T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU VE DEĞİŞMELİ HALKALARDA LİNEER KODLAR

AYŞEGÜL BAYRAM ELELE

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
DOÇ. DR. FATİH DEMİRKALE

İSTANBUL, 2017

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SONLU VE DEĞİŞMELİ HALKALARDA LİNEER KODLAR

Ayşegül BAYRAM ELELE tarafından hazırlanan tez çalışması 09.06.2017 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Doç. Dr. Fatih DEMİRKALE

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Doç. Dr. Fatih DEMİRKALE

Yıldız Teknik Üniversitesi _____

Prof. Dr. Ünsal TEKİR

Marmara Üniversitesi _____

Prof. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi _____

Doç. Dr. Emre KOLOTOĞLU

Yıldız Teknik Üniversitesi _____

Doç. Dr. Esra Sevim ŞENGELEN

İstanbul Bilgi Üniversitesi _____

Bu çalışma, 2013-2016 yılları arasında 2211 kodlu TÜBİTAK Yurt İçi Doktora Bursu ve 2015-2017 yılları arasında Yıldız Teknik Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü'nün 2015-01-DOP01 numaralı projeleri ile desteklenmiştir.

ÖNSÖZ

Lisansüstü eğitim hayatım boyunca bilgisinden ve tecrübesinden istifade ettiğim tüm değerli hocalarıma ve bu çalışmanın tamamlanması için varlığı ile beni destekleyen hocam Doç. Dr. Fatih DEMİRKALE'ye sonsuz teşekkür ederim.

Paylaşılarak çoğalınacağına ve öğrettikçe öğrenileceğini tecrübe etmeme vesile olan değerli çalışma arkadaşlarıma ve ayrıca tez jürimde olmayı kabul eden çok değerli hocalarım sayın Prof. Dr. Ünsal Tekir'e, sayın Prof. Dr. Bayram Ali ERSOY'a teşekkür eder, saygılarımı sunarım.

Ayrıca, öğrenim hayatım boyunca maddi ve manevi desteklerini benden esirgemeyen ve hep yanımda hissettiğim sevgili eşime, anne ve babama ve çok değerli kardeşlerime sonsuz teşekkür ederim.

Son olarak tez süresince maddi destek sağlayan Yıldız Teknik Üniversitesi BAP Birimi'ne ve TÜBİTAK-Bilim İnsanı Destekleme Daire Başkanlığı'na teşekkür ederim.

Haziran, 2017

Ayşegül BAYRAM ELELE

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

$+,*$	İkili işlemler
I	İdeal
μ	Halka homomorfizması
F_q	q elemanlı sonlu cisim
$GF(q)$	q elemanlı sonlu cisim
F_q^*	$q-1$ elemanlı devirli grup
γ	F_q^* sonlu cisminin ilkel elemanı
φ	Euler fonksiyonu
C	Lineer kod
$C^{\perp}$	C lineer kodunun duali
$boy(C)$	C lineer kodunun boyutu
$\langle .,. \rangle$	Öklid iç çarpımı
(n,k,d)	Uzunluğu n, boyutu k, uzaklığı d olan bir kod
$[n,k,d]$	Uzunluğu n, boyutu k, uzaklığı d olan bir lineer kod
$d_{\min}(C)$	C kodunun minimum Hamming uzaklığı
$B_q(n,d)$	F_q cismi üzerinde n uzunluğuna ve d uzaklığına sahip kodunun maksimum eleman sayısı
π	Devirli kodu polinoma resmeden dönüşüm
$\lvert\langle\mu\rangle\rvert$	μ otomorfizmasının mertebesi
$\langle S \rangle$	S kümesi ile üretilen uzay
$F[x;\mu]$	F cisim katsayılı μ otomorfizması ile belirli çarpık polinom halkası
σ	Devirli öteleme
σ_1	Sabit devirli öteleme
σ_2	Çarpık sabit devirli öteleme
$\phi_1, \phi_2, \Phi, \phi$	Gray dönüşüm
$\langle u,v \rangle$	u ve v elemanlarının ürettiği eleman
$w_H(x)$	x elemanının Hamming ağırlığı
$w_L(x)$	x elemanının Lee ağırlığı

$d_H(x,y)$ x ve y elemanlarının Hamming uzaklığı

$supp(x)$ x elemanın destek kümesi

$\langle \alpha \rangle$ α elemanın ürettiği temel ideal

$|C|$ C lineer kodunun eleman sayısı

$[\![n,k]\!]$ Uzunluğu n, boyutu k olan quantum kod

$[\![n,k,d]\!]_q$ F_q cisminde tanımlı uzunluğu n, boyutu k, uzaklığı d olan quantum kod

$|\ \rangle$ Ket vektörü

$C = \langle g(x) \rangle$ $g(x)$ polinomu ile üretilen C devirli kodu

$A \oplus B$ A ve B kümelerinin iç direkt toplamı

$p^*(x)$ $p(x)$ polinomunun ters sıralısı

u^r u vektörünün ters sıralısı

u^c u vektörünün tamamlayıcısı

u^{rc} u vektörünün ters sıralı tamamlayıcısı

Υ DNA bazları ile eşleme dönüşümü

ξ Halka elemanları ile DNA bazlarının eşleme dönüşümü

Θ Kodsözler ile DNA görüntülerinin eşleme dönüşümü

S_{D_4} 4 elemanlı DNA bazları

$S_{D_{16}}$ 16 elemanlı DNA bazları

$S_{D_{256}}$ 256 elemanlı DNA $4-$lü bazları

$E(g)$ $g(x)$ kümesi ile üretilen ψ - küme

U_R R halkasının birimsel elemanları

π_i $i.$ izdüşüm dönüşümü

$x \perp y$ x ve y diktir

KISALTMA LİSTESİ

CSS	Calderbank-Shor-Steane
TS	Ters sıralı
TST	Ters sıralı tamlanan

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖZET

SONLU VE DEĞİŞMELİ HALKALARDA LİNEER KODLAR

Ayşegül BAYRAM ELELE

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Doç. Dr. Fatih DEMİRKALE

Bilgi çağında yaşadığımız günümüzde dijital bilgi transferi sırasında kaynaktan alıcıya bilgi aktarırken kanalda, gürültü olarak adlandırılan etkenlerin neden olduğu bazı hatalar meydana gelmektedir. Kodlama teorisi bu hataların belirlenmesi ve düzeltilmesi ile ilgilenen bir bilim dalıdır. Bu alandaki ilk çalışmalar cisimler üzerinde gerçekleştirilmiştir. Mümkün olan en iyi hata düzeltme kapasitesine sahip özel kod aileleri belirlenmiştir. Örneğin; Hamming kod, Goppa kod ve BCH kod bu özel kod ailelerindendir. Sonlu cisimler üzerinde çalışılan kod ailelerinin cebirsel yapısı halkalar üzerinde incelenmeye başlandığında, bazı kod ailelerinin özel bir dönüşüm olan Gray dönüşüm altındaki görüntülerinin literatürde bilinen kodlardan daha iyi hata düzeltebilen kodlar elde edildiği gözlemlenmiştir. Böylece halkaların yapısına göre kod ailelerinin karakterizasyonları merak edilmiştir.

Bu çalışmada farklı zincir olmayan halkalar üzerinde tanımlanan kod ailelerinin yapıları incelenerek bazıları için tam karakterizasyonlar elde edilmiştir. Bu kod aileleri için hata düzeltme kapasitelerini ifade eden kod parametreleri verilmiştir. Bu kod ailelerinden bazıları; devirli, sabit devirli, çarpık devirli, kuantum ve DNA kodlardır.

Bölüm 1'de literatür özeti verilerek bu çalışmanın amacı ve literatüre olan orijinal katkısı ifade edilecektir. Bölüm 2'de cebirsel kodlama teorisi ile ilgili temel tanım ve teoremler ifade edilecektir. Bu çalışmada kullanılan özel kod aileleri ile ilgili temel tanım ve teoremler verilecektir. Bölüm 3'de ilk defa tanımlanan $R_{q,2}$ halkasının cebirsel yapısı incelenerek bu halka üzerinde lineer ve devirli kodlar ile bu kodların dual kodlarının yapısı verilecektir. Ayrıca $R_{q,2}$ halkası üzerinde kendine dik kodlar

kullanılarak kuantum kodlar elde edilecektir. Bölüm 4'de ilk defa tanımlanan R_{v^2-v} halkasının cebirsel yapısı incelenerek bu halka üzerinde lineer, sabit devirli ve çarpık sabit devirli kodların yapısı verilecektir. Ayrıca R_{v^2-v} halkası üzerinde ters sıralı ve ters sıralı tamlanan kodların cebirsel özelikleri incelenecektir. Ayrıca R_{v^2-v} halkası üzerinde DNA kodlar elde edilecektir. Bölüm 5'de R_{v^4-v} halkası üzerinde lineer, devirli, ters sıralı ve ters sıralı tamlanan kodların cebirsel özelikleri incelenecektir. Ayrıca R_{v^4-v} halkası üzerinde DNA kodlar elde edilecektir. Bölüm 6'da bu tezin sonucu ve ilerki çalışmalar için öneriler verilecektir.

Anahtar Kelimeler: Lineer kod, devirli kod, sabit devirli kod, çarpık devirli kod, kuantum kod, DNA kodlar.

ABSTRACT

LINEAR CODES OVER FINITE AND COMMUTATIVE RINGS

Ayşegül BAYRAM ELELE

Department of Mathematics

PhD. Thesis

Adviser: Doç. Dr. Fatih DEMİRKALE

In these technology ages, reliable digital data transmission in noisy environments is becoming a very critical issue. Coding theory aims to correct, or at least detect the errors caused by noisy environments with an acceptable rate. The primary studies of coding theory were related with fields. In these studies, special coding families, such as Hamming codes, Goppa codes, BCH codes which have efficient error correction capacities, they are determined. The algebraic structure of these code families are first studied on finite fields and then examined on rings. It was observed that codes which are obtained by using the images under Gray Map, a special type of conversion, outperform the existing codes in the literature in terms of error correction. Thus, the characterization of these code families become a significant research area. The complexity is an important factor. In this context, the characterization of the rings that cannot be ranked as chains according to their proximity coverage, is more challenging than the rings that can be ranked.

In this study, we give the exact characterization of codes over different rings by investigating the algebraic structure. We obtain the parameters of correcting capabilities. Some of these code families are cyclic, constacyclic, skew cyclic, quantum and DNA codes.

In Chapter 1, we will give the aim of this thesis and state original contribution to literature of this thesis by giving summary of this work. In Chapter 2, we will state the basic definitions and theorems of algebraic coding theory. Basic definitions and theorems about special codes families used in this thesis will be given. In Chapter 3, for the first time, structure of linear and cyclic codes and the dual of these codes over $R_{q,2}$

will be given by investigating the algebraic structure of ring. Furthermore, quantum codes will be obtained by using the self orthogonal codes over $R_{q,2}$. In Chapter 4, the structure of linear, constacyclic and skew constacyclic codes will be given by investigating algebraic structure of R_{v^2-v} defined for first time. Moreover the algebraic structure of reversible and reverse-complement cyclic codes over R_{v^2-v} will be investigated. Furthermore, DNA codes over R_{v^2-v} will be obtained. In Chapter 5, the structure of linear, cyclic, reversible and reverse-complement cyclic will be investigated. Furthermore, DNA codes over R_{v^4-v} will be obtained. In Chapter 6, the conclusions of this thesis and succestions for the previous study will be given.

Keywords: Linear codes, cyclic codes, constacyclic codes, skew cyclic codes, quantum codes, DNA codes.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Kodlama teorisinin asıl amacı; iletişim sırasında oluşan hataları düzeltmek ve kaliteli iletişimi sağlamaktır. Bu amaçla sonlu cisimler üzerinde tanımlı hata düzeltebilen kodlar ile ilgili pek çok araştırma yapılmıştır. Claude Shannon'ın 1948 yılında yaptığı "A Mathematical Theory of Communication" [1] adlı meşhur makalesi cebirsel kodlama teorisinin ilk çalışması olarak kabul edilmektedir. 1994 yılında, Hammons ve arkadaşlarının "The Z_4-linearity of Kerdock, Preparata, Goethals and Related Codes" [2] adlı çalışması halkalar üzerindeki kod çalışmaları için ciddi bir kaynak olmuştur. Özellikle [2] çalışmasından sonra araştırmacılar Z_4 halkası üzerindeki kodları incelemeye önem göstermişlerdir. Bu çalışmada Z_4-lineer kodlar ile Z_2 üzerindeki lineer olmayan kodlar arasında uzaklığı koruyan özel bir dönüşüm tanımlanmış ve bu dönüşüm "**Gray dönüşüm**" olarak adlandırılmıştır. Bu dönüşüm yardımıyla pek çok lineer olmayan ve çok hata düzelten ikili kod elde edilmiştir. Son zamanlarda bazı özel zincir halkaları üzerindeki lineer kod aileleri tanımlanmış olmasına rağmen Z_4 halkasındaki kod aileleri latisler, dizayn teori, kriptoloji ve pek çok yönüyle uygulanabilirlikleri açısından kodlama teorisinde özel bir alan olarak kalmıştır. Özellikle, Bonnecaze ve Udaya [3] $R = Z_2 + uZ_2 = Z_2 \big/ < u^2 > \ \left(u^2 = 0\right)$ zincir halkası üzerindeki devirli kodları çalışmış ve bu halka üzerindeki devirli kodların R halkasının temel idealleri olduklarını göstermişlerdir. Böylece zincir halkası üzerindeki devirli kodlar ile

bölüm halkasının idealleri arasındaki ilişki verilmiştir. Blackford [4] Z_4 halkası üzerindeki çift uzunluğa sahip negacyclic kodları çalışmıştır. Bu durum Yıldız ve Karadeniz tarafından [5, 6, 7] $Z_2 + uZ_2$ halkasını k tane değişkene genelleyerek lineer, devirli, kendine dual başta olmak üzere pek çok kod ailesini tanımlamış ve hata düzeltme kabiliyetleri en yüksek olan yeni kodlar literatüre kazandırılmıştır. Son zamanlarda zincir halkalarının dışında zincir olmayan halkalar üzerindeki kodlar da önem kazanmıştır. Boucher ve arkadaşları [8], $R = Z_2 + uZ_2 = Z_2[u] / \langle u^2 - u \rangle$ halkası üzerinde değişmeli olmayan bir çarpma işlemi ile çarpık devirli kod (skew cyclic codes) ailelerini tanımlamışlardır. Ayrıca Harada ve arkadaşları [9], $R = Z_2[u] / \langle u^2 - u \rangle$ halkası üzerinde kendine dual optimal kodlar elde etmişlerdir. Bayram ve Şiap [10], zincir olmayan $R = Z_3[u] / \langle u^3 - u \rangle$ halkası üzerinde lineer ve devirli kod ailelerini tanımlayarak bu halka üzerindeki kodlar ile dual kodların ağırlıkları arasındaki ilişkiyi veren ağırlık sayaçlarını elde etmişlerdir. Aynı yazarlar [11], bir önceki çalışmayı [10] herhangi bir p asalı için $Z_p[u] / \langle u^p - u \rangle$ zincir olmayan halka üzerinde genelleştirilip sabit devirli (constacyclic) kodların yapısı da incelenmiştir. Ayrıca devirli ve sabit devirli kodların yapısı ile F_p sonlu cismi üzerindeki devirli ve sabit devirli kodların yapıları arasındaki ilişki verilmiştir.

1.2 Tezin Amacı

İyi hata düzeltme kapasitesine ilaveten iletişimin düşük maliyetli ve yüksek bilgi transferinin elde edilmesi de kodlama teorisinin avantajlarındandır. Cebirsel kodlama teorisi literatürüne bakıldığında farklı kod ailelerinin hata düzeltme kapasiteleri üzerinde çalışılan cisim, halka veya modül gibi cebirsel yapılara göre farklılıklar göstermektedir.

Bu tezin amacı çeşitli zincir olmayan halka yapıları üzerinde tanımlanan özel kod ailelerinin cebirsel yapılarını ve uygulamalarını vermektir. Bu çalışmada, Bölüm 1'de literatür özeti verilerek bu çalışmanın amacı ve literatüre olan orijinal katkısı ifade edilmektedir.

Bölüm 2'de cebirsel kodlama teorisi ile ilgili temel tanım ve teoremler ifade edilmektedir. Bu bölümde çeşitli halkalar üzerinde karakterizayonları bölüm 4 ve 5'te verilen özel kod aileleri ile ilgili temel tanım ve teoremler verilmektedir.

Bölüm 3'de ilk defa tanımlanan $R_{q,2} \coloneqq F_q[u,v] \Big/ < u^q - u, v^q - v >$ halkasının cebirsel yapısı incelenerek bu halka üzerinde lineer ve devirli kodlar ile bu kodların dual kodlarının yapısı verilmektedir. $R_{q,2}$ halkası üzerindeki kendine dik devirli kodlar yardımı ile F_q sonlu cismi üzerindeki kuantum kodlar inşa edilmektedir. Bu şekilde inşa edilen kuantum kodların parametreleri belirtilmektedir. Özel olarak, $R_{2,2}$ halkası üzerinde uzunluğu 7 olan kendine dik kodlar kullanılarak F_2 cismi üzerindeki tüm denk olmayan kuantum kodların parametreleri bir çizelge ile verilmektedir.

Bölüm 4'de ilk defa tanımlanan $R_{v^2-v} \coloneqq F_4[v] \Big/ \langle v^2 - v \rangle$ halkasının cebirsel yapısı incelenerek bu halka üzerinde tüm lineer, sabit devirli ve çarpık sabit devirli kodların yapısı verilmektedir. Ayrıca R_{v^2-v} halkası üzerindeki otomorfizmalar ve devirli kod üreten polinomlar ile özel bir küme tanımlanarak DNA kod uygulaması elde edilmektedir.

Bölüm 5'de R_{v^4-v} halkası üzerinde lineer, devirli, ters sıralı ve ters sıralı tamlanan kodların cebirsel özelikleri incelenmektedir. Ayrıca R_{v^4-v} halkası üzerinde DNA kodlar elde edilmektedir.

Bölüm 6'da bu tezin sonucu ve ilerki çalışmalar için öneriler verilmektedir.

1.3 Orijinal Katkı

Zincir halkalarının ideal yapısının aksine, zincir olmayan halkalar üzerinde kodların yapısını belirlemek daha karmaşık bir problemdir. Bu çalışmada özel olarak tanımlanan zincir olmayan halka üzerindeki devirli kodlar kullanılarak kuantum kodlar elde edilmektedir.

Ayrıca zincir olmayan halkalar üzerindeki ters sıralılık özelliğine sahip devirli kodların yapısı belirlenmektedir ve bu devirli kodların özel bir dönüşüm altındaki görüntüsü

olacak şekilde DNA kodlar elde edilmektedir. DNA görüntüsüne sahip optimal kodlar verilmektedir.

BÖLÜM 2

CEBİRSEL KODLAMA TEORİSİ

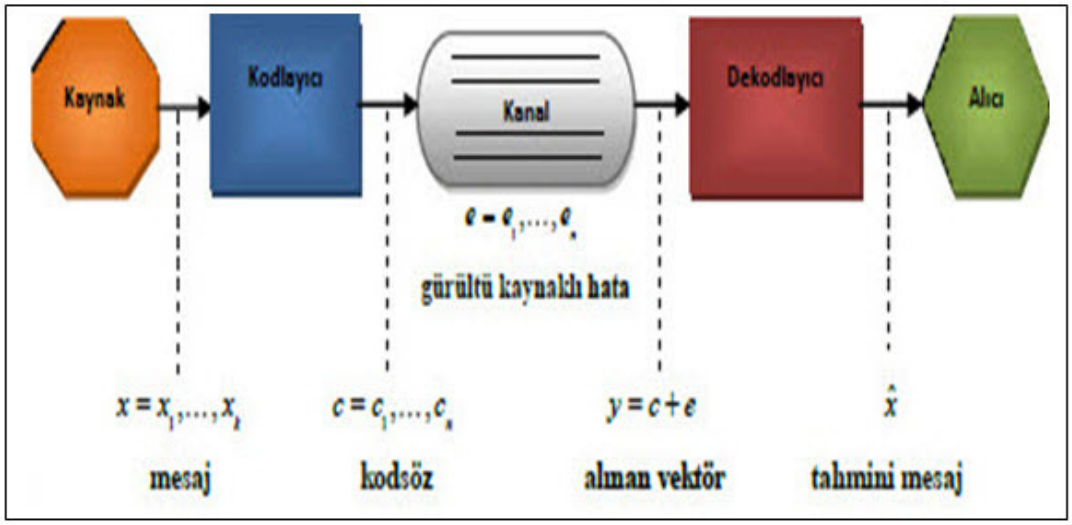
2.1 Kodlama Teorisine Giriş

Bilginin bir kaynaktan alıcıya etkili ve doğru bir şekilde aktarılmasını sağlayacak metotları belirleyen çalışma alanına **kodlama teorisi** denir. Bilginin transfer edildiği ortama **kanal** denir. İnternet ve telefon birer kanal örneği olarak verilebilir. Bilgi iletilirken çeşitli olumsuz faktörlerden dolayı iletişim sırasında bazı hatalar oluşması doğal bir sonuçtur. Oluşabilecek tüm olumsuz koşullara **gürültü** adı verilir.

İletilen bilginin kanalda maruz kaldığı gürültüden dolayı oluşan hatayı belirlemek ve hatta mümkünse bu hatayı düzeltmek için bir yöntem kullanılması akıllıca olacaktır. Cebirsel kodlama teorisinin asıl amacı da çeşitli yöntemler kullanarak hatayı belirlemek hatta mümkünse düzeltmektir. Bilginin kanala gönderilmeden öncesinde sembollere dönüştürülmesi yani **kodlama** sırasında sembollere bazı cebirsel işlemler uygulayarak kanala sokulması ve kanaldan çıkarken de uygun işlemlerin yapılması ile semboller tekrar bilgi haline dönüştürülür. Burada önemli ve zor olan kısım sembollerin bilgiye dönüştürmesi yani **çözümleme** dediğimiz kısımdır.

Kodlama teorisi, bilgi iletimi sırasında kanaldaki gürültü nedeniyle meydana gelen hataları tespit etme ve bu hataları düzeltme problemi üzerinde çalışır. Kodlama teorisi; bilginin hızlı kodlanması, mesajların kolay taşınması, alınan mesajların hızlı çözümlenmesi, oluşan hataların doğru çözümlenmesi ve maksimum bilgi transferini en

kısa sürede yapmak üzere yapılan iletişim prensipleri üzerine kuruludur. Bilgi iletimi aşağıdaki şekilde düşünülebilir.



Şekil 2.1 Bilgi transfer şeması

2.2 Genel Bilgiler

2.2.1 Halkalar ile İlgili Temel Tanım ve Kavramlar

İlk olarak, David Hilbert (1862-1943) tarafından tanımlanan halka kavramı daha sonra Emmy Noether tarafından değişmeli halkalar teorisi olarak "Ideal Theory in Rings" [12] makalesinde verilmiştir. Bu makalede ideal yapıları içerme bağıntısına göre sıralandığında zincir yapısına sahip idealleri olan halka yapısı incelenmiştir. Bu bölümde halkalar ile ilgili bazı tanımlar verilmektedir.

Genel olarak halka teorisi ile ilgili tanım ve özellikler için [13] ve [14], kodlama teorisi ile ilgili tanım ve teroemler için [15] ve [16] kullanılmıştır.

Tanım 2.1 R boştan farklı bir küme ve "$+, .$" işlemleri R üzerinde tanımlı birer ikili işlem olsun. Eğer R bu ikili işlemler ile aşağıdaki özellikleri sağlıyor ise $(R, +, .)$ yapısına **halka** denir.

1. $(R, +)$ değişmeli bir gruptur.

2. R üzerinde . işlemine göre birleşme özelliği sağlanır. Yani, her $a,b,c \in R$ için $a.(b.c) = (a.b).c$ olur.

3. R üzerinde . işleminin $+$ işlemi üzerine dağılma özelliği vardır. Yani,

$a.(b+c) = (a.b)+(a.c)$ ve $(a+b).c = (a.c)+(b.c)$ sağlanır.

Tanım 2.2 Her $a \in R$ için $a.1_R = 1_R.a = a$ özelliğini sağlayan $1_R \in R$ $(1_R \neq 0_R)$ elemanı var ise bu elamana halkanın **birim elemanı** denir.

Eğer $1_R \in R$ elemanı var ise halkaya **birimli halka** denir. Ayrıca, her $a,b \in R$ için $a.b = b.a$ özelliği sağlanıyorsa halkaya **değişmeli halka** denir.

Tanım 2.3 [13, 14] R bir halka ve $\varnothing \neq I \subseteq R$ olsun. Her $a,b \in I$ ve her $r \in R$ elemanı için $a-b \in I$ ve $ra \in I$ özellikleri sağlanıyor ise I alt kümesine R halkasının **ideali** denir. Böylece, $\{0\}$ ve R idealleri R halkasının **aşikar idealleri**dir.

Tanım 2.4 R halkasının bir ideali $M \neq R$ ve R halkasında M idealini kapsayan herhangi bir aşikar olmayan ideal yok ise M idealine **maksimal ideal** denir. R halkasının tek bir maksimal ideali var ise R halkasına **yerel (local) halka** denir. Tüm idealleri içerme bağıntısına göre zincir şeklinde sıralanabilen halkaya **zincir halkası** denir.

Tanım 2.5 $(R,+_R,._R)$ ve $(S,+_S,._S)$ üzerlerinde tanımlanan işlemler ile birlikte iki halka ve $\mu : R \to S$ dönüşümü her $r_1, r_2 \in R$ için

1. $\mu(r_1 +_R r_2) = \mu(r_1) +_S \mu(r_2)$,

2. $\mu(r_1 ._R r_2) = \mu(r_1) ._S \mu(r_2)$ ve

3. $\mu(1_R) = 1_S$

şartlarını sağlıyor ise μ dönüşümüne **halka homomorfizması** denir.

Ayrıca, bir halka homomorfizması birebir ve örten ise **izomorfizma** olarak adlandırılır. Bir halkanın kendi üzerine tanımlı izomorfizmasına **otomorfizma** denir.

2.2.2 Sonlu Cisimler

Tanım 2.6 F kümesi üzerinde tanımlanan toplama $(+)$ ve çarpma $(.)$ işlemleri ile aşağıdaki özellikleri sağlarsa $(F,+,.)$ yapısına **cisim** denir.

1. $(F,+)$ değişmeli gruptur.

2. $F^* = F - \{0\}$ olmak üzere $(F^*, .)$ değişmeli gruptur.

Bu bölümde sonlu cisim ve temel kodlama teorisi bilgileri için [15] kaynak olarak alınmıştır.

Eğer F sonlu sayıda elemana sahipse, F cismi **sonlu cisim** olarak adlandırılmaktadır. q tane elemana sahip sonlu cisim F_q ya da $GF(q)$ ile gösterilmektedir.

Teorem 2.7 F_q sonlu cismi için aşağıdaki özellikler sağlanmaktadır:

1. q eleman sayısı bazı p asal ve r pozitif tam sayısı için $q = p^r$ olur.

2. F_q sonlu cismi F_p alt cismini içerir.

3. F_q sonlu cismi F_p üzerinde boyutu r olan bir vektör uzayıdır.

4. Her $\alpha \in F_q$ için $p\alpha = 0$ olur.

5. F_q izomorfizma farkı ile tektir.

Tanım 2.8 Baş katsayısı 1 olan polinoma **monik polinom** denir.

Tanım 2.9 F_q sonlu cismi üzerinde tanımlanan çarpma işlemi ile F_q^* mertebesi $q-1$ olan devirli bir gruptur. $\gamma \in F_q^*$, bu devirli grubun üreteç elemanı ise $F_q = \{0, 1, \gamma, \gamma^2, ..., \gamma^{q-2}\}$ ve $\gamma^i = 1$ olması için gerek ve yeter şart $(q-1) \mid i$ olmasıdır. F_q^* devirli grubunun her üreteç elemanına **ilkel eleman** denir. γ elemanı F_q sonlu cisminin ilkel elemanı ise $\gamma^{q-1} = 1$ olur. F_q sonlu cisminin her elemanı $x^q - x$ polinomunun bir köküdür.

Teorem 2.10 φ Euler fonksiyonu 1'den n'ye kadar ve n ile aralarında asal pozitif tam sayıların sayısını verir ve $\varphi(n)$ ile gösterilmektedir. F_q sonlu cisminde $\varphi(q-1)$ tane ilkel eleman vardır.

Tanım 2.11 Katsayıları F_q sonlu cisminden alınan polinomlar halkası $F_q[x]$ olsun. $\deg(f(x))$ ile $f(x)$ polinomunda x değişkeninin en büyük kuvveti gösterilmektedir. Sabit polinomdan farklı bir $f(x) \in F_q[x]$ polinomu daha küçük dereceli polinomlara çarpanlara ayrılamıyorsa $f(x)$ elemanına **indirgenemez polinom** denir.

Tanım 2.12 $f(x) \in F_p[x]$ derecesi m olan indirgenemez polinom olmak üzere, $F_p[x] \Big/ \langle f(x) \rangle$ bölüm halkasına karakteristiği p olan, p^m elemanlı sonlu cisim denir.

Teorem 2.13 F_q karakteristiği p olan sonlu cisim olsun. Her $\alpha, \beta \in F_q$ için $(\alpha+\beta)^p = \alpha^p + \beta^p$ olur.

Teorem 2.14 p asal sayısı ve m pozitif tam sayısı için p^m elemanlı sonlu cisim daima vardır ve izomorfizma farkı ile tektir.

Tanım 2.15 $F_s \subseteq F_q$ alt kümesi cisim olma şartını sağlıyorsa F_s alt kümesine **alt cisim** denir. O halde, F_s mertebesi $s-1$ olan bir elemana sahiptir ve $(s-1) \mid (q-1)$.

