T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SONLU HALKALAR ÜZERİNDE TANIMLI BAZI ÖZEL KODLARIN İNCELENMESİ VE UYGULAMALARI

G. GÖZDE GÜZEL

DOKTORA TEZİ

HESAPLAMALI BİLİMLER ANABİLİM DALI

TEZ DANIŞMANI: DOÇ. DR. YASEMİN ÇENGELLENMİŞ

EDİRNE, 2019

G. Gözde GÜZEL'in hazırladığı **"Sonlu Halkalar Üzerinde Tanımlı Bazı Özel Kodların İncelenmesi Ve Uygulamaları"** başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından **Hesaplamalı Bilimler Anabilim Dalı**nda bir **Doktora Tezi** olarak kabul edilmiştir.

Jüri Üyeleri (Ünvan, Ad, Soyad):	İmza
Prof. Dr. Mustafa ÖZCAN	.....
Doç. Dr. Yasemin ÇENGELLENMİŞ	.....
Doç. Dr. M. Tolga SAKALLI	.....
Doç. Dr. İlker İNAM	.....
Doç. Dr. Zülfükar SAYGI	.....

Tez Savunma Tarihi: 04 / 01 / 2019

Bu tezin Doktora Tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Doç. Dr. Yasemin ÇENGELLENMİŞ

Tez Danışmanı .....

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

.....

Prof. Dr. Murat YURTCAN

Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ

HESAPLAMALI BİLİMLER ANABİLİM DALI DOKTORA PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

04 / 01 / 2019

G. Gözde GÜZEL

İmza

Doktora Tezi

SONLU HALKALAR ÜZERİNDE TANIMLI BAZI ÖZEL KODLARIN İNCELENMESİ VE UYGULAMALARI

T.Ü. Fen Bilimleri Enstitüsü
Hesaplamalı Bilimler A.B.D.

ÖZET

Bu tez R_{2^4}, R_{2^5} isimli iki yeni sonlu halka ve $k \geq 1$ pozitif tamsayısı ve p tek asal sayısı için $R_{(2^k)^4}$, R_{p^4} isimli iki yeni sonlu halka sınıfı üzerinde tanımlı bazı lineer kodlar üzerine yapılmış bir çalışmadır.

Başlangıçta, bu tezde verilen halka ve halka sınıflarının temel özellikleri araştırılmıştır. Bu halka ve halka sınıflarının birimselleri bulunmuş, idealleri ve tipleri belirlenmiştir. Ayrıca, bu halka tipleri üzerinde yeni Gray dönüşümler tanımlanmıştır.

Bu tezde verilen R_{2^4} sonlu halkası ve R_{p^4} halka sınıfı üzerinde devirli kodların yapısı belirlenmiş ve üreteçleri elde edilmiştir. Bu halka tipleri üzerinde, belirli uzunluğa sahip devirli ve sabit devirli kodlar tanımlanarak, aralarındaki ilişkiler ifade edilmiş ve bu kodların Gray görüntüleri belirlenmiştir. Böylece, sonlu cisimler üzerinde tanımlı optimal kodlar elde etme ihtimali arttırılmıştır.

Son olarak, bileşenleri $\mathbb{F}_{2^m}$ sonlu cisminden alınan 2×2 ve 3×3 boyutlu MDS (Maksimum Uzaklıkla Ayrılabilen) özellikli involutif matrisler elde etmek için genel bir form bulunmuştur. Bu tip matrisleri elde etmek için kullanılan tüm yöntemlerin sonuçlarını kapsayan bu form ile XOR sayısı açısından daha az maliyetli matrisler elde edilmiştir.

Yıl : 2019
Sayfa Sayısı : 98
Anahtar Kelimeler : Devirli Kodlar, Sabit Devirli Kodlar, Gray Dönüşüm, MDS Matrisler, Involutif Matrisler

Ph.D. Thesis

A STUDY OF SOME SPECIAL CODES OVER FINITE RINGS AND ITS APPLICATIONS

Trakya University Institute of Natural Sciences
Department of Computational Sciences

ABSTRACT

This thesis is a study on some linear codes over two new finite rings R_{2^4} and R_{2^5} and two new class of the finite rings $R_{(2^k)^4}$ and R_{p^4} for the conditions $k \geq 1$ and odd prime p.

Firstly, the fundamental properties of two new types of the finite rings and two new classes of the finite rings is investigated. The units are found, the ideals of the rings and the types of the ideals are determined and the new Gray maps are defined over them.

In this thesis, the structure of the cyclic codes over the finite ring R_{2^4} and the class of finite rings R_{p^4} are determined and their generators are obtained. The relationship between cyclic and constacyclic codes over them is explained, by defining the cyclic and constacyclic codes over them. The Gray images of cyclic and constacyclic codes are obtained over them. Thanks to this, the possibilities are increased in order to obtain optimal codes over the finite fields.

Finally, a general form is found to obtain 2×2 and 3×3 MDS (Maksimum Distance Seperable) involutive matrices over the finite field $\mathbb{F}_{2^m}$. With this form, which includes the results of all methods used to obtain such matrices, less costly matrices are obtained in terms of XOR counts.

Year : 2019
Number of Pages : 98
Keywords : Cyclic Codes, Constacyclic Codes, Gray Map, MDS matrices, Involutory Matrices.

Her şeyden çok sevdiğim sevgili oğlum Bulut'a…

ÖNSÖZ

Doktora Tez danışmanlığımı üstlenerek çalışmalarımın yürütülmesi sırasında yardımlarını esirgemeyen danışmanım, aynı zamanda çok sevgili hocam Sayın Doç. Dr. Yasemin ÇENGELLENMİŞ'e sonsuz teşekkür ederim.

Tez süresince çok değerli katkılarından dolayı değerli hocam Sayın Doç. Dr. Tolga SAKALLI'ya çok teşekkür ederim. Tez boyunca yaptığım akademik çalışmalarımın tümünde desteğini esirgemeyen Sayın Dr. Öğr. Üyesi Abdullah DERTLİ'ye çok teşekkür ederim.

Tez izleme komisyonunda yer alarak değerli önerileri için Prof. Dr. Mustafa ÖZCAN' a teşekkür ederim. Tez çalışmamın önemli bir bölümünü oluşturan kısmında fikir, öneri ve desteğini aldığım Sayın Doç. Dr. Sedat AKLEYLEK'e teşekkürlerimi sunarım.

Hesaplamalı Bilimler Anabilim Dalı'nı önererek bu alana ilk adımı atmamı sağlayanve doktora sürecinde moral ve desteğini esirgemeyen Sayın Dr. Öğr. Üyesi Hayati ARDA' ya çok teşekkür ederim.

Eğitim hayatım boyunca yanımda yer alan, maddi ve manevi desteklerini esirgemeyen anneme, babama, anneanneme ve çok sevgili tüm aileme çok teşekkür ederim. Tez yazımı boyunca maddi, manevi destekleriyle yanımda olan isimlerini sayamadığım tüm arkadaşlarıma çok teşekkür ederim.

Ayrıca, bana her zaman destek olan ve sabır gösteren sevgili eşim Müslüm GÜZEL'e ve oğlum Bulut GÜZEL'e çok teşekkür ederim.

G. Gözde GÜZEL

İÇİNDEKİLER

ÖZET ..... **iii**

ABSTRACT ..... **iv**

ÖNSÖZ ..... **vi**

İÇİNDEKİLER ..... **vii**

SEMBOLLER ve KISALTMALAR ..... **x**

ŞEKİLLER LİSTESİ ..... **xii**

ÇİZELGELER LİSTESİ ..... **xiii**

BÖLÜM 1 GİRİŞ **1**

1.1. Problem Tanımı 4

1.2. Katkılar 6

1.2.1. Kodlama Teorisi 6

1.2.2. Kriptoloji 7

1.3. Tez Organizasyonu 7

BÖLÜM 2 TEMEL KAVRAMLAR **8**

2.1. Cebir ile İlgili Alt Yapı 8

2.1.1. Grup, Halka ve Cisim 8

2.1.2. Modül ve Vektör Uzayı 15

2.2. Kodlama Teorisi ile İlgili Alt Yapı 18

2.2.1. Lineer Kodlar 19

2.2.2. Ağırlık ve Uzaklıklar 20

2.2.3. Singleton Sınırı ve MDS Kodlar 21

2.2.4. Devirli (Cyclic) Kodlar 22

BÖLÜM 3 R_{2^4} HALKASI VE R_{p^4} HALKA SINIFI ÜZERİNDEKİ DEVİRLİ KODLARIN İNŞASI ve GRAY GÖRÜNTÜLERİ 26

3.1. Giriş 26

3.2. R_{2^4} Sonlu Halkası Üzerinde Devirli Kod İnşası, Devirli ve $(1+u^2)-$ Sabit Devirli Kodların Gray Görüntüleri 28

3.2.1. R_{2^4} Kümesinin Cebirsel Yapısı 28

3.2.2. R_{2^4} Halkası Üzerinde Tek Uzunluklu $(1+u^2)-$ Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki 31

3.2.3. R_{2^4} Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+u^2)-$ Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri 33

3.2.4. R_{2^4} Halkası Üzerinde Devirli Kodların İnşası 37

3.2.5. R_{2^4} Halkası Üzerinde Tek Uzunluklu Devirli Kodlar ile $(1+u^2)-$ Sabit Devirli Kodların Gray Görüntülerinin İlişkisi 41

3.3. R_{p^4} Sonlu Halka Sınıfı Üzerinde Devirli Kod İnşası, Devirli Kodlar ve $\lambda-$ Sabit Devirli Kodların Gray Görüntüleri 42

3.3.1. R_{p^4} Kümesinin Cebirsel Yapısı 42

3.3.2. $kp-1$ Uzunluklu $\lambda-$ Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki 47

3.3.3. R_{p^4} Halkası Üzerinde Devirli Kodların İnşası 49

3.3.4. R_{p^4} Halkası Üzerinde Tanımlı Gray Dönüşüm 53

3.3.5. R_{p^4} Halkası Üzerindeki $kp-1$ Uzunluklu Devirli Kodlar ile $(1+u)-$ Sabit Devirli Kodların Gray Görüntülerinin İlişkisi 58

BÖLÜM 4 R_{2^5} HALKASI VE $R_{(2^k)^4}$ HALKA SINIFI ÜZERİNDE DEVİRLİ VE SABİT DEVİRLİ KODLARIN GRAY GÖRÜNTÜLERİ 59

4.1. Giriş 59

4.2. $R_{(2^k)^4}$ Sonlu Halka Sınıfı Üzerinde Devirli ve $(1+u)-$ Sabit Devirli Kodların Gray Görüntüleri 60

4.2.1. $R_{(2^k)^4}$ Kümesinin Cebirsel Yapısı 60

4.2.2. $4s-1$ Uzunluklu $(1+u)-$ Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki 64

4.2.3. $R_{(2^k)^4}$ Halkasında Tanımlı Gray Dönüşüm, Devirli ve Sabit Devirli Kodların Gray Görüntüleri 65
4.2.4. $R_{(2^k)^4}$ Halkası Üzerinde $4s-1$ Uzunluklu Devirli Kodlar ile $(1+u)-$ Sabit Devirli Kodlar Arasındaki İlişki 69
4.3. R_{2^5} Sonlu Halkası Üzerinde Devirli ve $(1+u^2+u^3)-$ Sabit Devirli Kodların Gray Görüntüleri 70
4.3.1. R_{2^5} Kümesinin Cebirsel Yapısı 70
4.3.2. R_{2^5} Halkası Üzerinde Tek Uzunluklu $\lambda-$ Sabit Devirli Kodlar 71
4.3.3. R_{2^5} Halkası Üzerinde Tanımlı Gray Dönüşüm, $\lambda-$ Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri 72
4.3.4. R_{2^5} Halkası Üzerinde Tanımlı Tek Uzunluklu Devirli Kodlar ile $\lambda-$ Sabit devirli Kodlar Arasındaki İlişki 75

BÖLÜM 5 $\mathbb{F}_{2^m}$ SONLU CİSMİ ÜZERİNE MDS ÖZELLİKLİ İNVOLUTİF MATRİSLER 76
5.1. Giriş 76
5.2. Bileşenleri $\mathbb{F}_{2^m}$ Sonlu Cisminden Alınan 2×2 Boyutlu MDS İnvolutif Matrisler 78
5.2.1. Teorem: 78
5.2.2. Sonuç: 79
5.3. Bileşenleri $\mathbb{F}_{2^m}$ Sonlu Cisminden Alınan Tüm 3×3 İnvolutif MDS Matrisleri Üreten Yeni Bir Matris Formu 79
5.3.1. Yeni 3×3 İnvolutif MDS Matris Formu 80
5.3.2. En Hafif 3×3 İnvolutif ve MDS Matrisler İçin Deneysel Sonuçlar 85

BÖLÜM 6 SONUÇLAR ve TARTIŞMALAR 88
6.1. Sonuçlar 88
6.2. Gelecek Çalışma 89

KAYNAKÇA 90

ÖZGEÇMİŞ 97

TEZ SIRASINDA YAPILAN ÇALIŞMALAR……... Hata! Yer işareti tanımlanmamış.

