. $\mu_a(F_i') = \mu_a(1-F_i) = 1-\mu_a(F_i) = 1-F_j = F_j'$. (7.11)

ii. $F_i' F_j' = (h+E_i)(h+E_j) = h^2 + h(E_i+E_j) + E_iE_j = h$. (7.12)

iii. $F_0' + F_1' + \cdots + F_{m-1}' = (h+E_0) + (h+E_1) + \cdots + (h+E_{m-1})$

$= m.h + E_0 + \cdots + E_{m-1} = 1-(m-1)h$ (7.13)

Tanım 7.9 $i \in \{0,1,...,m-1\}$ için $F_i' = 1-F_i = h+E_i$ olmak üzere F_i' idempotent elemanının ürettiği koda $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde p uzunluklu sınıf II teksel m-sel kalan kod denir.

7.3 $\mathbb{F}_q[v]/(v^2-v)$ Üzerinde Optimal m-sel Kalan Kod Örnekleri

Örnek 7.10 $\mathbb{F}_4[v]/(v^2-v)$ halkası üzerinde 17 uzunluklu 4-sel kalan kodların üreteç polinomlarını belirleyelim.

$\mathbb{F}_4$ cismi üzerinde 17 uzunluklu 4-sel kalan kodun sınıf I çiftsel kalan kodların idempotent üreteçleri; $l_0 = x + x^4 + x^{13} + x^{16}$, $l_1 = x^3 + x^5 + x^{12} + x^{14}$, $l_2 = x^2 + x^8 + x^9 + x^{15}$, $l_3 = x^6 + x^7 + x^{10} + x^{11}$ olmak üzere, $e_0 = l_0 + w.l_1 + l_2 + w^2.l_3$, $e_1 = w.l_0 + l_1 + w^2.l_2 + l_3$, $e_2 = l_0 + w^2.l_1 + l_2 + w.l_3$, $e_3 = w^2.l_0 + l_1 + w.l_2 + l_3$ şeklindedir. O halde $E_0 = v.e_0 + (1-v)e_2$ şeklinde alırsak, $E_1 = \mu_3(E_0) = v.e_3 + (1-v)e_1$, $E_2 = \mu_3(E_1) = v.e_2 + (1-v)e_0$, $E_3 = \mu_3(E_2) = v.e_1 + (1-v)e_3$ olur(ayrıca $E_0 = \mu_3(E_3)$ olduğu da görülür).

E_0 idempotent üretecine karşılık gelen üreteç polinom:

$$\begin{aligned}\text{ebob}(E_0, x^{17}-1) = \; & 1 + x + (v+w)x^2 + x^4 + (v+w)x^5 + (v+w^2)x^6 + (v+w^2)x^7 \\ & + (v+w)x^8 + x^9 + (v+w)x^{11} + x^{12} + x^{13}\end{aligned} \quad (7.14)$$

E_1 idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(E_1, x^{17}-1) = \begin{array}{c} 1+(v+w)x+(v+w)x^2+(v+w^2)x^3+x^4+(v+w)x^6 \\ +(v+w)x^7+x^9+(v+w^2)x^{10}+(v+w)x^{11}+(v+w)x^{12}+x^{13} \end{array} \quad (7.15)$$

E_2 idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(E_2, x^{17}-1) = \begin{array}{c} 1+x+(v+w^2)x^2+x^4+(v+w^2)x^5+(v+w)x^6+(v+w)x^7 \\ +(v+w^2)x^8+x^9+(v+w^2)x^{11}+x^{12}+x^{13} \end{array} \quad (7.16)$$

E_3 idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(E_3, x^{17}-1) = \begin{array}{c} 1+(v+w^2)x+(v+w^2)x^2+(v+w)x^3+x^4+(v+w^2)x^6 \\ +(v+w^2)x^7+x^9+(v+w)x^{10}+(v+w^2)x^{11}+(v+w^2)x^{12}+x^{13} \end{array} \quad (7.17)$$

Bu kodların parametreleri $[17,4,12]$'dir ve halkalar üzerinde Griesmer sınırına göre optimaldir.

E_0' idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(E_0', x^{17}-1) = 1+x+(v+w^2)x^2+x^3+x^4 \quad (7.18)$$

E_1' idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(E_1', x^{17}-1) = 1+(v+w)x+x^2+(v+w)x^3+x^4 \quad (7.19)$$

E_2' idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(E_2', x^{17}-1) = 1+x+(v+w)x^2+x^3+x^4 \quad (7.20)$$

E_3' idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(E_3', x^{17}-1) = 1+(v+w^2)x+x^2+(v+w^2)x^3+x^4 \quad (7.21)$$

Bu kodların parametreleri $[17,13,4]$'dir ve halkalar üzerinde Griesmer sınırına göre neredeyse optimaldir.

F_0 idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(F_0, x^{17}-1) = 1+(v+w)x^2+(v+w)x^3+x^5 \quad (7.22)$$

F_1 idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(F_1, x^{17}-1) = 1+(v+w^2)x+(v+w^2)x^2+(v+w^2)x^3+(v+w^2)x^4+x^5 \quad (7.23)$$

F_2 idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(F_2, x^{17}-1) = 1+(v+w^2)x^2+(v+w^2)x^3+x^5 \quad (7.24)$$

F_3 idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(F_3, x^{17}-1) = 1+(v+w)x+(v+w)x^2+(v+w)x^3+(v+w)x^4+x^5 \quad (7.25)$$

Bu kodların parametreleri $[17,12,4]$'dir ve halkalar üzerinde Griesmer sınırına göre optimale yakındır.