Teorem 2.16 $q = p^m$ olmak üzere $F_s \subseteq F_q$ alt cisim olması için gerek ve yeter şart $s = p^r$ olmak üzere $r \mid m$ olmasıdır.

2.2.3 Lineer Kodlar

Tanım 2.17 F_q cismi q elemanlı sonlu bir cisim olsun. F_q üzerinde uzunluğu n, eleman sayısı M olan bir C **kodu**, F_q^n uzayının bir alt kümesidir. Kodun herhangi bir elemanına **kodsöz** denir. Böyle bir kod $(n, M)_q -$ kod şeklinde gösterilir.

Tanım 2.18 F_q^n uzayının k boyutlu bir alt uzayına F_q üzerinde uzunluğu n, boyutu k olan bir C **lineer kodu** denir ve $[n,k]_q$ – kod şeklinde gösterilir. Özel olarak, F_2 üzerinde bir koda **ikili kod**, F_3 üzerinde bir koda **üçlü kod** denir.

Örnek 2.19 $C=\{0000,0011,1010,1001\}\subseteq F_2^4$ kodu bir $[2,2]_2$ ikili lineer koddur.

Tanım 2.20 [15] C kodu F_q üzerinde bir lineer kod olsun. C kodunun **dual kodu** $C^{\perp}=\{x\in F_q^n:\langle x,c\rangle=0,\forall c\in C\}$ şeklinde tanımlanmaktadır. C **kodunun boyutu**, C vektör uzayının boyutudur ve $boy(C)$ ile gösterilmektedir.

Teorem 2.21 [15] C kodu F_q üzerinde n uzunluğunda boyutu k olan bir lineer kod olmak üzere aşağıdakiler doğrudur:

1. $|C|=q^{boy(C)}\quad (M=q^k)$.

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

3. $(C^{\perp})^{\perp}=C$.

İspat:

1. C kodunun vektör uzayı olarak bir bazı $\{c_1,c_2,\ldots,c_k\}$ olsun. O halde C kodu,

$C=\{\lambda_1c_1+\lambda_2c_2+\ldots+\lambda_nc_n:\lambda_1,\lambda_2,\ldots,\lambda_n\in F_q\}$ olur. $|F_q|=q$ olduğundan her bir $1\le i\le k$ için λ_i katsayıları için q tane seçenek vardır. Sonuç olarak, C kodunun q^k elemanı vardır.

2. $C^{\perp}=\{x\in F_q^n:\langle x,c\rangle=0,\forall c\in C\}$ vektör uzayının, F_q^n vektör uzayının bir alt uzayı olduğunu göstereceğiz: $x,y\in C^{\perp}$ olsun. O halde, her $c\in C$ için $\langle x,c\rangle=0$ ve $\langle y,c\rangle=0$ olur. Her $c\in C$ için $\langle x+y,c\rangle=\langle x,c\rangle+\langle y,c\rangle=0$ ise $x+y\in C^{\perp}$ elde edilir.

Ayrıca, her $c\in C$ ve $\alpha\in F_q$ için $\langle \alpha x,c\rangle=\alpha\langle x,c\rangle=0$ olur. Sonuç olarak $\alpha x\in C^{\perp}$ elde edilir.

Böylece $C^{\perp}$ vektör uzayı F_q^n vektör uzayının bir alt uzayıdır, yani bir lineer koddur.

$C=\{0\}$ ise F_q^n cismindeki tüm vektörler C koduna diktir. Dolayısıyla $F_q^n = C^{\perp}$ olur.

$boy(C)=k\geq 1$ ve C kodunun bir bazı $\{c_1,c_2,\ldots,c_k\}$ olsun. $x\in C^{\perp}$ için gerek ve yeter şart $\langle c_1,x\rangle=\langle c_2,x\rangle=\ldots=\langle c_k,x\rangle=0$ olur. Yani, $\{c_1,c_2,\ldots,c_k\}$ bazının elemanlarını satır kabul eden matris $A=\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$ ise $Ax^T=0$ olur. Burada k lineer bağımsız denklem ve n bilinmeyen vardır. Böyle bir sistemin $n-k$ vardır. Dolayısıyla $C^{\perp}$ uzayının boyutu $n-k$ olur.

3. $c\in C$ olsun. Bu durumda her $d\in C^{\perp}$ için $\langle c,d\rangle=0$ ise $\langle d,c\rangle=0$ ve $c\in\left(C^{\perp}\right)^{\perp}$ elde edilir.

Öte yandan, C bir $[n,k]-$kod olduğundan $C^{\perp}$ kodunun parametreleri $[n,n-k]$ olur. $\left|\left(C^{\perp}\right)^{\perp}\right|=q^k=|C|$. Buradan, $\left(C^{\perp}\right)^{\perp}=C$ elde edilmektedir.

2.2.4 Kendine Dual ve Kendine Dik (Self Dual ve Self Orthogonal) Kodlar

Tanım 2.22 [15] C kodu F_q üzerinde bir lineer kod olsun. Eğer $C\subseteq C^{\perp}$ ise C koduna **kendine ortogonal (dik) kod** ve eğer $C=C^{\perp}$ ise C koduna **kendine dual kod** denir.

Kendine dual bir ikili kod $C=C^{\perp}$ olacağı için $k=n-k$ olup $k=\frac{n}{2}$ olur ve uzunluğu çifttir. C kodu F_q^n üzerinde bir $[n,k]_q-$kod olsun. C kodunun kendine dual olması için gerek ve yeter şart C kodunun kendine dik ve $k=\frac{n}{2}$ olmasıdır.

2.2.5 Üreteç ve Kontrol Matrisleri

Tanım 2.23 $[n,k]_q$ parametrelerine sahip C kodu F_q^n uzayının bir alt uzayıdır ve bir bazı vardır. C kodunun bir bazı $\{c_1,c_2,\ldots,c_k\}$ olmak üzere bu vektörleri satır kabul eden G matrisine, C kodunun **üreteç matrisi** denir.

Örnek 2.24 $C=\{00000,10121,12020,22111,20212,21010,11222,01101,02202\}$ kodu F_3 üzerinde bir lineer kodu olsun. $C=\{\alpha_1(10121)+\alpha_2(12020):\alpha_1,\alpha_2\in F_3\}$ ve $G=\begin{pmatrix}1&0&1&2&1\\1&2&0&2&0\end{pmatrix}_{2\times5}$ matrisinin F_3 üzerinde ürettiği kod C kodu olur.

Tanım 2.25 Bir C lineer kodu için **parite kontrol matris** H, dual kodun üreteç matrisidir ve $C=\{x\in F_q^n : Hx^T=0\}$ olur.

Örnek 2.26 $H=\begin{pmatrix}1&0&0&0\\0&1&0&1\\0&0&1&1\end{pmatrix}_{3\times4}$ matrisinin parite kontrol matrisi olduğu ikili C kodu $C=\left\{(x_1,x_2,x_3,x_4)\in F_2^4 : H\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\right\}$ olur. Böylece, $x_2+x_4=0$, $x_3+x_4=0$, $x_1=0$ ve $x_2=x_3=x_4=r$ elde edilir. Bu yüzden $C=\{(0rrr):r\in F_2\}=\{0000,0111\}$ olur.

Tanım 2.27 $G=[I_k \mid A]_{k\times n}$ matrisi, bir $[n,k]_q-$kodun üreteç matrisi olsun. Bu durumda G **standart formdadır** denir. Burada I_k boyutu $k\times k$ olan birim matris ve A boyutu $k\times(n-k)$ olan bir matristir.

Teorem 2.28 Bir $[n,k]_q-$kodunun üreteç matrisi standart formda verilmişse $H=[-A^T \mid I_k]$ matrisi parite kontrol matrisidir.

Örnek 2.29 C bir $[4,2]_3-$kodu ve $G=\begin{bmatrix}1&0&1&2\\0&1&1&1\end{bmatrix}$ matrisi C kodunun üreteç matrisi olsun. Bu durumda C kodunun farklı bir üreteç matrisini H kontrol matrisi ile belirlemek için $G=\begin{bmatrix}1&0&1&2\\0&1&1&1\end{bmatrix}$ standart formadaki üreteç matrisidir ve $A^t=\begin{bmatrix}1&1\\2&2\end{bmatrix}$ ve $A^t=\begin{bmatrix}1&1\\2&2\end{bmatrix}$ ise $-A^t=\begin{bmatrix}2&2\\1&2\end{bmatrix}$ olur. Böylece $H=\begin{bmatrix}2&2&1&0\\1&2&0&1\end{bmatrix}$ matrisi C kodunun

parite kontrol matrisidir. $C=\{(x_1x_2,x_3,x_4)\in F_3^4 : Hx^t=0\}$ ise $2x_1+2x_2+x_3=0$ elde edilir. Sonra $x_1+2x_2+x_4=0$ olur. Böylece $x_3=r$, $x_4=s$, $x_1=2r+s$, $x_2=2r+2s$ olur. Bu yüzden $C=\{(2r+s,2r+2s,r,s): r,s\in F_3\}$ olarak yazılır. $G'=\begin{pmatrix}1&2&0&1\\2&2&1&0\end{pmatrix}$ matrisi C kodu için üreteç matristir.

Tanım 2.30 n uzunluğunda **tekrarlı ikili kod** bir $[n,1]_2$ koddur.

2.2.6 Hamming Uzaklık- Hamming Ağırlık

Tanım 2.31 $x=(x_1,x_2,\ldots,x_n), y=(y_1,y_2,\ldots,y_n)\in F_q^n$ için x ile y arasındaki **Hamming uzaklık** $d_H(x,y)=d_H(x_1,y_1)+d_H(x_2,y_2)+\ldots+d_H(x_n,y_n)$ ile tanımlanmaktadır. Burada,

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

biçiminde tanımlanmaktadır. Yani; $d_H(x,y)=|\{i: x_i\neq y_i\}|$ olur.

Örnek 2.32 F_2^8 üzerinde $x=(10011110)$ ve $y=(10110001)$ ise $d_H(x,y)=5$ olur.

F_3^8 üzerinde $x=(10222101)$ ve $y=(11212210)$ ise $d_H(x,y)=5$ olur.

Teorem 2.33 Hamming uzaklığı F_q^n üzerinde bir metriktir. Yani her $x,y,z\in F_q^n$ için:

i. $d_H(x,x)=0$,

ii. $d_H(x,y)\geq 0$ veya $d_H(x,y)=0$ olması için gerek ve yeter şart $x=y$ olmasıdır.

iii. $d_H(x,y)=d_H(y,x)$,

iv. $d_H(x,z)\leq d_H(x,y)+d_H(y,z)$ sağlanır.

Tanım 2.34 F_q üzerinde n uzunluğunda bir C kodunun **minimum uzaklığı**,

$d_{\min}(C)=\min\{d_H(x,y): x\neq y, x,y\in C\}$ şeklinde tanımlanmaktadır. Minimum uzaklığı d olan bir $[n,k]_q$ – kod, $[n,k,d]_q$ – kod ile gösterilmektedir.

Tanım 2.35 Bir $x \in F_q^n$ vektörünün **Hamming ağırlığı**, x vektörünün sıfırdan farklı koordinatlarının sayısıdır ve $w_H(x)$ ile gösterilmektedir. Yani, $w_H(x) = d_H(x,0)$ olur.

Örnek 2.36 F_2 üzerinde $x = (10111101)$ ise $w_H(x) = 6$ olur. F_3 üzerinde $x = (12221101)$ ise $w_H(x) = 7$ olur.

Teorem 2.37 $x, y \in F_q^n$ için $d_H(x,y) = w_H(x-y)$ olur.

İspat: $x, y \in F_q^n$ olsun. O halde,

$$\begin{aligned} d_H(x,y) &= d_H(x_1,y_1) + d_H(x_2,y_2) + \ldots + d_H(x_n,y_n) \\ &= d_H(x_1-y_1,0) + d_H(x_2-y_2,0) + \ldots + d_H(x_n-y_n,0) \\ &= w_H(x_1-y_1) + w_H(x_2-y_2) + \ldots + w_H(x_n-y_n) = w_H(x-y) \end{aligned}$$

elde edilir.

Teorem 2.38 C kodu F_q üzerinde bir lineer kod ise $d_{\min}(C) = w_{\min}(C)$ olur.

İspat: C kodu F_q üzerinde bir lineer kod olmak üzere

$$\begin{aligned} d_{\min}(C) &= \min\{d_H(x,y) : x, y \in C, x \neq y\} \\ &= \min\{w_H(x-y) : x, y \in C, x \neq y\} \\ &= \min\{w_H(c) : c \in C, c \neq 0\} \end{aligned}$$

elde edilir.

Teorem 2.39 Bir lineer C kodunun minimum uzaklığının d olması için gerek ve yeter koşul kontrol matrisinin d lineer bağımlı sütununun olması fakat $d-1$ lineer bağımlı sütununun olmamasıdır.

Örnek 2.40 Bir $[5,2]_2$ parametrelerine sahip C kodunun kontrol matrisi $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ olsun. H_1 ile 1. sütun ve H_4 ile 4. sütun gösterilmek üzere $H_1 + H_4 = 0$ olur. Yani 1. ve 4. sütunlar lineer bağımlıdır, ancak herhangi 1 sütun alındığında lineer bağımsız olur. O halde, $d(C) = 2$ olarak elde edilir.

2.2.7 Lineer Kodların Denkliği

Tanım 2.41 C_1 ve C_2 iki $(n, M)_q$ – kod olsun. Eğer C_1 kodundan aşağıda verilen yollardan herhangi biri veya ikisiyle C_2 kodu elde ediliyor ise bu kodlara **denk kodlar** denir:

- Kodsözlerin n bileşeninin permütasyon edilmesi,
- Belli yerdeki bileşenlerin sıfırdan farklı bir skalerle çarpılması.

Örnek 2.42 $C_1 = \{0000, 0011, 0110, 0101\}$ ve $C_2 = \{0000, 0011, 1001, 1010\}$ kodları $(21)(43)$ permütasyonuna göre denktir.

Teorem 2.43 Herhangi bir C lineer kodu, standart formda üreteç matrisine sahip bir C' lineer koduna denktir.

Örnek 2.44 $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$ matrisi C kodu için bir üreteç matrisi olsun. G matrisinin sütunlarına $(24)(35)$ permütasyonu uygulanırsa $G' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$ matrisi elde edilir ve C koduna denk olan kod için bir üreteç matrisi elde edilir.

2.2.8 Kodlama Teorisinde Bazı Sınırlar

$(n, M, d)_q$ ile q – lu alfabe üzerinde n uzunluğunda, M eleman sayısına sahip, d hata düzeltme kapasitesine sahip bir kod gösterilmektedir. Böylece M ve d nin mümkün olduğunca büyük olması amaçlanmaktadır. Ancak bu her zaman mümkün değildir. Yapılan çalışmaların sonucunda literatürde verilen n ve d parametrelerine göre M verimlilik ölçüsünün alabileceği en büyük değer için bazı alt ve üst sınırlar belirtilmiştir. Bu sınırların bazıları, küre paketleme sınırı, Hamming sınırı, Singleton sınırı, Griesmer sınırı, Gilbert-Varshamov sınırı ve Plotkin sınırıdır [15]. Tezin ilerleyen bölümünde DNA kodlar için Griesmer sınırına göre parametrelere bakılacağı için bu bölümde sadece Griesmer sınırından bahsedilecektir.

2.2.8.1 Griesmer Sınırı

Tanım 2.45 q bir asal sayının kuvveti olmak üzere n uzunluğuna ve d minimum uzaklığına sahip bir kodun maksimum eleman sayısı $B_q(n,d) = \max\{q^k : C \subseteq F_q^n \text{ ve } C \text{ bir } [n,k,d]-\text{kod}\}$ olarak tanımlanmaktadır. C bir $[n,k,d]_q$ lineer kodu ve $q^k = B_q(n,d)$ ise C koduna **optimal** kod denir.

Tanım 2.46 $k \geq 1$ olmak üzere $[n,k,d]_q$ parametrelerine sahip lineer kodu için

$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$ sınırına **Griesmer sınırı** denir.

2.2.9 Bazı Özel Kod Aileleri

Bu bölümde, daha sonraki bölümlerde farklı yapılar üzerinde çalışılacak olan lineer kodlar üzerinde durularak, özel kod aileleri için genel tanım ve teoremler verilecektir.

2.2.9.1 Devirli Kodlar

Tanım 2.47 $C \subseteq F_q^n$ olmak üzere, her $c = (c_0, c_1, c_2, ..., c_{n-1}) \in C$ elemanı için $\sigma(c) = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$ koşulunu sağlıyor ise C koduna F_q üzerinde n uzunluğunda bir **devirli kod** denir.

Teorem 2.48 $C \subseteq F_q^n$ kodundan $R_n := F_q[x] / \langle x^n - 1 \rangle$ bölüm halkasına π fonksiyonu aşağıdaki biçimde tanımlansın:

$$\begin{aligned} \pi : C &\rightarrow R_n \\ (a_0, a_1, ..., a_{n-1}) &\rightarrow a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} \end{aligned}.$$

π bir izomorfizmadır. Böylece R_n bölüm halkasındaki her ideale karşılık F_q^n halkasında bir devirli kod vardır. C kodu F_q üzerinde n uzunluğunda bir devirli koddur ancak ve ancak $\pi(C)$ kümesi R_n bölüm halkası üzerinde bir idealdir.

Devirli kodlar ile ilgili detaylı bilgi, [15] gibi temel kodlama teori bilgisi içeren pek çok kaynakta bulunabilmektedir. Burada devirli kodlara karşılık gelen ideallerin üreteç polinomu ve bu polinom yardımı ile devirli kodlar için üreteç matrisi verilecektir. R_n halkasının her idealinin bir temel ideal olduğu bilinmektedir. Buna göre bir C devirli kodu $\pi(C)$ idealinin herhangi bir üreteci ile belirlenmektedir. Genellikle R_n halkasının bir ideali için birden çok üreteç bulunabilir. Aşağıdaki teoreme göre bazı ek özellikler ile tek türlü üreteç bulmak mümkündür.

Tanım 2.49 R_n temel ideal bölgesi olduğundan her I ideali için $I=\langle g(x)\rangle$ olacak şekilde bir monik $g(x)$ üreteç polinomu vardır. Sonuç olarak, $\pi(C)$ idealini üreten $g(x)$ polinomu x^n-1 polinomunun bir bölenidir ve bu polinoma C devirli kodunun **üreteç polinomu** denir. $\deg(g(x))=k$ olmak üzere $g^*(x)=x^k g\left(\frac{1}{x}\right)$ polinomuna $g(x)$ polinomunun **ters sıralı polinomu** denir.

Örnek 2.50 F_2 cisminde $C=\{000,110,101,011\}$ kodu 3 uzunluğunda devirli koddur ve $\pi(C)=\{0,1+x,1+x^2,x+x^2\}\subset F_2[x]/\langle x^3-1\rangle$ olur. Öte yandan $g(x)=1+x$ monik polinomu C kodunun üreteç polinomudur.

Sonuç 2.51 F_q^n üzerindeki devirli kodlar ile $x^n-1\in F_q[x]$ polinomunun monik bölenleri arasında birebir bir eşleme vardır.

Sonlu cisimler üzerinde tanımlı devirli kodlar üreteç polinomları ile tam olarak belirli oldukları için parametreleri de üreteç polinomları ile elde edilebilmektedir.

Teorem 2.52 $g(x)$ polinomu R_n halkasının bir idealinin üreteç polinomu olsun. $g(x)$ polinomunun derecesi $n-k$ ise bu ideale karşılık gelen devirli kodun boyutu k olur.

Teorem 2.53 $g(x)=g_0+g_1x+\ldots+g_{n-1}x^{n-1}$ $(g_{n-1}\neq 0)$ polinomu F_q^n üzerinde C devirli kodunun üreteç polinomu olsun. O halde

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

matrisi C devirli kodunun bir üreteç matrisidir.

2.2.9.2 Sabit Devirli (Constacyclic) Kodlar

Sabit devirli kod devirli kodları da kapsayan özel bir kod ailesidir ve ilk olarak [16] ve [17] makalelerinde tanıtılmıştır. Bu bölümde sabit devirli kodların tanım ve temel özellikleri verilecektir.

Tanım 2.54 [16] $\alpha \in F_q^* = F_q \setminus \{0\}$ birimsel eleman olmak üzere her $c=(c_0,c_1,c_2,...,c_{n-1}) \in C$ elemanı için $\sigma_1(c)=(\alpha c_{n-1},c_0,c_1,...,c_{n-2}) \in C$ koşulunu sağlıyor ise C koduna F_q üzerinde n uzunluğunda bir **sabit devirli (constacyclic) kod** denir.

Böylece, $R_n := F_q[x] \Big/ \langle x^n-\alpha \rangle$ olarak alındığında R_n halkasının her idealine karşılık F_q^n vektör uzayında bir sabit devirli kod vardır. C kodu F_q cisminde n uzunluğunda bir sabit devirli kod olması için gerek ve yeter şart $\pi(C)$ kümesinin R_n halkasında bir ideali olmasıdır. Özel olarak, $\alpha=1$ olarak alınırsa devirli kodlar elde edilmektedir.

2.2.9.3 Çarpık Devirli Kodlar

Çarpık devirli kodlar devirli kodların bir genellemesi olarak değişmeli olmayan halkalar üzerinde 2007 yılında Boucher ve arkadaşları tarafından çalışılmıştır [8]. Bu kodlar [18] ve [19] çalışmalarında $\theta-$devirli kod olarak da adlandırılmıştır. Değişmeli olmayan bir çarpma yardımı ile tanımlanan çarpık polinom halkasında sağ ve sol bölme algoritması sağlandığı için çarpık devirli kodlar devirli kodlara benzer cebirsel özelliklere sahiptirler.

Çarpık devirli kodlar, çarpık polinom halkaları üzerinde tanımlanır. Çarpık polinom halkaları ilk olarak Oystein Ore (1933) tarafından tanımlanmış, Nathan Jacobson (1943)

ve Bernard R. McDonald (1974) tarafından geliştirilmiştir. Bu bölümde, ilk olarak çarpık polinom halkaları ile ilgili temel tanımlar verilmektedir. Daha sonra çarpık devirli kodların tanımı ve temel özellikleri verilecektir.

Tanım 2.55 [8] F cismi üzerinde birebir ve örten μ homomorfizmasına **otomorfizma** denir. Ayrıca, $x \in F$ için $\mu^m(x) = x$ şartını sağlayan en küçük m tam sayısına μ otomorfizmasının **mertebesi** denir ve $|\langle \mu \rangle| = m$ ile gösterilmektedir.

Örnek 2.56 [20] $F_4 = \{0, 1, w, w+1\}$, $(w^2 + w + 1 = 0)$ sonlu cisim üzerinde tanımlı bir otomorfizma;

$$\begin{aligned} \mu : F_4 &\to F_4 \\ \alpha &\to \alpha^2 \end{aligned}$$

şeklinde tanımlanabilir. Burada, $|\langle \mu \rangle| = 2$ olur.

Tanım 2.57 [20] $F[x;\mu] = \{ f(x) = a_0 + a_1 x + \ldots + a_{n-1} : a_i \in F, \forall i \in \{0,1,\ldots,n-1\}\}$ olan polinomlar kümesi üzerinde toplama işlemi standart toplama, çarpma işlemi ise $(ax^i) * (bx^j) = a\mu^j(b)x^{i+j}$ kuralı ile verilsin. Eğer μ birim otomorfizması değil ise tanımlanan toplama ve değişmeli olmayan çarpma işlemi ile çarpık polinomlar kümesi bir halka belirtir ve bu halkaya **çarpık polinomlar halkası** denir. Bu halka sıfır bölen içermez ve birimsel elemanları sadece F cisminin sıfırdan farklı elemanlarıdır.

Tanım 2.58 [21] F sonlu cisim ve μ fonksiyonu F üzerinde tanımlı bir otomorfizma olsun. $C \subseteq F^n$ bir alt uzay ve her $(c_0, c_1, c_2, \ldots, c_{n-1}) \in C$ için $\sigma_2(c) = (\mu(c_{n-1}), \mu(c_0), \mu(c_1), \ldots, \mu(c_{n-2})) \in C$ oluyorsa C alt uzayına n uzunluğunda **çarpık devirli kod** denir. σ_2 dönüşümüne **çarpık devirsel öteleme (skew cyclic shift**) denir. Bazı sınırlamalar altında çarpık devirli kodlar devirli kodlarda olduğu gibi $F[x;\mu] \big/ \langle x^n - 1 \rangle$ halkasının idealleri ile belirlenebilir. Detaylı bilgi için [20] çalışmasına bakılabilir.

BÖLÜM 3

$R_{q,2}$ HALKASI ÜZERİNDE LİNEER KODLAR

Son zamanlarda bazı cebirsel yapılar (halka, modül) üzerindeki özel kod ailelerinin hata düzeltme kapasiteleri çalışılmaktadır. Ayrıca, bu yapılar üzerindeki kod aileleri ile sonlu cisimler ya da halkalar üzerindeki kod aileleri arasındaki ilişki verilerek sonlu cisimler ya da halkalar üzerinde daha iyi parametrelere sahip kodlar elde edilmeye çalışılmaktadır. Kodlama teorisinde yakın zamanlarda çalışılan bir halka yapısı $R_2 = F_2 + uF_2 + vF_2 + uvF_2$ olur. Burada $u^2 = v^2 = 0$ ve $uv = vu$ sınırlamaları sağlanmaktadır. R_2 üzerindeki lineer ve devirli kodlar çalışılmıştır [5, 6]. Bu halka üzerinde tanımlanan kodlardan optimal kendine dual ikili kodlar elde edilmiştir [23]. Öte yandan yarı devirli (quasi cyclic) kodlar literatürde hem sonlu cisimler hem de halkalar üzerinde önemli bir yer tutmaktadır. İyi parametrelere sahip kodlar bu kod ailesinden elde edilmiştir [24, 25, 26, 27]. Bayram ve Şiap [10] $A_3 = Z_3[v] \Big/ \langle v^3 - v \rangle$ halkası üzerindeki lineer ve devirli kodları incelemişlerdir. Bu çalışmada lineer kodların Gray görüntülerine ait üreteç matrislerinin nasıl temsil edildiğini ifade etmişlerdir. Bu çalışma tüm tek asal sayıda elemana sahip sonlu cisimler üzerine genelleştirilmiştir [11]. Bu bölümde $R_{q,2}$ halkasının cebirsel yapısı incelenmektedir. Bu bölümdeki çalışmada, [11] çalışmasındaki durum, taban cismi herhangi sonlu cisim üzerine ve değişken sayısı 2 olarak genelleştirilmiştir.

3.1 $R_{q,2}$ Halkasının Cebirsel Yapısı ve Ayrışımı

p asal sayı ve q sayısı, p asal sayısının pozitif bir tam sayı kuvveti olsun. u ve v, $u^q - u = 0$ ve $v^q - v = 0$ şartlarını sağlamak üzere, $F_q[u,v] \Big/ \langle u^q - u, v^q - v \rangle$ halkası $R_{q,2}$ ile gösterilmektedir. Yani, $R_{q,2} \coloneqq F_q[u,v] \Big/ \langle u^q - u, v^q - v \rangle$ olur.

Bu bölümde, $R_{q,2}$ halkasının cebirsel yapısı ve bu halkanın üzerindeki kod ailelerinin yapıları ve sonlu cisimler üzerindeki ilgili kodlar arasındaki ilişkiler incelenmektedir. Ayrıca bölümün sonunda CSS inşası kullanılarak kuantum kodları elde edilmektedir. Burada $R_{q,2}$ halkasının her elemanı F_q lineer kombinasyon olarak

$$\begin{aligned} R_{q,2} &= F_q + uF_q + u^2F_q + \ldots + u^{q-1}F_q + vF_q + \ldots + u^{q-1}vF_q + \ldots + v^{q-1}F_q + uv^{q-1}F_q + \ldots + u^{q-1}v^{q-1}F_q \\ &= \Big\{ a_0 + ua_1 + \ldots + u^{q-1}a_{(q-1)} + va_q + uva_{(q+1)} + \ldots + u^{q-1}va_{2q-1} + \ldots + v^{q-1}a_{q^2-q} + uv^{q-1}a_{q^2-q+1} + \ldots \\ &\quad + u^{q-1}v^{q-1}a_{(q^2-1)} \mid a_i \in F_q, 0 \le i \le q^2 - 1, u^q = u, v^q = v, q = p^r, p \text{ asal } r \in Z^+ \Big\} \end{aligned}$$

şeklinde yazılabilir.

$R_{q,2}$ Frobenius halkasıdır fakat ne zincir halkası ne de yerel halkadır. Bu özellikleri görmek için öncelikle halkanın yapısı incelenmektedir. $R_{q,2}$ halkasının her elemanı $a_i \in F_q$ ve $0 \le k \le q^2 - 1$ olmak üzere

$$\sum_{\substack{a_k \in F_q \\ 0 \le i,j \le q-1}} \left(a_k u^i v^j \right) = \left(\left(a_0 + ua_1 + u^2a_2 + \ldots + u^{q-1}a_{(q-1)} \right) + \ldots + v^{q-1} \left(a_{(q^2-q)} + \ldots + a_{(q^2-1)}u^{q-1} \right) \right)$$

olarak tekrar yazılabilir. Burada [11] çalışmasında tanımlanan dönüşümün genellemesi olarak özel bir dönüşüm tanımlanacaktır.