SEMBOLLER VE KISALTMALAR

$\mathbb{F}_q$	Finite Field with q elements	q elemanlı sonlu cisim
$\mathbb{F}_q^n$	n dimensional $\mathbb{F}_q$-vector space	n boyutlu $\mathbb{F}_q$-vektör uzayı
$d(x, y)$	The distance between x and y	x ile y arasındaki uzaklık
$d(C)$	Minimum distance of the code C	C kodunun minimum uzaklığı
$w(x)$	The weight of the element x	x elemanının ağırlığı
$w(C)$	The minimum weight of the code C	C kodunun minimum ağırlığı
(n, M, d)	The representation of a code with length n, M elements and minimum distance d	n uzunluklu, M elemanlı ve d minimum uzaklıklı kodun temsili
$[n, k, d]$	The representation of a linear code with length n, dimension k and minimum distance d	n uzunluklu, k boyutlu ve d minimum uzaklıklı lineer kodun temsili
$A_q(n, d)$	The maximum value of number of elements of a code with length n and minimum distance d over $\mathbb{F}_q$	n uzunluklu, d minimum uzaklıklı $\mathbb{F}_q$ üzerindeki bir kodun eleman sayısının alabileceği max değer
$F_q[x]$	The polynomial ring in one variable x over $\mathbb{F}_q$	Katsayıları $\mathbb{F}_q$'da olan tek x değişkenli polinom halkası

$\boldsymbol{F_q[x]/\langle f\rangle}$	The quotient ring of a polynomial ring	Bir polinom halkasının bölüm halkası
$\boldsymbol{MDS}$	Maximum Distance Seperable	Maksimum Uzaklıkla Ayrılabilen
$\boldsymbol{R_{2^4}}$	The finite ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2$	$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2$ sonlu halkası
$\boldsymbol{R_{(2^k)^4}}$	The class of finite rings $\mathbb{F}_{2^k} + u\mathbb{F}_{2^k} + u^2\mathbb{F}_{2^k} + v\mathbb{F}_{2^k}$	$\mathbb{F}_{2^k} + u\mathbb{F}_{2^k} + u^2\mathbb{F}_{2^k} + v\mathbb{F}_{2^k}$ sonlu halka sınıfı
$\boldsymbol{R_{2^5}}$	The finite ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + v\mathbb{F}_2$	$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + v\mathbb{F}_2$ sonlu halkası
$\boldsymbol{R_{p^4}}$	The class of finite rings $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + v\mathbb{F}_p$	$\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + v\mathbb{F}_p$ sonlu halka sınıfı
$\boldsymbol{\phi}$	The Gray map	Gray dönüşüm
$\boldsymbol{\sigma}$	The cyclic shift	Devirli öteleme
$\boldsymbol{\upsilon}$	The constacylic shift	Sabit devirli öteleme
$\boldsymbol{\sigma^{\otimes k}}$	The quasicyclic shift with index k	k indeksli quasicyclic öteleme
$\boldsymbol{(IM)_{3\times 3}}$	The 3×3 involutory MDS matrix	3×3'lük involutif MDS matris
$\lfloor \ldots \rfloor$	The greatest integer function	En büyük tam değer fonksiyonu

ŞEKİLLER LİSTESİ

Şekil 1.1 Temel İletişim Sistemi 1

Şekil 3.1 R_{2^4} Halkasının İdealleri 31

Şekil 3.2 R_{2^4} Halkası Üzerindeki Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı 42

Şekil 3.3 R_{p^4} Halkasının İdealleri 46

Şekil 3.4 R_{p^4} Halka Sınıfı Üzerindeki $kp-1$ Uzunluklu Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı 58

Şekil 4.1 $R_{(2^k)^4}$ Halkasının İdealleri 63

Şekil 4.2 $R_{(2^k)^4}$ Halkası Üzerindeki $4s-1$ Uzunluklu Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı 69

Şekil 4.3 R_{2^5} Halkasının İdealleri 71

Şekil 4.4 R_{2^5} Halkası Üzerindeki Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı 75

ÇİZELGELER LİSTESİ

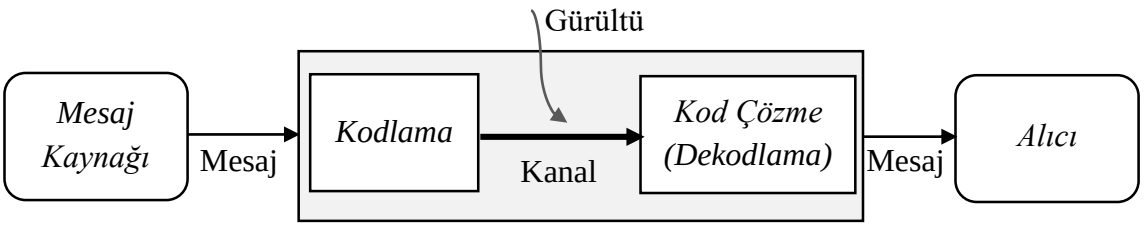
Çizelge 5.1 En Hafif 3×3 MDS ve İnvolutif Matrisler İçin Karşılaştırma 87

Çizelge 5.2 Bileşenleri $\mathbb{F}_{2^3}, \mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ Cisimlerinden Alınan En Hafif İnvolutif MDS Matrisleri 87

BÖLÜM 1

GİRİŞ

Kodlama teorisi, C. Shannon'ın bilgi teorisi çalışmasıyla (Shannon, 1949) üretilen fikirler doğrultusunda literatüre giren ve iletişim esnasında gürültülü bir kanal boyunca iletilmek istenen bir mesajın, alıcıya doğru olarak iletilmesini sağlayan matematiksel teoremler ve yöntemler bütünüdür. Bir temel iletişim sisteminde mesaj kaynağından alıcıya kadar gerçekleşen aşamalardan birisi olan kodlama, mesajda oluşabilecek hatalardan mesajı korumak için yapılmaktadır. Dekodlama ise, hataların tespiti ve düzeltilmesi için yapılmaktadır.



Şekil 1.1 Temel İletişim Sistemi

Şekil 1.1, bir temel iletişim sisteminde mesajın, *mesaj kaynağından alıcıya* gidene kadar ki izlediği süreci ifade etmektedir. Böyle bir iletişim sisteminde, *mesaj* önce dijital ortama aktarılır, kanalda mesajı bozarak hatalara sebep olan ve *gürültü* (noisy) adı verilen faktöre karşı kodlanır. *Kodlama,* çeşitli matematiksel yöntemler kullanılarak yapılır ve bu yöntemler ile gönderilen *orijinal mesaja* eklenen yeni bitler k*odlanan mesajı* oluşturur. *Kanal* bir telefon hattı, yüksek frekanslı bir radyo bağlantısı, bir uydu iletişim bağlantısı gibi dijital ortamlardır. Kodlanan mesajın bir takım hatalar ile *dekodlama (kod çözme)* birimine girişi gerçekleştiğinde, mesajın kodlama algoritmasına uygun tasarlanmış bir

dekodlama prensibi ile dekodlanıp alıcıya doğru olarak ulaştırılması amaçlanır. *Şekil 1.1*'de görülen bir temel iletişim sistemindeki, kodlama modülüne giren orijinal mesaj ile kod çözme modülünde çözülen *kod sözcüğü* her zaman aynı olmayabilir. Bu durumda, mesajın yeniden gönderilmesi istenir ve dekodlama biriminin yeniden yollanan mesajda oluşan hataları düzeltmesi beklenir. Alınan mesajın, iletilen orijinal mesaj ile aynı olabilmesi için, kodlama metodunun hatayı düzeltme kapasitesinin o iletişime uygun olarak inşa edilmesi ve dekodlama prosedürünün kanal yapısına uygun olarak geliştirilmesi gerekir.

Kodlama teorisinde, mesajın ifade edilmesinde kullanılan alfabe ya da diğer bir deyişle mesajın dijital ortamdaki karşılığı olan bitlerin ait olduğu küme sonlu elemanlıdır. Bu nedenle, kodlama teorisi sonlu kümeler (sonlu cisimler, sonlu halkalar gibi) üzerinde çalışmaktadır. Kodlama teorisi üzerine yapılan araştırmaların ilk yıllarında, teknolojinin kullandığı dil olan ikili sisteme (0, 1'lerden oluşan binary sistem) karşılık gelen $\mathbb{F}_2$ sonlu cismi ile çalışılmıştır. (Dougherty, 2017). Örneğin, 1972 yılında Mars'ın görüntülerinin Dünya'ya iletimi sırasında kullanılan $[2^5, 5^1 + 5^0, 2^4] = [32,6,16]$ parametreli $R(1,5)$ Reed Muller kodu bir ikili lineer koddur (Green, 1970). Sonlu cisimler üzerinde Hamming kodlar, Golay kodlar ve BCH kodlar gibi önemli kod aileleri de sonlu çalışılmıştır. İlk yıllarda $\mathbb{F}_2$ sonlu cismi üzerinde geliştirilen kodlar (binary kodlar), sonrasında $\mathbb{F}_q$ sonlu cismine (q bir asal sayının kuvveti olmak üzere) genelleştirilmeye başlanmıştır. Bu araştırma alanı, teknolojik gelişmeler açısından önemli olduğu kadar matematik açısından da ilginç araştırma problemleri ürettiğinden, kodlama teorisi üzerine çalışmalar farklı cebirsel yapılar üzerine inşa edilerek artmaya devam etmiştir.

Kodlama teorisinde çalışmalar, 1972 yılında ilk olarak Blake tarafından sonlu halkalar üzerine taşınmıştır (Blake, 1972; Blake 1975). Hammons ve diğerlerinin 1994 yılında yaptıkları çığır aşan çalışmasıyla beraber halkalar üzerindeki araştırmalar devam etmiştir (Hammons, Kumar, Calderbank, Sloane, Sole, 1994; Hammons, Kumar, Calderebank, Sloane, Sole, 1993). Bu çalışmalar, lineer olmayan iyi parametrelere sahip *Kerdock, Preparata, Goethals* ve ilişkili kodlara ulaşmanın, $\mathbb{Z}_4$ sonlu halkası üzerinde tanımlanan bir Gray dönüşümü yardımıyla kolaylıkla yapılabileceğini kanıtlamıştır. Bu teknik, halkaların zengin cebirsel özelliklerinden yararlanmayı mümkün kılmakla beraber, cisimler üzerinde eleman sayısı lineer olanlara kıyasla daha fazla olan, lineer

olmayan kodlar ile çalışmanın zorluklarını ortadan kaldırmıştır. Çünkü çeşitli sonlu halkalar üzerinde bazı özel lineer kodlar tanımlayarak Gray görüntü yardımıyla cisimler üzerinde lineer ya da lineer olmayan iyi kodlar elde etme olasılığı artmıştır. Bu bağlamda, kodlama teorisinin çalışma alanı ve materyalleri sonlu cisimlerden sonlu halkalara olmak üzere önemli ölçüde değişmiştir.

Cisim ya da halka üzerinde lineer ya da lineer olmayan kodlar tanımlamak mümkündür. Fakat lineer kodlar, çalışılan cebirsel yapıya bağlı olarak bir alt vektör uzayı ya da bir alt modüle karşı gelen ve matematiksel yapısı lineer olmayan kodlara kıyasla çalışmaya çok daha elverişli olan kodlardır. Aynı zamanda, lineer kodların kullanımı kodlama ve dekodlama prosedürleri açısından lineer olmayan kodlara kıyasla daha kolaydır. Hamming kodlar, BCH kodlar ve devirli (cyclic) kodlar lineer kodların önemli birkaç sınıfıdır.

Lineer kodların önemli bir sınıfı olan devirli kodlar 1957 yılında ilk olarak Prange tarafından tanımlanmıştır. Prange, bir cisim üzerinde n uzunluklu bir devirli kodu, katsayıları ilgili cisimde olan polinom halkasının $\langle x^n - 1 \rangle$ idealine bölünerek elde edilen bölüm halkasının ideallerine birebir karşılık getirmiştir (Prange, 1958; Prange, 1957). Bu birebir karşılık getirme fikri, devirli kodun matematiksel çalışmaya elverişsiz tanımı ile ilgilenmek yerine ideallerin zengin cebirsel yapısıyla çalışmaya olanak sunmuştur. Bu çalışmaları, farklı cebirsel yapıya sahip halkalar üzerinde elde edilen ve devirli kodları içeren çeşitli makaleler takip etmiştir (Abualrub, Siap, 2008; Abualrub, Siap, 2007; Bonnacaze, Udaya, 1999; Calderbank, Sloane, 1995; Özen, Uzekmek, Aydin, 2016; Pless, Qian, 1996; Pless, Sole, Qian, 1997; Qian, Zang, Zhu, 2005; Yıldız, Aydın, 2014). Devirli kodlardan daha geniş bir sınıf olan sabit devirli (constacyclic) kodların tanımlanmasıyla beraber, devirli kodlar ve sabit devirli kodların Gray görüntüleri arasındaki ilişkiyi açıklayan çeşitli çalışmalar günümüze kadar ulaşmıştır (Amarra, Nemenzo, 2008; Cengellenmis, 2009a; Cengellenmis, 2009b; Ding, Li, 2015; Dougherty, Yıldız, Karadeniz, 2011; Ozger, Kara, Yıldız, 2014; Qian, Zang, Zhu, 2006a; Qian, Zang, Zhu, 2006b; Udomkavanich, Jitman, 2009; Yu, Zhu, Kai, 2014).

Kodlama teorisi, bilginin kanalda iletimi sırasında olası hatalara karşı korumaya yönelik geliştirilen yöntemleri ve teorileri kapsarken; Kriptoloji bilimi, bilginin iletimi esnasında bilginin güvenliğini sağlamaya yönelik yöntemleri ve teorileri kapsamaktadır.

Diğer bir deyişle Kriptografi ve Kriptoanaliz bilimlerini birleştiren Kriptoloji, şifre tasarımı ve bu şifrelere karşı yapılan saldırılar ile ilgili bir bilimdir. Şifrelerin tasarımı ile ilgili olan Kriptografi bilimi, kodlama teorisi ve sonlu cisimler teorisi gibi önemli matematik dallarının uygulamalarını içermektedir. Örneğin Gelişmiş Şifreleme Standardı (Advanced Encryption Standard - AES) (FIPS 197, 2001) blok şifresi tasarımı sonlu cisimler ve özellikle de bu şifrenin yayılım tabakasının tasarımında (MixColumns dönüşümü) kodlama teorisi ile ilgili önemli uygulamalar içermektedir. AES *hesaplanabilir güvenlik* yaklaşımına uygun bir blok şifreyken, *ispatlanabilir güvenlik* yaklaşımı (Preneel, 1993; Stinson, 2002) kapsamında RSA (Rivest-Shamir-Adleman) (Forouzan, 2008) şifresi örnek verilebilir. Bu asimetrik şifrenin gücü, anahtar yapımının matematikte çözümü zor olan "asal çarpanlara ayırma" problemine dayanmasıdır.

Kriptolojide, mesajın şifrelenmesi ve şifre çözme aşamalarında kullanılan algoritmalarda MDS (veya involutif MDS) matrislerin kullanılması pek çok açıdan avantajlıdır. İnvolutif matrisler, tersi kendisine eşit matrisler olduğundan, şifreleme algoritmasının anahtarı olarak hem şifreleme kısmı hem de şifre çözme kısmında kullanılmaya elverişli elemanlardır. Bir blok şifrede kullanılan matrisin MDS matris özelliği taşıması ise yayılım katmanı (diffusion layer) açısından değerlidir. Bu nedenle, günümüze uzanan çalışmaların önemli bir kısmı bu tür matrislerin inşası ile ilgili pek çok arama tabanlı teknik geliştirmeye ve bulmaya odaklanmıştır. Bu açıdan bakıldığında, kodlama teorisinin önemli sınıflarından biri olan MDS kodlar yardımıyla elde edilen MDS matrisleri, kriptoloji biliminin kullandığı araçlardan biri olmuştur (Gupta, Ray, 2013; Lacan, Fimes, 2004; Li, Wang, 2016; Liu, Sim, 2016; Pehlivanoğlu, Sakallı, Akleylek, Duru, Rijmen, 2018; Sajadieh, Dakhilalian, Mala, Omoomi, 2012; Sarkar, Syed, 2017; Sim, Khoo, Oggier, Peyrin, 2015).