F_0' idempotent üretecine karşılık gelen üreteç polinom:

$$\text{ebob}(F_3, x^{17}-1) = 1+(v+w)x+(v+w)x^2+(v+w)x^3+(v+w)x^4+x^5 \quad (7.26)$$

$$\begin{aligned}\text{ebob}(F_0', x^{17}-1) = \; & 1+(v+w)x^2+(v+w)x^3+(v+w^2)x^4+x^5+(v+w)x^6 \\ & +x^7+(v+w^2)x^8+(v+w)x^9+(v+w)x^{10}+x^{12}\end{aligned}$$

F_1' idempotent üretecine karşılık gelen üreteç polinom:

$$\begin{aligned}\text{ebob}(F_1', x^{17}-1) = \; & 1+(v+w^2)x+x^2+(v+w)x^3+(v+w^2)x^4+(v+w^2)x^5+x^6 \\ & +(v+w^2)x^7+(v+w^2)x^8+(v+w)x^9+x^{10}+(v+w^2)x^{11}+x^{12}\end{aligned} \quad (7.27)$$

F_2' idempotent üretecine karşılık gelen üreteç polinom:

$$\begin{aligned}\text{ebob}(F_2', x^{17}-1) = \; & 1+(v+w^2)x^2+(v+w^2)x^3+(v+w)x^4+x^5+(v+w^2)x^6 \\ & +x^7+(v+w)x^8+(v+w^2)x^9+(v+w^2)x^{10}+x^{12}\end{aligned} \quad (7.28)$$

F_3' idempotent üretecine karşılık gelen üreteç polinom:

$$\begin{aligned}\text{ebob}(F_1', x^{17}-1) = \; & 1+(v+w)x+x^2+(v+w^2)x^3+(v+w)x^4+(v+w)x^5+x^6 \\ & +(v+w)x^7+(v+w)x^8+(v+w^2)x^9+x^{10}+(v+w)x^{11}+x^{12}\end{aligned} \quad (7.29)$$

Eğer n dereceli bir $p(x)$ polinomu için $p(x) = x^n p(x^{-1})$ ise $p(x)$ polinomuna ***palindromik polinom*** denir. Bu kod ailesinin üreteç polinomları ile palindromik polinomlar arasında bir ilişki kuracağız.

Şimdi $\mathbb{F}_q[v]/(v^2 - v)$ halkası üzerinde m-sel kalan kodların idempotent üreteçlerinin yapısını göreceğiz. Bu bize idempotent üreteç belirlemede yardımcı olacak.

7.4 m-sel Kalan Kodların Palindromik Üreteç Polinomları

Lemma 7.11

i. $(p-1)/m$ çift ve $i \in Q_j$ ise $-i \in Q_j$'dir.

ii. $\sum_{i \in Q_j} i = 0$.

İspat:

i. $(p-1)/m$ çift ise $(p-1)/(2m)$ bir tamsayıdır. $\mathbb{Z}_p^* = \langle b \rangle$ olsun, bu durumda

$b^{(p-1)/(2m)} \in \mathbb{Z}_p^*$ olur.

$\Rightarrow (b^{(p-1)/(2m)})^m = b^{(p-1)/2} = -1 \in Q_0$ (b üreteç olduğundan $b^{(p-1)/2} = -1$'dir)

Q_i'ler çarpımsal grup olduklarından her $i \in Q_0$ için $-i \in Q_0$'dır. Buradan her $i \in Q_j$ için $-i \in Q_j$ olduğu açıkça görülür.

ii. $\mathbb{Z}_p^* = \langle b \rangle$ ve $p - 1 = mt$ olsun. $\langle b^m \rangle = \{1, b^m, b^{2m}, \ldots b^{(t-1)m}\} = Q_0$ olur.

$\Rightarrow (1 + b^m + b^{2m} + \cdots b^{(t-1)m})(b^m - 1) = b^{tm} - 1 = 0$

$b^m - 1 \neq 0$ olduğundan $1 + b^m + b^{2m} + \cdots b^{(t-1)m} = 0$'dır. Böylece $\sum_{i \in Q_j} i = b^j \sum_{i \in Q_0} i = 0$

olduğu görülür.

Önerme 7.12 $k \geq 1 \in \mathbb{Z}$ olacak şekilde $q = 2^k$ ve $(p-1)/m$ çift ise $\mathbb{F}_q$ üzerinde p uzunluklu m-sel kalan kodların üreteç polinomları palindromiktir.

İspat: $f(x)$, $\mathbb{F}_q$ üzerinde p uzunluklu Q_0'a karşılık gelen m-sel kalan kodun üreteç polinomu olsun. Bu durumda $f(x)=\prod_{i\in Q_0}(x-\alpha^i)$ olur. Eğer $f'(x)=x^{\deg(f)}f(x^{-1})$ polinomu $f(x)$'e eşitse $f(x)$ polinomu palindromiktir.

$$f'(x)=x^{\deg(f)}f(x^{-1})$$

$$=x^{\deg(f)}\prod_{i\in Q_0}(x^{-1}-\alpha^i)=x^{\deg(f)}\prod_{i\in Q_0}(x^{-1}-\alpha^{-i}) \qquad \text{(Lemma 7.11-i'den)}$$

$$=x^{\deg(f)}\prod_{i\in Q_0}\left(\frac{\alpha^i-x}{x\alpha^i}\right)=\frac{x^{\deg(f)}}{x^{\deg(f)}}\prod_{i\in Q_0}\left(\frac{\alpha^i-x}{\alpha^i}\right) \qquad (7.30)$$

$$=\frac{1}{\alpha^{\sum_{i\in Q_0} i}}\prod_{i\in Q_0}(\alpha^i-x)=\frac{1}{\alpha^0}\prod_{i\in Q_0}(x-\alpha^i) \qquad \text{(Lemma 7.11-ii'den)}$$

$$=f(x)\ .$$

Önerme 7.13 p bir asal ve q 2'nin kuvveti olsun. $m\mid(p-1)$ olacak şekilde bir $m\in Z^+$ seçelim ve $a,q\in Q_0$ olsun. e_i ile e_j $\mathbb{F}_q$ üzerinde p uzunluklu m-sel kalan kodların idempotent üreteçleri ise $v.(\sum_{S\subseteq I, i\in S} e_i)+(1-v).(\sum_{P\subseteq I,\, j\in P} e_j)$'ler $\mathbb{F}_q[v]/(v^2-v)$ halkasında idempotentlerdir.