Tanım 3.1 [11] makalesinde tanımlanan halka $R_{q,1} \coloneqq F_q[u] \Big/ \langle u^q - u \rangle$ ile gösterilmektedir. Burada p asal, $q = p^r$ ve $a_0, a_1, \ldots, a_{q-1} \in F_q$ olmak üzere

$\alpha = a_0 + a_1 u + \ldots + a_{q-1} u^{q-1} \in R_{q,1}$ ve toplama işlemi F_q cismi üzeride tanımlanmak üzere $\alpha(i) \coloneqq a_0 + a_1 i + \ldots + a_{q-1} i^{q-1}$ olsun.

olsun. Böylece F_q üzerinde elemanlar sırası ile alındığında, $R_{q,1}$ halkasından F_q^q halkası üzerine $\alpha \in R_{q,1}$ olmak üzere $\phi_1(\alpha) = (\alpha(i))_{i \in F_q}$ şeklinde aşağıdaki biçimde tanımlanmaktadır:

$$\phi_1 : R_{q,1} \to F_q^q$$
$$\alpha \to \quad \phi_1(\alpha) = \{\alpha(i)\}_{i \in F_q}$$

Örnek 3.2 $\alpha = a_0 + a_1 u + a_2 u^2 + a_3 u^3 + a_4 u^4 \in R_{5,1}$ elemanı her $i \in F_5$ için $\alpha(i) \coloneqq a_0 + a_1 i + a_2 i^2 + a_3 i^3 + a_4 i^4$ olarak tanımlanır ve α elemanın Gray görüntüsü

$$\phi_1(\alpha) = \phi_1\left(a_0 + a_1 u + a_2 u^2 + a_3 u^3 + a_4 u^4\right) = \left(\alpha(0), \alpha(1), \alpha(2), \alpha(3), \alpha(4)\right)$$
$$= (a_0, a_0 + a_1 + a_2 + a_3 + a_4, a_0 + 2a_1 + 4a_2 + 3a_3 + a_4, a_0 + 3a_1 + 4a_2 + 2a_3 + a_4, a_0 + 4a_1 + a_2 + 4a_3 + a_4)$$

olarak elde edilir.

Dönüşümü tanımlayabilmek için ϕ_1 dönüşümüne benzer biçimde $R_{q,2}$ halkasından $R_{q,1}^q$ halkasına $\alpha(u,v) = \left(a_0 + u a_1 + u^2 a_2 + \ldots + u^{q-1} a_{(q-1)}\right) + v\left(a_q + \ldots + a_{2(q-1)} u^{q-1}\right) + \ldots +$

$v^{q-1}\left(a_{(q^2-q)} + \ldots + a_{(q^2-1)} u^{q-1}\right)\Big)$ olmak üzere ϕ_2 dönüşümü aşağıdaki biçimde tanımlanmaktadır:

$$\phi_2 : R_{q,2} \to R_{q,1}^q$$
$$\alpha \to \phi_2(\alpha(u,v)) = (\alpha(u,j))_{j \in F_q}.$$

Örnek 3.3 $\alpha = a_0 + b_0 u + c_0 u^2 + d_0 u^3 + \left(a_1 + b_1 u + c_1 u^2 + d_1 u^3\right) v + \left(a_2 + b_2 u + c_2 u^2 + d_2 u^3\right) v^2$

$+\left(a_3 + b_3 u + c_3 u^2 + d_3 u^3\right) v^3 \in R_{4,2}$ olsun. Her $j \in \{0, 1, w, w+1\} = F_4$ için

$$\alpha(u,j) \coloneqq a_0 + b_0 u + c_0 u^2 + d_0 u^3 + \left(a_1 + b_1 u + c_1 u^2 + d_1 u^3\right) j + \left(a_2 + b_2 u + c_2 u^2 + d_2 u^3\right) j^2$$
$$+\left(a_3 + b_3 u + c_3 u^2 + d_3 u^3\right) j^3$$

olarak tanımlandığında Gray görüntüsü

$$\phi_2(\alpha) = (a_0 + b_0u + c_0u^2 + d_0u^3, a_0 + a_1 + a_2 + a_3 + (b_0 + b_1 + b_2 + b_3)u + (c_0 + c_1 + c_2 + c_3)u^2 + (d_0 + d_1 + d_2 + d_3)u^3, a_0 + a_1w + a_2(w+1) + a_3 + (b_0 + b_1w + b_2(w+1) + b_3)u + (c_0 + c_1w + c_2(w+1) + c_3)u^2 + (d_0 + d_1w + d_2(w+1) + d_3u)^3, a_0 + a_1(w+1) + a_2w + a_3 + (b_0 + b_1(w+1) + b_2w + b_3)u + (c_0 + c_1(w+1) + c_2w + c_3)u^2 + (d_0 + d_1(w+1) + d_2w + d_3)u^3) \in R_{4,1}^4$$

şeklinde elde edilmektedir.

Tanım 3.1 yardımı ile $R_{q,2}$ halkasından $F_q^{q^2}$ halkası üzerine bir dönüşüm aşağıdaki biçimde tanımlanmaktadır.

Tanım 3.4 $R_{q,2}$ halkasından $F_q^{q^2}$ halkası üzerine

$$\Phi : R_{q,2} \to F_q^{q^2}$$
$$\alpha = \sum_{\substack{0 \le k \le q^2, \\ 0 \le i,j \le q-1}} \left(a_k u^i v^j\right) \to \{\alpha(i,j)\}_{\{i,j\} \in F_q} = \left\{\Phi_1(\alpha), ..., \Phi_{q^2}(\alpha)\right\}$$

dönüşümüne **Gray dönüşüm** denir.

NOT: ϕ_1 dönüşümünün $R_{q,1}^q$ halkasına genişletilmiş hali ϕ_1 olarak adlandırıldığıda

$\Phi = \phi_1\phi_2$ olur.

Örnek 3.5 $\alpha = \left(a + bu + cu^2\right) + \left(d + fu + hu^2\right)v + \left(e + gu + ku^2\right)v^2 \in R_{3,2}$ olsun. $R_{3,2}$ halkasından $R_{3,1}^2$ halkasına ϕ_2 dönüşümü $\alpha \in R_{3,2}$ olmak üzere

$$\phi_2(\alpha) = \left(a + bu + cu^2, (a + d + e) + (b + f + g)u + (c + h + k)u^2, (a + 2d + e) + (b + 2f + g)u + (c + 2h + k)u^2\right) \in R_{3,1}^2$$

ile tanımlanır. $R_{3,1}$ halkasına benzer biçimde $\alpha(i,j) = a + bi + ci^2 + dj + ej^2 + fij + gij^2 + hi^2j + ki^2j^2 \pmod 3$ olmak üzere

$$\Phi : R_{3,2} \to F_3^{3^2}$$
$$\alpha \to \Phi(\alpha) = (\alpha(0,0), \alpha(1,0), \alpha(2,0), \alpha(0,1), \alpha(1,1), \alpha(2,1), \alpha(2,0), \alpha(2,1), \alpha(2,2))$$

olarak tanımlanır.

Örnek 3.6 $\alpha = 1+u+v \in R_{4,2}$ olsun. Böylece $\phi_2(\alpha) = (1+u, u, 1+w+u, w+u) \in R_{4,1}^4$ ve $\Phi(\alpha) = (1,\ 0, 1+w, w, 0, 1, w, 1+w, 1+w, w, 1, 0, w, w+1, 0, 1) \in F_4^{16}$ olur.

Önerme 3.7 Φ Gray dönüşümü $R_{q,2}^n$ halkasından $F_q^{q^2 n}$ halkasına dikliği koruyan bir lineer dönüşümdür.

İspat: İspatı $n=1$ için yapmak yeterlidir. $R_{q,2}$ halkasında $x \perp y$ olacak şekilde iki eleman

$$x = (x_0 + x_1 u + x_2 u^2 + \ldots + x_{q-1} u^{q-1}) + (x_q + x_{q+1} u + \ldots + x_{2q-1} u^{q-1}) v + (x_{2q} + x_{2q+1} u + \ldots + x_{3q-1} u^{q-1}) v^2 + \ldots + (x_{q^2-q} + x_{q^2+1} u + \ldots + x_{q^2-1} u^{q-1}) v^{q-1}$$

ve

$$y = \left(y_0 + y_1 u + y_2 u^2 + \ldots + y_{q-1} u^{q-1}\right) + \left(y_q + y_{q+1} u + \ldots + y_{2q-1} u^{q-1}\right) v + \left(y_{2q} + y_{2q+1} u + \ldots + y_{3q-1} u^{q-1}\right) v^2 + \ldots + \left(y_{q^2-q} + y_{q^2+1} u + \ldots + y_{q^2-1} u^{q-1}\right) v^{q-1}$$

olsun. Böylece,

$$xy = x_0 y_0 + \left(x_0 y_1 + x_1 y_0 + x_1 y_{q-1} + x_2 y_{q-2} + \ldots + x_{q-1} y_1\right) u + \left(x_0 y_2 + x_1 y_1 + x_2 y_0 + \ldots + x_{q-1} y_2\right) u^2 + \ldots + \left(x_0 y_{q-1} + x_1 y_{q-2} + \ldots + x_{q-2} y_1 + x_{q-1} y_0\right) u^{q-1} + \ldots + \left(x_0 y_q\right) v + \left(x_0 y_{2q}\right) v^2 + \ldots + \left(x_0 y_{q^2-1} + x_1 y_{q^2-2} + \ldots + x_{q-1} y_{q^2-q} + \ldots + x_{q^2-1} y_{q^2-1}\right) u^{q-1} v^{q-1} = 0$$

olur. Yani,

$$x_0 y_0 = 0, \tag{3.1}$$

$$x_0 y_1 + x_1 y_0 + x_1 y_{q-1} + x_2 y_{q-2} + \ldots + x_{q-1} y_1 = 0, \tag{3.2}$$

$$x_0 y_2 + x_1 y_1 + x_2 y_0 + \ldots + x_{q-1} y_2 = 0, \tag{3.3}$$

…

$$x_0 y_{q^2-1} + x_1 y_{q^2-2} + \ldots + x_{q-1} y_{q^2-q} + \ldots + x_{q^2-1} y_{q^2-1} = 0 \tag{3.4}$$

olur. Sonuç olarak,

$$\langle \Phi(x), \Phi(y) \rangle = x_0 y_0 + \left(x_0 y_0 + x_0 y_1 + x_1 y_0 + x_1 y_{q-1} + x_2 y_{q-2} + \ldots + x_{q-1} y_1\right) + \ldots + \left(x_0 y_0 + x_0 y_1 + x_1 y_0 + x_1 y_{q-1} + x_2 y_{q-2} + \ldots + x_{q-1} y_1 + \ldots + x_{q^2-1} y_{q^2-1}\right) = 0$$

olur ve ispat tamamlanır.

Önerme 3.8 Aşağıdaki özellikler $R_{q,2}$ üzerinde sağlanmaktadır:

1. w elemanı F_q sonlu cisminin bir ilkel elemanı olmak üzere

$$R_{q,2} \cong R_{q,1}[v]/\langle v \rangle \oplus R_{q,1}[v]/\langle v-1 \rangle \oplus \ldots \oplus R_{q,1}[v]/\langle v-w^{q-2} \rangle .$$

2. $R_{q,2}$ halkası 2^{q^2} ideale sahiptir.

3. $R_{q,2}$ halkasının maksimal ideallerinin sayısı q^2 olur.

4. $R_{q,2}$ halkasında $(q-1)^{q^2}$ tane birimsel eleman vardır.

İspat:

1. $v \in \{0,1,...,w^{q-2}\}$ olmak üzere her $\alpha \in R_{q,2}$ elemanında bir v değeri alındığında $R_{q,2} \cong R_{q,1}[v]/\langle v \rangle \oplus R_{q,1}[v]/\langle v-1 \rangle \oplus \ldots \oplus R_{q,1}[v]/\langle v-w^{q-2} \rangle$ elde edilir.

2. Önermenin 1 maddesinden $R_{q,2} \cong F_q^{q^2}$ elde edilir. Buradan $R_{q,2}$ halkasının ideal sayısı, F_q cisminin aşikar ideallerinden farklı idealleri olmadığı için 2^{q^2} olur.

3. $R_{q,2}$ halkasının maksimal ideallerinin sayısı $F_q^{q^2}$ halkasının bir bileşeninin 0 olduğu ideal sayısına eşittir. Yani, $R_{q,2}$ halkasının maksimal ideallerinin sayısı q^2 olur.

4. $R_{q,2}$ halkasının birimsel elemanlarının sayısı $F_q^{q^2}$ halkasının tüm bileşeninin 0 elemanından farklı olduğu eleman sayısına eşittir. Yani, $R_{q,2}$ halkasında $(q-1)^{q^2}$ tane birimsel eleman vardır.

Tanım 3.9 $a=(a_1,a_2,..,a_{q^2}) \in F_q^{q^2}$ olmak üzere $supp(a)=\{i \mid a_i \neq 0\} \subseteq \{1,2,...,q^2\}$ ile a elemanının **destek** (**support) kümesi** tanımlanır.

Sonuç 3.10 $\alpha, \beta \in R_{q,2}$ olsun.

1) Eğer $supp\left(\Phi(\alpha)\right) = supp\left(\Phi(\beta)\right)$ ise $w_L(\alpha) = w_L(\beta)$ olur.

2) $R_{q,2}$ halkasında iki ideal $\langle\alpha\rangle$ ve $\langle\beta\rangle$ olsun. O zaman $\langle\alpha\rangle = \langle\beta\rangle$ olması için gerek ve yeter şart $supp\left(\Phi(\alpha)\right) = supp\left(\Phi(\beta)\right)$ olmasıdır.

İspat: İspat Tanım 3.9'dan elde edilir.

Teorem 3.11 $R_{q,2}$ temel ideal halkasıdır ve $R_{q,2}$ halkasının sonlu üretilmiş bir ideali $I = \langle\alpha_1, \alpha_2, \ldots, \alpha_s\rangle$ ise $supp\left(\Phi(\beta)\right) = \bigcup_{i=1}^{s} supp\left(\Phi(\alpha_i)\right)$ olmak üzere $I = \langle\beta\rangle$ temel idealidir.

İspat: $R_{q,2}$ halkasının sonlu üretilmiş bir ideali $I = \langle\alpha_1, \alpha_2, \ldots, \alpha_s\rangle$ olsun. $F_q^{q^2}$ halkası üzerinde $\eta \in F_q^{q^2}$ olmak üzere $\Phi(I) = \left\langle\Phi(\alpha_1), \Phi(\alpha_2), ..., \Phi(\alpha_s)\right\rangle = \langle\eta\rangle$ olur. $\beta = \Phi^{-1}(\eta)$ olarak alınırsa sonuç elde edilir.

Örnek 3.12 $R_{3,2}$ üzerinde $\alpha_1 = u$ ve $\alpha_2 = v$ olsun. $I = \langle\alpha_1, \alpha_2\rangle = \langle\beta\rangle$ ideali

$supp(\Phi(\alpha_1)) = supp(\Phi(u)) = supp\left(\{0,1,2,0,1,2,0,1,2\}\right) = \{2,3,5,6,8,9\}$,

$supp(\Phi(\alpha_2)) = supp\left(\Phi(v)\right) = supp\left(\{0,0,0,1,1,1,2,2,2\}\right) = \{4,5,6,7,8,9\}$ ve

$supp\left(\Phi(\beta)\right) = \bigcup_{i=1}^{2} supp\left(\Phi(\alpha_i)\right) = \{2,3,4,5,6,7,8,9\}$ ve $\Phi\left(u^2 + v^2\right) = (0,1,1,1,2,2,1,2,2)$ olduğu için $\beta = u^2 + v^2 \in R_{3,2}$ olarak alınabilir.

Aşağıdaki teoremde $R_{q,2}$ halkasının tüm maksimal idealleri karakterize edilmektedir.

Teorem 3.13 F_q sonlu cisminin bir ilkel elemanı w olsun. $R_{q,2}$ halkasının tüm maksimal idealleri $u_i \in \left\{u, u-1, u-w, \ldots, u-w^{q-2}\right\}$ ve $v_j \in \left\{v, v-1, v-w, \ldots, v-w^{q-2}\right\}$ olmak üzere $\left\langle u_i, v_j\right\rangle$ olur. Ayrıca her maksimal idealin eleman sayısı q^{q^2-1} olur**.**

İspat: w, F_q sonlu cisminin ilkel elemanı olmak üzere $u_i \in \{u, u-1, u-w, \ldots, u-w^{q-2}\}$ ve $v_j \in \{v, v-1, v-w, \ldots, v-w^{q-2}\}$ olsun. $R_{q,2} \Big/ \left\langle u_i, v_j\right\rangle \cong F_q$ olduğu için $\left\langle u_i, v_j\right\rangle$ ideali $R_{q,2}$

halkasının maksimal idealidir. F_q sonlu cisminin idealleri sadece aşikar idealleri olduğu için $R_{q,2}$ halkasının idealleri aşikar ideallerin direkt toplamından oluşur. Böylece maksimal ideallerin sayısı q^2 ve eleman sayısı q^{q^2-1} olur.

Örnek 3.14 $\mathrm{R}_{3,2}$ halkasının tüm maksimal idealleri:

- $\langle u, v\rangle = \langle u^2 + v^2\rangle$,
- $\langle u, v-1\rangle = \langle 1 + v + u^2 + v^2\rangle$,
- $\langle u, v-2\rangle = \langle 1 + 2v + u^2 + v^2\rangle$,
- $\langle u-2, v-2\rangle = \langle 2 + 2u + 2v + u^2 + v^2\rangle$,
- $\langle u-1, v\rangle = \langle 1 + u + u^2 + v^2\rangle$,
- $\langle u-1, v-1\rangle = \langle 2 + u + v + u^2 + v^2\rangle$,
- $\langle u-1, v-2\rangle = \langle 2 + u + v + u^2 + v^2\rangle$,
- $\langle u-2, v\rangle = \langle 1 + 2u + u^2 + v^2\rangle$,
- $\langle u-2, v-1\rangle = \langle 2 + 2u + u^2 + v + v^2\rangle$

olur.

Tanım 3.15 $a \in R_{q,2}$ olmak üzere a elemanın **Hamming ağırlığı** a elemanı sıfırdan farklı ise 1 aksi durumda 0 olarak tanımlanır ve $w(a)$ ile gösterilir. İlaveten, $a = (a_1, a_2, \ldots, a_n) \in R_{q,2}^n$ olmak üzere a elemanın **Hamming ağırlığı** $w(a) = \sum_{i=1}^{n} w(a_i)$ olarak tanımlanır.

Tanım 3.16 $R_{q,2}$ halka ve $a = (a_0, a_1, ..., a_{n-1})$, $b = (b_0, b_1, ..., b_{n-1}) \in R_{q,2}^n$ olsun. a ve b elemanları arasındaki **Hamming uzaklık** $d_H(a,b) = w_H(a-b)$ olarak tanımlanır.

Tanım 3.17 $R_{q,2}$ halka ve $a \in R_{q,2}$ olmak üzere a elemanın **Lee ağırlığı** Gray görüntüsünün Hamming ağırlığı olarak tanımlanır ve $\mathrm{w}_L(a)$ ile gösterilir. Yani,

$\mathrm{w}_L(a) = w(\Phi(a))$.

Özellik 3.18 $\alpha \in R_{q,2}$ olmak üzere $I = \langle \alpha \rangle$ olsun.

1. $w_L(\alpha) = q^2$ ise α birimsel elemandır.

2. $| I | = q^{w_L(\alpha)}$.

İspat:

1. Önerme 3.8 de $R_{q,2} \cong F_q^{q^2}$ ve $F_q^{q^2}$ halkasının sıfır bölen olmayan elemanları bileşenlerinde sıfır elemanını içermeyen elemanlardır. Bu elemanların Lee ağırlıkları q^2 olur. Böylece ispat tamamlanır.

2. $F_q^{q^2}$ halkasının ideallerini listelemek kolaydır. α elemanı ve $\Phi(\alpha)$ elemanı izomorfik idealleri üretir. $I = \langle \alpha \rangle$ idealinin eleman sayısı $\Phi(I)$ idealinin eleman sayısına eşittir ve bu sayı $F_q^{q^2}$ halkasında $\Phi(\alpha)$ elemanının sıfırdan farklı bileşen yerlerinin sayısına bağlıdır. $F_q^{q^2}$ üzerinde $|\Phi(I)| = q^{w_L(\alpha)}$ olur. Böylece ispat tamamlanır.

Φ dönüşümünün tersi $F_q^{q^2}$ halkasından $R_{q,2}$ halkasına tanımlanmaktadır. Örneğin, $q = 3$ için;

$$\Phi^{-1}(x, y, z, t, m, n, q, p, r) = x + (2y + z)u + 2(x + y + z)u^2 + (2t + q)v + 2(x + t + q)v^2 +$$

$$(m + 2n + 2p + r)uv + (y + 2z + m + 2n + p + 2r)uv^2 + (t + m + n + 2(p + q + r))u^2v +$$

$$(x + y + z + t + m + n + q + p + r)u^2v^2 \in R_{3,2}$$

elde edilir.

Tanım 3.19 [14] Bir R halkasında $e^2 = e$ şartını sağlayan $e \in R$ elemanına **idempotent eleman** denir. R halkasında e ve f idempotent elemanları için $ef = 0$ ise bu

elemanlara **dik idempotent elemanlar** denir. Ayrıca her $r \in R$ için $er = re = 0$ ise $e \in R$ idempotent elemanına **değişmeli (merkezi) dik eleman** denir.

Her $1 \le i \le n$ için $e_i^2 = e_i$, $1 = \sum_{i=1}^{n} e_i$ ve her $i \ne j$ için $e_i e_j = e_j e_i = 0$ şartlarını sağlayan $\{e_1, \ldots, e_n\} \in R$ elemanlarına **merkezi dik idempotent elemanlar** denir.

Eğer $R \cong R_1 \times R_2 \times \ldots \times R_n$ ve $1 \le j \le n$ için e_j elemanı R_j halkasının birimsel elemanı ise $\{e_{1,} e_2, \ldots, e_n\}$ elemanları toplamları 1 olan ikişerli ikişerli aralarında dik merkezi idempotent elemanların kümesi olur. Tersine, toplamları 1 olan ikişerli ikişerli aralarında dik merkezi idempotent elemanların kümesi $\{e_1, e_2, \ldots, e_n\}$ verildiğinde $R \cong R_1 \times R_2 \times \ldots \times R_n$ ve $R_i = Re_i$ olacak biçimde bir ayrışım vardır.

$R_{q,2}$ halkasının ayrışımını yapabilmek için istenilen idempotent elemanlar F_q sonlu cisminin bir ilkel elemanı w olmak üzere tüm $0 \le i \le q-2$ için $j_{1_i} = u + w^i$, $j_{2_i} = v + w^i$, $\vartheta_i = \dfrac{u^q - u}{j_{1_i}}$, $\upsilon_i = \dfrac{v^q - v}{j_{2_i}}$ ve $\vartheta_{q-1} = \dfrac{u^q - u}{u}$, $\upsilon_{q-1} = \dfrac{v^q - v}{v}$ ile gösterilirse $0 \le i, j \le q-1$ için $\eta_{i,j} = \vartheta_i \upsilon_j$, $R_{q,2}$ halkasının ikişerli ikişerli aralarında dik merkezi idempotent elemanlarıdır.

$R_{q,2}$ halkasının bu özellikleri sağlayan tam olarak q^2 tane elemanı vardır. Böylece, tüm $0 \le i, j \le q-1$ için $\eta_{i,j} = \vartheta_i \upsilon_j$ olmak üzere $R_{q,2} = \eta_{0,0} F_q \oplus \eta_{0,1} F_q \oplus \cdots \oplus \eta_{q-1,q-1} F_q$ olur. $R_{q,2}$ halkası F_q-modül ve her $c \in R_{q,2}$ için $\Phi_{i,j}(c) = \left(\phi_1\left(\phi_2(c)[j]\right)\right)[i]$ $c = \sum_{j=0}^{q-1} \sum_{i=0}^{q-1} \eta_{i,j} \Phi_{i,j}(c)$ tek türlü olarak yazılmaktadır. Kısalığın hatırı için $c = \sum_{j=0}^{q-1} \sum_{i=0}^{q-1} \eta_{i,j} \Phi_{i,j}(c) = \sum_{t=1}^{q^2} e_t \Phi_t(c)$ olmak üzere $0 \le i, j \le q-1$ ve $1 \le t \le q^2$ için $\eta_{i,j} = e_t$ olarak alınmaktadır.

Örnek 3.20

$e_1 = 1+2u^2+2v^2+u^2v^2, \quad e_2 = 2uv+2u^2v+uv^2+u^2v^2, \quad e_3 = u+2u^2+2uv^2+u^2v^2,$
$e_4 = 2v+u^2v+2v^2+u^2v^2, \quad e_5 = uv+u^2v+uv^2+u^2v^2, \quad e_6 = 2uv+u^2v+2uv^2+u^2v^2,$
$e_7 = v+2u^2v+2v^2+u^2v^2, \quad e_8 = 2uv+2u^2v+uv^2+u^2v^2, \quad e_9 = uv+2u^2v+2uv^2+u^2v^2,$

elemanları $R_{3,2}$ halkasında $1=\sum_{i=1}^{9} e_i$ ve her $i \neq j \quad (1 \le i, j \le 9)$ için $e_i e_j = e_j e_i = 0$

özelliklerini sağladığı için $R_{3,2} = \sum_{i=1}^{9} e_i F_3$ şeklinde ayrıştırılabilir. Yani, her $x \in R_{3,2}$

elemanı $x = \sum_{j=0}^{2}\sum_{i=0}^{2} \eta_{i,j}\Phi_{i,j}(c)$ şeklinde tek türlü ifade edilebilir. Örneğin;

$$\underbrace{1+u+v+uv+u^2v+2v^2+2uv^2}_{x} = \underset{\Phi_{0,0}(x)}{\underbrace{1}}\underbrace{\left(1+2u^2+2v^2+u^2v^2\right)}_{e_1} + \underset{\Phi_{1,0}(x)}{\underbrace{2}}\underbrace{\left(2u+2u^2+uv^2+u^2v^2\right)}_{e_2} +$$
$$\underset{\Phi_{2,0}(x)}{\underbrace{0}}\underbrace{\left(u+2u^2+2uv^2+u^2v^2\right)}_{e_3} + \underset{\Phi_{0,1}(x)}{\underbrace{1}}\underbrace{\left(2v+u^2v+2v^2+u^2v^2\right)}_{e_4} + \underset{\Phi_{1,1}(x)}{\underbrace{0}}\underbrace{\left(uv+u^2v+uv^2+u^2v^2\right)}_{e_5} +$$
$$\underset{\Phi_{2,1}(x)}{\underbrace{1}}\underbrace{\left(2uv+u^2v+2uv^2+u^2v^2\right)}_{e_6} + \underset{\Phi_{0,2}(x)}{\underbrace{2}}\underbrace{\left(v+2u^2v+2v^2+u^2v^2\right)}_{e_7} + \underset{\Phi_{1,2}(x)}{\underbrace{0}}\underbrace{\left(2uv+2u^2v+uv^2+u^2v^2\right)}_{e_8} +$$
$$\underset{\Phi_{2,2}(x)}{\underbrace{2}}\underbrace{\left(uv+2u^2v+2uv^2+u^2v^2\right)}_{e_9} \in R_{3,2}$$

şeklinde tek türlü yazılmaktadır.

Örnek 3.21 F_9 cisminin bir ilkel elemanı w olmak üzere

$$\prod_{\substack{i=0,\\ i\neq 7}}^{7}\left(u-w^i\right)\prod_{\substack{i=0,\\ i\neq 7}}^{7}\left(v-w^i\right) = u^8v^8+u^8v^7w+u^8v^7+u^8v^6w+2u^8v^6+2u^8v^5w+2u^8v^4+2u^8v^3w+$$
$$2u^8v^3+2u^8v^2w+u^8v^2+u^8vw+u^7v^8w+u^7v^8+u^7v^7w+2u^7v^7+2u^7v^6w+2u^7v^5+2u^7v^4w+$$
$$2u^7v^4+2u^7v^3w+u^7v^3+u^7v^2w+u^7v+u^6v^8w+2u^6v^8+2u^6v^7w+2u^6v^6+2u^6v^5w+2u^6v^5+$$
$$2u^6v^4w+u^6v^4+u^6v^3w+u^6v^2+u^6vw+u^6v+2u^5v^8w+2u^5v^7+2u^5v^6w+2u^5v^62u^5v^5w+u^5v^5+$$
$$u^5v^4w+u^5v^3+u^5v^2w+u^5v^2+u^5vw+2u^5v+2u^4v^8+2u^4v^7w+2u^4v^7+2u^4v^6w+u^4v^6+u^4v^5w+$$
$$u^4v^4+u^4v^3w+u^4v^3+u^4v^2w+2u^4v^2+2u^4vw+2u^3v^8w+2u^3v^8+2u^3v^7w+u^3v^7+u^3v^6w+u^3v^5+$$
$$u^3v^4w+u^3v^4+u^3v^3w+2u^3v^3+2u^3v^2w+2u^3v+2u^2v^8w+u^2v^8+u^2v^7w+u^2v^6+u^2v^5w+u^2v^5+$$
$$u^2v^4w+2u^2v^4+2u^2v^3w+2u^2v^2+2u^2vw+2u^2v+uv^8w+uv^7+uv^6w+uv^6+uv^5w+2uv^5+$$
$$2uv^4w+2uv^3+2uv^2w+2uv^2+2uvw+uv$$

$R_{9,2}$ halkasının bir merkezi idempotent elemanıdır.

3.2 $R_{q,2}$ Halkası Üzerinde Tanımlı Lineer Kodlar

Tanım 3.22 $R_{q,2}$ üzerinde n uzunluğunda bir C **lineer kodu** $R_{q,2}^n$ modülünün bir $R_{q,2}$-alt modülüdür.

Tanım 3.23 $R_{q,2}$ üzerindeki n uzunluğundaki C lineer kodunun **duali** $C^{\perp} = \{c^* \in R_{q,2}^n \mid \langle c, c^* \rangle = 0 \text{ , her } c \in C \quad \text{için}\}$ olarak tanımlanmaktadır. Burada $\langle c, c^* \rangle$, $R_{q,2}^n$ halkasında c ve c^* elemanlarının standart Öklid iç çarpımıdır.