1.1. Problem Tanımı

Kodlama teorisinin asıl problemi, hatayı tespit etme ve düzeltme kapasitesi yüksek, günümüz teknolojisi gereksinimlerine ve gelecekteki teknolojik gelişmelere uygun hızda performans gösteren iyi kodlar elde etmektir. Lineer kodlar, bu araştırma problemini matematiksel açıdan çözmek için iyi bir zemin oluşturur. Örneğin, bir sonlu

cisim üzerinde lineer kod üretmek için bir üreteç matrisi yeterlidir. Bu üreteç matrise bağlı olarak, kodun parametrelerine ilişkin bilgilere ulaşmak oldukça kolaydır. Bir sonlu halka üzerinde lineer kod üretmek için ise çoğunlukla üreteç matris elde etmek zordur fakat bunu karşılayan teknikler geliştirilmiştir ve geliştirilmeye devam etmektedir. Örneğin, devirli kodların halka üzerinde tanımlanmasında minimal üreteç kümeleri elde edilmektedir.

Tezin araştırma problemi, belirli ve yeni bir takım sonlu halkalar (ya da halka aileleri) üzerinde tanımlı özel bir takım kodları kullanarak Gray dönüşüm yardımıyla cisimler üzerinde iyi parametrelere sahip kodları bulmak ve aynı zamanda yeni halkalar üzerinde tanımlı bazı özel kodların cebirsel yapısını ve bazı özelliklerini incelemektir. Tez kapsamında araştırılan bir diğer problem ise, kodlama teorisinin sunduğu avantajlardan ve hesaplama tekniklerinden yararlanılarak kriptolojinin temel araştırma problemlerinden biri olan şifre tasarımı için iyi elemanlar üretmektir. Özel olarak, tezin kapsadığı önemli problem başlıkları aşağıdaki şekildedir:

- Yeni bir sonlu halkanın cebirsel olarak tanıtılması, bu halkanın katsayıları herhangi bir asal sayıya genelleştirilerek bir halka sınıfı elde edilmesi, bu iki cebirsel yapı üzerindeki devirli kodun üreteç idealleri ve minimal üreteç kümelerinin bulunması, bu halka ve halka sınıfları için tanımlanan belirli uzunluğa sahip devirli ve sabit devirli kodların Gray görüntüleri ve arasındaki ilişkinin belirlenmesi,
- İlk probleme ilişkin tanıtılan yeni sonlu halkanın katsayıları 2^k alınarak yeni bir sonlu halka sınıfı elde edilmesi, aynı halkadan koşullar değiştirilerek 2^5 elemanlı yeni bir sonlu halka bulunması, bu sonlu halka ve halka sınıfı üzerinde belirli uzunluğa sahip devirli ve sabit devirli kodların Gray görüntüleri ve arasındaki ilişkinin verilmesi,
- $\mathbb{F}_{2^m}$ genişletilmiş sonlu cisminde kodlama teorisindeki MDS kodlardan elde edilen 3×3 boyutlu involutif matrislerin, MDS özellikli olanlarının genel formunun araştırılması ve uygulama için kullanılacak iyi elemanların elde edilmesi.

1.2. Katkılar

Katkılar, kodlama teorisi ve kriptoloji olmak üzere 2 ana bölümde incelenmektedir.

1.2.1. Kodlama Teorisi

Yeni R_{2^4} sonlu halkası üzerinde tek uzunluklu $(1+u^2)-$ sabit devirli ve devirli kodların görüntülerinin, $4n$ uzunluklu ve indeksi 4 olan ikili (binary) quasicyclic kodlara denk olduğu elde edilmiştir. Bu sonlu halka üzerinde tanımlanan tek uzunluklu devirli bir kodun iki üreteçli ideali ve minimal üreteç kümesi bulunmuştur.

p tek asalı için, yeni R_{p^4} sonlu halka sınıfının birimsel elemanları ve idealleri sınıflandırılmıştır. Bu halka sınıfı üzerindeki devirli kodların üreteç idealleri ve minimal üreteç kümesi elde edilmiştir. Aynı halka sınıfı üzerinde, p tek asalı için genel bir ϕ_{p^4} Gray dönüşümü verilmiştir. k pozitif tam sayı olmak üzere, bu halka sınıfı üzerindeki $kp-1$ uzunluklu devirli ve $(1+u)$, $(1-u+u^2)$ birimsel elemanları için tanımlanan sabit devirli kodların Gray görüntüleri elde edilmiştir ve bu görüntülerin $(kp-1)(p+1)$ uzunluklu ve indeksi $p+1$ olan $\mathbb{F}_p$ cismi üzerinde quasicyclic kodlar olduğu gösterilmiştir.

k pozitif tam sayı olmak üzere, yeni R_{2^k} sonlu halka sınıfı üzerindeki, $(1+u)-$ sabit devirli kodlar ile devirli kodlar arasındaki ilişkileri veren Gray dönüşüm, halka izomorfizması ve permütasyonlar elde edilmiştir. Bu halka sınıfı üzerindeki n uzunluklu $(1+u)-$ sabit devirli ve devirli kodların Gray görüntülerinin, $\mathbb{F}_{2^k}$ sonlu cismi üzerindeki $12n$ uzunluklu ve indeksi 12 olan quasicyclic koda denk kodlar olduğu ispatlanmıştır.

Yeni R_{2^5} sonlu halkası üzerinde, tek uzunluklu $(1+u^2+u^3)-$ sabit devirli kodların ve devirli kodların Gray görüntüleri elde edilmiştir. Bu görüntüler arasındaki ilişkileri veren halka izomorfizmaları ve permütasyonlar belirlenmiştir. Aynı halka üzerindeki $(1+u^2+u^3)-$ sabit devirli ve devirli kodların görüntülerinin $6n$ uzunluklu ve indeksi 6 olan ikili quasicyclic kodlara denk kodlar olduğu elde edilmiştir.

1.2.2. Kriptoloji

$\mathbb{F}_{2^m}$ sonlu cismi üzerindeki, 2×2 boyutunda MDS ve involutif matris formu elde edilmiştir. Bu form yardımıyla, bu matrislerin sayısını veren formül bulunmuştur.

$\mathbb{F}_{2^m}$ sonlu cismi üzerindeki, 3×3 boyutunda tüm involutif ve MDS matrislerin elde edilmesini sağlayan genel bir matris formu ve bu matrislerin sayısını veren formül elde edilmiştir. Buna ek olarak elde edilen genel form yardımıyla, donanım uygulamaları için en iyi *XOR* sayısını veren, 3×3 boyutunda, $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ sonlu cisimlerinde sırasıyla $43\ XOR$ sayılı 12 adet MDS ve involutif matris, $108\ XOR$ sayılı 24 adet MDS ve involutif matris bulunmuştur. Bu bağlamda, literatürde elde edilmiş sonuçlar iyileştirilmiştir.

1.3. Tez Organizasyonu

Tezin kalan kısmı şu şekilde düzenlenmektedir: Bölüm 2, tezde kullanılacak olan sonlu cisimler, sonlu halkalar ve kodlama teorisi ile ilgili bir takım temel teorem ve sonuçları kapsayan iki alt bölümden oluşmaktadır. Bölüm 3'de, R_{2^4} ve R_{p^4} ile adlandırılan kümelerin cebirsel yapısı, bu yapılar üzerindeki devirli kodların inşası, yeni Gray dönüşümlerin tanımları ve ayrıca devirli ve bazı sabit devirli kodların Gray görüntülerinin birbirleri ile ilişkileri anlatılmaktadır. Bölüm 4'te, yeni R_{2^5} sonlu halkası ve yeni $R_{(2^k)^4}$ sonlu halka sınıfı için sırasıyla $(1 + u^2 + u^3)$ ve $(1 + u)$ birimsel elemanları kullanılarak sabit devirli kodlar ile devirli kodların Gray görüntülerinin eldesi sağlanmaktadır. Bölüm 5'te, elemanları $\mathbb{F}_{2^m}$ genişletilmiş cisminden alınan 2×2 ve 3×3 boyutlarındaki tüm involutif MDS matrislerin elde edilmesi için yeni bir matris formu geliştirilmektedir. Bölüm 6'da, tezin kapsamında elde edilen sonuçlar ve gelecek çalışmalara yer verilmektedir.

BÖLÜM 2

TEMEL KAVRAMLAR

2.1. Cebir ile İlgili Alt Yapı

Kodlama teorisi ve kriptoloji, matematiğin alt dallarından biri olan cebir ile yakından ilişkidir. Kodlama teorisi ya da kriptoloji disiplininde; sayılar teorisi, soyut cebir, lineer cebir gibi önemli cebir konularını içeren çok sayıda tanım, teorem, sonuç veya yöntemler yoğun bir şekilde kullanılmaktadır. Dolayısıyla tezin bu bölümünde tezin bütünlüğünün korunması amacıyla, tezin kapsamı içinde kalan konularla ilgili birçok cebir kitabında da yer alan bazı temel tanım, teorem ve sonuçlara yer verilmektedir.

2.1.1. Grup, Halka ve Cisim

2.1.1.1. Tanım:

$X \neq \emptyset$ bir küme olsun. $X \times X$ kartezyen kümesinden X kümesine tanımlı bir

$$\circ : X \times X \to X$$

$$(a, b) \mapsto a \circ b$$

fonksiyonuna X içinde bir "*ikili işlem*" denir. Bir küme üzerinde bir veya daha fazla ikili işlem tanımlı ise, bu ikili işlem (veya işlemler) ile birlikte o kümeye bir "*cebirsel yapı*" denir (Karakaş, 2012).

2.1.1.2. Tanım:

$G \neq \emptyset$ bir küme ve $\circ$, G kümesi üzerinde bir ikili işlem olsun. Eğer aşağıdaki üç koşul sağlanıyorsa, $(G,\circ)$ cebirsel yapısına bir "*grup*" denir:

(i) $(G,\circ)$'ın birleşme özelliği vardır,

(ii) $(G,\circ)$'ın etkisiz elemanı vardır,

(iii) G'nin her elemanı $\circ$ işlemine göre tersinirdir.

Ek olarak,

(iv) $(G,\circ)$'ın değişme özelliği vardır.

koşulu sağlanıyorsa, $(G,\circ)$ "*değişmeli grup*" (veya *Abel grubu*) adını alır (Karakaş, 2012).

2.1.1.3. Tanım:

Boş olmayan bir K kümesi ve bir $f: K \to K$ fonksiyonu verilmiş olsun. Eğer f fonksiyonu birebir ve örten ise, f fonksiyonuna K kümesi üzerinde bir "*permütasyon*" denir. Özel olarak, $K_n = \{1,2,\dots,n\}$ kümesi üzerindeki tüm permütasyonların grubu S_n ile gösterilir ve S_n kümesine "$n-inci$ *simetrik grup*" denir. S_n'deki herhangi bir α permütasyonu, $\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}$ biçiminde de gösterilir (Karakaş, 2012).

2.1.1.4. Tanım:

$K_n = \{k_1, k_2, \dots, k_r\}$ olmak üzere, eğer $\delta \in S_n$ permütasyonu, $\delta(k_1) = k_2$, $\delta(k_2) = k_3$, …, $\delta(k_{r-1}) = k_1$ ve her $j \in K_n \backslash \{k_1, \dots, k_r\}$ için $\delta(j) = j$ sağlıyorsa, δ'ye bir "*çevrim*" denir. Bu tanımdaki çevrim, $\delta = (k_1\ k_2\ \dots\ k_r) = (k_2\ k_3\ \dots\ k_r\ k_1) = \dots = (k_r\ k_1\ \dots\ k_{r-1})$ biçiminde yazılır. Bu çevrimin uzunluğu r'dir (Karakaş, 2012).

2.1.1.5. Tanım:

S_n içinde uzunluğu 2 olan her çevrime bir "*devrinim (transpozisyon)*" denir (Karakaş, 2012).

2.1.1.6. Önerme:

Uzunluğu $r > 1$ olan her çevrim, $r - 1$ tane devrinimin çarpımı olarak yazılabilir (Karakaş, 2012).

2.1.1.7. Tanım:

$R \neq \emptyset$ bir küme ve " $+$ " ve "." , R üzerinde tanımlı iki ikili işlem olsun. Aşağıdakileri sağlayan R cebirsel yapısına bir "*halka*" denir:

(i) $(R, +)$ değişmeli bir gruptur,

(ii) Her $a, b, c \in R$ için $(a.b).c = a.(b.c)$,

(iii) Her $a, b, c \in R$ için $(a + b).c = a.c + b.c$ ve $a.(b + c) = a.b + a.c$

Eğer yukarıdaki üç koşula ek olarak,

(iv) Her $a, b \in R$ için $a.b = b.a$

koşulu sağlanıyorsa, R'ye "*değişmeli halka*" denir.

Eğer R halkası,

(v) Her $a \in R$ için $1_R.a = a.1_R = a$

koşulunu sağlayan bir 1_R elemanını içeriyorsa, R'ye "*birimli halka*" denir (Hungerford, 1973).

2.1.1.8. Tanım:

$a \in R$ sıfırdan farklı bir eleman olsun. Eğer $a.b = 0$ $(b.a = 0)$ sağlayan sıfırdan farklı bir $b \in R$ elemanı varsa a elemanına bir "*sol (sağ) bölen*" denir. R'nin hem sağ hem de sol bölen elemanına bir "*sıfır bölen*" denir (Hungerford, 1973).

2.1.1.9. Tanım:

$1_R \neq 0$ birim elemanlı R değişmeli bir halka olsun. R'nin sıfır böleni yoksa R halkasına bir "*tamlık bölgesi*" denir. $1_D \neq 0$ birim elemanlı D halkasının sıfırdan farklı her elemanı tersinir (birimsel) ise D'ye "*kesir halkası (division ring)*" denir. Her "*cisim*" değişmeli bir kesir halkasıdır (Hungerford, 1973).