İspat: q 2'nin kuvveti olduğundan $\mathbb{F}_q[v]/(v^2-v)$ halkasının karakteristiği 2'dir. Dolayısıyla $I=\{0,1,\ldots m-1\}$ olmak üzere,

$$[v.(\sum_{S\subseteq I, i\in S} e_i)+(1-v).(\sum_{P\subseteq I,\, j\in P} e_j)]^2=(v.(\sum_{S\subseteq I, i\in S} e_i))^2+((1-v).(\sum_{P\subseteq I,\, j\in P} e_j))^2$$

$$=v.(\sum_{S\subseteq I, i\in S} e_i)^2+(1-\mathrm{v})(\sum_{P\subseteq I,\, j\in P} e_j)^2 \qquad (7.31)$$

$$=v.(\sum_{S\subseteq I, i\in S} e_i)+(1-\mathrm{v})(\sum_{P\subseteq I,\, j\in P} e_j)$$

olur.

Örnek 7.14 Bir önceki örnekte, $E_0 = v(e_0 + e_1) + (1-v)(e_1 + e_2)$ alırsak,

$E_1 = v(e_3 + e_0) + (1-v)(e_0 + e_1)$, $E_2 = v(e_2 + e_3) + (1-v)(e_3 + e_0)$ ve

$E_3 = v(e_1 + e_2) + (1-v)(e_2 + e_3)$ olur.

E_0 idempotent üretecine karşılık gelen üreteç polinom:

$$ebob(E_0, x^{17}-1) = \begin{array}{l} 1 + w^2x + (v+w)x^2 + (vw+w)x^3 + vwx^4 + vwx^5 \\ +(vw+w)x^6 + (v+w)x^7 + w^2x^8 + x^9 \end{array} \quad (7.32)$$

E_1 idempotent üretecine karşılık gelen üreteç polinom:

$$ebob(E_1, x^{17}-1) = \begin{array}{l} 1 + (v+w^2)x + w^2x^2 + vw^2x^3 + (vw+w)x^4 + (vw+w)x^5 \\ +vw^2x^6 + w^2x^7 + (v+w^2)x^8 + x^9 \end{array} \quad (7.33)$$

E_2 idempotent üretecine karşılık gelen üreteç polinom:

$$ebob(E_2, x^{17}-1) = \begin{array}{l} 1 + wx + (v+w^2)x^2 + (vw^2+w^2)x^3 + vw^2x^4 + vw^2x^5 \\ +(vw^2+w^2)x^6 + (v+w^2)x^7 + wx^8 + x^9 \end{array} \quad (7.34)$$

E_3 idempotent üretecine karşılık gelen üreteç polinom:

$$ebob(E_3, x^{17}-1) = \begin{array}{l} 1 + (v+w)x + wx^2 + vwx^3 + (vw^2+w^2)x^4 + (vw^2+w^2)x^5 \\ +vwx^6 + wx^7 + (v+w)x^8 + x^9 \end{array} \quad (7.35)$$

Bu kodların parametreleri $[17,8,8]$'dir ve halkalar üzerinde Griesmer sınırına göre neredeyse optimaldir.

Teorem 7.15 $k \geq 1 \in \mathbb{Z}$ olmak üzere $(p-1)/m$ çift ise $\mathbb{F}_{2^k}[v]/(v^2-v)$ halkası üzerinde p uzunluklu m-sel kalan kodların üreteç polinomları palindromiktir.

İspat: $\mathbb{F}_{2^k}[v]/(v^2-v)$ halkası üzerinde p uzunluklu bir m-sel kalan kodun üreteç polinomu $v.(\sum_{S\subseteq I, i\in S} e_i) + (1-v).(\sum_{P\subseteq I, j\in P} e_j)$, $(p-1)/m$ ve $k \geq 1 \in \mathbb{Z}$ olsun. f_i ve f_j, $\mathbb{F}_{2^k}$ üzerinde sırasıyla $\sum_{S\subseteq I, i\in S} e_i$ ve $\sum_{P\subseteq I, j\in P} e_j$ idempotent üreteçlerin ürettikleri p uzunluklu m-sel kalan kodlara karşılık gelen üreteç polinomlar olsun. İspatın bundan sonraki kısmında $\sum_{S\subseteq I, i\in S} e_i$ ve $\sum_{P\subseteq I, j\in P} e_j$'yi sırasıyla $\sum e_i$ ve $\sum e_j$ ile göstereceğiz.

Bu durumda $\text{ebob}(\sum e_i, x^n-1) = f_i$ ve $\text{ebob}(\sum e_j, x^n-1) = f_j$ olur ve

$a\sum e_i + b(x^n-1) = 1$ ve $c\sum e_j + d(x^n-1) = 1$ olacak şekilde $a,b,c,d \in \mathbb{F}_{2^k}[x]$ vardır.

f de $\mathbb{F}_{2^k}[v]/(v^2-v)$ halkası üzerinde $v.(\sum_{S\subseteq I, i\in S} e_i) + (1-v).(\sum_{P\subseteq I, j\in P} e_j)$ idempotent

üretecin ürettiği p uzunluklu m-sel kalan kodun üreteç polinomu olsun. Bu durumda

$ebob(v.(\sum_{S\subseteq I, i\in S} e_i) + (1-v).(\sum_{P\subseteq I, j\in P} e_j), x^n-1) = f$ olur. Bizim iddiamız $f = vf_i + (1-v)f_j$

olduğu.

$$(va+(1-v)c)(v\sum e_i + (1-v)\sum e_j) + (vb+(1-v)d)(x^n-1) = (va\sum e_i + (1-v)c\sum e_j) + (vb+(1-v)d(x^n-1))$$

$$= v(a\sum e_i + b(x^n-1)) + (1-v)(c\sum e_j + d(x^n-1)) \qquad (7.36)$$

$$= vf_i + (1-v)f_j \ .$$

$\text{ebob}(v.(\sum_{S\subseteq I, i\in S} e_i) + (1-v).(\sum_{P\subseteq I, j\in P} e_j), x^n-1) = f$ olduğundan ve $vf_i + (1-v)f_j$'in

$v.(\sum_{S\subseteq I, i\in S} e_i) + (1-v).(\sum_{P\subseteq I, j\in P} e_j)$ ile x^n-1'in lineer kombinasyonu olduğundan f

$vf_i + (1-v)f_j$'yi böler.