Sonlu cisimler üzerinde bir lineer kodun minimal üreteç kümesi matris ile temsil edilebilir. Fakat halkalar üzerinde lineer kodlar tabana sahip olmadığı için üreteç kümesini bu şekilde ifade etmek zor bir problemdir, hatta imkansız olabilir. $Z_2 + uZ_2$ ve $Z_2 + uZ_2 + u^2Z_2 + ... + u^kZ_2$ halkaları sonlu zincir halkaları, yani; idealleri kapsamaya göre zincir oluşturan halka olup sonlu zincir halkalarında minimal üreteç kümeleri için de üreteç matrisi tanımlanmıştır. $R_{q,2}$ zincir halkası olmadığı için üreteç matrisi kolay bir şekilde elde edilememektedir. Burada kodun Gray dönüşümü altındaki görüntüsü için üreteç matrisi tanımlanacaktır.

Teorem 3.24 $R_{q,2}$ üzerinde n uzunluğunda bir C lineer kodu için üreteç kümesi $g_i = (g_{i1}, g_{i2}, ..., g_{in})$ olmak üzere $\{g_1, g_2, ..., g_k\} \subset R_{q,2}^n$ olsun. O halde,

$$\Phi(G)=\begin{bmatrix} \Phi(g_{11}) & \Phi(g_{12}) & \dots & \Phi(g_{1n-1}) & \Phi(g_{1n}) \\ \Phi(vg_{11}) & \Phi(vg_{12}) & \dots & \Phi(vg_{1n-1}) & \Phi v(g_{1n}) \\ \dots & \dots. & \dots & \dots & \dots. \\ \Phi(v^{q-1}g_{11}) & \Phi(v^{q-1}g_{12}) & \dots & \Phi(v^{q-1}g_{1n-1}) & \Phi(v^{q-1}g_{1n}) \\ \Phi(ug_{11}) & \Phi(ug_{12}) & \cdots & \Phi(ug_{1n-1}) & \Phi(ug_{11}) \\ \dots. & \dots & \dots & \dots & \dots \\ \Phi(g_{21}) & \Phi(g_{21}) & \dots & \Phi(g_{2n-1}) & \Phi(gn) \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \Phi(u^{q-1}v^{q-1}g_{k1}) & \Phi(u^{q-1}v^{q-1}g_{k2}) & \dots & \Phi(u^{q-1}v^{q-1}g_{kn-1}) & \Phi(u^{q-1}v^{q-1}g_{kn}) \end{bmatrix}_{kq^2\times n}$$

matrisi $\Phi(C)$ kodunu üretmektedir.

İspat: $R_{q,2}$ üzerinde n uzunluğunda bir C lineer kodu için üreteç kümesi $g_i=(g_{i1},g_{i2},...,g_{in})$ olmak üzere $\{g_1, g_2,..., g_k\}\subset R_{q,2}^n$ olsun. C kodunun tanımından $R_{q,2}$-alt modüldür. $F_q\subseteq R_{q,2}$ olduğu için C kodu F_q- alt modül olarak da görülebilir. İlaveten, $\{g_1,ug_1,...,vg_1,...,u^{q-1}v^{q-1}g_1,...,g_k,ug_k,...,u^{q-1}v^{q-1}g_k\}$ üreteç kümesi ile C kodu F_q- alt modüldür. $\Phi(C)$ kodu $\{\Phi(g_1),\Phi(ug_1),...,\Phi(vg_1),...,\Phi(u^{q-1}v^{q-1}g_1),...,\Phi(g_k),$ $\Phi(ug_k),...,\Phi(u^{q-1}v^{q-1}g_k)$ ile F_q alt modül olarak üretilmektedir.

Tanım 3.25 $R_{q,2}$ üzerinde n uzunluğunda C lineer kodu için üreteç kümesi $g_i=(g_{i1},g_{i2},...,g_{in})$ olmak üzere $\{g_1,\ g_2,...,\ g_k\}\subseteq R_{q,2}^n$ olsun.

$$\{\Phi(g_1),\Phi(ug_1),...,\Phi(u^{q-1}g_1),\Phi(vg_1),...,\Phi(uvg_1),...,\Phi(uv^{q-1}g_1),...,\Phi(u^{q-1}v^{q-1}g_1),\Phi(g_2),$$
$$...,\Phi(u^{q-1}v^{q-1}g_2),...,\Phi(u^{q-1}v^{q-1}g_k)\}\subset F_q^{q^2n}$$

kümesi F_q lineer bağımsız ise $\{g_1,\ g_2,...,\ g_k\}\subset R_{q,2}^n$ kümesine n uzunluğundaki bir C lineer kodu için **minimal lineer bağımsız üreteç kümesi** denir.

Teorem 3.26 $\{g_1, g_2,..., g_k\}\subseteq R_{q,2}^n$ minimal lineer bağımsız üreteç kümesi olmak üzere $C=\langle\{g_1, g_2,..., g_k\}\rangle$ ise $|C|=q^{q^2k}$ olarak elde edilir.

İspat: $\{g_1, g_2,..., g_k\} \subseteq R_{q,2}^n$ minimal lineer bağımsız üreteç kümesi olmak üzere $C = \langle \{g_1, g_2,..., g_k\} \rangle$ olsun. $R_{q,2}$ halkasında lineer bağımsız her bir eleman q^{q^2} eleman üretmektedir. Böylece k minimal lineer bağımsız eleman olduğu için C kodunda $q^{q^2 k}$ tane eleman vardır.

3.2.1 $R_{q,2}$ Halkası Üzerinde Tanımlı Lineer Kodun Duali

Bu alt bölümde Gray dönüşüm yardımıyla tanımlanan bir iç çarpım ile lineer kodun duali tanımlanmaktadır. Ayrıca, kodun duali ile Gray görüntüsü arasındaki ilişki bir özellik olarak verilmektedir. $g_i = g_{i1} + ug_{i2} + u^2 g_{i2} + ... + u^{q-1} g_{iq} + vg_{i(q+1)} + ... + u^{q-1} v^{q-1} g_{iq^2}$

ve $h_i = h_{i1} + uh_{i2} + u^2 h_{i2} + ... + u^{q-1} h_{iq} + vh_{i(q+1)} + ... + u^{q-1} v^{q-1} h_{iq^2}$

olmak üzere $g = (g_1, g_2,..., g_n)$, $h = (h_1, h_2,..., h_n) \in R_{q,2}^n$ elemanları ve $j,k \in F_q$ için

$g_i(j,k) := g_{i1} + jg_{i2} + j^2 g_{i2} + ... + j^{q-1} g_{iq} + kg_{i(q+1)} + ... + j^{q-1} k^{q-1} g_{iq^2}$,

$h_i(j,k) := h_{i1} + jh_{i2} + j^2 h_{i2} + ... + j^{q-1} h_{iq} + kh_{i(q+1)} + ... + j^{q-1} k^{q-1} h_{iq^2}$

tanımlansın. Böylece $\langle g,h \rangle_\Phi = \sum_{i=1}^{n} \sum_{j,k \in F_q} g_i(j,k), h_i(j,k)$ iç çarpımı tanımlanmaktadır.

Tanım 3.27 $R_{q,2}$ üzerinde n uzunluğunda C lineer kodunun duali $C^\perp = \left\{ c^* \in R_{q,2}^n \mid \langle c, c^* \rangle_\Phi = 0, \quad \text{her } c \in C \quad \text{için} \right\}$ olarak tanımlanır.

Özellik 3.28 $R_{q,2}$ halkası üzerinde bir lineer kod C ve $C^\perp \subseteq C$ ise $\Phi(C)^\perp \subseteq \Phi(C)$ olur.

İspat: $\Phi(C^\perp) = \Phi(C)^\perp$ ve $C^\perp \subseteq C$ olduğu için $\Phi(C)^\perp = \Phi(C^\perp) \subseteq \Phi(C)$ elde edilir**.**

Özellik 3.29 $R_{q,2}$ üzerinde n uzunluğunda bir lineer kod C olsun. O halde, $1 \le i \le q^2$ için C_i kodu F_q üzerinde lineer kod olmak üzere $C = \sum_{i=1}^{q^2} e_i C_i$ şeklinde tek türlü yazılabilir. Böylece, C kodu F_q- modül olur.

İspat: Tanım 3.19'dan halkadaki her eleman idempotent elemanların ve Gray görüntülerinin bileşenleri ile tek türlü yazılabildiği için C kodu da F_q- modül olarak $C=\sum_{i=1}^{q^2} e_i C_i$ şeklinde tek türlü yazılabilir.

Örnek 3.30

$$C=\left\langle \left(1+2u^2+2v^2+u^2v^2, 2uv+2u^2v+uv^2+u^2v^2, 2uv+u^2v+2uv^2+u^2v^2\right)\right\rangle =$$

$$\{(0,0,0),(0,0,2uv+u^2v+2uv^2+u^2v^2),(0,0,uv+2u^2v+uv^2+2u^2v^2),$$
$$(0,2uv+2u^2v+uv^2+u^2v^2,0),(0,2uv+2u^2v+uv^2+u^2v^2,2uv+u^2v+2uv^2+u^2v^2),$$
$$(0,2uv+2u^2v+uv^2+u^2v^2,uv+2u^2v+uv^2+2u^2v^2),(2+u^2+v^2+2u^2v^2,0,0),$$
$$(0,uv+u^2v+2uv^2+2u^2v^2,0),(0,uv+u^2v+2uv^2+2u^2v^2,2uv+u^2v+2uv^2+u^2v^2),$$
$$(0,uv+u^2v+2uv^2+2u^2v^2,uv+2u^2v+uv^2+2u^2v^2),(1+2u^2+2v^2+u^2v^2,0,0),$$
$$(1+2u^2+2v^2+u^2v^2,0,2uv+u^2v+2uv^2+u^2v^2),(1+2u^2+2v^2+u^2v^2,0,uv+2u^2v+uv^2+2u^2v^2),$$
$$(1+2u^2+2v^2+u^2v^2,2uv+2u^2v+uv^2+u^2v^2,0),(2+u^2+v^2+2u^2v^2,2uv+2u^2v+uv^2+u^2v^2,0),$$
$$(1+2u^2+2v^2+u^2v^2,2uv+2u^2v+uv^2+u^2v^2,2uv+u^2v+2uv^2+u^2v^2),$$
$$(1+2u^2+2v^2+u^2v^2,2uv+2u^2v+uv^2+u^2v^2,uv+2u^2v+uv^2+2u^2v^2),$$
$$(1+2u^2+2v^2+u^2v^2,uv+u^2v+2uv^2+2u^2v^2,0),(2+u^2+v^2+2u^2v^2,uv+u^2v+2uv^2+2u^2v^2,0),$$
$$(2+u^2+v^2+2u^2v^2,0,uv+2u^2v+uv^2+2u^2v^2),(2+u^2+v^2+2u^2v^2,0,2uv+u^2v+2uv^2+u^2v^2),$$
$$(1+2u^2+2v^2+u^2v^2,uv+u^2v+2uv^2+2u^2v^2,2uv+u^2v+2uv^2+u^2v^2),$$
$$(1+2u^2+2v^2+u^2v^2,uv+u^2v+2uv^2+2u^2v^2,uv+2u^2v+uv^2+2u^2v^2),$$
$$(2+u^2+v^2+2u^2v^2,2uv+2u^2v+uv^2+u^2v^2,2uv+u^2v+2uv^2+u^2v^2),$$
$$(2+u^2+v^2+2u^2v^2,2uv+2u^2v+uv^2+u^2v^2,uv+2u^2v+uv^2+2u^2v^2),$$
$$(2+u^2+v^2+2u^2v^2,uv+u^2v+2uv^2+2u^2v^2,2uv+u^2v+2uv^2+u^2v^2),$$
$$(2+u^2+v^2+2u^2v^2,uv+u^2v+2uv^2+2u^2v^2,uv+2u^2v+uv^2+2u^2v^2)\}$$

$R_{3,2}$ üzerinde 3 uzunluğunda bir lineer kod olsun. Burada

$C_1=\langle(1,0,0,0,0,0,0,0,0)\rangle$, $C_6=\langle(0,0,0,0,0,1,0,0,0)\rangle$, $C_8=\langle(0,0,0,0,0,0,0,1,0)\rangle$ ve

$C_2=C_3=C_4=C_5=C_7=C_9=\langle(0,0,0,0,0,0,0,0,0)\rangle$ olmak üzere $C=\sum_{i=1}^{9} e_i C_i$ olur.

Sonuç 3.31 $R_{q,2}$ üzerinde n uzunluğunda bir lineer kod C olsun. $1 \le i \le q^2$ için F_q üzerinde lineer kod C_i olmak üzere $C = \sum_{i=1}^{q^2} e_i C_i$ kodunun duali $C^{\perp} = \sum_{i=1}^{q^2} e_i C_i^{\perp}$ kodudur.

İspat: $1 \le i \le q^2$ için F_q üzerinde lineer kod C_i olmak üzere $R_{q,2}$ üzerinde n uzunluğunda bir lineer kod $C = \sum_{i=1}^{q^2} e_i C_i$ olup $1 \le i \le q^2$ için F_q üzerinde C_i kodunun duali literatürden iyi bilinmektedir. $1 \le i \le q^2$ için $e_i^2 = e_i$, $e_i e_j = e_j e_i = 0$ olup her $c \in C_i$ ve $c^* \in C_i^{\perp}$ için $cc^* = c^* c = 0$ olduğu için $R_{q,2}$ üzerinde $C^{\perp}$ kodu F_q üzerinde $C_i^{\perp}$ kod yardımı ile $C^{\perp} = \sum_{i=1}^{q^2} e_i C_i^{\perp}$ kodu olarak elde edilir.

3.3 $R_{q,2}$ Halkası Üzerinde Tanımlı Devirli Kodlar

Bu bölümde $R_{q,2}$ halkası üzerindeki devirli kodlar tanımlanacaktır. Daha sonra bu devirli kod ailelerinden kendine dik olan devirli kodlar belirlenerek Gray görüntülerinden kuantum kodlar elde edilecektir.

Aşağıdaki teorem $R_{q,2}$ üzerindeki devirli kodların tam karakterizasyonunu vermektedir.

Teorem 3.32 $R_{q,2}$ üzerinde n uzunluğunda bir lineer kod $C = \sum_{i=1}^{q^2} e_i C_i$ olsun. $R_{q,2}$ üzerinde C devirli kod olması için gerek ve yeter şart F_q üzerinde $1 \le i \le q^2$ için C_i devirli kod olmasıdır.

İspat: Her $j = 0,...,n-1$ için $c_j = \sum_{i=1}^{q^2} e_i \Phi_i(c_j)$ olmak üzere $c = (c_0, c_1, ..., c_{n-1}) \in C$ olsun. σ, sağ deviri göstermek üzere F_q üzerinde devirli kod C_i olsun. O halde her $1 \le i \le q^2$ ve $0 \le j \le n-1$ için $\sigma(\Phi_i(c_j)) \in C_i$ olur. Böylece, $\sigma(c) = \sum_{i=1}^{q^2} e_i \sigma(\Phi_i(c_j)) \in C$ olur. Sonuç olarak, $R_{q,2}$ üzerinde C devirli koddur.

Aksine $c_i \in C_i$ ve $c_i = \sum_{j=1}^{q^2} e_j \Phi_j(c_i)$ olsun. O halde $\sigma(c) = \sum_{i=1}^{q^2} e_i \sigma\left(\Phi_i(c_j)\right) \in C$ kodunun Gray görüntüsü $\sigma(c) = (\sigma(c_1),...,\sigma(c_{n-1})) \in \otimes_{i=1}^{n-1} C_i$ olur. Yani, F_q üzerinde her $1 \le i \le q^2$ için C_i devirli koddur.

Sonuç 3.33 $R_{q,2}$ üzerinde n uzunluğunda bir devirli kod $C = \sum_{i=1}^{q^2} e_i C_i$ olsun. O halde C_i devirli kodunun üreteç polinomu $g_i(x)$ olmak üzere $C = \left\langle \sum_{i=1}^{q^2} e_i g_i(x) \right\rangle$ ve $|C| = q^{q^2 n - \sum_{i=1}^{q^2} deg(g_i(x))}$ olur.

İspat: F_q sonlu cismi üzerinde devirli kodların parametreleri üreteç polinomu $g(x)$ ile belirlenebildiği literatürden iyi bilinmektedir. $R_{q,2}$ halkası üzerinde n uzunluğunda bir $C = \sum_{i=1}^{q^2} e_i C_i$ devirli kod tüm elemanları F_q sonlu cisminin elemanları ve idempotent elemanlar ile tek türlü belirlidir. Böylece, üreteç polinomu da C_i devirli kodunun üreteç polinomu $g_i(x)$ ve idempotent elemanlar ile tek türlü belirlidir. O halde, $C = \left\langle \sum_{i=1}^{q^2} e_i g_i(x) \right\rangle$ olur ve $|C| = q^{q^2 n - \sum_{i=1}^{q^2} deg(g_i(x))}$ elde edilir.

3.3.1 $R_{q,2}$ Halkası Üzerinde Tanımlı Devirli Kodun Duali

Bu bölümde $R_{q,2}$ halkası üzerinde tanımlanan devirli kodun duali üreteç polinomları yardımı ile elde edilecektir.

Teorem 3.34 $R_{q,2}$ üzerinde n uzunluğunda bir devirli kod $C = \sum_{i=1}^{q^2} e_i C_i$ ve $1 \le i \le q^2$ için $C_i = \langle g_i(x) \rangle$ olsun. O halde $\Phi(C^\perp) = \otimes_{i=1}^{q^2} C_i^\perp$ ve $C^\perp = \sum_{i=1}^{q^2} e_i C_i^\perp$ olur.

İlaveten, $1 \le i \le q^2$ için $g_i(x)h_i(x) = x^n - 1$ ve $h_i^r(x)$, $h_i(x)$ polinomunun ters sıralı polinomu olmak üzere $\left|C^{\perp}\right| = q^{\sum_{i=1}^{q^2} deg(g_i(x))}$ olur.

İspat: Teorem 3.32, Sonuç 3.33 ve lineer kodların tek türlü yazılmasının bir sonucu olarak sonlu cisimler üzerindeki devirli kodların parametreleri iyi bilindiğinden ispat açıktır.

Örnek.3.35 F_4 üzerinde 7 uzunluğunda devirli kod üreten bazı polinomlar

$g_1(x) = g_6(x) = g_{11}(x) = g_{12}(x) = g_{15}(x) = g_{16}(x) = x+1,\ g_2(x) = g_3(x) = g_8(x) =$

$g_{13}(x) = 1+x+x^3,\ g_9(x) = 1+x^2+x^3,\ g_4(x) = g_5(x) = g_7(x) = g_{10}(x) = g_{14}(x) = 0$

olarak seçildiğinde

$e_1 = 1+u^3+v^3+u^3v^3,$

$e_2 = u+u^2+u^3+uv^3+u^2v^3+u^3v^3,$

$e_3 = u+u^3+uv^3+u^3v^3+uw+u^2w+uv^3w+u^2v^3w,$

$e_4 = u^2+u^3+u^2v^3+u^3v^3+uw+u^2w+uv^3w+u^2v^3w,$

$e_5 = v+u^3v+v^2+u^3v^2+v^3+u^3v^3,$

$e_6 = uv+u^2v+u^3v+uv^2+u^2v^2+u^3v^2+uv^3+u^2v^3+u^3v^3,$

$e_7 = uv+u^3v+uv^2+u^3v^2+uv^3+u^3v^3+uvw+u^2vw+uv^2w+u^2v^2w+uv^3w+u^2v^3w,$

$e_8 = u^2v+u^3v+u^2v^2+u^3v^2+u^2v^3+u^3v^3+uvw+u^2vw+uv^2w+u^2v^2w+uv^3w+u^2v^3w,$

$e_9 = v+u^3v+v^3+u^3v^3+vw+u^3vw+v^2w+u^3v^2w,$

$e_{10} = uv+u^2v+u^3v+uv^3+u^2v^3+u^3v^3+uvw+u^2vw+u^3vw+uv^2w+u^2v^2w+u^3v^2w,$

$e_{11} = u^2v+u^3v+uv^2+u^2v^2+uv^3+u^3v^3+uvw+u^3vw+u^2v^2w+u^3v^2w+uv^3w+u^2v^3w,$

$e_{12} = uv+u^3v+uv^2+u^2v^2+u^2v^3+u^3v^3+u^2vw+u^3vw+uv^2w+u^3v^2w+uv^3w+u^2v^3w,$

$e_{13} = v^2+u^3v^2+v^3+u^3v^3+vw+u^3vw+v^2w+u^3v^2w,$

$$e_{14} = uv^2 + u^2v^2 + u^3v^2 + uv^3 + u^2v^3 + u^3v^3 + uvw + u^2vw + u^3vw + uv^2w + u^2v^2w + u^3v^2w,$$

$$e_{15} = uv + u^2v + u^2v^2 + u^3v^2 + uv^3 + u^3v^3 + u^2vw + u^3vw + uv^2w + u^3v^2w + uv^3w + u^2v^3w\ ,$$

$$e_{16} = uv + u^2v + uv^2 + u^3v^2 + u^2v^3 + u^3v^3 + uvw + u^3vw + u^2v^2w + u^3v^2w + uv^3w + u^2v^3w$$

idempotent elemanlar olup $R_{4,2}$ üzerindeki 7 uzunluğunda devirli kod üreten

$$g(x) = (1 + u^2 + u^3 + v + uv + u^3v + v^2 + uv^2 + u^2v^2 + v^3 + uv^3 + uw + u^2w + u^2vw + u^3vw + uv^2w + u^3v^2w + uv^3w + u^2v^3w) + (1 + u^2 + u^3 + uv + v^2 + uv^2 + u^2v^2 + uv^3 + u^3v^3 + uw + u^2w + vw + u^2vw + v^2w + uv^2w + uv^3w + u^2v^3w)x + (v + u^3v + v^3 + u^3v^3 + vw + u^3vw + v^2w + u^3v^2w)x^2 + (u^2 + v + u^2v + v^2 + u^2v^2 + u^3v^3 + uw + u^2w + uvw + u^2vw + uv^2w + u^2v^2w)x^3$$

polinomu elde edilir ve ters sıralı polinomları

$$h_1^r(x) = h_6^r(x) = h_{11}^r(x) = h_{12}^r(x) = h_{15}^r(x) = h_{16}^r(x) = x + 1,$$
$$h_2^r(x) = h_3^r(x) = h_8^r(x) = h_{13}^r(x) = 1 + x^2 + x^3,$$
$$h_9^r(x) = 1 + x + x^3,\ h_4^r(x) = h_5^r(x) = h_7^r(x) = h_{10}^r(x) = h_{14}^r(x) = 0$$

olmak üzere dual kod

$$h^r(x) = 1 + u^2 + u^3 + v + u^2v + u^3v + v^2 + uv^2 + u^3v^2 + v^3 + u^3v^3 + uw + u^2w + (1 + u^2 + u^3 + u^2v + v^2 + uv^2 + u^3v^2 + uw + u^2w + vw + u^3vw + v^2w + u^3v^2w)x + \left(1 + u^2 + u^3 + v + u^2v + u^3v + v^2 + uv^2 + u^3v^2 + v^3 + u^3v^3 + uw + u^2w\right)x^2 + \left(1 + u^3 + v + uv^2 + u^2v^2 + u^3v^2 + u^3v^3 + vw + uvw + u^2vw + u^3vw + v^2w + uv^2w + u^2v^2w + u^3v^2w\right)x^3 + \left(1 + u^2 + u^3 + v + u^2v + u^3v + v^2 + uv^2 + u^3v^2 + v^3 + u^3v^3 + uw + u^2w\right)x^4 + \left(1 + u^3 + u^3v + uv^2 + u^2v^2 + u^3v^2 + v^3 + uvw + u^2vw + uv^2w + u^2v^2w\right)x^5 + \left(1 + u^3 + u^3v + uv^2 + u^2v^2 + u^3v^2 + v^3 + uvw + u^2vw + uv^2w + u^2v^2w\right)x^6$$

polinomu ile üretilmektedir.

3.4 $R_{q,2}$ Halkası Üzerindeki Devirli Kodlardan Kuantum Kod Elde Edilmesi

Bu bölümde $R_{q,2}$ halkası üzerindeki devirli kodlar yardımı ile F_q cismi üzerinde kuantum kodlar elde edilmektedir.

Tanım 3.36 [28, 29, 30] H iki boyutlu Hilbert uzayı olmak üzere $H^n = \underbrace{H \otimes H \otimes .... \otimes H}_{n}$, 2^n boyutlu Hilbert uzayıdır. Kuantum kodlar Hilbert uzayları üzerinde tanımlanmaktadır. $k < n$ olmak üzere 2^n boyutlu Hilbert uzayının 2^k boyutlu

alt uzayı n uzunluğunda **hata düzeltebilen bir kuantum kod** olarak tanımlanmaktadır ve kısaca $[\![n,k]\!]$ ile gösterilmektedir. Ayrıca, F_q alfabesi üzerinde tanımlanan $[\![n,k]\!]$ kuantum kod herhangi $\left\lfloor \frac{d-1}{2} \right\rfloor$ tane bit ya da faz hatası düzeltebiliyorsa $[\![n,k,d]\!]_q$ ile gösterilmektedir.

Kuantum kodlar pek çok farklı yöntemler ile elde edilebilmektedir. Bu çalışmada bunlardan bir tanesi verilip klasik hata düzeltebilen devirli kodlardan kuantum kod elde edilmektedir. Öncelikle, C_1 boyutu k_1 olan lineer kod ve C_2 boyutu k_2 olan alt uzay kodu olsun. C_1 kodunda C_2 alt kodunu kullanarak bir denklik bağıntısı aşağıdaki gibi tanımlanmaktadır:

$x, y \in C_1$ denk olması için gerek ve yeter şart $x = y + z$ olacak biçimde $z \in C_1$ var olmasıdır. Böylece C_2 kodunun C_1 kodundaki kosetleri denklik sınıflarıdır. Bu kosetler kuantum kodlar için tabanları tanımlamaktadır. Yani, u elemanı C_1 kodunda C_2 kodunun koset lideri olmak üzere $|v\rangle = \frac{1}{\sqrt{|C_2|}} \sum_u |u + C_1\rangle$ taban olarak alındığında kuantum kodlar elde edilebilmektedir. Burada, "$|\ \rangle$" ile ilk olarak Paul Adrien Maurice Dirac tarafından kullanılan dirac notasyonunda bir sütun vektörü belirtilmektedir. Sonuç olarak $k_2 - k_1$ koset sayısına eşit sayıda elemana sahip kuantum kod oluşturulmasına katkıda bulunmaktadır. Böylece C_1 lineer kodundaki klasik bit hatası düzeltimi kuantum koddaki bit hatası düzeltimine ve $C_2^{\perp}$ lineer kodundaki klasik hata düzeltimi de C kodundaki faz hatası düzeltimine denk olur. Sonuç olarak tüm bunlar ile birlikte CSS inşası denilen $[\![n, 2k_1 - n, d_1]\!]_q$ parametrelerine sahip kuantum kodu elde edilmektedir. Aşağıdaki teoremde [31, 32] çalışmalarında ifade edilen CSS inşası verilmektedir.

Teorem 3.37 [31, 32] (CSS İnşaası) C_1 ve C_2, F_q üzerinde sırası ile $[n, k_1, d_1]_q$ ve $[n, k_2, d_2]_q$ parametrelerine sahip iki lineer kod ve $C_2 \subseteq C_1$ olsun. O halde $d_2^{\perp}$, $C_2^{\perp}$ dual kodunun minimum uzaklığı olmak üzere $[\![n, k_1 - k_2, \min\{d_1, d_2^{\perp}\}]\!]_q$ parametrelerine

sahip hata düzeltebilen kuantum kod vardır. Ayrıca, $C_2 = C_1^{\perp}$ ise $[[n, 2k_1 - n, d_1]]_q$ parametrelerine sahip kuantum kod vardır.

Teorem 3.38 [32] F_q üzerinde $g(x)$ tarafından üretilen bir devirli kod C ve $g(x)h(x) = x^n - 1$ olsun.

$C^{\perp} \subseteq C$ ancak ve ancak $h(x)h^r(x) \equiv 0 \pmod{x^n - 1}$ (3. 5)

ya da denk olarak

$C^{\perp} \subseteq C$ ancak ve ancak $x^n - 1 \equiv 0 \pmod{g(x)g^r(x)}$ (3. 6)

elde edilir. Aşağıdaki teoremler $\Phi(C^{\perp}) = \Phi(C)^{\perp}$ eşitliğinden dolayı elde edilmektedir. Bu özellik $\mathrm{R}_{q,2}$ üzerinde kuantum kod elde etmek için kullanılmaktadır.

Teorem 3.39 F_q cismi üzerinde $1 \le i \le q^2$ için $x^n - 1$ polinomunun bir böleni $g_i(x)$ için $C_i = \langle g_i(x) \rangle$ olmak üzere $C = \left\langle g(x) = \sum_{i=1}^{q^2} e_i g_i(x) \right\rangle$ kodu $R_{q,2}$ üzerinde n uzunluğunda bir devirli kod olsun. O halde, $C^{\perp} \subseteq C$ olur ancak ve ancak her $1 \le i \le q^2$ için $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^r(x)}$ olur.

İspat: Her $1 \le i \le q^2$ için $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^r(x)}$ olsun. Teorem 3.38'den F_q üzerinde $1 \le i \le q^2$ için $C_i^{\perp} \subseteq C_i$ elde edilir. Buradan $C = \sum_{i=1}^{q^2} e_i C_i$ olduğu için $C^{\perp} \subseteq C$ olur.

Aksine $C^{\perp} \subseteq C$ olsun. O halde F_q cismi üzerinde $1 \le i \le q^2$ için $C_i^{\perp} \subseteq C_i$ elde edilir. Teorem 3.38'den her $1 \le i \le q^2$ için $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^r(x)}$ olur.

Sonuç 3.40 $R_{q,2}$ üzerinde n uzunluğunda bir devirli kod $C = \sum_{i=1}^{q^2} e_i C_i$ olsun. O halde $C^{\perp} \subseteq C$ olması için gerek ve yeter şart $1 \le i \le q^2$ için $C_i^{\perp} \subseteq C_i$ olmasıdır.

İspat: Teorem 3.39'dan açıktır.