2.1.1.10. Tanım:

R ve S halkaları verilsin. Her $a, b \in R$ için $f(a+b) = f(a) + f(b)$ ve $f(ab) = f(a)f(b)$ koşullarını sağlayan $f: R \to S$ fonksiyonuna "*halka homomorfizması*" denir (Hungerford, 1973).

2.1.1.11. Not:

Eğer, $f: R \to S$ halka homomorfizması;

(i) $1-1$ ise f bir "*monomorfizma"*,

(ii) Örten ise f bir "*epimorfizma"*,

(iii) $1-1$ ve örten ise f bir "*izomorfizma"*dır (Bu durumda, R ve S halkaları *izomorftur* denir ve $R \cong S$ ile gösterilir).

R bir halka olmak üzere, eğer $f: R \to R$ bir izomorfizma ise f'ye R'nin "*otomorfizması"* denir (Hungerford, 1973).

2.1.1.12. Tanım:

O_s, S halkasının etkisiz elemanı olmak üzere, $f: R \to S$ bir halka homomorfizması ise f'nin "*çekirdeği*",

$$Çek\ f = \{a \in R: f(a) = O_s\}$$

kümesi ile tanımlanır (Çallıalp, 2013).

2.1.1.13. Önerme:

R bir halka ve $\emptyset \neq S \subseteq R$ olsun. S'nin bir "*alt halka"* olması için gerekli ve yeterli koşul her $a, b \in S$ için $a - b \in S$ ve $ab \in S$ olmasıdır (Çallıalp, 2013).

2.1.1.14. Teorem:

R bir halka ve $\emptyset \neq I \subseteq R$ olsun. I kümesinin bir "*sol (sağ) ideal*" olması için gerekli ve yeterli koşul her $a, b \in I$ ve $r \in R$ için,

(i) $a - b \in I$ ve

(ii) $ra \in I$ $(ar \in I)$

olmasıdır (Hungerford, 1973).

2.1.1.15. Tanım:

R bir halka ve X, R'nin bir alt kümesi olsun. $\{A_i \mid i \in I\}$ ailesi R'nin X kümesini içeren tüm ideallerin ailesi olsun. Bu durumda, $\bigcap_{i\in I} A_i$ ailesine "*X kümesi ile üretilen ideal*" denir ve bu ideal (X) ile gösterilir.

X'in elemanlarına (X) idealinin "*üreteçleri*" denir. X sonlu bir küme ise, (X) idealine "*sonlu üretilmiştir*" denir. $X = \{x\}$ tek elemanlı bir küme ise (x) tek eleman ile üretilen ideale "*esas ideal*" denir. Tüm idealleri esas ideal olan halkaya "*esas ideal halkası*" denir. Bir esas ideal halkası, tamlık bölgesi ise bu halkaya "*esas ideal bölgesi*" denir (Hungerford, 1973).

2.1.1.16. Teorem:

$f: R \to S$ bir halka homomorfizması ise Çek f kümesi R'nin bir idealidir. Tersine, I, R'nin bir ideali ise $\varphi: R \to {}^{R}/_{I}$, $\varphi(r) = r + I = \bar{r}$ dönüşümü I çekirdek kümesi ile bir epimorfizmadır. Bu dönüşüm, *"doğal epimorfizma"* (ya da *projeksiyon dönüşümü*) olarak adlandırılır (Hungerford, 1973).

2.1.1.17. Teorem:

P, R halkasının R'den farklı bir ideali olsun. Eğer her $a, b \in R$ için

$$ab \in P \implies a \in P \text{ veya } b \in P$$

koşulu sağlanıyorsa P "*asal ideal*"*dir*. Tersine, P asal ideal ve R değişmeli ise P ideali yukarıdaki koşulu sağlar (Hungerford, 1973).

2.1.1.18. Teorem:

R, $1_R \neq 0$ birimi ile değişmeli bir halka ve P, R halkasının bir ideali olsun. P'nin asal ideal olması için gerekli ve yeterli koşul ${}^{R}/_{P}$'nin tamlık bölgesi olmasıdır (Hungerford, 1973).

2.1.1.19. Tanım:

M, R halkasının bir ideali olsun. Eğer $M \neq R$ ve her $M \subset N \subset R$ koşulunu sağlayan N ideali için $N = M$ ya da $N = R$ oluyorsa M'ye R halkasının bir "*maksimal ideali*" denir (Hungerford, 1973).

2.1.1.20. Teorem:

R, $1_R \neq 0$ birimi ile değişmeli bir halka ve M, R halkasının bir ideali olsun.

(i) M maksimal ideal ve R değişmeli ise R/M bölüm halkası bir cisimdir.

(ii) R/M bölüm halkası bir kesir halkası ise M maksimal idealdir (Hungerford, 1973).

2.1.1.21. Tanım:

Her esas ideal bölgesi tek türlü asal çarpanlarına ayrılabilen bölgedir (Hungerford, 1973).

2.1.1.22. Tanım:

Tek bir maksimal ideale sahip halkaya bir "*yerel (local) halka*" denir. Birden fazla sonlu sayıda maksimal ideali olan halkaya ise "*yarı yerel (semilocal) halka*" denir (Jitman, Udomkavanich, Ling, 2012).

2.1.1.23. Tanım:

R birimli bir sonlu değişmeli halka olsun. R halkasının tüm ideallerinin ailesi kapsama bağıntısına göre tam sıralı ise R halkasına "*sonlu bir zincir halkası (finite chain ring)*" denir (Jitman, vd., 2012).

2.1.1.24. Önerme:

R bir sonlu zincir halkası ise R halkasının tüm idealleri esas idealdir ve R tek maksimal ideale sahiptir. γ, R halkasının maksimal idealinin bir üreteci olmak üzere R halkasının tüm idealleri

$$R = \langle 1 \rangle \supsetneq \langle \gamma \rangle \supsetneq \langle \gamma^2 \rangle \supsetneq \cdots \supsetneq \langle \gamma^{t-1} \rangle \supsetneq \langle \gamma^t \rangle = \langle 0 \rangle$$

şeklinde zincir formundadır (Jitman, vd., 2012). Burada t, R halkasının "*nilpotentlik derecesi*"dir.

2.1.1.25. Teorem:

R bir halka olsun. $R[x]$, R halkasının elemanlarından oluşan ve belli bir yerden sonraki terimleri 0 olan $(a_0, a_1, \dots, a_i, 0,0, \dots)$ biçimindeki dizilerin kümesi olsun.

(i) $R[x]$ aşağıdaki toplama ve çarpma işlemleri ile bir halkadır:

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

$c_n = \sum_{k+j=n} a_k b_j$ olmak üzere, $(a_0, a_1, \dots)(b_0, b_1, \dots) = (c_0, c_1, \dots)$

(ii) R değişmeli (birimli bir halka veya sıfır bölensiz bir halka veya bir tamlık bölgesi) ise $R[x]$ halkası da değişmeli (birimli veya sıfır bölensiz veya tamlık bölgesi)'dir.

(iii) $\psi: R \to R[x]$, $r \mapsto \psi(r) = (r, 0,0, \dots)$ dönüşümü bir halka monomorfizmasıdır.

Buradaki $R[x]$ halkasına "*polinom halkası*" denir. Bu halkanın elemanlarına "*polinom*" denir (Hungerford, 1973).

2.1.1.26. Teorem:

R halkası birimli bir halka olsun ve $R[x]$'in $(0, 1_R, 0,0, \dots)$ elemanı x ile gösterilsin. Bu durumda,

(i) $x^n = (0,0, \dots, 0, 1_R, 0, \dots)$, burada 1_R elemanı dizinin $(n+1)$. bileşenidir.

(ii) $r \in R$ ise her $n \geq 0$ için, $rx^n = x^n r = (0, \dots, 0, r, 0, \dots)$, burada r elemanı dizinin $(n+1)$. bileşenidir.

(iii) Her sıfırdan farklı $f \in R[x]$ için, $f = a_0 x^0 + a_1 x^1 + \cdots + a_n x^n$ eşitliği tek şekilde olacak biçimde bir n pozitif tamsayısı ve $a_0, a_1, \dots, a_n \in R$ elemanları vardır (Hungerford, 1973).

2.1.1.27. Not:

$f = \sum_{i=0}^{n} a_i x^i$ polinom fonksiyonu için, a_i elemanlarına "f*'nin katsayıları*", a_0 elemanına "*sabit terim*" ve a_n elemanına "f*'nin baş katsayısı*" denir. Baş katsayısı 1_R

olan polinoma "*monik polinom*" denir. $x = (0, 1_R, 0, 0, \dots)$ elemanına "*bilinmeyen (indeterminate)*" denir.

2.1.1.28. Teorem:

R bir halka ve $R[x_1, x_2, \dots, x_n]$ kümesi, $u \in N^n$ elemanlarının en çok sonlu tanesi için $f(u) \neq 0$ sağlayan tüm $f: N^n \to R$ fonksiyonlarının kümesi olsun. Bu durumda,

(i) $f, g \in R[x_1, x_2, \dots, x_n]$ olmak üzere, $R[x_1, x_2, \dots, x_n]$ aşağıdaki gibi tanımlı toplama ve çarpma işlemleri ile bir halkadır:

$$(f+g)(u) = f(u) + g(u),\ (fg)(u) = \sum_{\substack{v+w=u \\ v,w \in N^n}} f(v)g(w)$$

(ii) R değişmeli (birimli bir halka veya sıfır bölensiz bir halka veya bir tamlık bölgesi) ise $R[x_1, x_2, \dots, x_n]$ 'de öyledir.

(iii) $R \to R[x_1, x_2, \dots, x_n], r \mapsto f_r$, $f_r(0,0, \dots, 0) = r$ ve tüm diğer $u \in N^n$ için $f(u) = 0$ ile tanımlı dönüşümü bir halka monomorfizmasıdır (Hungerford, 1973).

2.1.1.29. Not:

2.1.1.28 Teorem'deki $R[x_1, x_2, \dots, x_n]$ halkasına "*R üzerinde n bilinmeyenli polinom halkası*" denir (Hungerford, 1973).

2.1.2. Modül ve Vektör Uzayı

2.1.2.1. Tanım:

$(R, +, \cdot)$ bir halka ve $(A, +)$ bir toplamsal değişmeli grup olsun.

$\cdot : R \times A \to A, (r, a) \mapsto r.a$ ile tanımlı fonksiyonu, her $r, s \in R$ ve her $a, b \in A$ için,

(i) $r \cdot (a + b) = r \cdot a + r \cdot b$

(ii) $(r + s) \cdot a = r \cdot a + s \cdot a$

(iii) $r(s \cdot a) = (rs) \cdot a$

koşullarını sağlayan A'ya bir "*(sol) $R-$ modül*" denir.

Eğer $1_R \in R$ ve

(iv) Her a için $1_R \cdot a = a$ koşulu sağlanıyorsa,

A'ya bir "*birimli* $R-$ *modül* (*unitary* $R-$ *modül*)" denir. Eğer R bir kesir halkası ise, bir birimli $R-$ modüle bir "*(sol) vektör uzayı*" denir (Hungerford, 1973).

Bu tanım, $\cdot : A \times R \to A, (a,r) \mapsto a \cdot r$ tanımlı fonksiyon ile (sağ) $R-$ modül için benzer şekilde ifade edilebilir.

2.1.2.2. Tanım:

A ve B bir R halkası üzerinde iki modül olsun. Her $a, c \in A$ ve her $r \in R$ için $f(a+c) = f(a) + f(c)$ ve $f(ra) = rf(a)$ koşullarını sağlayan $f: A \to B$ fonksiyonuna bir "$R-$ *modül homomorfizması*" denir.

Eğer R bir kesir halkası ise, bir $R-$ modül homomorfizmasına bir "*doğrusal dönüşüm*" denir (Hungerford, 1973).

2.1.2.3. Tanım:

R bir halka, A kümesi bir $R-$ modül ve B kümesi A'nın boş kümeden farklı bir alt kümesi olsun. B kümesi, A'nın toplamsal alt grubu ve her $r \in R,\ b \in B$ için $rb \in B$ oluyorsa, B'ye A'nın bir "*alt modülü*" denir. Bir kesir halkası üzerindeki bir vektör uzayın alt modülüne "*alt uzay*" denir (Hungerford, 1973).

2.1.2.4. Tanım:

M bir $R-$ modül olsun ve bir $n \in \mathbb{N}$ için B kümesi M'nin bir alt kümesi olsun.

(i) B kümesi M'yi üretir. Yani her $x \in M$ için, $a_1, a_2, \dots, a_n \in R$ olmak üzere $x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ olacak şekilde $x_1, x_2, \dots, x_n \in B$ vardır.

(ii) B kümesi doğrusal bağımsızdır. Yani $a_1, a_2, \dots, a_n \in R$ ve $x_1, x_2, \dots, x_n \in B$ için $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ ise $a_1 = a_2 = \cdots = a_n = 0$.

koşulları sağlanıyorsa B kümesine M $R-$ modülü için bir "*baz*" denir. Bazın eleman sayısına "*rank*" denir. Bir baza sahip olan modüle "*serbest modül*" denir (Taşçı, 2007).

2.1.2.5. Tanım:

F bir cisim, V boş kümeden farklı bir küme ve " $+$ " işlemi V kümesi üzerinde bir ikili işlem olsun. Eğer,

(i) $(V, +)$ değişmeli grup ve

(ii) Her $c \in F$ ve $\alpha \in V$ için $c\alpha \in V$ skalerle çarpma işlemi olmak üzere,

a) Her $\alpha \in V$ için $1\alpha = \alpha$

b) Her $c_1, c_2 \in F$ ve $\alpha \in V$ için, $(c_1 c_2)\alpha = c_1(c_2\alpha)$

c) Her $c \in F$ ve $\alpha, \beta \in V$ için, $c(\alpha + \beta) = c\alpha + c\beta$

d) Her $c_1, c_2 \in F$ ve $\alpha \in V$ için, $(c_1 + c_2)\alpha = c_1\alpha + c_2\alpha$

özellikleri sağlanıyorsa, V kümesine F cismi üzerinde bir "*vektör uzayı*" denir. V'nin elemanlarına "*vektör*", F'nin elemanlarına "*skaler*" denir (Hoffman, Kunze, 1971).

2.1.2.6. Tanım:

V, F cismi üzerinde bir vektör uzayı ve $\beta \in V$ bir vektör olsun.

$$\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = \sum_{i=1}^{n} c_i\alpha_i$$

sağlayan $c_1, c_2, \ldots, c_n \in F$ skalerleri varsa β vektörüne $\alpha_1, \alpha_2, \ldots, \alpha_n \in V$ vektörlerinin "*doğrusal birleşimi*" denir (Hoffman, vd., 1971).