Diğer taraftan, $f_i \mid \sum e_i$ ve $f_j \mid \sum e_j$ olduğundan $tf_i = \sum e_i$ ve $sf_j = \sum e_j$ olacak

şekilde $t,s \in \mathbb{F}_{2^k}[x]$ vardır.

$$(tv+s(1-v))(vf_i + (1-v)f_j) = vtf_i + (1-v)sf_j = v\sum e_i + (1-v)\sum e_j \qquad (7.37)$$

O halde

$$(vf_i + (1-v)f_k) \mid (v\sum e_i + (1-v)e_j) \ . \qquad (7.38)$$

Buna ek olarak $f_i \mid (x^n-1)$ ve $f_j \mid (x^n-1)$ olduğundan $kf_i = x^n-1$ ve $mf_j = x^n-1$

olacak şekilde $k,m \in \mathbb{F}_{2^k}[x]$ vardır.

$$(kv+m(1-v))(vf_i + (1-v)f_j) = x^n-1 \qquad (7.39)$$

Böylece

$$(vf_i + (1-v) f_k) \mid (x^n - 1) \tag{7.40}$$

diyebiliriz. (7.38) ve (7.40)'tan $(vf_i + (1-v) f_k) \mid f$ olduğu görülür, yani

$$\text{ebob}(v.(\sum_{S \subseteq I, i \in S} e_i) + (1-v).(\sum_{P \subseteq I,\, j \in P} e_j), x^n - 1) = (vf_i + (1-v) f_j).$$

f_i ve f_j palindromik olduğundan $vf_i + (1-v) f_j$ polinomu da palindromiktir.

Burada bulacağımız palindromik üreteç polinomlar DNA kod inşa ederken karşımıza çıkan ters sıralılık problemini çözmede ve kod inşasında oldukça kolaylık sağlayacaktır.

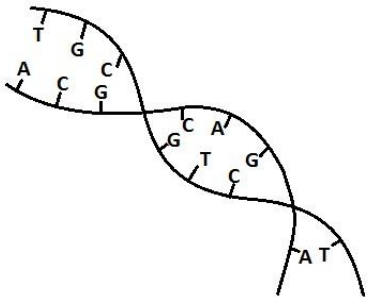
BÖLÜM 8

$\mathbb{F}_{4^{2k}}[v]/(v^2-v)$ HALKASI ÜZERİNDE TERS SIRALI DNA KODLAR

Bu bölümde $R_{2k}=\mathbb{F}_{4^{2k}}/(v^2-v)$ üzerinde ters sıralı DNA kodlar için m-sel kalan kodların üreteç polinomlarını ve palindromik çarpanları kullanarak genel bir teorem vereceğiz.

8.1 DNA İle İlgili Temel Bilgiler

DNA (Deoksiribo Nükleik Asit), tüm organizmaların genetik bilgilerini ve biyolojik hareketliliği için gerekli olan talimatları taşıyan bir nükleik asittir. DNA'nın kimyasal yapısı iki polimer ipliği ve nükleotid denilen Adenine (A), Thymine (T), Guanine (G) ve Cytosine (C) isimli 4 molekülden oluşur. Sarmal şeklinde uzanan iki polimer ipliğine karşılıklı olarak 2'şerli halde tutunarak dizilen nükleotidler WCC modellemesine göre dizilirler. Bu modellemede Adenine'in tamlayanı Thymine, Guanine'in tamlayanı Cytosine'dir [18]. Bu modellemeye göre bir DNA parçacığı örneği Şekil 8.1'de gösterilmiştir.



Şekil 8.1 DNA yapısı ve dizilim örneği

Polimerler boyunca uzanan nükleotid dizilimi genetik bilgiyi kodlamaktadır. Bu bölümde kullanılacak DNA k-bazlısı k tane nükleotidin sıralı haline denir [18]. DNA k-bazlılarının tamlayanı, her bir nükleotidin tamlayanının dizilimine denir [18]. DNA k-bazlılarının ters sıralısı nükleotidlerin tersten sıralanmış haline denir [18]. Örneğin $ATCTGCTC$ DNA 8-bazlısının tamlayanı $TAGACGAG$, ters sıralısı $CTCGTCTA$ ve ters sıralısının tamlayanı $GAGCAGAT$'dir.

8.2 Ters Sıralama Problemi

DNA kodlarda DNA bazlarının dizilimleri ile cebirsel kodlardaki kodsözlerin arasındaki bağlantıda gerekli olan, ters sıralama ilişkisinin kurulmasıdır. Ters sıralama problemini açıklamak için küçük bir örnek verelim. $a_1 \to ATGG$, $a_2 \to CTGA$, $a_3 \to TGAG$ ve $a_1, a_2, a_3 \in R_4$ olmak üzere (a_1, a_2, a_3), $ATGGCTGATGAG$'ye karşılık gelen kodsöz olsun. (a_1, a_2, a_3)'ün ters sıralısı (a_3, a_2, a_1)'dir ve (a_3, a_2, a_1)'e karşılık $TGAGCTGAATGG$ gelir. Fakat $TGAGCTGAATGG$, $ATGGCTGATGAG$'nin ters sıralısı değildir, $ATGGCTGATGAG$'nin ters sıralısı $GAGTAGTCGGTA$'dır. Burada a_i'leri ters sıraladığımız zaman buna karşılık gelen DNA kodsözünün de ilk baştaki kodsözün ters sıralısı olmasını istiyoruz.