Teorem 3.41 $1 \le i \le q^2$ için $C_i = \langle g_i(x) \rangle$ kodu F_q üzerinde n uzunluğunda bir devirli kod olmak üzere $R_{q,2}$ üzerinde n uzunluğunda bir devirli kod $C = \sum_{i=1}^{q^2} e_i C_i$ olsun. Eğer $C^{\perp} \subseteq C$ ise F_q üzerinde $[[q^2 n, q^2 n - 2t, d_L]]_q$ parametrelerine sahip kuantum kod vardır. Burada t ile tüm $g_i(x)$ polinomlarının dereceleri toplamı ve d_L ile C kodunun Lee uzaklığını gösterilmektedir.

İspat: Teorem 3.34 ve Teorem 3.39'un bir sonucu ve Φ Gray görüntüsünün dikliği ve uzaklığı koruma özelliklerinden ve CSS inşasından sonuç elde edilir.

Örnek 3.42 F_3 üzerinde $x^8 - 1 = (x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$ olur. $g_1(x) = g_3(x) = g_5(x) = g_6(x) = g_7(x) = x^2 + 2x + 2$ ve $g_2(x) = g_4(x) = g_8(x) = g_9(x) = x^2 + x + 2$ olarak seçildiğinde $R_{3,2}$ üzerinde C kodu $g(x) = 2 + (2 + u + u^2 + v + 2uv + 2u^2 v + v^2 + u^2 v^2)x + x^2$ polinomu tarafından üretilmektedir. Ayrıca $\Phi(C)$ kodu F_3 üzerinde $[72, 54, 2]_3$ parametrelerine sahiptir. Her $1 \le i \le 9$ için F_3 üzerinde $g_i(x) g_i^r(x) \mid x^8 - 1$ özelliğini sağladığı için $\Phi(C)^{\perp} \subseteq \Phi(C)$ olur. F_3 üzerinde CSS inşası ile $[[72, 36, 2]]_3$ parametrelerine sahip kuantum kod vardır.

Örnek 3.43 F_2 üzerinde $x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$ olur. F_2 üzerinde 7 uzunluğunda $C_1 = \langle g_1(x) = 1 + x^2 + x^3 \rangle$, $C_2 = \langle g_2(x) = (1 + x + x^3) \rangle$ ve $C_3 = \langle g_3(x) = 1 \rangle$ kodları kendine dik kodlardır. Böylece $R_{2,2}$ üzerinde tam olarak 81 tane kuantum kod inşa edilmektedir. Tüm denk olmayan kuantum kodları Çizelge 3. 1'deki parametreleri ile elde edilmektedir.

Çizelge 3.1 $R_{2,2}$ halkasından elde edilen F_2 üzerindeki kuantum kodlar

$g(x)$	$\Phi(C)$	Kuantum Kod
1	$[28, 28, 1]_2$	$[\![28, 28, 1]\!]_2$
$1+uvx+uvx^3$	$[28, 25, 1]_2$	$[\![28, 22, 1]\!]_2$
$1+uvx^2+uvx^3$	$[28, 25, 1]_2$	$[\![28, 22, 1]\!]_2$
$1+ux+ux^3$	$[28, 22, 1]_2$	$[\![28, 16, 1]\!]_2$
$1+(u+uv)x+uvx^2+ux^3$	$[28, 22, 1]_2$	$[\![28, 16, 1]\!]_2$
$1+ux^2+ux^3$	$[28, 22, 1]_2$	$[\![28, 16, 1]\!]_2$
$1+(u+v+uv)x+(u+v+uv)x^3$	$[28, 19, 1]_2$	$[\![28, 10, 1]\!]_2$
$1+(u+v)x+uvx^2+(u+v+uv)x^3$	$[28, 19, 1]_2$	$[\![28, 10, 1]\!]_2$
$1+x+x^3$	$[28, 16, 3]_2$	$[\![28, 4, 3]\!]_2$
$1+(1+uv)x+uvx^2+x^3$	$[28, 16, 3]_2$	$[\![28, 4, 3]\!]_2$
$1+(1+u)x+ux^2+x^3$	$[28, 16, 3]_2$	$[\![28, 4, 3]\!]_2$
$1+uvx+(1+uv)x^2+x^3$	$[28, 16, 3]_2$	$[\![28, 4, 3]\!]_2$
$1+x^2+x^3$	$[28, 16, 3]_2$	$[\![28, 4, 3]\!]_2$
$1+(1+u+v+uv)x+ux^2+(1+v+uv)x^3$	$[28, 19, 1]_2$	$[\![28, 10, 1]\!]_2$
$1+(u+v+uv)x^2+(u+v+uv)x^3$	$[28, 19, 1]_2$	$[\![28, 10, 1]\!]_2$

BÖLÜM 4

R_{v^2-v} HALKASI ÜZERİNDE LİNEER KODLAR

4.1 R_{v^2-v} Halkası Üzerinde Tanımlı Lineer Kodlar

Bu bölümde v değişkenli katsayıları F_4 cisminden alınan polinom halkası $F_4[v]$ olmak üzere $R_{v^2-v} := F_4 + vF_4 = F_4[v] \Big/ \langle v^2 - v \rangle$ halkasının cebirsel yapısına bakılarak, bu halka üzerindeki lineer, devirli ve sabit devirli kodların yapısı incelenmektedir. R_{v^2-v} halkası ile F_4^2 arasında uzaklığı koruyan özel bir dönüşüm olan Gray dönüşüm tanımlanmaktadır ve bu halka üzerinde değişmeli olmayan bir çarpık çarpma tanımlayarak bu çarpma işlemi ile tanımlı çarpık sabit devirli kodların tamamı karakterize edilmektedir.

$$R_{v^2-v} = F_4[v] \Big/ \langle v^2 - v \rangle = \{a + bv \,|\, a,b \in F_4, v^2 - v = 0\}$$

$$= \{(a_0 + a_1 w) + (b_0 + b_1 w)v \,|\, a_0, a_1, b_0, b_1 \in F_2, v^2 - v = 0\}$$

olur ve 16 elemana sahiptir.

Tanım 4.1 $\alpha = a + bv \in R_{v^2-v}$ ve sırası ile $i = 1$ ve $i = 0$ olmak üzere $\alpha(i) := a + bi \in F_4$ olsun. a, $b \in F_4$ olduğu için $a_0, a_1, b_0, b_1 \in F_2$ olmak üzere $a = a_0 + a_1 w$ ve $b = b_0 + b_1 w$ dur. O halde R_{v^2-v} halkasından F_4^2 halkasına bir dönüşüm aşağıdaki biçimde tanımlanır:

$\phi : R_{v^2-v} \to F_4^2$

$$\alpha \to \phi(\alpha) = \{\phi_1(\alpha), \phi_2(\alpha)\} = \{a_0 + b_0 + (a_1 + b_1)w, \quad (a_0 + a_1 w)\}.$$

ϕ dönüşümünün modül izomorfizma olduğu açıktır.

Böylece $R_{v^2-v} \cong F_4[v]/\langle v \rangle \oplus F_4[v]/\langle v-1 \rangle \cong F_4^2$ olur.

Aşağıdaki özellikler R_{v^2-v} halkası için sağlanmaktadır.

Özellik 4.2

1. R_{v^2-v} temel ideal halkasıdır.
2. R_{v^2-v} halkasının tam 4 ideali vardır.

İspat:

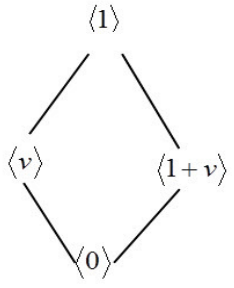
1. R_{v^2-v} halkasında sıfır bölen elemanlarının ürettiği temel ideal olmayan tek ideal $\langle v, 1+v \rangle$ ideali olup, aslında $\langle v, 1+v \rangle = \langle 1 \rangle$ ideali temel idealdir. O halde, R_{v^2-v} temel ideal halkasıdır.
2. R_{v^2-v} halkasının tüm idealleri incelendiğinde: $R_{v^2-v} = \langle 1 \rangle = \langle w \rangle = \langle w+1 \rangle = \ldots$

$= \langle 1 + v(1+w) + v^2(1+w) + v^3(1+w) \rangle$.

Maksimal idealler 4 elemanlıdır ve aşağıdaki gibi üretilmektedir:

- $\langle v \rangle = \langle vw \rangle = \langle v(1+w) \rangle = \{0, v, vw, v(1+w)\}$.
- $\langle 1+v \rangle = \langle (1+v)w \rangle = \langle (1+v)(1+w) \rangle = \{0, 1+v, (1+v)w, (1+v)(1+w)\}$.

Ayrıca $\langle 0 \rangle = \{0\}$ olur. Böylece tam olarak 4 tane ideal vardır.



Şekil 4.1 halkasının ideal şeması

Öte yandan ϕ dönüşümünün tersi

$\phi^{-1}: F_4^2 \to R_{v^2-v}$

$\{x, y\} = \{(x_0 + x_1 w), (y_0 + y_1 w)\} \to (y_0 + y_1 w) + ((x_0 + y_0) + (x_1 + y_1) w) v = y + (x + y) v$

olur.

Bölüm 3'te tanımı verilen destek kümesi kullanılarak temel ideallerin üreteç elemanlarının nasıl belirlendiği belirtmektedir.

Özellik 4.3 R_{v^2-v} halkasında sonlu üretilmiş bir ideal $I = \langle \alpha_1, \alpha_2, ..., \alpha_s \rangle$ olsun. O halde $supp(\phi(\beta)) = \bigcup_{i=1}^{s} supp(\phi(\alpha_i))$ olacak şekildeki bir $\beta \in R_{v^2-v}$ için $I = \langle \alpha_1, \alpha_2, ..., \alpha_s \rangle = \langle \beta \rangle$ olur.

İspat: R_{v^2-v} halkasının sonlu üretilmiş bir ideali $I = \langle \alpha_1, \alpha_2, \ldots, \alpha_s \rangle$ olsun. F_4^2 halkasında $\eta \in F_q^n$ olmak üzere $\Phi(I) = \langle \Phi(\alpha_1), \Phi(\alpha_2), ..., \Phi(\alpha_s) \rangle = \langle \eta \rangle$ olur. $\beta = \Phi^{-1}(\eta)$ olarak alınırsa sonuç elde edilir.

Örnek 4.4 $\alpha_2 = vw \in R_{v^2-v}$ olmak üzere $\phi(\alpha_1) = \{w, 1\}$ ve $\phi(\alpha_2) = \{w, 0\}$ olur. Dolayısı ile $supp(\phi(\alpha_1)) = \{1, 2\}$ ve $supp(\phi(\alpha_2)) = \{1\}$ olup $\{1, 2\} \cup \{1\}$ olduğu için $\beta = 1$ olarak alınabilir.

Özellik 4.5 $\alpha \in R_{v^2-v}$ olsun. Aşağıdaki ifadeler doğrudur:

1. $supp(\phi(\alpha)) = \{1, 2\}$ ise α birimsel elemandır. Dolayısı ile R_{v^2-v} halkasında 9 tane birimsel eleman vardır.

2. R_{v^2-v} halkasında bir ideal $I = \langle \alpha \rangle$ olsun. $|supp(\phi(\alpha))| = 1$ ise I maksimal idealdir. Böylece R_{v^2-v} halkasında 2 maksimal ideal vardır.

3. $|I| = q^{w_L(\alpha)}$ olur.

İspat:

1. F_4 cisminde sıfırdan farklı elemanlar birimsel olduğu için $supp(\phi(\alpha)) = \{1, 2\}$

olduğunda bu elemanlar R_{v^2-v} halkasında birimsel elemanlardır ve 9 tane birimsel eleman vardır.

2. R_{v^2-v} halkasındaki sıfır bölen elemanların Gray görüntülerinde en az bir sıfır bileşeni vardır. Yani, $\left|supp\left(\phi(\alpha)\right)\right|=1$ olur. Buradan α elemanının ürettiği ideal maksial idealdir. O halde R_{v^2-v} halkasında 2 maksimal ideal vardır.

3. F_4^2 halkasının ideallerini listelemek kolaydır. α elemanı ve $\Phi(\alpha)$ elemanı izomorfik idealleri üretir. $I=\langle\alpha\rangle$ idealinin eleman sayısı $\Phi(I)$ idealinin eleman sayısına eşittir ve bu sayı F_4^2 halkasında $\Phi(\alpha)$ elemanının sıfırdan farklı bileşen yerlerinin sayısına bağlıdır. F_4^2 üzerinde $\left|\Phi(I)\right|=q^{w_L(a)}$ olur. Böylece ispat tamamlanır.

R_{v^2-v} halkasının merkezi idempotent elemanları $e_1=v$ ve $e_2=1+v$ ve $R_{v^2-v}=\sum_{i=1}^{2}e_iF_4$ olup R_{v^2-v} halkası F_4-modüldür. Her $\alpha=a+bv\in R_{v^2-v}$ $(a,b\in F_4)$ için $\alpha=a+bv=(a+b)e_1+(a)e_2=\sum_{i=1}^{2}\phi_i(\alpha)e_i\in R_{v^2-v}$ şeklinde merkezi idempotent elemanlar aracılığıyla tek türlü olarak yazılmaktadır.

Örnek 4.6 $1+vw=\underbrace{(1+w)}_{\phi_1(1+vw)}(v)+\underbrace{(1)}_{\phi_2(1+vw)}(1+v)\in R_{v^2-v}$ olur.

A ve B iki lineer kod olsun. $\otimes$ ve $\oplus$ sırası ile aşağıdaki şekilde tanımlanmaktadır:

$A\otimes B=\{(a,b):a\in A,b\in B\}$ ve $A\oplus B=\{a+b:a\in A,b\in B\}$.

Tanım 4.7 [36] R_{v^2-v} üzerinde n uzunluğunda C **lineer kodu** $R_{v^2-v}^n$ modulünün bir alt $R_{v^2-v}-$modülüdür.

R_{v^2-v} üzerinde n uzunluğunda her C lineer kodunun üreteç matrisi bazı satır veya sütun işlemleri ve koordinatlar üzerindeki permütasyon işlemleri ile

$$G=\begin{bmatrix} I_{k_1} & (1+v)B_1 & vA_1 & (1+v)A_2+vB_2 & (1+v)A_3+vB_3 \\ 0 & vI_{k_2} & 0 & vA_4 & 0 \\ 0 & 0 & (1+v)I_{k_3} & 0 & (1+v)B_4 \end{bmatrix}$$

formuna sahiptir. Burada, $1\le i,j\le 4$ için A_i ve B_j matrisleri F_4 üzerinde tanımlı matrislerdir [36].

R_{v^2-v} üzerinde tanımlı bir lineer kod C olsun. Aşağıdaki ifadeler [36] çalışmasından elde edilmektedir.

$C_1=\{x+y\in F_4^n : x,y\in F_4^n \text{ için } (x+y)v+x(v+1)\in C\}$ ve

$C_2=\{x\in F_4^n : y\in F_4^n \text{için } (x+y)v+x(v+1)\in C\}$

olsun. O halde, $C=vC_1\oplus(1+v)C_2$ ve $|C|=16^{k_1}4^{k_2}4^{k_3}$ olur. Burada C_1 ve C_2 kodlarının F_4 üzerinde tanımlı n uzunluğunda lineer kodlar olduğuna dikkat edilmelidir.

Özellik 4.8 [36] R_{v^2-v} üzerinde n uzunluğunda lineer kod $C=vC_1\oplus(1+v)C_2$ ve $i=1,2$ için F_4 üzerinde $[n,k_i,d_H(C_i)]$ parametrelerine sahip lineer kod C_i olmak üzere $\phi(C)$ kodu $[2n,k_1+k_2,\min\{d_H(C_1),d_H(C_2)\}]$ parametrelerine sahip lineer koddur.

4.2 R_{v^2-v} Halkası Üzerinde Tanımlı Sabit Devirli Kodlar

Devirli kodları da içeren sabit devirli kod ailesi zengin cebirsel yapısı ve uygulamadaki avantajlarından dolayı önemli bir kod ailesidir. Sabit devirli kodların çözümlenmesi de oldukça pratiktir.

Tanım 4.9 R_{v^2-v} üzerinde n uzunluğunda bir lineer kod C ve $\alpha\in U_{R_{v^2-v}}$ birimsel elemanı için σ_1 otomorfizması altında değişmez kalırsa yani; her $c\in C$ için $\sigma_1(c_0,c_1,c_2,...,c_{n-1})=(\alpha c_{n-1},c_0,c_1,...,c_{n-2})$ şartını sağlarsa C koduna $\alpha-$**sabit devirli kod** denir.

Özel olarak $\alpha=1$ birimsel elemanı alındığında devirli kod elde edilmektedir.

Eğer $c=(c_1,c_2,...,c_{n-1})$ elemanı $\alpha-$sabit devirli kodun bir elemanı ise $R_{v^2-v}[x]$ üzerinde $c(x)=c_0+c_1x+c_2x^2+...+c_{n-1}x^{n-1}$ polinomu ile temsil edilebilir ve $c\in C$ için sağ sabit devirli öteleme $c(x)$ için $xc(x) \bmod (x^n-\alpha)$ çarpımına eşittir.

$R_{v^2-v,n} := R_{v^2-v}[x] \Big/ \langle x^n-\alpha \rangle$ olsun. $i=1,\ 2$ için iz düşüm dönüşümü

$$\begin{aligned} \pi_i : F_4 \otimes F_4 &\rightarrow F_4 \\ (a_1,a_2) &\rightarrow \pi_i(a_1,a_2) = a_i \end{aligned}$$

olarak tanımlanmaktadır.

$$L_n := F_4[x] \Big/ \langle x^n-(\pi_1(\phi(\alpha))) \rangle \otimes F_4[x] \Big/ \langle x^n-(\pi_2(\phi(\alpha))) \rangle$$

olmak üzere bu Gray dönüşüm aşağıdaki gibi genelleştirilir:

$$\begin{aligned} \phi : R_{v^2-v,n} &\rightarrow L_n \\ \phi\left(\sum_{i=0}^{n} a_i x^i\right) &\rightarrow \left(\sum_{i=0}^{n} \pi_1(\phi(a_i))x^i, \sum_{i=0}^{n} \pi_2(\phi(a_i))x^i\right) . \end{aligned}$$

Böylece, $R_{v^2-v}[x] \Big/ \langle x^n-\alpha \rangle \cong F_4[x] \Big/ \langle x^n-\pi_1(\phi(\alpha)) \rangle \otimes F_4[x] \Big/ \langle x^n-\pi_2(\phi(\alpha)) \rangle$ olur.

Sonuç olarak, $i=1,\ 2$ için $F_4[x] \Big/ \langle x^n-\pi_i(\phi(\alpha)) \rangle$ bölüm halkasının yapısı bilindiği için ϕ dönüşümü kullanılarak $R_{v^2-v}[x] \Big/ \langle x^n-\alpha \rangle$ bölüm halkasının yapısı dolayısı ile sabit devirli kodların yapısı elde edilmektedir.

Teorem 4.10 R_{v^2-v} üzerinde n uzunluğunda bir lineer kod $C=vC_1 \oplus (1+v)C_2$ olsun. C kodu R_{v^2-v} üzerinde n uzunluğunda $\alpha-$sabit devirli koddur ancak ve ancak C_1 ve C_2 sırası ile F_4 üzerinde n uzunluğunda $\pi_1(\phi(\alpha))$ ve $\pi_2(\phi(\alpha))-$sabit devirli koddur.

İspat: Her $i=0,1,...,n-1$ için $c_i=vx_i+(1+v)y_i=y_i+v(x_i+y_i)$ olmak üzere $c=(c_0,\ c_1,\ ...,\ c_{n-1})\in C$ olsun. Kabul edelim ki, C_1 ve C_2 sırası ile F_4 üzerinde n

uzunluğunda $\pi_1(\phi(\alpha))$ ve $\pi_2(\phi(\alpha))-$sabit devirli kod olsun. $x=(x_0,x_1,...,x_{n-1})$ ve $y=(y_0,y_1,...,y_{n-1})$ ise $\sigma_1(x)=\sigma_1(x_0,x_1,...,x_{n-1})=(\pi_1(\phi(\alpha))x_{n-1},x_0,...,x_{n-2})\in C_1$

$\sigma_1(y)=\sigma_1(y_0,y_1,...,y_{n-1})=(\pi_1(\phi(\alpha))y_{n-1},y_0,...,y_{n-2})\in C_2$ elde edilir.

Böylece,

$\sigma_1(c)=\sigma_1(c_0,c_1,...,c_{n-1})=(\alpha(vx_{n-1}+(1+v)y_{n-1}),(vx_0+(1+v)y_0),...,(vx_{n-2}+(1+v)y_{n-2}))$
ve $\alpha\in U_{R_{v^2-v}}$ için $\alpha v=\pi_1(\phi(\alpha))v$ ve $\alpha(1+v)=\pi_2(\phi(\alpha))(1+v)$ olduğundan

$\sigma_1(c)=\sigma_1(c_0,c_1,...,c_{n-1})=(\alpha(vx_{n-1}+(1+v)y_{n-1}),(vx_0+(1+v)y_0),...,(vx_{n-2}+(1+v)y_{n-2}))$
$(\pi_1(\phi(\alpha))vx_{n-1}+\pi_2(\phi(\alpha))(1+v)y_{n-1},vx_0+(1+v)y_0,...,vx_{n-2}+(1+v)y_{n-2})=$
$v(\alpha x_{n-1},x_0,...,x_{n-2})+(1+v)(\alpha y_{n-1},y_0,...,y_{n-2})\in C$

elde edilir. Sonuç olarak C kodu $\alpha-$sabit devirli koddur.

Aksine kabul edelim ki C kodu $\alpha-$sabit devirli kod ve her $i=0,1,...,n-1$ için $c_i=vx_i+(1+v)y_i$ olmak üzere $x=(x_0,x_1,...,x_{n-1})\in C_1$ ve $y=(y_0,y_1,...,y_{n-1})\in C_2$ olsun. Her $\alpha\in U_{R_{v^2-v}}$ için $\alpha v=\pi_1(\phi(\alpha))v$ ve $\alpha(1+v)=\pi_2(\phi(\alpha))(1+v)$ olduğu için

$\sigma_1(c)=v\sigma_1(x)+(1+v)\sigma_1(y)=v(\pi_1(\phi(\alpha))x_{n-1},...,x_{n-2})+(1+v)(\pi_2(\phi(\alpha))y_{n-1},...,y_{n-2})\in C$
olması her $c\in C$ için sağlanır. Böylece C_1 ve C_2 sırası ile $\pi_1(\phi(\alpha))$ ve $\pi_2(\phi(\alpha))-$sabit devirli koddur.

Bu teoremin sonucu olarak, R_{v^2-v} üzerindeki tüm sabit devirli kodlar Çizelge 4.1'de karakterize edilmektedir:

Çizelge 4.1 R_{v^2-v} halkasındaki sabit devirli kod ile F_4 üzerindeki kodlar arasındaki ilişki

C	C_1	C_2
$w-$ sabit devirli	$w-$ sabit devirli	$w-$ sabit devirli
$(1+w)-$ sabit devirli	$(1+w)-$ sabit devirli	$(1+w)-$ sabit devirli
$(v+w)-$ sabit devirli	$(1+w)-$ sabit devirli	$w-$ sabit devirli
$(1+v+w)-$ sabit devirli	$w-$ sabit devirli	$(1+w)-$ sabit devirli
$(1+vw)-$ sabit devirli	$(1+w)-$ sabit devirli	Devirli
$(1+w+vw)-$ sabit devirli	Devirli	$(1+w)-$ sabit devirli
$(1+v+vw)-$ sabit devirli	$w-$ sabit devirli	Devirli
$(v+w+vw)-$ sabit devirli	Devirli	$w-$ sabit devirli

Sonuç 4.11 [36]

1. C kodu R_{v^2-v} üzerinde n uzunluğunda lineer kod olsun. C devirli koddur ancak ve ancak C_1 ve C_2 sırası ile F_4 üzerinde n uzunluğunda devirli koddur.

2. $C=\langle g(x)=vg_1(x)+(1+v)g_2(x)\rangle$ kodu R_{v^2-v} üzerinde n uzunluğunda devirli kod olsun. O halde $|C|=4^{2n-\deg(g_1(x))-\deg(g_2(x))}$ olur. Burada $g_1(x)$ ve $g_2(x)$ sırası ile C_1 ve C_2 devirli kodlarının monik üreteç polinomlarıdır.

4.3 R_{v^2-v} Halkası Üzerinde Tanımlı Çarpık Sabit Devirli Kodlar

Son zamanlarda, çarpık devirli kodlar oldukça çalışılmaktadır. Boucher [8, 18], değişmeli olmayan halka üzerinde devirli kodların cebirsel yapılarını incelemiştir. Zhu ve Xu [36], F_4+vF_4 üzerinde çarpık devirli kodları incelemiştir. Daha sonra Gürsoy ve arkadaşları [38], çarpık devirli kodların yapısını F_q+vF_q üzerinde incelemiştir. [39]

çalışmasında çarpık devirli kodlar Galois halkası üzerinde tanımlanmıştır. Jitman ve arkadaşları [37], bu kod ailesini sonlu zincir halkası üzerine genelleştirmiştir.

Bu bölümde, R_{v^2-v} halkası üzerindeki çarpık sabit devirli kodların yapısı incelenmekte ve tamamı karakterize edilmektedir.

F_q cisminin bir genişlemesi olan F_{q^m} (m pozitif bir tam sayı) sonlu cismi üzerindeki Frobenius otomorfizması tüm $\alpha \in F_{q^m}$ ve $j = 0,1,...,m-1$ için $\sigma_j(\alpha) = \alpha^{q^j}$ dönüşümdür. Böylece,

$$\begin{array}{rccc} f: & F_4 & \to & F_4 \\ & \alpha & \to & \alpha^2 \end{array}$$

F_4 üzerindeki birimsel olmayan tek otomorfizmadır [38].

Böylece, R_{v^2-v} üzerinde birimsel olmayan iki farklı otomorfizma aşağıdaki gibi tanımlanmaktadır [38]:

$$\begin{array}{rccc} \psi: & R_{v^2-v} & \to & R_{v^2-v} \\ & a+bv & \to & a+(1+v)b \end{array} \quad \text{ve} \quad \begin{array}{rccc} \vartheta: & R_{v^2-v} & \to & R_{v^2-v} \\ & a+bv & \to & a^2+vb^2 \end{array}$$

Bu bölümde, ψ otomorfizması bir permütasyon ile elde edildiği için ψ otomorfizmasından ziyade ϑ otomorfizması ele alınmıştır. ϑ otomorfizması cebirsel olarak daha zengin bir yapıya sahiptir ve $F_4[x;\vartheta]$ çarpık polinom halkası $(ax^i)*(bx^j) = a\vartheta^j(b)x^{i+j}$ otomorfizması birim otomorfizması olmadığı durum da değişmeli olmayan bir çarpma işlemi ile Bölüm 2'deki gibi tanımlanmaktadır.

Tanım 4.12 R_{v^2-v} üzerinde n uzunluğunda bir lineer kod olsun. Her $c = (c_0, c_1, c_2, ..., c_{n-1}) \in C$ için σ_2 otomorfizması altında değişmez kalırsa yani; her $c = (c_0, c_1, c_2, ..., c_{n-1}) \in C$ için $\sigma_2(c) = (\vartheta(c_{n-1}), \vartheta(c_0), \vartheta(c_1), ..., \vartheta(c_{n-2})) \in C$ şartını sağlarsa C koduna **çarpık devirli kod** denir.

Devirli kodlara benzer şekilde çarpık devirli kodlar ve çarpık sabit devirli kodlar polinom halkası üzerinde ifade edilmektedir. F_4 üzerinde n uzunluğunda bir lineer C kodu $F_4[x;\vartheta] \Big/ \langle x^n - 1 \rangle$ bölüm halkasının $F_4[x;\vartheta]-$sol alt modülüdür ancak ve ancak C

çarpık devirli koddur. Öte yandan C kodunun polinom karşılığı $F_4[x;\vartheta]/\langle x^n-1\rangle$ bölüm halkasının bir sol alt modülü ise C kodu $F_4[x;\vartheta]$ polinom halkasında x^n-1 polinomunun monik bir sağ böleni olan $g(x)$ polinomu tarafından üretilmektedir [36].

Teorem 4.13 [36] $C = vC_1 \oplus (1+v)C_2$ kodu R_{v^2-v} üzerinde n uzunluğunda lineer kod olsun. C çarpık devirli koddur ancak ve ancak C_1 ve C_2 kodları F_4 üzerinde n uzunluğunda çarpık devirli koddur.

Tanım 4.14 [38] R_{v^2-v} üzerinde bir otomorfizma ϑ ve R_{v^2-v} halkasının birimsel elemanı α olsun. O halde R_{v^2-v} üzerindeki bir lineer C kodu **çarpık sabit devirli kod** veya ϑ_α – **sabit devirli kod** olarak adlandırılır ancak ve ancak C kodunun polinom karşılığı $F_4[x;\vartheta]/\langle x^n-\alpha\rangle$ bölüm halkasının $F_4[x;\vartheta]$ – sol alt modülüdür.

İlaveten C kodu $F_4[x;\vartheta]/\langle x^n-\alpha\rangle$ bölüm halkasının bir alt modülü ise $F_4[x;\vartheta]$ halkasında $x^n-\alpha$ polinomunun monik bir böleni olan $g(x)$ polinomu tarafından üretilmektedir.

Teorem 4.15 C kodu ϑ_α – sabit devirli koddur ancak ve ancak C_1 ve C_2 kodları F_4 üzerinde n uzunluğunda sırası ile $\vartheta_{\pi_1(\phi(\alpha))}$ ve $\vartheta_{\pi_2(\phi(\alpha))}$ – sabit devirli koddur.