2.1.2.7. Tanım:

V, F cismi üzerinde bir vektör uzayı ve $W \subseteq V$ olsun.

W kümesi V üzerindeki vektör toplamı ve skalerle çarpma işlemlerine göre bir vektör uzayı oluyorsa, W kümesine "*V 'nin bir alt uzayı*" denir (Hoffman, vd., 1971).

2.1.2.8. Teorem:

V, F cismi üzerinde bir vektör uzayı ve $W \subseteq V$ olsun.

W kümesinin V'nin bir alt uzayı olması için gerekli ve yeterli koşul her $\alpha, \beta \in W$ ve $c \in F$ için $c\alpha + \beta \in W$ olmasıdır (Hoffman, vd., 1971).

2.1.2.9. Tanım:

V bir vektör uzayı ve $S \subseteq V$ olsun.

V vektör uzayının S'yi kapsayan tüm alt uzaylarının arakesiti W'ye "*S tarafından gerilen alt uzay*" denir. $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ sonlu kümesi için W'ya "*$\alpha_1, \alpha_2, \dots, \alpha_n$ elemanları ile gerilen alt uzay*" denir (Hoffman, vd., 1971).

2.1.2.10. Teorem:

Herhangi bir vektör uzayının boş kümeden farklı S kümesi ile gerilen alt uzayı, S'deki vektörlerin tüm doğrusal kombinasyonlarının kümesidir (Hoffman, vd., 1971).

2.1.2.11. Tanım:

V, F cismi üzerinde bir vektör uzayı ve $S \subseteq V$ olsun. Eğer,

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$$

sağlayan $\alpha_1, \alpha_2, \dots, \alpha_n \in S$ vektörleri ve hepsi 0 olmayan $c_1, c_2, \dots, c_n \in F$ skalerleri varsa, S kümesine "*doğrusal bağımlıdır*" aksi halde, "*doğrusal bağımsızdır*" denir. Buna denk tanım şu şekildedir: S kümesinin vektörlerinin doğrusal bağımsız olması için gerekli ve yeterli koşul her $\alpha_1, \alpha_2, \dots, \alpha_n \in S$ için $c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$ eşitliğini sağlayan tüm i'ler için $c_i = 0$ olmasıdır (Hoffman, vd., 1971).

2.1.2.12. Tanım:

V bir vektör uzayı olsun. V'yi geren ve V'nin doğrusal bağımsız vektörlerinden oluşan kümeye V'nin bir "*tabanı*" denir. V'nin tabanı sonlu ise, V uzayına "*sonlu boyutlu*" denir (Hoffman, vd., 1971).

2.2. Kodlama Teorisi ile İlgili Alt Yapı

Bilgi iletimi ya da bilginin depolanması aşamalarında iletişim kanalında meydana gelen gürültü faktöründen bilginin korunarak muhafaza edilmesi için kodlama ve dekodlama yapılır. Kodlama teorisi, mesajın kodlanmasından başlayıp alıcıya ulaşana kadar ki (varsa hataların tespiti ve düzeltilmesine kadar olan) tüm aşamaları

kapsamaktadır. Bu bölümde, kodlama teorisinin kapsadığı bu aşamaların daha iyi kavranabilmesi için kullanılan terminoloji, genel tanım ve teoremlere yer verilecektir.

2.2.1. Lineer Kodlar

$\mathbb{F}_q^n$ kümesi, $\mathbb{F}_q$ sonlu cismi üzerindeki sıralı n'lilerin kümesi olsun, bu küme $\mathbb{F}_q$-vektör uzayıdır. $\mathbb{F}_q^n$ kümesinin M elemanlı bir C alt kümesine, $\mathbb{F}_q$ sonlu cismi üzerindeki (n, M) kodu denir. $(a_1, a_2, \dots, a_n) \in F_q^n$ vektörü $a_1 a_2 \dots a_n$ formunda da gösterilir ve C'deki vektörlere "*kod sözcükleri*" denir. C kümesi $\mathbb{F}_q^n$ vektör uzayının $k-$ boyutlu bir alt uzayı ise C'ye $\mathbb{F}_q$ sonlu cismi üzerinde bir $[n, k]$ "*lineer kodu*" denir. C lineer kodun q^k tane kod sözcüğü vardır. Bir lineer kodun gösterilmesinin en genel iki yolu vardır: üreteç matrisi ya da kontrol matrisi (parity check matrisi). Satırları C alt uzayının bir tabanı ile yazılan bir $k \times n$'lik G matrisine, C $[n, k]$ lineer kodunun "*üreteç matrisi*" denir. Bir G üreteç matrisinin her doğrusal bağımsız k sütununun kümesi için, onunla ilişkili koordinatlarının kümesi C'nin "*bilgi kümesini*" oluşturur. $r = n - k$ olmak üzere, r'ye C'nin "*kalanı (redundancy)*" denir. I_k matrisi $k \times k$'lık birim matris olmak üzere, kodun $[I_k|A]$ formundaki üreteç matrisine "*standart form*" denir. $C = \{x \in \mathbb{F}_q^n \mid Hx^T = 0\}$ ile tanımlı $(n - k) \times k$'lık H matrisine, C $[n, k]$ lineer kodu için "*kontrol matrisi (parity-check matrisi)*" denir (Huffman, Cary, Pless, 2003).

2.2.1.1. Teorem:

Eğer $G = [I_k|A]$ matrisi bir C $[n, k]$ lineer kodunun standart formdaki üreteç matrisi ise, $H = [-A^T|I_k]$ matrisi C'nin bir kontrol matrisidir (Huffman, vd., 2003).

2.2.1.2. Teorem:

R sonlu bir halka ve n pozitif tamsayı olsun. C kümesi,

$$R^n = \{(u_1, u_2, \dots, u_n) : u_i \in R, i = 1,2, \dots, n\}$$

kümesinin bir $R-$ alt modülü ise C'ye "*lineer kod*" adı verilir. R^n kümesinin herhangi bir elemanına "*sözcük*", C kodunun herhangi bir elemanına "*kod sözcüğü*" denir (Huffman, vd., 2003).

2.2.2. Ağırlık ve Uzaklıklar

Bir kodun minimum uzaklık parametresi en önemli unsurlarından birisidir. Kodun minimum uzaklığı, kodun hatayı tespit etme ve düzeltme kapasitesini ortaya koyar.

2.2.2.1. Tanım:

$d: \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N} \cup \{0\}, \quad (x, y) \mapsto d(x, y) = |\{i : x_i \neq y_i\}|$ dönüşümüne "*Hamming uzaklığı*" denir, d dönüşümü *2.2.2.2 Önerme'*yi sağlayan bir metriktir (Ling, Xing, 2004).

2.2.2.2. Önerme:

x, y ve $z \in \mathbb{F}_q^n$ olsun. Aşağıdakiler sağlanır:

(i) $0 \leq d(x, y) \leq n$

(ii) $d(x, y) = 0$ olması için gerekli ve yeterli koşul $x = y$ olmasıdır.

(iii) $d(x, y) = d(y, x)$

(iv) $d(x, z) \leq d(x, y) + d(y, z)$ (üçgen eşitsizliği) (Ling, vd., 2004).

2.2.2.3. Tanım:

En az iki kod sözcüğü içeren bir C kodu için, C'nin "*minimum uzaklığı*",

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

biçiminde tanımlıdır (Ling, vd., 2004).

2.2.2.4. Tanım:

Bir n uzunluklu, M elemanlı ve d minimum uzaklıklı kod, bir "(n, M, d) *kodu*" olarak adlandırılır. n, M ve d sayılarına kodun "*parametreleri*" denir (Ling, vd., 2004).

2.2.2.5. Teorem:

d minimum uzaklıklı bir kod, $d - 1$ hata tespit eder ve $\left\lfloor \frac{d-1}{2} \right\rfloor$ hata düzeltir (Ling, vd., 2004).

2.2.2.6. Tanım:

$x \in \mathbb{F}_q^n$ sözcüğü için, x'in (Hamming) ağırlığı sıfırdan farklı koordinatlarının sayısıdır. Yani, $wt(x) = d(x, \bar{0})$ sağlanır. Burada $\bar{0}$ vektörü tüm bileşenleri 0 olan kod sözcüğüdür (Ling, vd., 2004).

2.2.2.7. Lemma:

$x, y \in \mathbb{F}_q^n$ ise, $d(x, y) = wt(x - y)$ sağlanır (Ling, vd., 2004).

2.2.2.8. Tanım:

C bir kod olsun. C kodunun sıfır vektöründen farklı kod sözcüklerinin ağırlıklarının en küçüğüne C'nin "*minimum (Hamming) ağırlığı*" denir ve $wt(C)$ ile gösterilir (Ling, vd., 2004).

2.2.2.9. Teorem:

C lineer bir kod ise $d(C) = wt(C)$ sağlanır (Ling, vd., 2004).

2.2.3. Singleton Sınırı ve MDS Kodlar

C, $\mathbb{F}_q$ cismi üzerinde N elemanlı, $n = k + r$ uzunluklu ve d minimum uzaklıklı bir lineer kod olsun.

2.2.3.1. Tanım:

n kodun uzunluğu ve $r = n - k$ olmak üzere, eleman sayısı $M = q^k$ olan ve $d = r + 1$ sağlayan kodlara "*maksimum uzaklıkla ayrılabilir* (Maximum Distance Separable – MDS) *kodlar*" denir (Singleton, 1964).

2.2.3.2. Teorem:

$M = q^k$ ise $r = n - k$ olmak üzere, $d \leq r + 1$ sağlanır (Singleton, 1964).

Buradaki sınır koşuluna "*Singleton sınırı*" denir, bu sınırın eşitlik durumunu sağlayan kodlara "*MDS kodlar*" denir (Huffman, vd., 2003).

2.2.3.3. Sonuç:

Sonlu bir cisim üzerinde tanımlı n uzunluklu C lineer kodunun MDS kod olması için gerekli ve yeterli koşul $k \times n$ mertebeli G üreteç matrisinin her k sütunun doğrusal bağımsız olmasıdır. Buna denk koşul ise, $(n-k) \times n$ mertebeli H kontrol matrisinin $n-k$ sütunun doğrusal bağımsız olmasıdır (MacWilliams, Sloane, 1983).

2.2.3.4. Teorem:

C, $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı $[n, k, -]$ parametreli, $H = [A|I_{n-k}]$ kontrol matrisli bir lineer kod olsun. C kodunun bir MDS kod olabilmesi için gerekli ve yeterli koşul A matrisinin her kare alt matrisinin terslenebilir olmasıdır (MacWilliams, vd., 1983).

2.2.3.5. Teorem:

C, $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı $[n, k, -]$ parametreli, $G = [I_k|A]$ üreteç matrisli bir lineer kod olsun. C kodunun bir MDS kod olabilmesi için gerekli ve yeterli koşul A matrisinin her kare alt matrisinin terslenebilir olmasıdır (MacWilliams, vd., 1983).

2.2.3.6. Tanım:

$XOR(a)$, $\mathbb{F}_2[x]/\langle p(x)\rangle$ sonlu cismindeki keyfi bir b sayısının $\mathbb{F}_2[x]/\langle p(x)\rangle$ sonlu cismindeki a sayısı ile çarpıldığında uygulanması gerekli olan XOR işlemlerinin sayısıdır (Sim, vd., 2015; Khoo, Peyrin, Poschmann, Yap, 2014).

2.2.4. Devirli (Cyclic) Kodlar

2.2.4.1. Tanım:

$C \subseteq \mathbb{F}_q^n$ alt küme olsun. σ dönüşümü her $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n$ için $\sigma(c) = (c_{n-1}, c_0, \dots, c_{n-2}) \in \mathbb{F}_q^n$ ile tanımlı "*devirli öteleme* (*cyclic shift*)" olmak üzere, $\sigma(C) = C$ oluyorsa C kümesine "*devirli (cyclic) küme*" denir. C, bir lineer kod ve devirli bir küme ise bu koda "*devirli (cyclic) kod*" denir (Hill, 1986).

2.2.4.2. Tanım:

n bir pozitif tamsayı olsun ve $1 \leq l < n$ sağlayan l sayısı n'nin bir böleni olsun. $\mathbb{F}_q$ sonlu cismi üzerindeki C lineer kodu için, $c = (c_0, c_1, \dots, c_{n-1}) \in C$ iken $(c_{n-l}, c_{n-l+1}, \dots, c_{n-1}, c_0, c_1, \dots, c_{n-l-1}) \in C$ oluyorsa C koduna "l *indeksli quasicyclic kod*" veya "$l-$ *quasicyclic kod*" denir. Özellikle de, bir $1-$ quasicyclic kod devirli koddur (Ling, vd., 2004).

2.2.4.3. Tanım:

$\lambda \in \mathbb{F}_q^*$ olsun. $\mathbb{F}_q$ üzerindeki C lineer kodu için, her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ iken $(\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$ oluyorsa C'ye "$\lambda-$ *sabit devirli kod* ($\lambda-$ *constacyclic kod*)" denir. Özellikle de, $\lambda = -1$ ise C koduna "*negacyclic kod*" denir (Ling, vd., 2004).

$\lambda = 1$ durumunda sabit devirli kod tanımı, devirli kod tanımı ile çakışır. Buradaki, her $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n$ için $\upsilon(c) = (\lambda c_{n-1}, c_0, \dots, c_{n-2}) \in \mathbb{F}_q^n$ ile tanımlı υ'ye "*sabit devirli öteleme (constacyclic shift)*" denir.

2.2.4.4. Teorem:

$n \neq 1$ ve $n \in \mathbb{N}$ olmak üzere, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ polinom halkası bir esas ideal halkasıdır (MacWilliams, vd.,1983).

2.2.4.5. Teorem:

$$\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/\langle x^n - 1\rangle$$

$$a = (a_0, a_1, \dots, a_{n-1}) \longmapsto \pi(a) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$$

ile tanımlı π lineer dönüşüm olmak üzere, $C \subseteq \mathbb{F}_q^n$ lineer kodunun devirli kod olması için gerekli ve yeterli koşul $I = \pi(C)$ nin $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasının bir ideali olmasıdır (Ling, vd., 2004).

λ birimsel eleman olmak üzere, 2.2.4.5 Teorem'deki $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ bölüm halkasının yerine $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ bölüm halkası alınırsa π yine bir lineer dönüşümdür ve $C \subseteq \mathbb{F}_q^n$ lineer kodu için $\pi(C)$ ideali $\lambda-$ sabit devirli koda; $\lambda = -1$ için negacyclic koda karşılık gelir.