$\mathbb{F}_4[v]/(v^2 - v)$ üzerinde, lineer kodlardan DNA kodlara geçişi sağlayan ψ-küme çalışılmıştı [32]. Burada çalışılan halkadan daha genel olarak $\mathbb{F}_{4^{2k}}[v]/(v^2 - v)$ halkası üzerinde DNA kodlar için ters sıralama problemini, bir otomorfizma ile ψ-küme'nin genel bir formu çalışılacaktır. Ayrıca daha önceki DNA kod çalışmalarındaki palindromik üreteç polinom üretme işlemini m-sel kalan kodlar vasıtasıyla çok daha pratik hale getirilecektir.

8.3 $\mathbb{F}_{4^{2k}}[v]/(v^2 - v)$ Halkasının Yapısı ve DNA Kodlar

Şimdi üzerinde çalıştığımız halkanın yapısını inceleyelim. $v^2 = v$ olmak üzere R zincir olmayan değişmeli bir halka olsun. Çin Kalan Teoreminden faydalanarak R'yi

Çizelge 8.1 $\mathbb{F}_{16}$'nın elemanarı ile DNA 2-bazlılarının eşleştirmesi [18]

$\mathbb{F}_{16}$ (çarpımsal)	$\mathbb{F}_{16}$(toplamsal)	DNA çiftleri
0	0	AA
α^0	1	TT
α^1	α^1	AT
α^2	α^2	GC
α^3	α^3	AG
α^4	$1+\alpha$	TA
α^5	$\alpha+\alpha^2$	CC
α^6	$\alpha^2+\alpha^3$	AC
α^7	$1+\alpha+\alpha^3$	GT
α^8	$1+\alpha^2$	CG
α^9	$\alpha+\alpha^3$	CA
α^{10}	$1+\alpha+\alpha^2$	GG
α^{11}	$\alpha+\alpha^2+\alpha^3$	CT
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	GA
α^{13}	$1+\alpha^2+\alpha^3$	TG
α^{14}	$1+\alpha^3$	TC

$R=v\mathbb{F}_{4^{2k}}\oplus(1-v)\mathbb{F}_{4^{2k}}$ şeklinde ayrıştırabiliriz. Şimdi bir Gray dönüşüm tanımlayalım;

$$\begin{array}{rcl}\phi: R & \rightarrow & \mathbb{F}_{4^{2k}}^2 \\ a+vb & \rightarrow & (a+b,a)\end{array} \qquad (8.1)$$

θ Öztaş vd. tanımlandığı gibi [18], $2k$ uzunluğundaki DNA kodsözlerini $\mathbb{F}_{4^{2k}}$'nın elemanlarına dönüştürmek için kullanılır. Çizelge 1'de $\mathbb{F}_{16}$'nın elemanları ile 2'li DNA kodsözlerinin eşleşmesi gösteriliyor. θ_1, $\theta_1(a+vb)=(\theta(a+b),\theta(a))$ şeklinde $4k$ uzunluğundaki DNA bazlarını R_{2k}'nın elemanlarına dönüştürür. Ayrıca Θ da, $c=(c_0,c_1,\ldots,c_{n-1})$ kodsöz olmak üzere $\Theta(c)=(\theta_1(c_0),\theta_1(c_1),\ldots,\theta_1(c_{n-1}))$ şeklinde, kodsözleri DNA bazlarına dönüştürür.

Şimdi küçük bir örnekle R_2'nin herhangi bir elemanına ϕ, θ ve θ_1 dönüşümlerinin nasıl etki ettiğini görelim.

Örnek 8.1 $\beta=\alpha^3+\alpha^6v\in R_2$ ve $\phi(\beta)=(\alpha^2,\alpha^3)$ olsun. Bu durumda $\theta_1(\beta)=(\theta(\alpha^2),\theta(\alpha^3))=GCAG$ olur.

Benzer şekilde Θ'nın kodsözler üzerindeki etkisini bir örnekle görelim.

Örnek 8.2 $c=(\alpha^3+\alpha^6v,\alpha^3+\alpha^9v)$ bir kodun bir kodsözü olsun. $\phi(\alpha^3+\alpha^6v)=(\alpha^2,\alpha^3)$, $\phi(\alpha^3+\alpha^9v)=(\alpha,\alpha^3)$ olur ve

$\Theta(c)=(\theta_1(\alpha^3+\alpha^6v),\theta_1(\alpha^3+\alpha^9v))=(\theta(\alpha^2),\theta(\alpha^3),\theta(\alpha),\theta(\alpha^3))=GCAGATAG$

şeklinde DNA kodsözüne dönüştürür.

R'nin herhangi bir elemanının DNA ters sıralısını elde etmek için R üzerinde yeni bir otomorfizma tanımlayacağız;

$$\begin{aligned}\psi: R_{2k} &\rightarrow R_{2k}\\ a+vb &\rightarrow \alpha^{4^k}+(1+v)b^{4^k}\\ &= (a+b)^{4^k}+vb^{4^k}\end{aligned} \qquad (8.2)$$

Tanımladığımız bu dönüşümün R_2'nin herhangi bir elemanına nasıl etki ettiğini bir örnekle görelim.

Örnek 8.3 $\beta=\alpha^3+\alpha^6v\in R_2$ ve $\theta_1(\beta)=GCAG$ olsun.

$\psi(\beta)=\alpha^{12}+\alpha^9(v-1)=\alpha^8+v\alpha^9$ ve $\theta_1(\psi(\beta))=\theta_1(\alpha^8+v\alpha^9)=(\theta(\alpha^{12}),\theta(\alpha^8))=GACG$

olur. Böylece R_2'nin bir elemanının ters sıralısını elde etmiş oluruz.