İspat: ϑ otomorfizmasının tanımı ve her $\alpha \in U_{R_{v^2-v}}$ için $\vartheta(\alpha)v = \vartheta(\pi_1(\phi(\alpha)))v$ ve $\vartheta(\alpha)(1+v) = \vartheta(\pi_1(\phi(\alpha)))(1+v)$ olduğu için teoremin ispatı sabit devirli kodlar için ifade edilen Teorem 4.10'un ispatına benzer şekilde elde edilmektedir.

Bu teoremin sonucu olarak, R_{v^2-v} üzerindeki tüm ϑ_α – sabit devirli kodlar Çizelge 4.2 de karakterize edilmektedir.

Çizelge 4.2 C , α – sabit devirli kod ile C_1 ve C_2 kodları arasındaki ilişki

C	C_1	C_2
ϑ_w	ϑ_w	ϑ_w
$\vartheta_{(1+w)}$	$\vartheta_{(1+w)}$	$\vartheta_{(1+w)}$
$\vartheta_{(v+w)}$	$\vartheta_{(1+w)}$	$\vartheta_{(w)}$
$\vartheta_{(1+v+w)}$	$\vartheta_{(w)}$	$\vartheta_{(1+w)}$
$\vartheta_{(1+vw)}$	$\vartheta_{(1+w)}$	çarpık devirli
$\vartheta_{(1+w+vw)}$	çarpık devirli	$\vartheta_{(1+w)}$
$\vartheta_{(1+v+vw)}$	$\vartheta_{(w)}$	çarpık devirli
$\vartheta_{(v+w+vw)}$	çarpık devirli	$\vartheta_{(w)}$

4.4 R_{v^2-v} Halkası Üzerinde Tanımlı TS ve TST Kodlar

DNA kodların özellikleri ve inşa şekilleri cisimler üzerinde [34, 40, 41], zincir halkaları üzerinde [42] ve [43] makalelerinde çalışılmıştır.

Tanım 4.16 [33] Bir polinomun katsayıları ters sıralandığında aynı polinom elde ediliyorsa bu polinoma **ters sıralı polinom (TS)** denir. Yani; $p_r \neq 0$ olmak üzere her bir $p(x) = p_0 + p_1 x + \ldots + p_r x^r$ polinomunun **ters sıralı polinomu (reciprocal)** $p^*(x) = x^r p\left(\frac{1}{x}\right) = p_r + p_{r-1}x + \ldots + p_0 x^r$ olarak tanımlanır.

Burada $\deg p^*(x) \leq \deg p(x)$ olur. Eğer $p_0 \neq 0$ ise, $p(x)$ ve $p^*(x)$ aynı dereceye sahiptirler. Kısaca $p(x) = p^*(x)$ ise $p(x)$ polinomuna **ters sıralı polinom (TS, self-reciprocal)** denir.

Her bir $u=(u_0,u_1,\ldots,u_{n-1})$ kodsözü için **ters sıralısı** (**reverse**) $u^r=(u_{n-1},u_{n-2},...u_0)$, **tamamlayıcısı** (**complement**) $u^c=(u_0^c,u_1^c,...,u_{n-1}^c)$ ve **ters sıralı tamamlayıcısı** $u^{rc}=(u_{n-1}^c,...,u_0^c)$ şeklinde gösterilmektedir.

Tanım 4.17 [33] Tüm kodsözlerinin ters sıralanışı bir C kodunun içinde ise o koda **ters sıralı** (**TS) kod** denir.

Massey [33], sonlu cisim üzerindeki TS kodların ancak ve ancak ters sıralı polinomlar ile üretilmekte olduğunu göstermiştir.

Bu bölümde ilk defa zincir olmayan R_{v^2-v} halkasında TS (ters sıralı) ve TST (ters sıralı tamlanan) DNA kodlarının nasıl oluşturulabileceği gösterilmektedir. Daha önceki bölümlerde R_{v^2-v} halkası üzerindeki devirli, sabit devirli ve çarpık sabit devirli kodların $g(x)$ üreteç polinomunun, F_4 üzerindeki $g_1(x)$ ve $g_2(x)$ polinomları ile elde edilebileceği ifade edilmektedir. Buradan hareketle F_4 üzerindeki $g_1(x)$ ve $g_2(x)$ polinomlarının ters sıralı polinomlar olması $g(x)=vg_1(x)+(1+v)g_2(x)$ polinomunun R_{v^2-v} üzerinde ters sıralı polinom olmasını gerektireceği düşünülebilir. Oysa bu durum her zaman sağlanmamaktadır. Aşağıdaki örnekler zıt durumlara örnek olarak verilmektedir:

1. $g_1(x)$ ve $g_2(x)$ polinomları F_4 üzerinde ters sıralı polinomlar olmak üzere R_{v^2-v} halkasında bir polinom $g(x)=(v)g_1(x)+(1+v)g_2(x)$ olsun. $g(x)$ ters sıralı polinom olmak zorunda değildir.

Örnek 4.18 $g_1(x)=x^2+wx+1$ ve $g_2(x)=x^6+wx^4+x^3+wx^2+1$ polinomları F_4 cismi üzerinde ters sıralı polinomlar olsun.

$$g(x)=(1+v)x^6+(vw+w)x^4+(v+1)x^3+(wv+w+v)x^2+vwx+1$$

polinomu R_{v^2-v} üzerinde ters sıralı polinom değildir.

2. $g_1(x)$ veya $g_2(x)$ polinomları F_4 üzerinde tes sıralı polinomlar olmasın. $g(x)$ polinomu ters sıralı polinom olmak zorunda değildir.

Örnek 4.19 $g_1(x)=x+1$ ve $g_2(x)=x+w$ polinomları F_4 üzerinde tanımlı ve $g_2(x)$ ters sıralı polinom olmasın. $g(x)=x+v+w+vw$ polinomu R_{v^2-v} üzerinde ters sıralı polinom değildir.

Teorem 4.20 $C=\langle g(x)=vg_1(x)+(1+v)g_2(x)\rangle$ kodu R_{v^2-v} üzerinde n uzunluğunda bir TS koddur ancak ve ancak $g_1(x)$ ve $g_2(x)$ polinomları F_4 üzerinde x^n-1 polinomunu bölen ters sıralı polinomlardır.

İspat: $\deg(g_1(x))=t$ ve $\deg(g_2(x))=m$ olsun. Kabul edelim ki $t\le m$ olsun. Eğer $t=m$ ise ters sıralılık açık bir şekilde gözlemlenmektedir. Genelliği bozmaksızın $t<m$, $g_1(x)=a_0+a_1x+...+a_1x^{t-1}+a_0x^t$ ve $g_2(x)=b_0+b_1x+...+b_1x^{m-1}+b_0x^m$ olmak üzere $C=\langle g(x)=vg_1(x)+(1+v)g_2(x)\rangle$ olduğunu kabul edelim. $C=\langle g(x)\rangle$ olduğu için $g(x)\in C$ olur. Öte yandan $vx^{n-t-1}g_1(x)+(v+1)x^{n-m-1}g_2(x)$ polinomu $g(x)$ polinomunun ters sıralı polinomu olmak üzere $vx^{n-t-1}g_1(x)+(v+1)x^{n-m-1}g_2(x)\in C$ olur. İlaveten, eğer $x^ig(x)\in C$ ise $vx^{n-t-i-1}g_1(x)+(v+1)x^{n-m-i-1}g_2(x)$ polinomu $x^ig(x)\in C$ polinomunun ters sıralı polinomu olmak üzere $vx^{n-t-i-1}g_1(x)+(v+1)x^{n-m-i-1}g_2(x)\in C$ olur. C lineer bir kod olmak üzere $x^ig(x)$ polinomunun tüm lineer kombinasyonları C koduna düşmektedir. Böylece her elemanın ters sıralısı C koduna düşmektedir. Sonuç olarak, $C=\langle vg_1(x)+(1+v)g_2(x)\rangle$ kodu bir TS koddur.

Tersine, kabul edelim ki $C=\langle vg_1(x)+(1+v)g_2(x)\rangle$ TS kod olsun. Böylece, Gray dönüşümü kullanarak $C_1=\langle g_1(x)\rangle$ ve $C_2=\langle g_2(x)\rangle$ kodları F_4 üzerinde TS kodlar olduğu için [33] çalışmasından $g_1(x)$ ve $g_2(x)$ polinomları F_4 üzerinde ters sıralı polinomlar olmaktadır.

Örnek 4.21 F_4 cismi üzerinde $g_1(x)=x-1$ ve $g_2(x)=x^2+wx+1$ polinomları x^5-1 polinomunu bölen ters sıralı polinomlar ve $C=\langle v(x-1)+(1+v)(x^2+wx+1)\rangle$ olsun. $C=\langle v(x-1)+(1+v)(x^2+wx+1)\rangle$ ve $g(x)=v(x-1)+(1+v)(x^2+wx+1)\in C$ olur.

Öte yandan, $\left(vx^3+(1+v)x^2\right)g(x)=x^4+(v+w+vw)x^3+(1+v)x^2\in C$ olur. Böylece C kodu R_{v^2-v} üzerinde 5 uzunluğunda TS koddur.

4.5 R_{v^2-v} Halkası Üzerinde Tanımlı DNA Kodlar

Bu bölümde R_{v^2-v} halkasının elamanları ile DNA 4-bazlarının nasıl eşleştirildiği ve bunlardan faydalanarak, cebirsel olarak üretilen bu kodlar ile TS ve TST özelliklerine sahip DNA kodların nasıl üretildiği açıklanmaktadır.

DNA kodlarındaki ters sıralama problemi şu örnek ile açıklanabilir: $(w,1+v,wv)$ kodsözü R_{v^2-v} halkasında üç uzunluklu bir kodsöz olsun. Bu kodsözün DNA karşılığı "$CCATCA$" iken kodsözün ters sıralısı $(wv,1+v,w)^r=(w,1+v,wv)$ ve bunun DNA karşılığı "$CAATCC$" olur. Bu kodsözlerin DNA karşılığı birbirlerinin ters sıralısı olmamaktadır. Çünkü "$CCATCA$" kodsözünün ters sıralısı "$ACTACC$" olur. Bu problem ψ-küme şeklinde bir üreteç kümesi tanımlayarak çözülmektedir.

DNA bazları $S_{D_4}=\{A,T,G,C\}$ kümesi ile tanımlansın ve DNA 4-bazlarıda $S_{D_{16}}=\{AA,\ AT,\ AG,\ AC,\ TT,\ TA,\ TG,\ TC,\ GG,\ GA,\ GC,\ GT,\ CC,\ CA,\ CG,\ CT\}$ kümesi ile ifade edilsin [41].

DNA 4-bazları ile R_{v^2-v} halkasının elamanlarının eşlemesi ξ dönüşümü ile Çizelge 4.3 'teki gibi sağlanmaktadır. [40] makalesinde DNA bazlarının eşleşmesi Υ ile aşağıdaki gibi gösterilsin:

$\Upsilon(0)=A, \Upsilon(1)=T, \Upsilon(w^2)=G, \Upsilon(w)=C$ DNA yapısının bir özelliği olan Watson-Crick tamamlama $A^c=T$, $T^c=A$, $C^c=G$, $G^c=C$ şeklinde, DNA zincirindeki karşılıklı gelen bazların kuralını belirtmektedir. DNA 4-bazları için Watson-Crick tamamlama özelliği $(AATG)^c=TTAC$, …, $(TCGG)^c=AGCC$ şeklinde gösterilir. Aşağıdaki tanım bir kodsözün DNA karşığının dönüşümünü ifade etmektedir:

Tanım 4.22 C kodu R_{v^2-v} halkasında n uzunluğunda bir lineer kod olsun. $c_i \in R_{v^2-v}$ ve $c=(c_0,c_1,...,c_{n-1}) \in C$ bir kodsöz olmak üzere Θ dönüşümü C kodunun kodsözlerini DNA bazlarına aşağıdaki şekilde karşılık getirmektedir:

$\Theta : C \to S_{D_4}^{2n}$ ve $\Theta(c)=(\xi(c_0)\xi(c_1)...\xi(c_{n-1}))$.

Örnek 4.23 $c=(c_0,c_1,c_2,c_3)=(1,v,w,1+v+w)$ kodsözü

$\Theta(c)=(\xi(1)\xi(v)\xi(w)\xi(1+v+w))=(TTTACCCG)$ DNA bazına karşılık gelmektedir.

Çizelge 4.3 R_{v^2-v} halkasının elemanları ile DNA bazlarının eşleme tablosu

a elemanı	*Gray dönüşümü*	$\xi(a)$
0	$(0,0)$	AA
1	$(1,1)$	TT
w	$(w,\ w)$	CC
$1+w$	$(1+w,\ 1+w)$	GG
v	$(1,\ 0)$	TA
$1+v$	$(0,\ 1)$	AT
$v+w$	$(1+w,\ w)$	GC
$1+v+w$	$(w,\ 1+w)$	CG
vw	$(w,\ 0)$	CA
$1+vw$	$(1+w,\ 1)$	GT
$w+vw$	$(0,w)$	AC
$1+w+vw$	$(1,\ 1+w)$	TG
$v+vw$	$(1+w,\ 0)$	GA
$1+v+vw$	$(w,\ 1)$	CT
$w+v+vw$	$(1,w)$	TC
$1+w+v+vw$	$(0,\ 1+w)$	AG

R_{v^2-v} üzerinde $\psi(a+bv)=a+b(v+1)$ bir otomorfizmadır ve bu otomorfizma yardımıyla $\psi-$**küme** olarak da adlandırılan $E(g)$ kümesi aşağıdaki gibi ifade edilmektedir:

$$E_i = \begin{cases} x^i g(x) & \text{eğer } i \text{ çift ise,} \\ x^i \psi(g(x)) & \text{eğer } i \text{ tek ise,} \end{cases}$$

olmak üzere,

$$E(g) = \{E_0, E_1, ..., E_{\ell-1}\}$$

şeklinde tanımlanmaktadır. $E(g)$ kümesi R_{v^2-v} halkası üzerinde C lineer kodu için bir üreteç kümesidir ve $C = \langle g(x) \rangle_\psi$ ile gösterilmektedir.

Not: Burada $\langle g(x) \rangle_\psi$ veya $\langle E(g) \rangle$ ile $E(g)$ ile üretilen R_{v^4-v} modülü göstermektedir. $(g(x))$ ile $g(x)$ tarafından üretilen ideali göstermektedir.

R_{v^2-v} üzerinde $g(x) = a_0 + a_1 x + ... + a_t x^t$ olmak üzere $g(x) = a_0 + a_1 x + ... + a_t x^t$ kümesinin ürettiği lineer kodun üreteç matrisi aşağıdaki biçimde gösterilmektedir:

$$E(g) = \begin{pmatrix} a_0 & a_1 & a_2 & ... & a_t & 0 & ... & ... & ... & 0 \\ 0 & \psi(a_0) & \psi(a_1) & ... & ... & \psi(a_t) & 0 & ... & ... & 0 \\ 0 & 0 & a_0 & a_1 & ... & ... & a_t & 0 & ... & 0 \\ 0 & 0 & 0 & \psi(a_0) & \psi(a_1) & ... & ... & \psi(a_t) & 0... & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \end{pmatrix}.$$

Teorem 4.24 $g_1(x)$ ve $g_2(x)$ polinomları F_4 üzerinde, dereceleri sırasıyla t_1, t_2 olan ve $x^n - 1$'i bölen ters sıralı polinomlar ve $2 \le \ell$ bir çift tam sayı olsun.

1. $\deg g_1(x) = \deg g_2(x)$ veya $g_1(x)$ ya da $g_2(x)$ polinomundan herhangi birisi 0 ise $g(x) = v g_1(x) + (v+1) g_2(x)$ olmak üzere sırası ile $|E(g)| = 16^l$ ya da $|E(g)| = 4^l$ olur.

2. $\deg g_1(x) \neq \deg g_2(x)$ ve $2 \le s = |t_1 - t_2|$ çift tam sayı olsun. O halde,

$\deg g_1(x) > \deg g_2(x)$ için $g(x) = v g_1(x) + (v+1) x^{s/2} g_2(x)$ ve $\deg g_1(x) < \deg g_2(x)$ için $g(x) = v x^{s/2} g_1(x) + (v+1) g_2(x)$ olmak üzere $|\langle E(g) \rangle| = 16^\ell$ olur.

Her iki durumda da $C = \langle E(g) \rangle$ kodu R_{v^2-v} üzerinde bir lineer koddur ve $\Theta(C)$ kodu TS DNA koddur.

İspat: $\alpha \in R_{v^2-v}$ ve $0 \le i \le \ell - 1$ olmak üzere

$$\left(\Theta\left(\sum_i \alpha_i E_i\right)\right)^r = \Theta\left(\sum_i \psi(\alpha_i) E_{\ell-1-i}\right) \tag{4.1}$$

olduğu için her DNA kodsözünün ters sıralılarının da $C = \langle E(g) \rangle$ kodunun içinde olduğunu göstermektedir.

Diğer özellikler daha önce verilen tanımlardan elde edilmektedir.

Aşağıdaki örnek ile teoremin ispatında gösterilen bir DNA kodsözünün ters sıralı hali, üreteç matrisin hangi satırlarının kombinasyonundan elde edildiğini veren (4.1) denklemi örneklendirilmiştir.

Örnek 4.25 $g_1(x) = 1 + w^2 x + w^2 x^2 + x^3$ ve $g_2(x) = 1 + x$, F_4 üzerinde $x^5 - 1$ polinomunun ters sıralı bölenidirler. Böylece,

$$g(x) = v g_1(x) + (v+1) x g_2(x) = v + (1 + v + vw^2) x + (1 + v + vw^2) x^2 + v x^3$$

elde edilir. $C = \langle E(g) \rangle$ kodu için $E(g)$ kümesi aşağıdaki matris ile de ifade edilebilmektedir:

$$\begin{pmatrix} E_0 \\ E_1 \end{pmatrix} = \begin{pmatrix} v & 1+v+vw^2 & 1+v+vw^2 & v & 0 \\ 0 & 1+v & v+w^2+vw^2 & v+w^2+vw^2 & 1+v \end{pmatrix}.$$

Eğer $\alpha_0 = w + v$, $\alpha_1 = 1 + vw$ alınırsa $\alpha_0 E_0 + \alpha_1 E_1 = vw + v + (v + w + 1) x + x^2 + (vw + v + w + 1) x^3 + (v+1) x^4$ polinomuna karşılık $c_1 = (vw + v, v + w + 1, 1, vw + v + w + 1, v + 1)$ kodsözü elde edilmektedir. Bu kodsözün DNA karşılığı $\Theta(c_1) = (GACGTTAGAT)$ olmakta ve $\Theta(c_1)$ kodsözünün ters sıralısı Teorem 4.24'ün ispatında belirtildiği gibi aşağıdaki şekilde bulunmaktadır:

$\left(\Theta(\alpha_0 E_0 + \alpha_1 E_1)\right)^r = \Theta(\psi(\alpha_0) E_1 + \psi(\alpha_1) E_0)$ elde edilir. Ayrıca

$$\psi(\alpha_0) E_1 + \psi(\alpha_1) E_0 = v + (v + vw) x + x^2 + (v + w) x^3 + (1 + v + w + vw) x^4$$

polinomuna $c_2=(v,vw+v,1,v+w,vw+v+w+1)$ kodsözüne karşılık gelir ve bu kodsözün DNA karşılığı $\Theta(c_2)=(TAGATTGCAG)$ olur. Kısaca; $(\Theta(c_1))^r=\Theta(c_2)$ olur.

Sonuç 4.26 $g_1(x)$ ve $g_2(x)$ polinomları F_4 cisminde x^n-1 polinomunu bölen ters sıralı polinomlar ve $C=\langle E(g)\rangle$ kodu R_{v^2-v} halkasında bir lineer kod olmak üzere, $r(x)=1+x+x^2+...+x^{n-1}$ polinomunu içeriyorsa, $\Theta(C)$ bir TST DNA koddur.

İspat: DNA baz eşlemeleri ve Çizelge 4.3'den açıktır.

Sonuç 4.27 $g_1(x)$ ve $g_2(x)$, F_4 üzerinde x^n-1'i bölen ters sıralı polinomlar ve $C=\langle E(g)\rangle$ kodu R_{v^2-v} halkasında bir lineer kod olmak üzere, $r(x)=1+x+x^2+...+x^{n-1}$ polinomu C kodunun üreteç kümesine eklenirse, $\Theta(C)$ bir TST DNA koddur.

İspat: Sonuç DNA baz eşlemeleri ve Teorem 4.24'den elde edilir.

Teorem 4.28 $g_1(x)=g_2(x)$ ve F_4 cisminde x^n-1 polinomunu bölen ters sıralı polinom ve $g(x)=\sum_{i=1}^{2}e_ig_i$ olsun. $C=\langle g(x)\rangle$ (veya $C=\langle g(x)\rangle_\psi=\langle E(g)\rangle$) kodu R_{v^2-v} halkasında TS devirli bir koddur ve $\Theta(C)$ kodu TS DNA koddur. Eğer $x-1$ polinomu $g(x)$ polinomunu bölmüyor ise $\Theta(C)$ kodu TST DNA koddur. Burada C kodu aynı zamanda bir çarpık devirli koddur.

İspat: C kodunun boyutu k olsun. Kabul edelim ki C kodunun üreteç matrisinin satırları $g(x),xg(x),x^2g(x),...,x^{k-1}g(x)$ olsun. Eğer üreteç kümesi olarak $\psi-$kümesi $E(g)$ alınırsa $\left(\Theta\left(\sum_i\alpha_ix^ig(x)\right)\right)^r=\Theta\left(\sum_i\psi(\alpha_i)x^{k-1-i}g(x)\right)$ elde edilir. Burada $\alpha\in R_{v^2-v}$ ve $0\le i\le k-1$ olur. $g(x)=e_1g_1(x)+e_2g_1(x)$ ve $g(x)$ polinomunun katsayıları sadece F_4 cisminden alındığı için DNA'daki TS özelliği sağlanmaktadır. Sonuç olarak, ψ otomorfizması katsayıları etkilemediği için $\psi-$kümesi $E(g)$ üreteç matrisi olarak alınabilir. $x-1$ polinomu $g(x)$ polinomunun bir böleni değil ise C kodu

$r(x)=1+x+x^2+\ldots+x^{n-1}$ polinomunu içermektedir. Dolayısı ile $\Theta(C)$ bir TST DNA koddur.

Teorem 4.29 [44] $\sum_{\alpha\in\Lambda} e_\alpha = 1$ olmak üzere R halkasının e_α merkezi idempotent elemanları ve $R=\oplus_{\alpha\in\Lambda} Re_\alpha$ ayrışımı verilsin. O halde her $\alpha\in\Lambda$ için $R_\alpha := Re_\alpha$ bir halkadır. C kodu R halkasında n uzunluğunda sağ (sol) lineer kod ise $C_\alpha := Ce_\alpha$ $(C_\alpha := e_\alpha C)$ kodu da Re_α üzerinde n uzunluğunda sağ (sol) lineer koddur.

Teorem 4.30 [44] C kodu R üzerinde n uzunluğunda sağ (sol) lineer kod ise

1. $k(C)=\max_{\alpha\in\Lambda}\{k(C_\alpha)\}$,
2. $d(C)=\min_{\alpha\in\Lambda}\{d(C_\alpha)\}$

olur.

Teorem 4.31 [45] (Griesmer Sınırı) Her $\alpha\in\Lambda$ için R_α yerel halka olmak üzere $R=\oplus_{\alpha\in\Lambda} Re_\alpha$ sonlu halka ve q_α bir asal sayının kuvveti olmak üzere $\left|R_\alpha / J(R_\alpha)\right| = q_\alpha$ olsun. C kodu R üzerinde n uzunluğunda sağ (sol) lineer kod ise $q := \max_{\alpha\in\Lambda}\{q_\alpha\}$ olmak üzere

$$n \geq \sum_{i=0}^{k(C)-1} \left\lceil \frac{d(C)}{q^i} \right\rceil$$

olur.

Aşağıdaki çizelgede R_{v^2-v} üzerinde $g_1(x)=g_2(x)$ olarak alındığında Griesmer sınırına göre elde edilen bazı optimal özel TS DNA kodlar ve üreteç matrisleri listelenmektedir.

Çizelge 4.4 R_{v^2-v} halkasının üzerindeki Griesmer sınırını sağlayan bazı optimal DNA kodlar

n	$g(x)$ $\left(\text{burada } g_1(x)=g_2(x)\right)$	Parametreler
10	$1+w^2x+w^2x^2+x^3+x^5+w^2x^6+w^2x^7+x^8$	$[10,2,8]$
10	$1+wx+wx^2+x^3+x^5+wx^6+wx^7+x^8$	$[10,2,8]$
15	$1+w^2x+w^2x^2+x^3+x^5+w^2x^6+w^2x^7+x^8+x^{10}+w^2x^{11}+w^2x^{12}+x^{13}$	$[15,2,12]$
15	$1+w^2x+wx^3+wx^4+x^5+x^6+wx^7+wx^8+w^2x^{10}+x^{11}$	$[15,4,10]$
17	$1+x+wx^2+x^4+wx^5+w^2x^6+w^2x^7+wx^8+x^9+wx^{11}+x^{12}+x^{13}$	$[17,4,12]$
35	$1+wx+wx^2+x^3+x^5+wx^6+wx^7+x^8+x^{10}+wx^{11}+wx^{12}+x^{13}+x^{15}$ $+wx^{16}+wx^{17}+x^{18}+x^{20}+wx^{21}+wx^{22}+x^{23}+x^{25}+wx^{26}+wx^{27}+x^{28}$ $+x^{30}+wx^{31}+wx^{32}+x^{33}$	$[35,2,28]$

BÖLÜM 5

R_{v^4-v} HALKASI ÜZERİNDE LİNEER KODLAR

Bu bölümde zincir olmayan $F_4[v]/\langle v^4-v\rangle$ halkanın cebirsel yapısı incelenerek bu halka üzerinde tanımlanan lineer ve devirli kodların inşası verilmektedir. Ayrıca, bu halka üzerinde tanımlı devirli kodlardan ters sıralı (TS) ve ters sıralı tamlanan (TST) kodlar elde edilmektedir. Bölümün son kısmında halkanın elemanları ile DNA $4-$bazları arasında tam eşleme yapılarak özel bir küme tanımlanmaktadır. Bu küme yardımı ile DNA kodları elde edilmektedir.

5.1 R_{v^4-v} Halkası Üzerinde Tanımlı Lineer Kodlar

Katsayıları F_4 cisminden alınan v değişkenli polinom halkası $F_4[v]$ olsun.

$$R_{v^4-v}=\left\{a+bv+cv^2+dv^3 \mid a,b,c,d\in F_4\right\}$$
$$=\left\{(a_0+a_1w)+(b_0+b_1w)v+(c_0+c_1w)v^2+(d_0+d_1w)v^3 \mid a_0,a_1,b_0,b_1,c_0,c_1,d_0,d_1\in F_2,\ v^4-v=0\right\}$$

olsun. Böylece $R=F_4[v]/\langle v^4-v\rangle$ bölüm halkası 256 elemana sahiptir.

Tanım 5.1 $\alpha=a+bv+cv^2+dv^3\in R_{v^4-v}$ ve sırası ile $i\in\{0,1,w,1+w\}$ olmak üzere her $i\in F_4$ için $\alpha(i):=a+bi+ci^2+di^3\in F_4$ olsun. $\alpha(i)$ yardımı ile R_{v^4-v} halkasından F_4^4 halkasına özel bir ϕ dönüşümü

$$\phi_1(\alpha)=a_0+a_1w,$$
$$\phi_2(\alpha)=(a_0+b_0+c_0+d_0)+(a_1+b_1+c_1+d_1)w,$$

$\phi_3(\alpha)=(a_0+b_1+c_0+c_1+d_0)+(a_1+b_0+b_1+c_0+d_1)w$,

$\phi_4(\alpha)=(a_0+b_0+b_1+c_1+d_0)+(a_1+b_0+c_0+c_1+d_1)w$

olmak üzere $\phi(\alpha)=(\phi_1(\alpha),\phi_2(\alpha),\phi_3(\alpha),\phi_4(\alpha))$ olarak tanımlanmaktadır. Bu dönünüşüm modül izomorfizmasıdır. Bu izomorfizmadan dolayı

$R_{v^4-v}\cong F_4[v]/\langle v\rangle\oplus F_4[v]/\langle v-1\rangle\oplus F_4[v]/\langle v-w\rangle\oplus F_4[v]/\langle v-w^2\rangle\cong F_4\oplus F_4\oplus F_4\oplus F_4\cong F_4^4$

olur.

Önerme 5.2 R_{v^4-v} halkasında tam 16 ideal vardır.

İspat: Tüm elemanlarını üreten birimsel elemanlar:

$R_{v^4-v}=\langle 1\rangle=\langle w\rangle=\langle w+1\rangle=\langle v+v^2+w\rangle=\ldots=\langle 1+v(1+w)+v^2(1+w)+v^3(1+w)\rangle$.

Tüm maksimal idealler 64 elemanlıdır ve aşağıdaki biçimde üretilmektedir:

1. $\langle v\rangle=\langle vw\rangle=\langle v(1+w)\rangle=\ldots=\langle vw+v^2(1+w)+v^3(1+w)\rangle$.
2. $\langle 1+v\rangle=\langle (1+v)w\rangle=\langle (1+v)(1+w)\rangle=\ldots.=\langle 1+w+v(1+w)+v^2(1+w)+v^3(1+w)\rangle$.
3. $\langle v+w\rangle=\langle 1+w+vw\rangle=\langle 1+v(1+w)\rangle=\ldots\langle 1+v+w+v^2(1+w)+v^3(1+w)\rangle$.
4. $\langle 1+v+w\rangle=\langle 1+vw\rangle=\langle w+v(1+w)\rangle=\ldots=\langle 1+w+vw+v^2(1+w)+v^3(1+w)\rangle$.