π dönüşümü yardımıyla, C kodunun herhangi bir $a = (a_0, a_1, \dots, a_{n-1})$ elemanına $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ bölüm halkasının bir $\pi(a) = a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$ denklik sınıfı karşılık getirilir. Fakat kolay ve sade gösterim için $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$ denklik sınıfı yerine $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ polinomu kullanılacaktır. Bu durumda, bir devirli kodun elemanlarını onlara karşılık gelen polinom gösterimleri ile yazmak mümkündür.

2.2.4.6. Teorem:

I, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasının bir ideali ve $\overline{g(x)}$, I idealinin sıfırdan farklı bir en küçük dereceli monik polinomu olsun.

(i) $\overline{g(x)}$ polinomu I idealinin bir üretecidir ve bu monik polinom tektir.

(ii) $g(x)$ polinomu $x^n - 1$ polinomunu böler (Ling, vd., 2004).

2.2.4.7. Tanım:

C, $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda bir devirli kod olsun. C koduna karşılık gelen $g(x)$ polinomu, $\pi(C)$ idealinin sıfırdan farklı, en küçük dereceli monik polinomu olmak üzere, $g(x)$ polinomuna C kodunun "*üreteç polinomu*" denir ve

$$C = \langle\overline{g(x)}\rangle = \{\overline{f(x)}.\overline{g(x)} : \overline{f(x)} \in \mathbb{F}_q[x]/\langle x^n - 1\rangle\}$$

biçiminde yazılır (Ling, vd., 2004).

2.2.4.8. Teorem:

$\mathbb{F}_q[x]$ halkasında, $x^n - 1$ polinomunun her monik böleni $\mathbb{F}_q$ üzerinde tanımlı bir devirli kod üretir (Ling, vd., 2004).

2.2.4.9. Lemma:

$g(x) = g_0 + g_1x + \cdots + g_rx^r$ polinomu devirli kodun üreteci ise $g_0 \neq 0$ sağlanır (Hill, 1986).

2.2.4.10. Teorem:

$der(g(x)) = r$ olmak üzere, n uzunluklu C devirli kodunun üreteç polinomu $g(x) = g_0 + g_1x + \cdots + g_rx^r$ olsun. C kodunun boyutu $boy(C) = n - r = k$ ve üreteç matrisi,

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & & & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_r \end{bmatrix}$$

biçimindedir (Hill, 1986).

BÖLÜM 3

R_{2^4} HALKASI VE R_{p^4} HALKA SINIFI ÜZERİNDEKİ DEVİRLİ KODLARIN İNŞASI VE GRAY GÖRÜNTÜLERİ

3.1. Giriş

Bir temel iletişim sisteminde amaç, kaynaktan gönderilen mesajı alıcıya doğru olarak ulaştırmaktır. Mesaj, bir dilin alfabesi kullanılarak ifade edilir ve alfabe sonlu bir kümedir. Bu, iletişimin sonlu bir küme üzerinde yapılacağını ifade eder. Sonlu kümelere matematiksel anlamlar yüklemek için, üzerinde cebirsel yapının tanımlı olduğu sonlu cisim ya da sonlu halkalar tanımlanır. Bu sonlu cebirsel yapılar kullanılarak, iletilmek istenen mesaj dijital ortama aktarılır. Dijital ortamdaki mesaj bir kodlama birimi tarafından kodlanır ve kanala gönderilir. Kod sözcüğü denilen bu mesajlar, iletişim esnasında gürültülü bir kanalda seyrederken bazı hatalar oluşabilir. Bunun anlamı, kod sözcüğünün bazı sembolleri değişmiş demektir. Dekodlama birimi, gürültülü kanaldan geçen hatalı kod sözcüğündeki hataları tespit eder ve düzeltir. Aksi takdirde, mesajın tekrar iletimi istenir. Dekodlanan mesaj orijinal mesaja dönüştürülerek alıcıya ulaştırılır.

Bu bölümde, böyle bir iletişim sistemi içerisinde gerçekleştirilen ve kodlama işlemini yapan kodlama biriminin matematiksel alt yapısını hazırlayacak olan lineer kodlar yeni bazı sonlu halkalar üzerinde tartışılmaktadır. Bu yeni sonlu halkalar üzerinde lineer kodların önemli bir sınıfı olan devirli kodlar ve onların Gray görüntüleri optimal kod bulma amacıyla araştırılmaktadır. Son 50 yılı aşkın süredir pek çok bilim insanı tarafından incelenen devirli kodlar, ilk olarak 1957 yılında Prange tarafından

tanımlanmıştır. Prange bir $\mathbb{F}$ sonlu cismi üzerindeki n uzunluklu devirli bir kodun, $\mathbb{F}[x]/\langle x^n - 1\rangle$ bölüm halkasının bir idealine birebir karşılık geldiğini göstermiştir (Prange, 1958; Prange, 1957). n uzunluklu devirli bir kodun üreteçleri, $x^n - 1$ polinomunun monik bölenleridir. Dolayısıyla, $x^n - 1$ polinomunun tanımlandığı bölüm halkasında çarpanlara ayırılışının bilinmesi gerekliliği ortaya çıkar. Halkalar üzerinde çarpanlara ayırma, cisimler üzerinde çarpanlara ayırmadan farklı ve daha zor olacağı için, halkalar üzerinde devirli kodların tanımlanmasında bir takım zorluklar olacağı açıktır. Bu problemin çözüm metotları, üzerinde çalışılan halkanın yapısına göre değişkenlik gösterdiği için birçok araştırmacı, farklı cebirsel özellikteki halkaları karakterize ederek, devirli kodların üreteçlerini bulmaya ilişkin metotlar geliştirmişlerdir. Bu metotlardan biri, devirli kodun üreteçlerinin bulunacağı halkadan, devirli kodların üreteçlerinin bilindiği bir cisme ya da halkaya tanımlanan dönüşümün "çekirdek ve görüntü" kümeleri yardımıyla, devirli kodların üreteçlerinin birden fazla üreteçli idealler olarak belirlenmesidir. Bu tekniğe, kısaca "*çek-gör fikri*" diyelim. Pless, (Pless, vd., 1996) çalışmasında $\mathbb{Z}_4$ halkası üzerindeki tek uzunluklu devirli kodların üreteçlerini elde etmiştir. $\mathbb{Z}_4$ halkasındaki devirli kodların üreteçleri ve "*çek-gör fikri*" kullanılarak, $\mathbb{Z}_2 + u\mathbb{Z}_2$ ve $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$ halkalarında (Abualrub, vd., 2007) çalışmasında, $\mathbb{Z}_4$ halkası üzerindeki devirli kodların uzunluk kısıtlaması olmaksızın (Abualrub, vd., 2008) çalışmasında, $\mathbb{Z}_4 + u\mathbb{Z}_4$ $(u^2 = 0)$ halkası üzerindeki devirli kodların üreteçleri ve bu devirli kodların Gray görüntüleri (Yıldız, Aydın, 2014) çalışmasında, $\mathbb{Z}_4 + u\mathbb{Z}_4$ $(u^2 = 1)$ halkası üzerindeki devirli kodların üreteçleri ve bu devirli kodların Gray görüntüleri (Özen, vd., 2016) çalışmasında, $\mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$ halkasındaki devirli kodların inşası (Sing, Kewat, 2015) çalışmasında ve $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ çok değişkenli halkasındaki devirli kodların üreteçleri de (Yıldız, vd., 2011) çalışmasında verilmiştir. Bir diğer metot ise, sonlu zincir halkalarındaki devirli kodların üreteçlerinin belirlenmesidir. Herhangi bir R sonlu zincir halkasında, n halkanın rezidü cisminin karakteristiğini bölmeyen bir sayı olmak üzere, n uzunluklu bir C devirli kodun üretecinin, R'nin maksimal ideali $\langle a\rangle$ ve a'nın nilpotentlik derecesi t olmak üzere, $g_{t-1}|\dots|g_1|g_0|x^n - 1$ koşulunu sağlayan polinomlar kullanılarak $\langle g_0, ag_1, \dots, a^{t-1}g_{t-1}\rangle$ ideali olduğu gösterilmiştir (Dinh, Lopez-Peremouth, 2004). $\mathbb{F}_p[u]/\langle u^n\rangle$ halkaları sonlu zincir halkası olduğundan bu halkalar üzerindeki devirli kodların üreteçleri, Dinh'in çalışması kullanılarak elde edilir. (Qian, vd., 2005) makalesi

de bu sonucu kullanarak, $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$ sonlu zincir halkasındaki devirli kodların üreteçlerini vermiştir. Devirli kodların üreteçlerini bulmaya yönelik bir başka metot ise, $\mathbb{F}_2 + v\mathbb{F}_2$ halkası için çalışılmıştır (Zhu, Wang, Sji, 2010). Bu metot, Çin'in Kalan Teoremi (Chineese Remainder Theorem) yardımıyla halkanın başka halkaların direkt toplamı biçiminde yazılarak, o halkalardaki devirli kodların üreteçlerinin bilinmesiyle yeni halka üzerindeki devirli kodların üreteçlerini belirlemeye yöneliktir.

Tezin bu bölümünde, yeni bir sonlu halka ve bir sonlu halka sınıfı tanıtılmaktadır. Burada çalışılan değişmeli sonlu halkaların her biri iki değişkenli esas ideal halkası, yarı yerel halka ve Frobenious halkasıdır. Bu halka ve halka sınıfı üzerindeki çalışmalar iki alt başlıkta verilmektedir. Her iki alt başlıkta da, ilgili halkalar üzerinde devirli kodların yapısı araştırılmakta ve tek uzunluklu devirli kodların üreteçleri "*çek-gör fikri*" yardımıyla elde edilmektedir ve her biri için farklı Gray dönüşümler tanımlanarak, elde edilen devirli ve sabit devirli kodların Gray görüntüleri arasındaki ilişkiler ispatlanmaktadır. Ayrıca bu bölümde verilen sonlu halka sınıfına ait birimsel elemanlar ve idealler sınıflandırılmaktadır.

3.2. R_{2^4} Sonlu Halkası Üzerinde Devirli Kod İnşası, Devirli ve $(1+u^2)-$ Sabit Devirli Kodların Gray Görüntüleri

3.2.1. R_{2^4} Kümesinin Cebirsel Yapısı

$\mathbb{F}_2[u,v]/\langle u^3, v^2 - v, uv\rangle$ bölüm halkası göz önüne alınsın.

$\mathbb{F}_2[u,v]/\langle u^3, v^2 - v, uv\rangle = \{a + bu + cu^2 + dv + euv + fu^2v + \langle u^3, v^2 - v, uv\rangle : a,b,c,d \in \mathbb{F}_2\}$ halkası için, $u^3 = 0$, $v^2 - v = 0$ ve $uv = 0$ koşulları göz önüne alındığında,

$$\begin{aligned} a + bu + cu^2 + dv + euv + fu^2v + \langle 0\rangle & \\ &= \{a + bu + cu^2 + dv + 0t : a,b,c,d \in \mathbb{F}_2, t \in \mathbb{F}_2[u,v]\} \\ &= \{a + bu + cu^2 + dv\} \end{aligned}$$

$$\mathbb{F}_2[u,v]/\langle u^3, v^2 - v, uv\rangle = \{\{a + bu + cu^2 + dv\} : a,b,c,d \in \mathbb{F}_2\}$$

halkası elde edilir.

3.2.1.1. Teorem:

$$f: \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2 \longrightarrow \mathbb{F}_2[u,v]/\langle u^3, v^2 - v, uv\rangle$$

$$a + bu + cu^2 + dv \longmapsto f(a + bu + cu^2 + dv) = \{a + bu + cu^2 + dv\}$$

dönüşümü bir izomorfizmadır.

Kanıt:

Herhangi $a_1 + b_1u + c_1u^2 + d_1v,\ a_2 + b_2u + c_2u^2 + d_2v \in R_{2^4}$ için,

$$a_1 + b_1u + c_1u^2 + d_1v = a_2 + b_2u + c_2u^2 + d_2v$$

$$\Leftrightarrow a_1 = a_2, b_1 = b_2, c_1 = c_2, d_1 = d_2$$

$$\Leftrightarrow \{a_1 + b_1u + c_1u^2 + d_1v\} = \{a_2 + b_2u + c_2u^2 + d_2v\}$$

$$\Leftrightarrow f(a_1 + b_1u + c_1u^2 + d_1v) = f(a_2 + b_2u + c_2u^2 + d_2v)$$

çift taraflı gerektirmeler sağlandığından, f dönüşümü iyi tanımlı ve birebirdir.

$|R_{2^4}| = |\mathbb{F}_2[u,v]/\langle u^3, v^2 - v, uv\rangle| = 16$ ve f dönüşümü birebir olduğundan, f dönüşümü örtendir.