Tanım 8.4 $g(x)$, R üzerinde t dereceli bir polinom olsun.

$$\Lambda_i = \begin{cases} x^i g(x) & , \ i \text{ çiftse} \\ x^i \psi(g(x)) & , \ i \text{ tekse} \end{cases} \tag{8.3}$$

olmak üzere,

$$\Lambda_g = \{\Lambda_0, \Lambda_1, \ldots, \Lambda_{t-1}\} \tag{8.4}$$

olsun. R üzerinde Λ_g ile üretilen C kodu bir lineer koddur. Buradaki Λ_g'ye ψ ***-küme*** denir.

Şimdi $\mathbb{F}_{4^{2k}} / (v^2 - v)$ halkası üzerindeki palindromik üreteçlerle DNA kod üretilebilmesini sağlayacak teorem verilecek.

Teorem 8.5 $f(x)$, $\mathbb{F}_{4^{2k}} / (v^2 - v)$ halkası üzerinde $n - \deg(f)$ bir çift pozitif tamsayı olacak şekilde $x^n - 1$'in palindromik bir çarpanı olsun. ψ-küme bir lineer C kodu üretirse $\Theta(C)$ bir ters sıralı DNA koddur.

İspat Bir sonraki teoremin ispatı ile benzer.

Sıradaki teoremde $\mathbb{F}_{4^{2k}} / (v^2 - v)$ halkası üzerindeki palindromik üreteçlerle nasıl DNA kod üretebileceğimizi göreceğiz. Bu teoreme m-sel kalan kodların idempotent üreteçlerinin özellikleri sayesinde ulaşabildik.

Teorem 8.6 $g(x)$, $\mathbb{F}_{4^{2k}} / (v^2 - v)$ üzerinde bir m-sel kalan kodun bir üreteç polinomu ve $\deg(g(x))$ bir çift pozitif tamsayı olsun. ψ-küme bir lineer C kodu üretirse $\Theta(C)$ bir ters sıralı DNA koddur.

İspat $g(x)$, $\mathbb{F}_{4^{2k}} / (v^2 - v)$ üzerinde bir m-sel kalan kodun bir üreteç polinomu ise Teorem 7.15'ten bu polinomun palindromik olduğunu biliyoruz. Λ_g, $g(x)$'in ψ-kümesi olsun. $c \in C$ olmak üzere her $\psi(c)$ DNA kodsözünün ters sıralısı aşağıdaki eşitlik ile elde edilir:

$$\Theta\left(\sum_{i=0}^{k-1} \beta_i \Lambda_i\right)^r = \Theta\left(\sum_{i=0}^{k-1} \psi(\beta_i) \Lambda_{k-1-i}\right) \tag{8.5}$$

Burada $k = n - \deg(g(x))$ ve $\beta_i \in R_{2k}$'dır, ayrıca polinomları kodsöz olarak düşündüğümüzü de belirtmek gerekir. $\sum_i \psi(\beta_i)\Lambda_{k-1-i} \in C$ olduğundan $\Theta(C)$ bir ters sıralı DNA koddur.

Örnek 8.7

$g(x) = x^{13} + x^{12} + (v + (\alpha^2 + \alpha))x^{11} + x^9 + (v + (\alpha^2 + \alpha))x^8 + (v + (\alpha^2 + \alpha + 1))x^7 +$
$(v + (\alpha^2 + \alpha + 1))x^6 + (v + (\alpha^2 + \alpha))x^5 + x^4 + (v + (\alpha^2 + \alpha))x^2 + x + 1$, $\mathbb{F}_{16} / (v^2 - v)$ üzerinde 17 uzunluklu bir m-sel kalan kodun üreteç polinomu olsun. $g(x)$'in ψ-kümesi aşağıdaki gibidir:

$$\begin{aligned}\{\Lambda_0, \Lambda_1, \Lambda_2, \Lambda_3\} = \quad & \Big\{\Big\{1,1,v+\alpha^2+\alpha,0,1,v+\alpha^2+\alpha,v+\alpha^2+\alpha+1,v+\alpha^2+\alpha+1,\\ & v+\alpha^2+\alpha,1,0,v+\alpha^2+\alpha,\ 1,\ 1,\ 0,\ 0,\ 0\Big\},\\ & \Big\{0,1,1,v+\alpha^2+\alpha+1,0,1,v+\alpha^2+\alpha+1,v+\alpha^2+\alpha,\\ & v+\alpha^2+\alpha,v+\alpha^2+\alpha+1,1,0,v+\alpha^2+\alpha+1,1,1,0,0\Big\},\\ & \Big\{0,0,1,1,v+\alpha^2+\alpha,0,1,v+\alpha^2+\alpha,v+\alpha^2+\alpha+1,\\ & v+\alpha^2+\alpha+1,v+\alpha^2+\alpha,1,0,v+\alpha^2+\alpha,1,1,0\Big\},\\ & \Big\{0,0,0,1,1,v+\alpha^2+\alpha+1,0,1,v+\alpha^2+\alpha+1,v+\alpha^2+\alpha,\\ & v+\alpha^2+\alpha,v+\alpha^2+\alpha+1,1,0,v+\alpha^2+\alpha+1,1,1\Big\}\Big\}.\end{aligned} \tag{8.6}$$

C'nin parametreleri $[17,4,10]$ şeklindedir. Herhangi bir kodsöz seçelim, bu kodsözün DNA karşılığına ve ters sıralı DNA karşılığına bakalım.