16 elemanlı idealler aşağıdaki gibi üretilmektedir:

1. $\langle v+v^2\rangle=\langle vw+v^2w\rangle=\langle v(1+w)+v^2(1+w)\rangle=\ldots=\langle v^2(1+w)+v^3(1+w)\rangle$.
2. $\langle v^2+vw\rangle=\langle v^2w+v(1+w)\rangle=\langle v^3+v^2w\rangle=\ldots=\langle v+v^2w+v^3(1+w)\rangle$.
3. $\langle v^2+w+v(1+w)\rangle=\langle 1+v+w+v^2w\rangle=\ldots=\langle w+vw+v^2(1+w)+v^3(1+w)\rangle$.
4. $\langle v+v^2w\rangle=\langle vw+v^2(1+w)\rangle=\langle v^3+vw\rangle=\ldots=\langle v^2w+v^3(1+w)\rangle$.
5. $\langle 1+v^2+w+vw\rangle=\langle 1+v^2w+v(1+w)\rangle=\ldots=\langle 1+v+v^2(1+w)+v^3(1+w)\rangle$.
6. $\langle 1+v+v^2\rangle=\langle 1+w+v(1+w)+v^2(1+w)\rangle=\ldots=\langle 1+vw+v^2w+v^3(1+w)\rangle$.

Minimal idealler 4 elemanlıdır ve aşağıdaki gibi üretilmektedir:

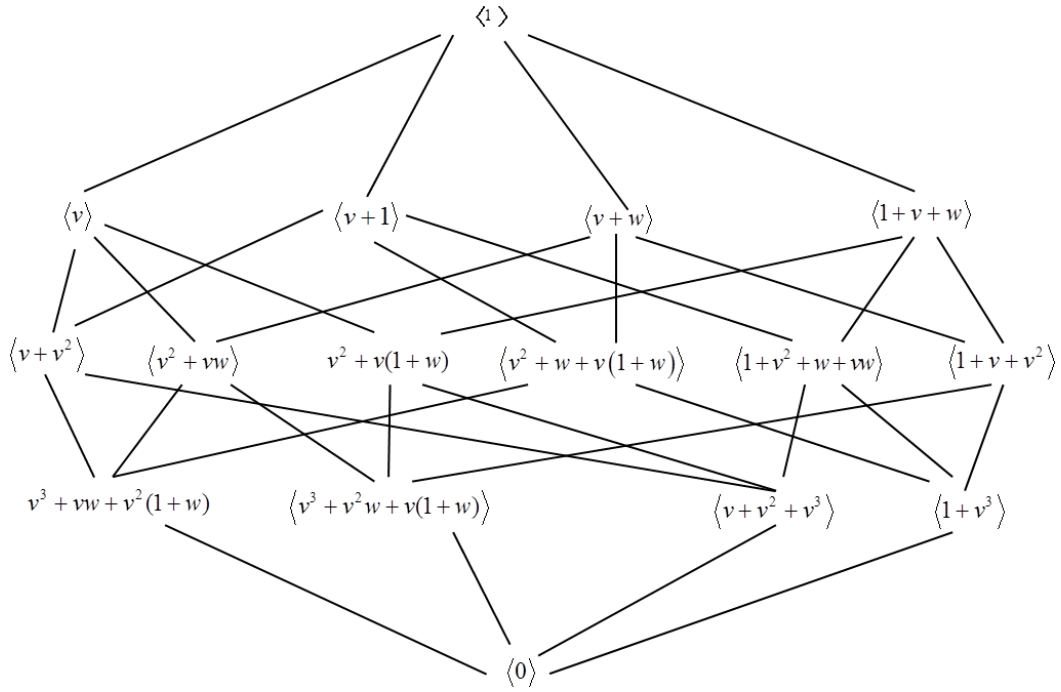
1. $\langle v^3+vw+v^2(1+w)\rangle=\langle v^2+v^3w+v(1+w)\rangle=\langle v+v^2w+v^3(1+w)\rangle$.

2. $\left\langle v^3+v^2w+v(1+w)\right\rangle=\left\langle v+v^3w+v^2(1+w)\right\rangle=\left\langle v^2+vw+v^3(1+w)\right\rangle$.

3. $\left\langle v+v^2+v^3\right\rangle=\left\langle vw+v^2w+v^3w\right\rangle=\left\langle v(1+w)+v^2(1+w)+v^3(1+w)\right\rangle$.

4. $\left\langle 1+v^3\right\rangle=\left\langle w+v^3w\right\rangle=\left\langle 1+w+v^3(1+w)\right\rangle$.

5. $\langle 0\rangle=\{0\}$ ideali.



Şekil 5.1 R_{v^4-v} halkasının ideal şeması

Burada bölüm 2'de verilen bazı tanımlar R_{v^4-v} halkası için verilmektedir.

Tanım 5.3 $r\in R_{v^4-v}$ olmak üzere r elemanı sıfırdan farklı ise r elemanının **Hamming ağırlığı** 1 aksi durumda Hamming ağırlığı 0 olur ve $w_H(r)$ ile gösterilmektedir. İlaveten, $r=(r_0,r_2,...,r_{n-1})\in R_{v^4-v}^n$ ise $w_H(r)=\sum_{i=0}^{n-1}w_H(r_i)$ olarak tanımlanmaktadır.

Tanım 5.4 $r\in R_{v^4-v}$ olmak üzere r elemanının **Lee ağırlığı** ϕ görüntüsünün Hamming ağırlığı olarak tanımlanmaktadır ve $w_L(r)$ olarak gösterilmektedir. Dolayısı ile $w_L(r)=w_H(\phi(r))$ olur.

Özellik 5.5 $I=\langle\alpha\rangle$ ve $\alpha=a+bv+cv^2+dv^3\in R_{v^4-v}$ olmak üzere

1. $w_L(\alpha)=4$ ise α elemanı R_{v^4-v} halkasının birimsel elemanıdır.

2. $|I|=q^{w_L(\alpha)}$ olur.

İspat: Özellik 4.5'in ispatına benzer şekilde elde edilektedir.

Önerme 5.6 $\alpha\in R_{v^4-v}$ olsun. R_{v^4-v} halkasında aşağıdaki özellikler sağlanmaktadır:

1. $supp(\phi(\alpha))=\{1,2,3,4\}$ ise α birimsel elemandır ve R_{v^4-v} halkasında tam 81 tane birimsel eleman vardır.

2. $I=\langle\alpha\rangle$ ideali R_{v^4-v} halkasında bir ideal olsun. $|supp(\phi(\alpha))|=3$ ise I maksimal idealdir ve R_{v^4-v} halkasında 4 tane maksimal ideal vardır.

İspat: Özellik 5.5 ve destek kümesi tanımından sonuç elde edilmektedir.

Öte yandan ϕ dönüşümünün tersi

$$\phi^{-1}: F_4^4 \to R_{v^4-v}$$
$$(x_0+x_1w,\ y_0+y_1w,\ z_0+z_1w,\ t_0+t_1w)\to(x_0+x_1w)+\big((y_0+z_0+z_1+t_1)+(y_1+z_0+t_0+t_1)w\big)v$$
$$+\big((y_0+z_1+t_0+t_1)+(y_1+z_0+z_1+t_0)w\big)v^2+\big((x_0+y_0+z_0+t_0)+(x_1+y_1+z_1+t_1)w\big)v^3$$

şeklinde tanımlanmaktadır.

Önerme 5.7 R_{v^2-v} temel ideal halkasıdır.

İspat: Teorem 4.2'nin ispatına benzer şekilde elde edilmektedir.

Önerme 5.8 $I=\langle\alpha_1,\alpha_2,...,\alpha_s\rangle$ ideali R_{v^4-v} halkasında sonlu üretilmiş bir ideal olsun. O halde $supp(\phi(\beta))=\bigcup_{i=1}^{s} supp(\phi(\alpha_i))$ özelliğini sağlayan her $\beta\in R_{v^4-v}$ elemanı için $I=\langle\alpha_1,\alpha_2,...,\alpha_s\rangle=\langle\beta\rangle$ olur.

İspat: R_{v^4-v} halkasının sonlu üretilmiş bir ideali $I=\langle\alpha_1,\alpha_2,\ldots,\alpha_s\rangle$ olsun. F_4^4 halkası üzerinde $\eta\in F_4^4$ olmak üzere $\Phi(I)=\langle\Phi(\alpha_1),\Phi(\alpha_2),...,\Phi(\alpha_s)\rangle=\langle\eta\rangle$ olur. Buradan $\beta=\Phi^{-1}(\eta)$ olarak alınırsa sonuç elde edilir.

Örnek 5.9 $\alpha_1 = 1+v^2w+v(1+w)$, $\alpha_2 = 1+v^2+v^3 \in R_{v^4-v}$ ve $I = \langle \alpha_1, \alpha_2 \rangle = \langle \beta \rangle$ olmak üzere $\phi(\alpha_1) = (1,0,1,0)$ ve $\phi(\alpha_2) = (1,1,1+w,w)$ olur. Böylece $supp(\phi(\alpha_1)) = \{1,3\}$ ve $supp(\phi(\alpha_2)) = \{1,2,3,4\}$ olup $\{1,3\} \cup \{1,2,3,4\} = \{1,2,3,4\}$ olduğu için $\beta = 1$ olarak alınabilir.

R_{v^4-v} halkası merkezi idempotent elemanların ürettiği ideallerin direkt toplamı olarak ele alındığında $F_4 -$modül olmaktadır. Çünkü R_{v^4-v} halkasının merkezi idempotent elemanları: $e_1 = 1+v^3 = (v-1)(v-w)(v-w^2)$, $e_2 = v+v^2+v^3 = v(v-w)(v-w^2)$,

$e_3 = v(1+w)+v^2w+v^3 = (v-1)(v-1)(v-w^2)$, $e_4 = vw+v^2(1+w)+v^3 = v(v-1)(v-w)$ olur. Yani, her $1 \le i, j \le 4$ için $e_i^2 = e_i$, $\sum_{i=1}^{4} e_i = 1$ ve $i \neq j$ için $e_i e_j = e_j e_i = 0$ olur. Her $\alpha = a+bv+cv^2+dv^3 = ae_1 + (a+b+c+d)e_2 + (a+c+d+(b+c)w)e_3 + (a+b+d+(b+c)w)e_4 \in R_{v^4-v}$ biçiminde merkezi idempotent elemanlar aracılığı ile tek türlü olarak yazılmaktadır. Sonuç olarak, her $\alpha \in R_{v^4-v}$ için $\alpha = \bigoplus_{i=1}^{4} \phi_i(\alpha) e_i$ şeklinde idempotent elemanlar aracılığıyla tek türlü olarak yazılmaktadır. $R_{v^4-v} = F_4e_1 \oplus F_4e_2 \oplus F_4e_3 \oplus F_4e_4$ olarak yazılmaktadır.

Örnek 5.10 $1+v^2+w+vw = \underbrace{(1+w)}_{\phi_1(1+v^2+w+vw)} .(1+v^3) + \underbrace{0}_{\phi_2(1+v^2+w+vw)} .(v+v^2+v^3) +$

$\underbrace{(1+w)}_{\phi_3(1+v^2+w+vw)} .(v(1+w)+v^2w+v^3) + \underbrace{(0)}_{\phi_4(1+v^2+w+vw)} .(vw+v^2(1+w)+v^3)$ olur.

Tanım 5.11 R_{v^4-v} üzerindeki n uzunluğundaki C **lineer kodu**; $R_{v^4-v}^n$ halkasının bir alt $R_{v^4-v} -$modülü olarak tanımlanmaktadır.

A, B, C, D kodları R_{v^4-v} üzerinde n uzunluğunda lineer kodlar olmak üzere $\oplus$ işlemi $A \oplus B \oplus C \oplus D = \{a+b+c+d \,|\, a \in A, b \in B, c \in C, d \in D\}$ şeklinde tanımlanmaktadır. R_{v^4-v} üzerinde n uzunluğunda bir C lineer kodunun elemanları merkezi idempotent elemanlar yardımı ile tek türlü olarak yazılabileceği için C lineer kodunun üreteç matrisi aşağıdaki formda elde edilmektedir:

$G=\begin{bmatrix}\left(1+v^3\right)G_1\\ \left(v+v^2+v^3\right)G_2\\ \left(v\left(1+w\right)+v^2w+v^3\right)G_3\\ \left(vw+v^2\left(1+w\right)+v^3\right)G_4\end{bmatrix}$. Burada G_1,G_2,G_3 ve G_4 matrisleri F_4 üzerinde n sütuna sahip matrislerdir. Dolayısı ile $\phi(G)=\begin{bmatrix}\phi\left(\left(1+v^3\right)G_1\right)\\ \phi\left(\left(v+v^2+v^3\right)G_2\right)\\ \phi\left(\left(v\left(1+w\right)+v^2w+v^3\right)G_3\right)\\ \phi\left(\left(vw+v^2\left(1+w\right)+v^3\right)G_4\right)\end{bmatrix}$ olur.

Böylece aşağıdaki sonuçlar elde edilmektedir:

$C_1=\{a\in F_4^4 \mid \text{bazı } b,c,d\in F_4 \text{ elemanları için,}$
$ae_1+(a+b+c+d)e_2+(a+c+d+(b+c)w)e_3+(a+b+d+(b+c)w)e_4\in C\}$

$C_2=\{(a+b+c+d)\in F_4^4 \mid ae_1+(a+b+c+d)e_2+(a+c+d+(b+c)w)e_3+(a+b+d+$
$(b+c)w)e_4\in C\}$

$C_3=\{(a+c+d+(b+c)w)\in F_4^4 \mid ae_1+(a+b+c+d)e_2+(a+c+d+(b+c)w)e_3+(a+b+d+(b+c)w)e_4\in C\}$

$C_4=\{(a+b+d+(b+c)w)\in F_4^4 \mid ae_1+(a+b+c+d)e_2+(a+c+d+(b+c)w)e_3+(a+b+d+(b+c)w)e_4\in C\}$

olsun. C_1,C_2,C_3 ve C_4 kodları F_4-lineer koddur. Ayrıca G_1,G_2,G_3 ve G_4 sırası ile C_1,C_2,C_3 ve C_4 kodları için üreteç matrisleridir.

Sonuç olarak; $C=e_1C_1\oplus e_2C_2\oplus e_3C_3\oplus e_4C_4$ şeklinde bir lineer koddur.

Önerme 5.12 $C=e_1C_1\oplus e_2C_2\oplus e_3C_3\oplus e_4C_4$ kodu R_{v^4-v} üzerinde n uzunluğunda bir lineer kod ve her $1\le i\le 4$ için C_i kodu F_4 üzerinde $\left[n,k_i,d_H(C_i)\right]$ parametrelerine sahip lineer kod olmak üzere F_4 cismi üzerinde $\phi(C)$ kodunun parametresi $\left[4n,\sum_{i=1}^{4}k_i,\min\left\{d_H(C_1),d_H(C_2),d_H(C_3),d_H(C_4)\right\}\right]$ olur.

İspat: Direkt toplam kodların parametreleri literatürden iyi bilinmektedir. $\phi(C)$ kodu F_4 üzerinde direkt toplam kodu olarak ele alınabileceğinden her $1\le i\le 4$ için C_i kodu

$\left[n, k_i, d_H(C_i)\right]$ parametrelerine sahip olduğunda $\phi(C)$ kodunun parametreleri $\left[4n, \sum_{i=1}^{4} k_i, \min\left\{d_H(C_1), d_H(C_2), d_H(C_3), d_H(C_4)\right\}\right]$ olarak elde edilmektedir.

5.2 R_{v^4-v} Halkası Üzerinde Tanımlı Devirli Kodlar

Tanım 5.13 R_{v^4-v} üzerinde n uzunluğunda bir lineer kod C olsun. Her $c = (c_0, c_1, ..., c_{n-2}, c_{n-1}) \in C$ elemanı iken $\sigma(c) = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$ oluyorsa C koduna **devirli kod** denir.

R_{v^4-v} üzerinde n uzunluğundaki her C devirli kodu ile $R_{v^4-v}[x] \Big/ \langle x^n - 1 \rangle$ bölüm halkasının idealleri arasında birebir ilişki vardır.

O halde $R_{v^4-v}[x]$ polinom halkasında $x^n - 1$ polinomunun bölenleri devirli kodların üretilmesinde önemli rol oynamaktadır.

Önerme 5.14 R_{v^4-v} üzerinde n uzunluğunda bir devirli kod C olsun. $C = \langle g(x) \rangle$ ise $g(x)$ polinomu $R_{v^4-v}[x]$ halkasında $x^n - 1$ polinomunun bir bölenidir ve $1 \le i \le 4$ için $F_4[x]$ halkası üzerinde $x^n - 1$ polinomunun bir böleni $g_i(x)$ olmak üzere $g(x) = e_1 g_1(x) + e_2 g_2(x) + e_3 g_3(x) + e_4 g_4(x)$ olur.

İspat: R_{v^4-v} halkası üzerindeki her eleman idempotent elemanlar ve Gray görüntü yardımı ile tek türlü yazılabileceği için $R_{v^4-v}[x]$ polinom halkasındaki her polinomun katsayısıda idempotent elemanlar ve Gray görüntü ile tek türlü yazılabilir. Buradan $g(x)$ polinomunun görüntüsü $\{g_1(x), g_2(x), g_3(x), g_4(x)\}$ olmak üzere $g(x) = e_1 g_1(x) + e_2 g_2(x) + e_3 g_3(x) + e_4 g_4(x)$ olacak biçimde elde edilir. $C = \langle g(x) \rangle$ olsun. $x^n - 1 = g(x)h(x) + r(x)$ ve $\deg(r(x)) < \deg(g(x))$ olacak biçimde $h(x), r(x) \in R_{v^4-v}[x]$ polinomlarının var olduğu kabul edildiğinde $r(x) \in C$ olur. $\deg(r(x)) < \deg(g(x))$ olduğu için $C = \langle g(x) \rangle$ olması ile çelişir. O halde $g(x)$

polinomu $R_{v^4-v}[x]$ halkasında x^n-1 polinomunun bir bölenidir. Böylece $1 \le i \le 4$ için $g_i(x)$ polinomu $F_4[x]$ halkası üzerinde x^n-1 polinomunun bir bölenidir.

5.3 R_{v^4-v} Halkası Üzerinde Tanımlı TS Devirli Kodlar

Bu bölümde daha sonra DNA kodların elde edilmesinde yardımcı olacak olan TS kodlarının R_{v^4-v} halkası üzerinde nasıl elde edilebileceği incelenmiştir.

Aşağıdaki teorem R_{v^4-v} halkası üzerindeki tüm TS kodları karakterize etmektedir.

Teorem 5.15 R_{v^4-v} halkası üzerinde n uzunluğunda devirli kod $C=\langle g(x)\rangle$ olsun. C, TS koddur ancak ve ancak $g(x)=e_1g_1(x)+e_2g_2(x)+e_3g_3(x)+e_4g_4(x)$ olmak üzere her $1 \le i \le 4$ için $g_i(x) \in F_4[x]$ ters sıralı polinomdur.

İspat: Her $1 \le i \le 4$ için $\deg(g_i(x))=t_i$ olsun. Genelliği bozmaksızın kabul edelim ki $t_1 \le t_2 \le t_3 \le t_4$ olsun. $g_1(x)=a_0+a_1x+\ldots+a_1x^{t_1-1}+a_0x^{t_1}$, $g_2(x)=b_0+b_1x+\ldots+b_1x^{t_2-1}+b_0x^{t_2}$, $g_3(x)=c_0+c_1x+\ldots+c_1x^{t_3-1}+c_0x^{t_3}$ ve $g_4(x)=d_0+d_1x+\ldots+d_1x^{t_4-1}+d_0x^{t4}$ olmak üzere $C=\left\langle g(x)=\sum_{i=1}^{4}e_ig_i(x)\right\rangle$ olduğunu kabul edelim. $C=\langle g(x)\rangle$ olduğu için $g(x) \in C$ olur.

Öte yandan $e_1x^{n-t_1-1}g_1(x)+e_2x^{n-t_2-1}g_2(x)+e_3x^{n-t_3-1}g_3(x)+e_4x^{n-t_4-1}g_4(x)$ polinomu $g(x)$ polinomunun ters sıralı polinomu olmak üzere $e_1x^{n-t_1-1}g_1(x)+e_2x^{n-t_2-1}g_2(x)+e_3x^{n-t_3-1}g_3(x)+e_4x^{n-t_4-1}g_4(x) \in C$ olur. İlaveten, eğer $x^ig(x) \in C$ ise $e_1x^{n-t_1-i-1}g_1(x)+e_2x^{n-t_2-i-1}g_2(x)+e_3x^{n-t_3-i-1}g_3(x)+e_4x^{n-t_4-i-1}g_4(x)$ polinomu $x^ig(x) \in C$ polinomunun ters sıralı polinomu olmak üzere $vx^{n-t-i-1}g_1(x)+(v+1)x^{n-m-i-1}g_2(x) \in C$ olur. C lineer bir kod olmak üzere $x^ig(x)$ polinomunun tüm lineer kombinasyonları C koduna düşmektedir. Böylece her elemanın ters sıralısı C koduna düşmektedir. Sonuç olarak, C kodu bir TS koddur.

Tersine, kabul edelim ki C kodu TS kod olsun. Böylece, Gray dönüşümü kullanarak $1 \le i \le 4$ için $C_i = \langle g_i(x) \rangle$ kodları F_4 üzerinde TS kodlar olduğu için [33] makalesinden her $1 \le i \le 4$ için $g_i(x)$ polinomları F_4 üzerinde ters sıralı polinomlar olmaktadır.

Sonuç 5.16 $C = \langle g(x) \rangle$ üzerinde n uzunluğunda devirli kod olsun. C, TST koddur ancak ve ancak $g(x) = e_1 g_1(x) + e_2 g_2(x) + e_3 g_3(x) + e_4 g_4(x)$ olmak üzere her $1 \le i \le 4$ için $C_i = \langle g_i(x) \rangle$, F_4 üzerinde TS koddur.

İspat: Teorem 5.15 ve [33] makalesindeki Teorem 1'den elde edilmektedir.

5.4 R_{v^4-v} Halkası Üzerinde Tanımlı DNA Kodlar

Bu bölümde, R_{v^4-v} halkasının elamanları ile DNA 4-bazlısının nasıl eşleştirildiği ve bunlardan faydalanarak, cebirsel olarak üretilen bu kodlar ile ters sıralı ve ters sıralı tamlanan özelliğe sahip DNA kodların nasıl üretildiği açıklanmaktadır.

DNA kodlarındaki ters sıralama problemi şu örnek ile açıklanabilmektedir. $(1+vw+wv^2, v^3+w)$ kodsözü R_{v^4-v} halkasında iki uzunluklu bir kodsöz olsun. Bu kodsözün DNA karşılığı "$TTGGCAAA$" iken kodsözün ters sıralısı $(1+vw+wv^2, v^3+w)^r = (v^3+w, 1+vw+wv^2)$ ve bunun DNA karşılığı "$CAAATTGG$" olur. Bu kodsözlerin DNA karşılığı birbirlerinin ters sıralısı olmamaktadır. Bu problem ψ-küme şeklinde bir üreteç kümesi tanımlayarak çözülmektedir.

DNA bazları $S_{D_4} = \{A, T, G, C\}$ kümesi ile tanımlandığında ve DNA $4-$bazları da [34] çalışmasında $S_{D_{256}} = \{AAAA, AAAT, ..., TTTT\}$ kümesi ile ifade edildiği gibi DNA $4-$bazları ile R_{v^4-v} halkasının elamanlarını [34] makalesinde tanımlanan ξ dönüşümü ile sağlanmaktadır.

[35] çalışmasındaki DNA bazlarının eşleşmesi Υ ile aşağıdaki gibi gösterilsin. $\Upsilon(0) = A$, $\Upsilon(1) = T$, $\Upsilon(w^2) = G$, $\Upsilon(w) = C$ ile gösterilmektedir. Her $a = e_1 m_1 + e_2 m_2 + e_3 m_3 + e_4 m_4 \in R$ için $\xi(a) = \Upsilon(m_1)\Upsilon(m_2)\Upsilon(m_3)\Upsilon(m_4)$ öyle ki $m_1, m_2, m_3, m_4 \in F_4$ olur ve $e_1, e_2, e_3, e_4 \in R_{v^4-v}$ merkezi idempotent elemanlarıdır.

Örneğin, $1+v+v^2(1+w)=e_1 1+e_2(1+w)+e_3(1)+e_4(1+w)\in R_{v^4-v}$ elemanın DNA karşılığı $\xi(1+v+v^2(1+w))=\Upsilon(1)\Upsilon(1+w)\Upsilon(1)\Upsilon(1+w)=TGTG$ olarak ifade edilmektedir.

DNA'nın bir özelliği olan Watson-Crick tamamlama özelliği $A^c=T$, $T^c=A$, $C^c=G$, $G^c=C$ şeklinde, DNA zincirindeki karşılıklı gelen bazların kuralını belirtmektedir. DNA 4-bazları için Watson-Crick tamamlama özelliği $(AATG)^c=TTAC$, ..., $(TCGG)^c=AGCC$ şeklinde gösterilmektedir.

$u=(u_0,...,u_{n-1})$ kodsözünün tamamlayıcısı $u^c=(u_0^c,...,u_{n-1}^c)$ şeklinde ve ters sıralı-tamlayıcısı $u^{rc}=(u_{n-1}^c,...,u_0^c)$ şeklinde gösterilmektedir.

Aşağıdaki tanım bir kodsözün DNA karşığını ifade etmektedir.

Tanım 5.17 C kodu R_{v^4-v} üzerinde n uzunluğunda bir kod olsun. $c_i\in R_{v^4-v}$ ve $c=(c_0,c_1,...,c_{n-1})\in C$ bir kodsöz olmak üzere

$$\Theta(c):C\to S_{D_4}^{2n}$$
$$(c_0,c_1,...,c_{n-1})\to(\xi(c_0)\xi(c_1)...\xi(c_{n-1}))$$

dönüşümü kodsözleri DNA $4n-$ bazlarına karşılık getirmektedir.

Örnek 5.18 $c=(c_0,c_1,c_2,c_3)=(1,v^2+v^3(1+w),1+v^3w,v+v^2+w+v^3w)$ kodsözü $\Theta(c)=(\xi(1)\xi(v^2+v^3(1+w))\xi(1+v^3w)\xi(v+v^2+w+v^3w))=(TTTTACATTGGGCATT)$ kodsözüne karşılık gelmektedir.

Tanım 5.19 Her $1\le i\le 4$ için $g_i(x)$ polinomu F_4 sonlu cismi üzerinde dereceleri sırasıyla t_i olan ve x^n-1 polinomunu bölen monik polinomlar ve $\ell=\min\{n-t_1,n-t_2,n-t_3,n-t_4\}$ olsun. $R_{v^4-v}[x]$ halkasında $g(x)$ polinomu $g(x)=e_1g_1(x)+e_2g_2(x)+e_3g_3(x)+e_4g_4(x)$ şeklinde elde edilsin.

Ayrıca, R_{v^4-v} üzerinde $\psi(a+bv+cv^2+dv^3)=a+b(v+w^2)+c(v+w^2)^2+d(v+w^2)^3$ bir otomorfizmadır ve bu otomorfizma yardımıyla $\psi-$**küme** olarak da adlandırılan $E(g)$ kümesi aşağıdaki gibi ifade edilmektedir:

$$E_i = \begin{cases} x^i g(x) & \text{eğer } i \text{ çift ise,} \\ x^i \psi(g(x)) & \text{eğer } i \text{ tek ise,} \end{cases}$$

olmak üzere,

$$E(g) = \{E_0, E_1, ..., E_{\ell-1}\}$$

şeklinde tanımlanmaktadır. $E(g)$ kümesi R_{v^4-v} halkası üzerinde C lineer kodu için bir üreteç kümesidir ve $C = \langle g(x) \rangle_\psi$ ile gösterilmektedir.

Not: Burada $\langle g(x) \rangle_\psi$ veya $\langle E(g) \rangle$ ile $E(g)$ ile üretilen R_{v^4-v} modülü göstermektedir. $(g(x))$ ile $g(x)$ tarafından üretilen ideali göstermektedir.

R_{v^4-v} üzerinde $g(x) = a_0 + a_1 x + ... + a_t x^t$ olmak üzere $E(g)$ kümesinin ürettiği lineer kodun üreteç matrisi aşağıdaki biçimde gösterilmektedir:

$$E(g) = \begin{pmatrix} a_0 & a_1 & a_2 & ... & a_t & 0 & ... & ... & ... & 0 \\ 0 & \psi(a_0) & \psi(a_1) & ... & ... & \psi(a_t) & 0 & ... & ... & 0 \\ 0 & 0 & a_0 & a_1 & ... & ... & a_t & 0 & ... & 0 \\ 0 & 0 & 0 & \psi(a_0) & \psi(a_1) & ... & ... & \psi(a_t) & 0... & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \end{pmatrix}.$$

Teorem 5.20 Her $1 \le i \le 4$ için F_4 sonlu cismi üzerinde $g_i(x)$ polinomu dereceleri sırasıyla t_i olan ve $x^n - 1$ polinomunu bölen monik kendine ters sıralı polinomlar olsun. $2 \le \ell$ çift sayı ve $t_{\max} = \max\{t_1, t_2, t_3, t_4\}$ olsun. $1 \le i \le 4$ için $t_{\max} - t_i = s_i$ çift sayı olsun. $e_{j_i} \in \{e_1, e_2, e_3, e_4\}$ ve e_{j_i} idempotent elemanları birbirlerinden farklı olmak şartıyla

$$g(x) = e_{j_1} x^{s_1/2} g_1(x) + e_{j_2} x^{s_2/2} g_2(x) + e_{j_3} x^{s_3/2} g_3(x) + e_{j_4} x^{s_4/2} g_4(x)$$

olmak üzere $C = \langle E(g) \rangle$ kodu R_{v^4-v} halkası üzerinde bir lineer koddur ve $\Theta(C)$ ters sıralı bir DNA koddur. Ayrıca, $1 \le i \le 4$ için m sıfırdan farklı $g_i(x)$ polinomlarının sayısını göstermek üzere $|\langle E(g) \rangle| = 4^{l(4-m)}$ dir.