Herhangi $a_1 + b_1u + c_1u^2 + d_1v,\ a_2 + b_2u + c_2u^2 + d_2v \in R_{2^4}$ için,

$$\begin{aligned} f(a_1 + b_1u + c_1u^2 + d_1v + a_2 + b_2u + c_2u^2 + d_2v) \\ &= f((a_1 + a_2) + (b_1 + b_2)u + (c_1 + c_2)u^2 + (d_1 + d_2)v) \\ &= \{(a_1 + a_2) + (b_1 + b_2)u + (c_1 + c_2)u^2 + (d_1 + d_2)v\} \\ &= \{a_1 + b_1u + c_1u^2 + d_1v\} + \{a_1 + b_1u + c_1u^2 + d_1v\} \\ &= f(a_1 + b_1u + c_1u^2 + d_1v) + f(a_2 + b_2u + c_2u^2 + d_2v) \end{aligned}$$

$$f\big((a_1 + b_1u + c_1u^2 + d_1v).(a_2 + b_2u + c_2u^2 + d_2v)\big)$$
$$= f(a_1a_2 + (a_1b_2 + b_1a_2)u + (a_1c_2 + b_1b_2 + c_1a_2)u^2 + (a_1d_2 + d_1d_2 + d_1a_2)v)$$
$$= \{a_1a_2 + (a_1b_2 + b_1a_2)u + (a_1c_2 + b_1b_2 + c_1a_2)u^2 + (a_1d_2 + d_1d_2 + d_1a_2)v\}$$

$$f(a_1 + b_1u + c_1u^2 + d_1v).f(a_2 + b_2u + c_2u^2 + d_2v)$$
$$= \{a_1 + b_1u + c_1u^2 + d_1v\}.\{a_1 + b_1u + c_1u^2 + d_1v\}$$
$$= \{a_1a_2 + (a_1b_2 + b_1a_2)u + (a_1c_2 + b_1b_2 + c_1a_2)u^2 + (a_1d_2 + d_1d_2 + d_1a_2)v\}$$

bulunur ve bu durumda,

$$f((a_1 + b_1u + c_1u^2 + d_1v).(a_2 + b_2u + c_2u^2 + d_2v))$$
$$= f(a_1 + b_1u + c_1u^2 + d_1v).f(a_2 + b_2u + c_2u^2 + d_2v)$$

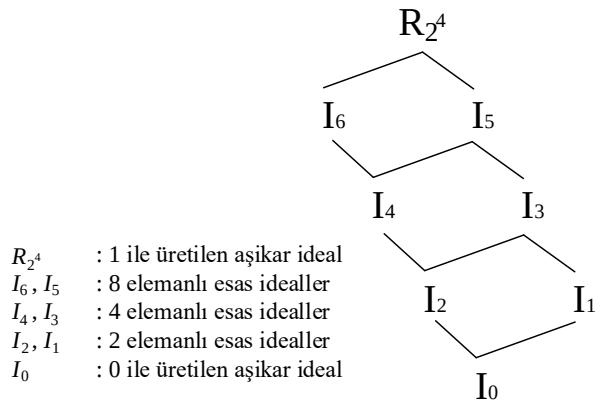
sağlanır. O halde, f dönüşümü bir halka homomorfizmasıdır. Dolayısıyla, f dönüşümü bir izomorfizmadır. Bu durumda,

$$R_{2^4} \coloneqq \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2 \cong \mathbb{F}_2[u, v]/\langle u^3, v^2 - v, uv\rangle$$

biçiminde yazılır.

$$R_{2^4} = \{0, 1, u, u^2, v, 1 + u, 1 + u^2, 1 + u + u^2, 1 + v, 1 + u + v, 1 + u^2 + v, 1 + u + u^2 + v, u + u^2, u + v, u^2 + v, u + u^2 + v\}$$

halkası, 16 elemanlı karakteristiği 2 olan değişmeli bir halkadır. R_{2^4} halkasının birimsel elemanları: $1, 1 + u, 1 + u^2$ ve $1 + u + u^2$ dir. R_{2^4} halkası, *Şekil 3.1*'de gösterilen ideal kafesine sahip olup $\langle 1 + u\rangle$ ve $\langle u + v\rangle$ maksimal idealleri ile yarı yerel bir halkadır. Aynı zamanda tüm idealleri esas ideal olduğundan, R_{2^4} bir esas ideal halkasıdır.



Şekil 3.1 R_{2^4} Halkasının İdealleri

3.2.2. R_{2^4} Halkası Üzerinde Tek Uzunluklu $(1 + u^2) -$ Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki

R_{2^4} halkasının karakteristiği 2 olduğundan $(1 + u^2)^2 = 1$. Sonuç olarak, $1 + u^2$ birimsel elemanının tüm çift kuvvetileri 1'dir. Bu sonuç doğrultusunda aşağıdaki önerme sağlanır:

3.2.2.1. Önerme:

n pozitif tek tamsayı ve

$$\mu: R_{2^4}[x]/\langle x^n - 1\rangle \to R_{2^4}[x]/\langle x^n - (1 + u^2)\rangle$$

dönüşümü,

$$\overline{f(x)} \mapsto \mu\big(\overline{f(x)}\big) = \overline{f((1 + u^2)x)}$$

biçiminde tanımlansın. O halde, μ bir halka izomorfizmasıdır.

Kanıt:

Her $\overline{f(x)}, \overline{g(x)} \in R_{2^4}[x]/\langle x^n - 1\rangle$ için $f(x) \equiv g(x)\ (mod\ x^n - 1)$ olsun. Bu durumda, $\overline{f(x)} - \overline{g(x)} = \overline{h(x)}.\overline{(x^n - 1)}$ eşitliğini sağlayan en az bir $\overline{h(x)} \in R_{2^4}[x]/\langle x^n - 1\rangle$ polinomu vardır. Son eşitlikte, x yerine $(1 + u^2)x$ yazılırsa $\overline{f((1 + u^2)x)} - \overline{g\big((1 + u^2)x\big)} = \overline{h\big((1 + u^2)x\big)}.\overline{((1 + u^2)^n x^n - 1)}$ eşitliği elde edilir. n tek tamsayı olduğundan $(1 + u^2)^n = 1 + u^2$ ve $(1 + u^2)^2 = 1$ eşitlikleri sağlanır. Dolayısıyla,

$\overline{f((1+u^2)x)} - \overline{g\big((1+u^2)x\big)} = \overline{h\big((1+u^2)x\big)}.\overline{((1+u^2)x^n - (1+u^2)^2)}$ eşitliği elde edilir. Buradan, $\mu\big(\overline{f(x)}\big) - \mu\big(\overline{g(x)}\big) = \overline{h\big((1+u^2)x\big)(1+u^2)}.\overline{(x^n - (1+u^2))}$ sonucu elde edilir. Böylece, $\mu(f(x)) \equiv \mu(g(x))\ (mod\ x^n - (1+u^2))$. O halde, μ iyi tanımlıdır. Yapılan işlemler tersine de sağlanacağından, μ birebirdir.

İspatın geri kalan kısmı için μ dönüşümünün örten bir homomorfizma olduğunu göstermek yeterlidir. Her $\overline{f(x)},\ \overline{g(x)} \in R_{2^4}[x]/\langle x^n - 1\rangle$ için, $\mu(\overline{f(x)} + \overline{g(x)}) = \mu(\overline{(f+g)(x)}) = \overline{(f+g)((1+u^2)x)} = \overline{f((1+u^2)x)} + \overline{g((1+u^2)x)} = \mu(\overline{f(x)}) + \mu(\overline{g(x)})$ eşitliği sağlanır. Benzer işlemler çarpma için de yapıldığında, μ dönüşümünün bir halka homomorfizması olduğu görülür. Her $\overline{f((1+u^2)x)} \in R_{2^4}[x]/\langle x^n - (1+u^2)\rangle$ elemanı için bir $\overline{f(x)} \in R_{2^4}[x]/\langle x^n - 1\rangle$ olduğundan μ örten bir dönüşümdür. O halde, μ bir halka izomorfizmasıdır.

3.2.2.2. Sonuç:

n pozitif tek tamsayı olsun. I kümesinin $R_{2^4}[x]/\langle x^n - 1\rangle$ bölüm halkasının bir ideali olması için gerekli ve yeterli koşul $\mu(I)$ kümesinin $R_{2^4}[x]/\langle x^n - (1+u^2)\rangle$ bölüm halkasının bir ideali olmasıdır.

Kanıt:

n tek tamsayı ve I kümesi $R_{2^4}[x]/\langle x^n - 1\rangle$ bölüm halkasının bir ideali olsun.

Her $\overline{f(x)}, \overline{g(x)} \in \mu(I)$ polinomları için $\overline{f(x)} = \mu(\overline{f_1(x)}),\ \overline{g(x)} = \mu(\overline{g_1(x)})$ eşitliklerini sağlayan en az birer $\overline{f_1(x)}, \overline{g_1(x)} \in I$ polinomları vardır.

$\overline{f(x)} + \overline{g(x)} = \mu(\overline{f_1(x)}) + \mu(\overline{g_1(x)})$ eşitliği ile μ dönüşümünün homomorfizma olduğu kullanılarak, $\overline{f(x) + g(x)} = \mu(\overline{f_1(x)} + \overline{g_1(x)})$ eşitliği elde edilir. $\overline{f_1(x)}, \overline{g_1(x)} \in I$ ve I ideal olduğundan, $\overline{f(x) + g(x)} \in \mu(I)$ bulunur.

Her $\overline{f(x)} \in \mu(I)$ polinomu için $\overline{f(x)} = \mu(\overline{f_1(x)})$ eşitliğini sağlayan bir $f_1(x) \in I$ polinomu vardır. μ örten dönüşüm olduğundan her $\overline{r(x)} \in R_{2^4}[x]/\langle x^n - (1+u^2)\rangle$ polinomu için $\overline{r(x)} = \mu(\overline{r_1(x)})$ eşitliğini sağlayan en az bir $r_1(x) \in R_{2^4}[x]/\langle x^n - 1\rangle$ polinomu vardır. $\overline{f(x)r(x)} = \mu(\overline{f_1(x)})\mu(\overline{r_1(x)})$ eşitliği ile μ dönüşümünün homomorfizma olduğu kullanılarak, $\overline{f(x)r(x)} = \mu(\overline{f_1(x)r_1(x)})$ eşitliği elde edilir.

$\overline{f_1(x)} \in I$, $\overline{r_1(x)} \in R_{2^4}[x]/\langle x^n - 1\rangle$ ve I ideal olduğundan, $\overline{f_1(x)}\,\overline{r_1(x)} \in I$ dolayısıyla $\overline{f(x)r(x)} \in \mu(I)$ bulunur.

O halde, $\mu(I)$ kümesi $R_{2^4}[x]/\langle x^n - (1+u^2)\rangle$ bölüm halkasının bir idealidir. μ dönüşümünün birebir ve örten olduğu kullanılarak bu işlemler yeterlilik kısmının ispatı için de kolaylıkla yapılabilir.

3.2.2.3. Sonuç:

n pozitif tek tamsayı ve C kümesi $R_{2^4}^n$ kümesinin bir alt kümesi olsun. $\bar{\mu}$ permütasyonu $R_{2^4}^n$ kümesi üzerinde aşağıdaki şekilde tanımlı olsun:

$$\bar{\mu}(c_0, c_1, \dots, c_{n-1}) = (c_0, (1+u^2)c_1, (1+u^2)^2 c_2, \dots, (1+u^2)^{n-1} c_{n-1})$$

Bu durumda, C'nin devirli kod olması için gerekli ve yeterli koşul $\bar{\mu}(C)$ kodunun $(1+u^2) -$ sabit devirli kod olmasıdır.

Kanıt:

C, n uzunluklu bir devirli kod olsun. C'nin polinom gösterimi, gösterim kolaylığı açısından yine C olsun. O halde, C kümesi $R_{2^4}[x]/\langle x^n - 1\rangle$'nin bir idealidir. Bir önceki sonuçtan, $\mu(C)$ kümesi $R_{2^4}[x]/\langle x^n - (1+u^2)\rangle$'nin bir ideali olacaktır. Bu durumda, $\bar{\mu}(C)$ kümesi R_{2^4} üzerinde tanımlı bir $(1+u^2) -$ sabit devirli koddur.

3.2.3. R_{2^4} Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+u^2) -$ Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri

3.2.3.1. Tanım:

$\phi: R_{2^4} \to \mathbb{F}_2^4$

$a + bu + cu^2 + dv \mapsto \phi(a + bu + cu^2 + dv) = (c, a+b, a+d, a+c)$

biçiminde tanımlanan ϕ dönüşümüne "*Gray dönüşümü*" denir.

$0 \le i \le n-1$ ve $a_i, b_i, c_i, d_i \in \mathbb{F}_2$ olmak üzere, her $z_i = a_i + b_i u + c_i u^2 + d_i v$ için yukarıdaki ϕ Gray dönüşümünün $R_{2^4}^n$ kümesine genişletilmiş hali aşağıdaki gibidir:

$\phi: R_{2^4}^n \to \mathbb{F}_2^{4n}$

$$(z_0, z_1, \dots, z_{n-1}) \mapsto \phi(z_0, z_1, \dots, z_{n-1})$$
$$= (c_0, \dots, c_{n-1}, a_0 + b_0, \dots, a_{n-1} + b_{n-1}, a_0 + d_0, \dots, a_{n-1}$$
$$+ d_{n-1}, a_0 + c_0, \dots, a_{n-1} + c_{n-1})$$

R_{2^4} kümesindeki bir x elemanının Gray ağırlığı, x elemanının Gray görüntüsünün Hamming ağırlığı olarak tanımlanır. Buna göre x'in Gray ağırlığı;

$$w_G(x) = \begin{cases} 0 & x = 0 \\ 1 & x = u, v, 1 + u + v, 1 + u + u^2 + v \\ 2 & x = u^2, 1 + u, 1 + v, u + v, 1 + u + u^2, 1 + u^2 + v \\ 3 & x = 1, 1 + u^2, u + u^2, u^2 + v \\ 4 & x = u + u^2 + v \end{cases}$$

biçiminde yazılır.

C, R_{2^4} halkası üzerinde n uzunluklu bir lineer kod olsun. Herhangi bir $c = (c_0, c_1, \dots, c_{n-1})$ kod sözcüğü için c elemanının Gray ağırlığı, $w_G(c) = \sum_{i=0}^{n-1} w_G(c_i)$ biçiminde tanımlıdır.

Herhangi $c' \in C$ ve $c \neq c'$ için $d_G(c, c') = w_G(c - c')$ olmak üzere C kümesinin minimum Gray uzaklığı $d_G(C) = min\{d_G(c, c') : c, c' \in C, c \neq c'\}$ şeklinde tanımlanır.

3.2.3.2. Önerme:

d_G minimum Gray uzaklığı, d_H mimimum Hamming uzaklığı olmak üzere, $(R_{2^4}^n, d_G)$ kümesinden $(\mathbb{F}_2^{4n}, d_H)$ kümesine tanımlı ϕ Gray dönüşümü hem doğrusal hem de uzaklık koruyan dönüşümdür.

Kanıt:

Herhangi iki $x, y \in R_{2^4}$ için, $x = a_1 + b_1 u + c_1 u^2 + d_1 v$ ve $y = a_2 + b_2 u + c_2 u^2 + d_2 v$ olmak üzere, $\phi(x + y) = \phi((a_1 + a_2) + (b_1 + b_2)u + (c_1 + c_2)u^2 + (d_1 + d_2)v)$ eşitliği ve ϕ'nin tanımı kullanılarak,

$$\phi(x + y) = (c_1 + c_2, a_1 + a_2 + b_1 + b_2, a_1 + a_2 + d_1 + d_2, a_1 + a_2 + c_1 + c_2)$$
$$= (c_1, a_1 + b_1, a_1 + d_1, a_1 + c_1)$$
$$+ (c_2, a_2 + b_2, a_2 + d_2, a_2 + c_2) = \phi(x) + \phi(y)$$

elde edilir.