$\alpha v + \alpha^3 + \alpha^2 + 0 = \alpha^6 + \alpha v \to (\alpha^{11}, \alpha^6) \to CTAC$,

$\alpha + \alpha v + \alpha^3 + \alpha^2 \to (\alpha^6, \alpha^{11}) \to ACCT$ ve $\alpha \to (\alpha, \alpha) \to TTTT$ olmak üzere,

$c_1 = \alpha\Lambda_0 = \{\alpha, \alpha, \alpha v + \alpha^3 + \alpha^2, 0, \alpha, \alpha v + \alpha^3 + \alpha^2, \alpha v + \alpha^3 + \alpha^2 + \alpha, \alpha v + \alpha^3 + \alpha^2 + \alpha,$
$\alpha v + \alpha^3 + \alpha^2, \alpha, 0, \alpha + \alpha^2 + \alpha^3, \alpha, \alpha, 0, 0, 0\}$ bir kodsöz olsun. Bu durumda c_1'in DNA karşılığı,

$\Theta(c_1) = \{ATAT\ ATAT\ CTAC\ AAAA\ ATAT\ CTAC\ ACCT\ ACCT\ CTAC\ ATAT\ AAAA$
$CTAC\ ATAT\ AAAA\ AAAA\ AAAA\}$ olur. Diğer taraftan c_1'in ters sıralı DNA karşılığı $\Theta(c_1)^r$ (3) eşitliğinden

$$\Theta(c_1)^r = \Theta(\psi(\alpha)\Lambda_3)$$

$$= \Theta(\alpha^4\Lambda_3)$$

$$= \Theta(\alpha^4 \times \{0,0,0,1,1,v+\alpha^2+\alpha,0,1,v+\alpha^2+\alpha,v+\alpha^2+\alpha+1,v+\alpha^2+\alpha+1,v+\alpha^2+\alpha,$$

$$1,0,v+\alpha^2+\alpha+1,1,1\}) \qquad (8.7)$$

$$= \Theta(0,0,0,\alpha^4,\alpha^4,\alpha^{14}+v\alpha^4,0,\alpha^4,\alpha^{14}+v\alpha^4,\alpha^9+v\alpha^4,\alpha^9+v\alpha^4,\alpha^{14}+v\alpha^4,\alpha^4,0,$$

$$\alpha^{14}+v\alpha^4,\alpha^4,\alpha^4)$$

$$= \{AAAA\ AAAA\ AAAA\ TATA\ TATA\ CATC\ AAAA\ TATA\ CATC\ TCCA\ TCCA$$

$$CATC\ TATA\ AAA\ CATC\ TATA\ TATA\}$$

olur.

BÖLÜM 9

SONUÇ VE ÖNERİLER

Bu çalışmada q. kuvvet kalan kodlar $\mathbb{F}_q[v]/(v^3-v)$ halkası üzerinde idempotent üreteçler vasıtasıyla tanımlandı ve optimale yakın kodlar verildi. m-sel kalan kodlar $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde tanımlandı, üreteç polinomların palindromik olması için gerekli koşullar verildi ve optimal kod örnekleri verildi. $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde m-sel kalan kodların palindromik üreteç polinomlarını kullanarak $\mathbb{F}_{4^{2k}}[v]/(v^2-v)$ halkası üzerinde DNA kodlar önceki yöntemlerden daha pratik bir şekilde tanımlandı.

Çeşitli koset yapıları üzerinden m-sel kalan kodların daha genel hali elde edilebilir ve bu elde edilen kod türü çeşitli cebirsel yapılar üzerinde çalışılabilir. $\mathbb{F}_q[v]/(v^2-v)$ halkası üzerinde tanımladığımız m-sel kalan kodların örnekleri incelenirse yeni ve optimal kod parametreleri elde edilebilir. Buna ek olarak oluşturduğumuz DNA kodlar için örnekler oluşturulup çeşitli canlıların DNA'ları ile kıyaslanabilir. Böylece elde edilen DNA kodlarla benzerlik bulunan canlıların DNA'ları üzerinde oluşan hasarlar bu kodlar sayesinde belirlenip düzeltilebilir.

KAYNAKLAR

[1] Mattson, H. F. ve E. F. Assumus Jr., (1964). "Research Program To Extend The Theory Of Weight Distribution And Related Problems For Cyclic Error-Correcting Codes", Sylvania Electric Products Inc Waltham Mass.

[2] Pless, V. S. ve Qian, Z., (1996). "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$", IEEE Transactions on Information Theory, 42(5): 1594-1600.

[3] Kaya, A., Yildiz, B. ve Siap, I., (2014). "New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$", Finite Fields and Their Applications, 29: 160-177.

[4] Kaya, A., Yildiz, B. ve Siap, I., (2014). "Quadratic residue codes over $\mathbb{F}_p+v\mathbb{F}_p$ and their Gray images", Journal of Pure and Applied Algebra, 218(11): 1999-2011.

[5] Taeri, B., (2009). "Quadratic residue codes over $\mathbb{Z}_9$", J. Korean Math Soc, 46: 13-30.

[6] Brualdi, R. A. ve Pless, V. S., (1989). "Polyadic codes", Discrete Applied Mathematics, 25(1-2): 3-17.

[7] Dong, X., Li, W. ve Zhang, Y., (2013). "Generating idempotents of cubic and quartic residue codes over field $\mathbb{F}_2$ ". Jisuanji Gongcheng yu Yingyong(Computer Engineering and Applications), 49(11): 41-44.

[8] van Lint, J. ve MacWilliams, F., (1978). "Generalized quadratic residue codes", IEEE Transactions on Information Theory, 24(6): 730-737.

[9] van Zanten, A. J., Bojilov, A. ve Dodunekov, S. M., (2015). "Generalized residue and t-residue codes and their idempotent generators", Designs, Codes and Cryptography, 75(2): 315-334.

[10] Job, V. R., (1992). "m-adic residue codes", IEEE Transactions on Information Theory, 38(2): 496-501.

[11] Adleman, L. M., (1994). "Molecular computation of solutions to combinatorial problems", Science, 266(5187): 1021-1024.

[12] Gaborit, P. ve King, O. D., (2005). "Linear constructions for DNA codes", Theoretical Computer Science, 334(1-3): 99-113.