İspat: $\alpha \in R_{v^4-v}$ ve $0 \le i \le \ell - 1$ olmak üzere

$$\left(\Theta\left(\sum_i \alpha_i E_i\right)\right)^r = \Theta\left(\sum_i \psi(\alpha_i) E_{\ell-1-i}\right) \tag{5.1}$$

denklemi DNA kodsözlerin ters sıralılarının da $C = \langle E(g) \rangle$ kodunun içinde olduğunu göstermektedir.

Aşağıdaki örnek ile Teorem 5.20'nin ispatında gösterilen bir DNA kodsözünün ters sıralı hali, üreteç matrisin hangi satırlarının kombinasyonundan elde edildiğini veren Denklem 5.1'i örneklendirilmiştir.

Örnek 5.21 $g_1(x) = 1 + w^2 x + w^2 x^2 + x^3$, $g_2(x) = 1 + x$, $g_3(x) = 0$, $g_4(x) = 0$ polinomları $F_4[x]$ halkası üzerinde $x^5 - 1$ polinomunu bölen ters sıralı polinomlar olsun. $t_{\max} = 3$, $s_1 = 0$, $s_2 = 2$ olur. Böylece,

$$g(x) = e_1 x^{s_1/2} g_1(x) + e_2 x^{s_2/2} g_2(x) + e_3 x^{s_3/2} g_3(x) + e_4 x^{s_4/2} g_4(x)$$
$$= \left(v^3 + 1\right) x^3 + x^2 \left(v^3 w + v^2 + v + w + 1\right) + x\left(v^3 w + v^2 + v + w + 1\right) + 1 + v^3$$

olarak elde edilmektedir. $E(g)$ kümesi aşağıdaki matris ile ifade edilmektedir:

$$\begin{pmatrix} E_0 \\ E_1 \end{pmatrix} = \begin{pmatrix} v^3+1 & wv^3+v^2+v+w+1 & wv^3+v^2+v+w+1 & v^3+1 & 0 \\ 0 & v^3+wv^2+v^2+wv & wv^3+wv & wv^3+wv & v^3+wv^2+v^2+wv \end{pmatrix}.$$

Özel olarak $\alpha_0 = w + v^2$ ve $\alpha_1 = 1 + v^3 w \in R$ alındığında

$$\alpha_0 E_0 + \alpha_1 E_1 = w + v^3 w + \left(1 + v^2 + v^3 + vw\right) x + \left(1 + v^2 + v^3 + vw + v^2 w + v^3 w\right) x^2 + \left(v + v^3 + w + v^3 w\right) x^3 + \left(v + v^3 + v^2 w + v^3 w\right) x^4$$

polinomuna karşılık

$$c_1 = \left(v^3 w + w, v^3 + v^2 + vw + 1, v^3 w + v^3 + v^2 w + v^2 + vw + 1, v^3 w + v^3 + v + w, v^3 w + v^3 + v^2 w + v\right)$$

kodsözü elde edilmektedir. Bu kodsözün DNA karşılığı $CAAATGAGTGGCCAGCAAAG$ olur. $\Theta(c_1)$ kodsözünün ters sıralısı Teorem 5.20'nin ispatında belirtildiği gibi aşağıdaki şekilde bulunur.

$\psi(\alpha_1)E_0+\psi(\alpha_0)E_1=1+v^3+w+v^3w+\left(v^3+w+v^2w+v^3w\right)x+\left(v+v^2+v^3+w+vw+v^3w\right)$
$x^2+\left(1+v^3+w+v^2w\right)x^3+\left(v+v^2+vw+v^3w\right)x^4$
polinomuna karşılık

$c_2=\left(v^3w+v^3+w+1,v^3w+v^3+v^2w+w,v^3w+v^3+v^2+vw+v+w,v^3+v^2w+w+1,v^3w+v^2\right.$
$\left.+vw+v\right)$

kodsözü karşılık gelmektedir ve bu kodsözün DNA karşılığı

$\Theta(c_2)=GAAACGACCGGTGAGTAAAC$ ve $\left(\Theta(c_1)\right)^r=\Theta(c_2)$

olur. Üretilen $C=\langle E(g)\rangle$ kodun DNA karşılığı aşağıdaki gibidir ve bu kod TS DNA koddur.

$\Theta(C)=\{$ *AAAAAAAAAAAAAAAAAAAA, AAAAAAAAAACAAACAAAAA,*
AAAAAAAAAGAAAGAAAAA, AAAAAAAAAATAAATAAAAA, AAAAAAACAAATAAATAAAC,
AAAAAAACAACTAACTAAAC, AAAAAAACAAGTAAGTAAAC, AAAAAAACAATTAATTAAAC,
AAAAAAAGAAACAAACAAAG, AAAAAAAGAACCAACCAAAG, AAAAAAAGAAGCAAGCAAAG,
AAAAAAAGAATCAATCAAAG, AAAAAAATAAAGAAAGAAAT, AAAAAAATAACGAACGAAAT,
AAAAAAATAAGGAAGGAAAT, AAAAAAATAATGAATGAAAT, AAAAACAAACAAAAAAAAAA,
AAAAACAAACCAAACAAAAA, AAAAACAAACGAAAGAAAAA, AAAAACAAACTAAATAAAAA,
AAAAACACACATAAATAAAC, AAAAACACACCTAACTAAAC, AAAAACACACGTAAGTAAAC,
AAAAACACACTTAATTAAAC, AAAAACAGACACAAACAAAG, AAAAACAGACCCAACCAAAG,
AAAAACAGACGCAAGCAAAG, AAAAACAGACTCAATCAAAG, AAAAACATACAGAAAGAAAT,
AAAAACATACCGAACGAAAT, AAAAACATACGGAAGGAAAT, AAAAACATACTGAATGAAAT,
AAAAAGAAAGAAAAAAAAAA, AAAAAGAAAGCAAACAAAAA, AAAAAGAAAGGAAAGAAAAA,
AAAAAGAAAGTAAATAAAAA, AAAAAGACAGATAAATAAAC, AAAAAGACAGCTAACTAAAC,
AAAAAGACAGGTAAGTAAAC, AAAAAGACAGTTAATTAAAC, AAAAAGAGAGACAAACAAAG,
AAAAAGAGAGCCAACCAAAG, AAAAAGAGAGGCAAGCAAAG, AAAAAGAGAGTCAATCAAAG,
AAAAAGATAGAGAAAGAAAT, AAAAAGATAGCGAACGAAAT, AAAAAGATAGGGAAGGAAAT,
AAAAAGATAGTGAATGAAAT, AAAAATAAATAAAAAAAAAA, AAAAATAAATCAAACAAAAA,
AAAAATAAATGAAAGAAAAA, AAAAATAAATTAAATAAAAA, AAAAATACATATAAATAAAC,
AAAAATACATCTAACTAAAC, AAAAATACATGTAAGTAAAC, AAAAATACATTTAATTAAAC,
AAAAATAGATACAAACAAAG, AAAAATAGATCCAACCAAAG, AAAAATAGATGCAAGCAAAG,
AAAAATAGATTCAATCAAAG, AAAAATATATAGAAAGAAAT, AAAAATATATCGAACGAAAT,
AAAAATATATGGAAGGAAAT, AAAAATATATTGAATGAAAT, CAAATAAATAAACAAAAAAA,
CAAATAAATACACACAAAAA, CAAATAAATAGACAGAAAAA, CAAATAAATATACATAAAAA,
CAAATAACTAATCAATAAAC, CAAATAACTACTCACTAAAC, CAAATAACTAGTCAGTAAAC,
CAAATAACTATTCATTAAAC, CAAATAAGTAACCAACAAAG, CAAATAAGTACCCACCAAAG,
CAAATAAGTAGCCAGCAAAG, CAAATAAGTATCCATCAAAG, CAAATAATTAAGCAAGAAAT,
CAAATAATTACGCACGAAAT, CAAATAATTAGGCAGGAAAT, CAAATAATTATGCATGAAAT,
CAAATCAATCAACAAAAAAA, CAAATCAATCCACACAAAAA, CAAATCAATCGACAGAAAAA,
CAAATCAATCTACATAAAAA, CAAATCACTCATCAATAAAC, CAAATCACTCCTCACTAAAC,
CAAATCACTCGTCAGTAAAC, CAAATCACTCTTCATTAAAC, CAAATCAGTCACCAACAAAG,
CAAATCAGTCCCCACCAAAG, CAAATCAGTCGCCAGCAAAG, CAAATCAGTCTCCATCAAAG,
CAAATCATTCAGCAAGAAAT, CAAATCATTCCGCACGAAAT, CAAATCATTCGGCAGGAAAT,

CAAATCATTCTGCATGAAAT, CAAATGAATGAACAAAAAAA, CAAATGAATGCACACAAAAA, CAAATGAATGGACAGAAAAA, CAAATGAATGTACATAAAAA, CAAATGACTGATCAATAAAC, CAAATGACTGCTCACTAAAC, CAAATGACTGGTCAGTAAAC, CAAATGACTGTTCATTAAAC, CAAATGAGTGACCAACAAAG, CAAATGAGTGCCCACCAAAG, CAAATGAGTGGCCAGCAAAG, CAAATGAGTGTCCATCAAAG, CAAATGATTGAGCAAGAAAT, CAAATGATTGCGCACGAAAT, CAAATGATTGGGCAGGAAAT, CAAATGATTGTGCATGAAAT, CAAATTAATTAACAAAAAAA, CAAATTAATTCACACAAAAA, CAAATTAATTGACAGAAAAA, CAAATTAATTTACATAAAAA, CAAATTACTTATCAATAAAC, CAAATTACTTCTCACTAAAC, CAAATTACTTGTCAGTAAAC, CAAATTACTTTTCATTAAAC, CAAATTAGTTACCAACAAAG, CAAATTAGTTCCCACCAAAG, CAAATTAGTTGCCAGCAAAG, CAAATTAGTTTCCATCAAAG, CAAATTATTTAGCAAGAAAT, CAAATTATTTCGCACGAAAT, CAAATTATTTGGCAGGAAAT, CAAATTATTTTGCATGAAAT, GAAACAAACAAAGAAAAAAA, GAAACAAACACAGACAAAAA, GAAACAAACAGAGAGAAAAA, GAAACAAACATAGATAAAAA, GAAACAACCAATGAATAAAC, GAAACAACCACTGACTAAAC, GAAACAACCAGTGAGTAAAC, GAAACAACCATTGATTAAAC, GAAACAAGCAACGAACAAAG, GAAACAAGCACCGACCAAAG, GAAACAAGCAGCGAGCAAAG, GAAACAAGCATCGATCAAAG, GAAACAATCAAGGAAGAAAT, GAAACAATCACGGACGAAAT, GAAACAATCAGGGAGGAAAT, GAAACAATCATGGATGAAAT, GAAACCAACCAAGAAAAAAA, GAAACCAACCCAGACAAAAA, GAAACCAACCGAGAGAAAAA, GAAACCAACCTAGATAAAAA, GAAACCACCCATGAATAAAC, GAAACCACCCCTGACTAAAC, GAAACCACCCGTGAGTAAAC, GAAACCACCCTTGATTAAAC, GAAACCAGCCACGAACAAAG, GAAACCAGCCCCGACCAAAG, GAAACCAGCCGCGAGCAAAG, GAAACCAGCCTCGATCAAAG, GAAACCATCCAGGAAGAAAT, GAAACCATCCCGGACGAAAT, GAAACCATCCGGGAGGAAAT, GAAACCATCCTGGATGAAAT, GAAACGAACGAAGAAAAAAA, GAAACGAACGCAGACAAAAA, GAAACGAACGGAGAGAAAAA, GAAACGAACGTAGATAAAAA, GAAACGACCGATGAATAAAC, GAAACGACCGCTGACTAAAC, GAAACGACCGGTGAGTAAAC, GAAACGACCGTTGATTAAAC, GAAACGAGCGACGAACAAAG, GAAACGAGCGCCGACCAAAG, GAAACGAGCGGCGAGCAAAG, GAAACGAGCGTCGATCAAAG, GAAACGATCGAGGAAGAAAT, GAAACGATCGCGGACGAAAT, GAAACGATCGGGGAGGAAAT, GAAACGATCGTGGATGAAAT, GAAACTAACTAAGAAAAAAA, GAAACTAACTCAGACAAAAA, GAAACTAACTGAGAGAAAAA, GAAACTAACTTAGATAAAAA, GAAACTACCTATGAATAAAC, GAAACTACCTCTGACTAAAC, GAAACTACCTGTGAGTAAAC, GAAACTACCTTTGATTAAAC, GAAACTAGCTACGAACAAAG, GAAACTAGCTCCGACCAAAG, GAAACTAGCTGCGAGCAAAG, GAAACTAGCTTCGATCAAAG, GAAACTATCTAGGAAGAAAT, GAAACTATCTCGGACGAAAT, GAAACTATCTGGGAGGAAAT, GAAACTATCTTGGATGAAAT, TAAAGAAAGAAATAAAAAAA, TAAAGAAAGACATACAAAAA, TAAAGAAAGAGATAGAAAAA, TAAAGAAAGATATATAAAAA, TAAAGAACGAATTAATAAAC, TAAAGAACGACTTACTAAAC, TAAAGAACGAGTTAGTAAAC, TAAAGAACGATTTATTAAAC, TAAAGAAGGAACTAACAAAG, TAAAGAAGGACCTACCAAAG, TAAAGAAGGAGCTAGCAAAG, TAAAGAAGGATCTATCAAAG, TAAAGAATGAAGTAAGAAAT, TAAAGAATGACGTACGAAAT, TAAAGAATGAGGTAGGAAAT, TAAAGAATGATGTATGAAAT, TAAAGCAAGCAATAAAAAAA, TAAAGCAAGCCATACAAAAA, TAAAGCAAGCGATAGAAAAA, TAAAGCAAGCTATATAAAAA, TAAAGCACGCATTAATAAAC, TAAAGCACGCCTTACTAAAC, TAAAGCACGCGTTAGTAAAC, TAAAGCACGCTTTATTAAAC, TAAAGCAGGCACTAACAAAG, TAAAGCAGGCCCTACCAAAG, TAAAGCAGGCGCTAGCAAAG, TAAAGCAGGCTCTATCAAAG, TAAAGCATGCAGTAAGAAAT, TAAAGCATGCCGTACGAAAT, TAAAGCATGCGGTAGGAAAT, TAAAGCATGCTGTATGAAAT, TAAAGGAAGGAATAAAAAAA, TAAAGGAAGGCATACAAAAA, TAAAGGAAGGGATAGAAAAA, TAAAGGAAGGTATATAAAAA, TAAAGGACGGATTAATAAAC, TAAAGGACGGCTTACTAAAC, TAAAGGACGGGTTAGTAAAC, TAAAGGACGGTTTATTAAAC, TAAAGGAGGGACTAACAAAG, TAAAGGAGGGCCTACCAAAG, TAAAGGAGGGGCTAGCAAAG, TAAAGGAGGGTCTATCAAAG, TAAAGGATGGAGTAAGAAAT, TAAAGGATGGCGTACGAAAT, TAAAGGATGGGGTAGGAAAT, TAAAGGATGGTGTATGAAAT, TAAAGTAAGTAATAAAAAAA, TAAAGTAAGTCATACAAAAA, TAAAGTAAGTGATAGAAAAA, TAAAGTAAGTTATATAAAAA, TAAAGTACGTATTAATAAAC, TAAAGTACGTCTTACTAAAC, TAAAGTACGTGTTAGTAAAC, TAAAGTACGTTTTATTAAAC,

TAAAGTAGGTACTAACAAAG, TAAAGTAGGTCCTACCAAAG, TAAAGTAGGTGCTAGCAAAG, TAAAGTAGGTTCTATCAAAG, TAAAGTATGTAGTAAGAAAT, TAAAGTATGTCGTACGAAAT, TAAAGTATGTGGTAGGAAAT, TAAAGTATGTTGTATGAAAT $\}$.

Sonuç 5.22 F_4 cismi üzerinde x^n-1 polinomunu bölen ters sıralı polinomlar $g_1(x), g_2(x), g_3(x)$ ve $g_4(x)$ ve R_{v^4-v} halkasında bir lineer kod $C=\langle E(g)\rangle$ olmak üzere, $r(x)=1+x+x^2+...+x^{n-1}$ polinomunu içeriyorsa, $\Theta(C)$ bir TST DNA koddur.

İspat Sonuç, DNA baz eşlemelerinden ve Teorem 5.20'den elde edilir.

Teorem 5.23 F_4 cismi üzerinde x^n-1 polinomunu bölen ters sıralı polinomlar $g_1(x)=g_2(x)=g_3(x)=g_4(x)$ ve $g(x)=\sum_{i=1}^{4}e_ig_i \in R_{v^4-v}[x]$ olsun. R_{v^4-v} halkası üzerinde $C=\langle g(x)\rangle$ (veya $C=\langle g(x)\rangle_\psi=\langle E(g)\rangle$) bir TS devirli koddur ve $\Theta(C)$ kodu TS DNA koddur. Eğer $x-1$ polinomu $g(x)$ polinomunu bölmüyor ise $\Theta(C)$ kodu TST DNA koddur. Burada C kodu aynı zamanda bir çarpık devirli koddur.

İspat: Teorem 4.28'in ispatı ile aynıdır. Burada $g_1(x)=g_2(x)=g_3(x)=g_4(x)$ olduğundan R_{v^4-v} halkası üzerinde $g(x)$ polinomunun katsayıları F_4 cisminin elemanları olduğundan ψ-kümesi oluşturuken ψ otomorfizması $g(x)$ polinomunun katsayılarını değiştirmemektedir ve $C=\langle g(x)\rangle_\psi$ devirli aynı zamanda çarpık devirli koddur.

BÖLÜM 6

SONUÇ VE ÖNERİLER

Bu çalışmada sonlu, bazı zincir olmayan halkalar üzerinde lineer kodlar çalışılmıştır. Bu halkalar üzerinde merkezi idempotent elemanlar belirlenerek halkaların yapısı sonlu cisimler yardımı ile ayrıştırılmıştır. Halka yapılarına göre kodlama teorisinin son zamanlarda biogenetik ve kuantum bilimiyle yakından ilgili olan kuantum ve DNA kodlar öncelikli olmak üzere lineer, devirli, sabit devirli, çarpık sabit devirli kodlar ve bu kodlara ait parametreler verilmiştir. Bu çalışma sırasında Wolfram Mathematica, Magma, C++, programları kullanılmıştır. Farklı cebirsel yapılar üzerinde tanımlanabilen optimal kod bulma araştırmaya açık bir problemdir.

KAYNAKLAR

[1] Shannon, C.E., (1948), "A Mathematical theory of Communication", The Bell System Technical Journal, 27: 379–423.

[2] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J., ve Solé, P., (1994). "The Z_4- linearity of Kerdock, Preparata, Goethals and Related Codes", IEEE Trans. Inform. Theory, 40: 301–319.

[3] Bonnecaze, A. ve Udaya, P., (2006). "Cyclic Codes and Self-Dual Codes over F_2+uF_2", *IEEE Trans. Inf. Theor,* 45: 1250-1255.

[4] Blackford, T., (2006). "Negacyclic Codes over Z_4 of Even Length", IEEE Trans. Inf. Theor. 49: 1417-1424.

[5] Yildiz, B., Karadeniz, S., (2010). "Linear Codes over $F_2+uF_2+vF_2+uvF_2$", Des. Codes Crypt. 54: 61-81.

[6] Yildiz, B. ve Karadeniz, S., (2010). "Cyclic Codes over $F_2+uF_2+vF_2+uvF_2$", Des. Codes Crypt., 58: 221-234.

[7] Dougherty, S. T., Yildiz, B. ve Karadeniz, S., (2011). "Codes over R_k, Gray Maps and Their Binary Images", Finite Fields and Their Applications. 17: 205-219.

[8] Boucher, D., Geiselmann, W. ve Ulmer, F., (2007). "Skew Cyclic Codes", Appl. Algebr. Eng. Commun.: 18, 379–389.

[9] Dougherty, S. T., Gaborit, P., Harada, M., ve Sole, P., (1999). "Type II Codes over F_2+uF_2", Trans. Inform. Theory, 45, 32–45.

[10] Bayram, A. ve Şiap, İ. (2013). "Structure of Codes over the Ring $Z_3[v]/\langle v^3-v\rangle$", Applicable Algebra in Engineering Communication And Computing, 2(5): 369-386.

[11] Bayram, A., Şiap, İ., (2014). "Cyclic and Constacyclic Codes over a Non-chain Ring", J. Algebra Comb. Discret. Struct. Appl. 1: 1-13.

[12] Noether, E., (1921). "Ideal Theorie in Ringbereichen", Mathematische Annalen, 83, 24-66.

[13] Hungerford T. W., (1974). Algebra, University of Washington, Addison-Wesley Publishing Company.

[14] Spindler K., (1994), Abstract Algebra with Applications (Volume II), Marcel Dekker, Inc.

[15] Ling, S. ve Xing, C., (2004), Coding Theory: A First Course, Cambridge University press.

[16] Berlekamp, E. R., (1968), "Negacyclic Codes for the Lee Metric", Proceedings of the Conference on Combinatorial Mathematics and Its Applications, 298–316.

[17] Berlekamp, E. R., (1984), Algebraic Coding Theory, Aegean Park Press.

[18] Boucher, D. ve Ulmer, F., (2009). "Coding with Skew Polynomial Rings", Journal of Symbolic Computation, 44: 1644-1656.

[19] Boucher, D. ve Ulmer, F.,(2009). "Codes as Modules over Skew Polynomial Rings", Proceedings of the 12th IMA conference on Cryptography and Coding, Lecture Notes in Computer Science, 5921: 38-55.

[20] Gürsoy, F., (2013), Değişmeli Olmayan Halkalar Üzerinde Lineer Kodlar.

[21] Şiap, İ., Abualrub, T., Aydin, N. ve Seneviratne, P., (2011). "Skew Cyclic Codes of Arbitrary Length", Int. J.Inform. Coding Theory, 2: 10-20.

[22] Yıldız, B. ve Karadeniz, S., (2010). "Self-dual Codes over $F_2 + uF_2 + vF_2 + uvF_2$", Journal of the Franklin Institute, 58: 221-234.

[23] Karadeniz, S., Yıldız, B., (2012). "Double-circulant and Double-bordered-circulant Constructions for Self-dual Codes over R_2", Adv. Math. Commun., 6(2): 193–202.

[24] Aydin, N., Şiap, İ., Ray-Chaudhuri, D., (2001). "The Structure of $1-$generator Quasi-twisted Codes and New Linear Codes", Des. Codes Cryptogr., 23 (3): 313–326.

[25] Daskalov, R.,Hristov, P., (2003). "New Binary One-generator Quasi-cyclic Codes", IEEE Trans. Inf. Theory, 49 (11): 3001–3005.

[26] Gulliver, T.A., Bhargava,V.K., (1992). "Nine Good Rate $m-1/pm$ Quasi-cyclic Codes", IEEE Trans. Inf. Theory, 38(4): 1366–1369.

[27] Heijnen, P., Von Tilborg, H., Verhoeff, T.,Weijs, S. (1998), "Some New Binary Quasi-cyclic Codes", IEEE Trans. Inf. Theory, 44(5): 1994–1996.

[28] Preskill, J., "Quantum Error Correction", theory.caltech.edu/~preskill/ph229/notes/chap7.pdf, (07.01.2013).

[29] Andrew, S., (1996). "Multiple-partical Interference and Quantum Error Correction", Proc. Roy. Soc. Lond., A452:2551-2577.

[30] Calderbank, A. R. ve W. Shor, P., (1996), "Good Quantum Error Correcting Codes Exist", Physc. Review A, 54:1098-1105.

[31] Nielsen, A. ve L. Chuang, I., (2008), Quantum Computation and Quantum Information, First Edition, The Press Syndicate of the University of Cambridge, Cambridge.

[32] Sarı, M.ve Şiap, İ., (2016). “On Quantum Codes from Cyclic Codes over a Class of Non Chain Rings”, Bulletin of the Korean Mathematical Society, 53(6): 1617-1628.

[33] Massey, J.L., (1964), ”Reversible Codes”, Information and Control, 7: 369-380.

[34] Öztaş, E. S., Şiap, İ., (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.

[35] Şiap, İ., Abualrub, T., Aydin, N., Seneviratne P., (2011), “Skew Cyclic Codes of Arbitrary Length”, Int. J. Inf. Coding Theory, 2: 10-20.

[36] Xu, X.Q., Zhu, S.X., (2011), “Skew Cyclic Codes over the Ring $F_4 + vF_4$”, J. Hefei Univ. Technol. Nat. Sci., 34: 1429–1432.

[37] Jitman, S., Ling S., Udomkavanich P., (2012), “Skew Constacyclic Codes over Finite Chain Rings”, Adv. Math. Commun., 6: 39–63.

[38] Gürsoy, F., Şiap, İ., ve Yıldız, B., (2014), “Construction of Skew Cyclic Codes over $F_q + vF_q$”, Advances in Mathematics of Communications, 8(3): 313-322.

[39] Boucher, D., Sole, P., ve Ulmer, F., (2008), “Skew Constacyclic Codes over Galois Rings”, Adv. Math. Commun., 2:273–292.

[40] Abualrub, T., Ghrayeb, A., ve Zeng X.N., (2006), “Consruction of Cyclic Codes over F_4 for DNA Computing”, Journal of the Franklin Ins., 343: 448-457.

[41] Öztaş, E.S., Şiap, İ., (2013), “Lifted Polynomials over F_{16} and Their Applications to DNA Codes”, Filomat, 27: 459–466.

[42] Şiap, İ., Abualrub, T. ve Ghrayeb, A. (2006), “Cyclic DNA Codes over the Ring $F_2[u]/(u^2-1)$ Based on the Deletion Distance”, J. Franklin Ins. 346: 731–740.

[43] Yıldız, B., Şiap İ., (2012). “Cyclic Codes over $F_2[u]/(u^4-1)$ and applications to DNA codes. Comput. Math.Appl.63: 1169–1176.

[44] Horimoto, H., Shiromoto, K., “MDS Codes over Finite Quasi-Frobenius Rings”, preprint.

[45] Shiromoto, K., Storme, L., (2003). A Griesmer Bound for Linear Codes over Finite Quasi-Frobenius Rings”, Discret. Appl. Math., 128: 263-274.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Ayşegül BAYRAM ELELE

Doğum Tarihi ve Yeri : 16.02.1987/ Araklı

Yabancı Dili : İngilizce

E-posta : aaysegulbayram@gmail.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Y. Lisans	Matematik Müh.	Yıldız Teknik Üniversitesi	2012
Lisans	Matematik	Sakarya Üniversitesi	2009
Lise	Fen-Matematik	Adapazarı Atatürk Lisesi (Y.D.A)	2005

İŞ TECRÜBESİ

Yıl	**Firma/Kurum**	**Görevi**
2010	M.E.B	Öğretmen
2012	Ondokuz Mayıs Üniversitesi	Araştırma Görevlisi
2012	Yıldız Teknik Üniversitesi	Araştırma Görevlisi

YAYINLARI

Makale

1. Bayram, A., Öztaş E. S., Şiap İ., (2016). "Codes over $F_4 + vF_4$ and Some DNA Applications". Designs, Codes and Cryptography, 2: 379–393.

2. Bayram, A. ve Siap İ., (2014). "Cyclic and Constacyclic Codes over a Non-Chain Ring". Journal of Algebra Combinatorics Discrete Structures and Applications, 1(1): 1-12.

3. Bayram, A., Şiap İ., (2013). "Structure of Codes Over the Ring $Z_3[v]/\langle v^3 - v \rangle$" Applicable Algebra in Engineering, Communication and Computing, 24(5): 369-386.

Bildiri

1: Bayram, A., Şiap İ., (2016). "Cyclic and Quantum Codes Over a Non-Chain Ring", ICQSA-2016, 25-27 Ağustos 2016, Eskişehir.

2. Bayram, A., Öztaş, E. S., Yıldız, B. ve Şiap, İ., (2016). "Construction of Cyclic Codes over a Family of Non-chain Rings and Applications to DNA", International Congress on Fundamental and Applied Sciences (ICFAS2016), 22-26 Ağustos 2016, İstanbul.

3. Bayram, A., Şiap, V., (2015). "Graph-Theoretic Approach to the Ideal Structure of a Family of Non-chain Rings", International Conference on Pure and Applied Mathematics (ICPAM2015), 25-28 Ağustos 2015, Van.

4. Bayram, A., Öztaş, E. S, Yıldız, B. ve Şiap, İ., (2015). "Construction Of Cyclic Codes Over A Special Non-Chain Ring For DNA Computing", The Second International Conference on Mathematics and Statistics, 1-5 Nisan 2015, Sharjah.

5. Bayram, A., Yıldız, B. ve Şiap, İ., (2014). "Construction of Linear Codes Over $F_q[u,v]/\langle u^q - u, v^q - v \rangle$", V Congress of the Mathematicians of Macedonia, 24-27 Eylül 2014, Ohrid.

6 . Bayram, A., Öztaş, E. S. ve Şiap, İ., (2014). "Codes over a Non Chain Ring with Some Applications to DNA", ICMS 2014, 5-9 Ağustos 2014, Seul.

7. Bayram, A. ve Şiap, İ., (2013). "Structure of Linear and Cyclic Codes Over $F_q[v]/\langle v^q - v \rangle$", Conference on Random network codes and Designs over $GF(q)$, 18-20 Eylül 2013, Gent.

8. Bayram, A. ve Şiap, İ., (2013). "Linear and Cyclic Codes Over a Finite Non-Chain Ring", CMMSE 2013: 13th International Conference Computational and Mathematical Methods in Science and Engineering, 23-27 Haziran 2013, Almeria.

Proje

1. YTÜ DOP projesi yöneticisi: Doç. Dr. Fatih DEMİRKALE (2015-2017) “Sonlu ve Değişmeli Halkalarda Lineer Kodlar”, Proje No: 2015-01-03-DOP01.

ÖDÜLLERİ

1. 2211- Yurtiçi Lisansustu Burs Programi (Bursiyer)