[13] Aboluion, N., Smith, D. H. ve Perkins, S., (2012). "Linear and nonlinear constructions of DNA codes with Hamming distance d, constant GC-content and a reverse-complement constraint", Discrete Mathematics, 312(5): 1062-1075.

[14] Faria, L. C. B., Rocha, A. S. L., Kleinschmidt, J. H., Palazzo, R. ve Silva-Filho, M. C., (2010). "DNA sequences generated by BCH codes over $GF(4)$", Electronics letters, 46(3): 203-204.

[15] Rocha, A. S. L., Faria, L. C. B., Kleinschmidt, J. H., Palazzo, R. ve Silva-Filho, M. C., (2010). "DNA sequences generated by $\mathbb{Z}_4$-linear codes", In Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on (pp. 1320-1324). IEEE.

[16] Feng, B., Bai, S., Chen, B. ve Zhou, X., (2015). "The constructions of DNA codes from linear self-dual codes over $\mathbb{Z}_4$", In International Conference on Computer Information Systems and Industrial Applications.

[17] Varbanov, Z., Todorov, T. ve Hristova, M., (2014). "A method for constructing DNA codes from additive self-dual codes over $GF(4)$", In Proc. CAIM conference, Romania (Vol. 40).

[18] Oztas, E. S. ve Siap, I., (2013). "Lifted Polynomials over $\mathbb{F}_{16}$ and Their Applications to DNA Codes", Filomat, 27(3): 459-466.

[19] Yildiz, B. ve Siap, I., (2012). "Cyclic codes over $\mathbb{F}_2[u]/(u^4-1)$ and applications to DNA codes", Computers and Mathematics with Applications, 63(7): 1169-1176.

[20] Liang, J. ve Wang, L., (2016). "On cyclic DNA codes over $\mathbb{F}_2+u\mathbb{F}_2$", Journal of Applied Mathematics and Computing, 51(1-2): 81-91.

[21] Pattanayak, S. ve Singh, A. K., (2015). "On cyclic DNA codes over the Ring $\mathbb{Z}_4+u\mathbb{Z}_4$", arXiv preprint arXiv:1508.02015.

[22] Ma, F., Cao, Y. and Gao, J., (2015). "On cyclic DNA codes over $\mathbb{F}_4[u]/(u^2+1)$", International Journal of Research and Reviews in Applied Sciences, vol. 24, no. 3, p. 101.

[23] Bennenni, N., Guenda, K. ve Mesnager, S., (2015). "New DNA cyclic codes over rings", arXiv preprint arXiv:1505.06263.

[24] Lidl, R. ve Niederreiter, H. (1997). Finite fields (Vol. 20). Cambridge University Press.

[25] Ling, S. ve Xing, C. (2004). Coding theory: a first course. Cambridge University Press.

[26] MacWilliams, F. J. ve Sloane, N. J. A. (1977). The theory of error-correcting codes. Elsevier.

[27] Morelos-Zaragoza, R. H. (2006). The art of error correcting coding. John Wiley and Sons.

[28] Shiromoto, K. ve Storme, L., (2003). “A Griesmer bound for linear codes over finite quasi-Frobenius rings”, Discrete applied mathematics, 128(1): 263-274.

[29] Huffman, W. C. ve Pless, V., (2010). “Fundamentals of error-correcting codes”, Cambridge University Press.

[30] Berlekamp, E. R., (1968). Algebraic Coding Theory. Series in Systems Science, New York-Toronto: McGraw Hill.

[31] Charters, P., (2009). “Generalizing binary quadratic residue codes to higher power residues over larger fields”, Finite Fields and Their Applications, 15(3): 404-413.

[32] Bayram, A., Oztas, E. S. ve Siap, I., (2016). “Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications”, Designs, Codes and Cryptography, 80(2): 379-393.

[33] Abualrub, T., Ghrayeb, A. ve Zeng, X. N., (2006). “Construction of cyclic codes over $GF(4)$ for DNA computing”, Journal of the Franklin Institute, 343(4-5): 448-457.

[34] Oztas, E. S. ve Siap, I., (2015). “On a generalization of lifted polynomials over finite fields and their applications to DNA codes”, International Journal of Computer Mathematics, 92(9): 1976-1988.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı :Ferhat KÜRÜZ

Doğum Tarihi ve Yeri :02.12.1988-Üsküdar

Yabancı Dili :İngilizce

E-posta :ferhatkuruz@gmail.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Y. Lisans	Matematik	Yıldız Teknik Üniversitesi	2012
Lisans	Matematik	Yıldız Teknik Üniversitesi	2010
Lise	Fen-Matematik	Ataşehir Habire Yahşi Lisesi	2005

İŞ TECRÜBESİ

Yıl	**Kurum**	**Görevi**
2013-	Yıldız Teknik Üniversitesi	Araştırma Görevlisi
2012-2013	Siirt Üniversitesi	Araştırma Görevlisi

YAYINLARI

Makale

1. Kürüz Ferhat, Öztaş Elif Segah, Şiap İrfan (2018). m-adic Residue Codes over $\mathbb{F}_q[v]/(v^2-v)$ and DNA Codes. Bulletin of the Korean Mathematical Society, Doi: 10.4134/BKMS.b170386

Bildiri

1. Kürüz Ferhat, Öztaş Elif Segah, Şiap İrfan (2016). m-adic Residue Codes over $\mathbb{F}_q[v]/(v^2-v)$ and DNA Codes. International Conference on Computational and Mathematical Methods in Science and Engineering 2016 (CMMSE 2016) (Tam metin bildiri)

2. Kürüz Ferhat, Şiap İrfan (2015). q^{th} Power Residue Codes over a Non-Chain Ring. The Second International Conference on Mathematics and Statistics (AUS-ICMS'15) (Özet Bildiri)

ÖDÜLLERİ

1. 2011 Milli Eğitim Bakanlığı YLSY Bursu.