Herhangi bir $k \in \mathbb{F}_2$ için, $\phi(kx) = (kc_1, k(a_1 + b_1), k(a_1 + d_1), k(a_1 + c_1)) = k(c_1, a_1 + b_1, a_1 + d_1, a_1 + c_1) = k\phi(x)$ elde edilir. O halde, ϕ doğrusal dönüşümdür. ϕ dönüşümünün genişletilmiş hali de doğrusaldır.

Son olarak, herhangi bir $x, y \in R_{2^4}^n$ için, $d_G(x, y) = w_G(x - y) = w_H\big(\phi(x - y)\big) = w_H(\phi(x) - \phi(y)) = d_H(\phi(x), \phi(y))$. Bu durumda, ϕ dönüşümü bir izometridir.

ϕ dönüşümü için yapılan ispat, genelleştirilmiş ϕ dönüşümü için de elde edilir. Bu önermenin sonucu olarak, yeni tanımlanan R_{2^4} sonlu halkasından $\mathbb{F}_2$ sonlu cismine geçişi sağlayan teorem aşağıdaki şekilde yazılır:

3.2.3.3. Teorem:

C, R_{2^4} halkası üzerinde tanımlı bir (n, M, d_G) lineer kod ise $d_G = d_H$ olmak üzere, $\phi(C)$ kodu $\mathbb{F}_2$ sonlu cismi üzerinde tanımlı bir $(4n, M, d_H)$ lineer koddur.

3.2.3.4. Önerme:

σ ve ν sırasıyla, $R_{2^4}^n$ üzerinde devirli ve $(1 + u^2) -$ sabit devirli öteleme olsun. $\{0,1, \dots, 4n - 1\}$ kümesi üzerinde tanımlı π permütasyonu $\pi = (0,3n)$ biçiminde olmak üzere, $\phi \circ \nu = \pi \circ \sigma^{\otimes 4} \circ \phi$ eşitliği sağlanır.

Kanıt:

$z = (z_0, z_1, \dots, z_{n-1}) \in R_{2^4}^n$ olsun. $0 \le i \le n - 1$ sağlayan her i için $z_i = a_i + b_i u + c_i u^2 + d_i v$ olmak üzere, $a_i, b_i, c_i, d_i \in \mathbb{F}_2$ olsun. Bu durumda, $\nu(z) = ((1 + u^2)z_{n-1}, z_0, z_1, \dots, z_{n-2})$. ϕ Gray dönüşümünün tanımından, $\phi\big(\nu(z)\big) = (a_{n-1} + c_{n-1}, c_0, \dots, c_{n-2}, a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2}, a_{n-1} + d_{n-1}, a_0 + d_0, \dots, a_{n-2} + d_{n-2}, c_{n-1}, a_0 + c_0, \dots, a_{n-1} + c_{n-1})$ elde edilir.

Diğer yandan, $\phi(z) = (c_0, \dots, c_{n-1}, a_0 + b_0, \dots, a_{n-1} + b_{n-1}, a_0 + d_0, \dots, a_{n-1} + d_{n-1}, a_0 + c_0, \dots, a_{n-1} + c_{n-1})$ eşitliğine $\sigma^{\otimes 4}$ dönüşümü uygulanırsa, $\sigma^{\otimes 4}(\phi(z)) = (c_{n-1}, c_0, \dots, c_{n-2}, a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2}, a_{n-1} + d_{n-1}, a_0 + d_0, \dots, a_{n-2} + d_{n-2}, a_{n-1} + c_{n-1}, a_0 + c_0, \dots, a_{n-2} + c_{n-2})$ eşitliği elde edilir. Son eşitliğin $\pi = (0,3n)$ permütasyonu altındaki görüntüsü, $\pi\left(\sigma^{\otimes 4}\big(\phi(z)\big)\right) = (a_{n-1} + c_{n-1}, c_0, \dots, c_{n-2}, a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2}, a_{n-1} + d_{n-1}, a_0 +$

$d_0, \dots, a_{n-2} + d_{n-2}, c_{n-1}, a_0 + c_0, \dots, a_{n-1} + c_{n-1})$ biçimindedir. Bu durumda, $\phi \circ \nu = \pi \circ \sigma^{\otimes 4} \circ \phi$ eşitliği sağlanır.

3.2.3.5. Teorem:

R_{2^4} halkası üzerinde, n uzunluklu $(1 + u^2) -$ sabit devirli kodun Gray görüntüsü, $\mathbb{F}_2$ üzerinde tanımlı, $4n$ uzunluklu ve indeksi 4 olan bir quasicyclic koda denktir.

Kanıt:

C, R_{2^4} halkası üzerinde n uzunluklu $(1 + u^2) -$ sabit devirli kod olsun. Bu durumda, $\nu(C) = C$. Bu eşitliğin her iki yanına ϕ Gray dönüşümü uygulanırsa, $\phi(\nu(C)) = \phi(C)$ bulunur. Son eşitlik ve *3.2.3.4 Önerme* kullanılırsa, $\phi(C) = \pi(\sigma^{\otimes 4}(\phi(C)))$ olduğu görülür. O halde $\phi(C)$, $4n$ uzunluklu ve indeksi 4 olan bir ikili quasicyclic koda denktir.

3.2.3.6. Önerme:

n tek bir tamsayı ve $\bar{\mu}$ permütasyonu *3.2.2.3 Sonuç*'taki gibi tanımlansın. Bu durumda, $\{0,1, \dots, 4n-1\}$ kümesi üzerindeki γ permütasyonu $\gamma = (1,3n+1)(3,3n+3) \dots (n-2,4n-2)$ biçiminde tanımlı olmak üzere, $\phi\bar{\mu} = \gamma'\phi$ eşitliğini sağlayan bir $\gamma'(z_0, z_1, \dots, z_{4n-1}) = (z_{\gamma(0)}, z_{\gamma(1)}, \dots, z_{\gamma(4n-1)})$ permütasyonu vardır.

Kanıt:

$0 \le i \le n-1$ için $z_i = a_i + b_i u + c_i u^2 + d_i v$ olmak üzere, $a_i, b_i, c_i, d_i \in \mathbb{F}_2$ olsun. Herhangi bir $z = (z_0, z_1, \dots, z_{n-1}) \in R_{2^4}^n$ elemanı için, $\bar{\mu}(z) = \bar{\mu}(z_0, z_1, \dots, z_{n-1}) = (z_0, (1+u^2)z_1, z_2, (1+u^2)z_3, \dots, z_{n-1})$ eşitliğinin, ϕ Gray dönüşümü altındaki görüntüsü $\phi(\bar{\mu}(z)) = (c_0, a_1 + c_1, c_2, a_3 + c_3 \dots, c_{n-1}, a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1}, a_0 + d_0, a_1 + d_1, \dots, a_{n-1} + d_{n-1}, a_0 + c_0, c_1, a_2 + c_2, c_3, \dots, a_{n-1} + c_{n-1})$ biçimindedir. $\phi(z)$ elemanına γ' permütasyonu uygulandığında istenilen sonuç elde edilir.

3.2.3.7. Teorem:

n tek tamsayı ve Δ, R_{2^4} halkası üzerinde devirli bir kodun Gray görüntüsü ise $\gamma'(\Delta), 4n$ uzunluklu, indeksi 4 olan ve $\mathbb{F}_2$ üzerinde tanımlı bir quasicyclic koda denktir.

Kanıt:

Δ , R_{2^4} halkası üzerinde tanımlı bir C devirli kodun Gray görüntüsü $\phi(C)$ olsun. *3.2.3.6 Önerme*'den $\phi(\bar{\mu}(C)) = \gamma'(\phi(C)) = \gamma'(\Delta)$ eşitliği elde edilir. *3.2.2.3 Sonuç* göz önüne alındığında, $\bar{\mu}(C)$'nin R_{2^4} halkası üzerinde bir D $(1+u^2)-$ sabit devirli kodu olduğu görülür. O halde, $\phi(\bar{\mu}(C)) = \phi(D)$ elde edilir. *3.2.3.5 Teorem* kullanılarak, $\phi(D)$ kodu $4n$ uzunluklu ve indeksi 4 olan bir ikili quasicyclic koda denktir.

3.2.3.8. Sonuç:

R_{2^4} halkası üzerinde tek uzunluklu devirli bir kodun Gray görüntüsü, $4n$ uzunluklu ve indeksi 4 olan bir ikili quasicylic koda denktir.

3.2.4. R_{2^4} Halkası Üzerinde Devirli Kodların İnşası

Bu alt bölümde, R_{2^4} halkası üzerinde tanımlı devirli kodların üreteçleri ve üreteç kümesi *çek-gör fikri* yardımıyla elde edilmektedir. Bu üreteçlerden yararlanarak R_{2^4} halkası üzerinde tanımlı $(1+u^2)-$ sabit devirli kodların üreteçleri ve bunlara ilişkin örnekler verilmektedir.

R_{2^4} halkası üzerinde tanımlı devirli kodların üreteçlerini *çek-gör fikri* yardımıyla elde etmek için (Abualrub, Şiap, 2007) çalışmasında verilen $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$ halkası üzerindeki tek uzunluklu devirli kodların üreteçlerinden yararlanılmaktadır:

3.2.4.1. Teorem (Abualrub, Şiap, 2007):

$S = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 = \{0, 1, u, u^2, 1+u, 1+u^2, u+u^2, 1+u+u^2\}$ kümesi için $u^3 = 0,\ (mod\ 2)$ olmak üzere C kümesi $S_n = S[x]/\langle x^n - 1\rangle$ bölüm halkasında devirli bir kod olsun.

(i) n tek ise S_n bir esas ideal halkasıdır ve $a_2(x)|a_1(x)|g(x)|(x^n-1)$ $(mod\ 2)$ koşulunu sağlayan $g(x)$, $a_1(x)$ ve $a_2(x)$ ikili polinomları için $C = (g, ua_1, u^2a_2) = (g + ua_1 + u^2a_2)$.

(ii) n tek değil ise,

a) $a_2|a_1|g|(x^n-1)\ \ (mod\ 2)$, $\mathbb{Z}_2+u\mathbb{Z}_2$'de $(g+up)|(x^n-1)$, S'de $(g+up_1+u^2p_2)|(x^n-1)$ ve $der\ p_2 < der\ p_1$ olmak üzere, $C=(g+ua_1+u^2a_2)$ ya da,

b) $a_2|g|(x^n-1)\ \ (mod\ 2)$, $\mathbb{Z}_2+u\mathbb{Z}_2$'de $(g+up)|(x^n-1)$, $g(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, $a_2(x)$ polinomu $p_1(x)\left(\frac{x^n-1}{g(x)}\right)$ ve $p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{g(x)}\right)$ polinomlarını böler ve $der\ p_2 < der\ a_2$ olmak üzere $C=(g+ua_1+u^2a_2, u^2a_2)$ ya da,

c) $a_2|a_1|g|(x^n-1)\ (mod\ 2)$, $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, $a_2(x)$ polinomu $q_1(x)\left(\frac{x^n-1}{a_1(x)}\right)$ ve $p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$ polinomlarını bölmek üzere $C=(g+ua_1+u^2a_2, u^2a_2)$ sağlanır ve $der\ p_2 < der\ a_2$, $der\ q_1 < der\ a_2, der\ p_1 < der\ a_1$.

3.2.4.1. Teorem'de verilen $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$ halkası yerine, ona izomorf olan $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ sonlu halkası S olsun. R_{2^4} sonlu halkasından S halkasına tanımlı, $\varphi(a+bu+cu^2+dv)=a+bu+cu^2\ (mod\ v)$ homomorfizması göz önüne alınsın. Bu homomorfizma aşağıdaki şekilde Ψ homomorfizmasına genelleştirilsin (Bölüm halkalarındaki elemanların, polinom fonksiyonların denklik sınıfı olduğu unutulmamalıdır. Gösterim kolaylığı açısından sadece temsilci polinomlar ile çalışılacaktır):

$$\Psi: R_{2^4}[x]/\langle x^n-1\rangle \to S[x]/\langle x^n-1\rangle$$

$$\Psi(z_0+z_1x+\cdots+z_{n-1}x^{n-1})=\varphi(z_0)+\varphi(z_1)x+\cdots+\varphi(z_{n-1})x^{n-1}$$

Ψ homomorfizmasının çekirdek kümesi,

$$çek\ \Psi=\{vp(x)|p(x)\in\mathbb{F}_2[x]/\langle x^n-1\rangle\}$$

biçiminde yazılır.

J kümesi, $J=\{p(x)|vp(x)\in çek(\Psi)\}$ biçiminde tanımlansın. J kümesi $\mathbb{F}_2[x]/\langle x^n-1\rangle$ bölüm halkasının idealidir. Bu durumda, J kümesi $\mathbb{F}_2[x]/\langle x^n-1\rangle$ kümesinde bir devirli koddur. $\mathbb{F}_2[x]/\langle x^n-1\rangle$ halkası bir esas ideal halkası olduğundan, $J=\langle t(x)\rangle$ olacak şekilde $(mod\ 2)$'ye göre, x^n-1 polinomunun bir $t(x)$ monik böleni

vardır. O halde, Ψ homomorfizmasının çekirdek kümesi de tek eleman ile üretilen $\langle vt(x)\rangle$ ideali olarak yazılır. Diğer yandan, Ψ homomorfizmasının görüntü kümesi de $S[x]/\langle x^n-1\rangle$ halkasının bir idealidir. $S[x]/\langle x^n-1\rangle$ halkasının *3.2.4.1. Teorem*'de n tek olması durumunda esas ideal halkası olduğu bilindiğinden, $Im(\Psi)$ kümesi S^n kümesinde devirli bir koddur ve tek eleman ile üretilir. *3.2.4.1. Teorem*'e göre S halkası üzerindeki n tek uzunluklu devirli kodların üreteçleri $a_2(x)|a_1(x)|g(x)|(x^n-1)$ $(mod\ 2)$ olmak üzere, $g(x), a_1(x)$ ve $a_2(x)$ ikili polinomları için $C=\langle g(x)+ua_1(x)+u^2a_2(x)\rangle$ biçiminde yazılır. *Çek-gör fikri* kullanılarak R_{2^4} halkası üzerindeki devirli kodun üreteci, $\langle g(x)+ua_1(x)+u^2a_2(x)+vh_0(x), vt(x)\rangle$ biçiminde yazılır. Burada, $v\big(g(x)+ua_1(x)+u^2a_2(x)+vh_0(x)\big)=v\big(g(x)+h_0(x)\big)\in\langle vt(x)\rangle=$ $çek\ \Psi$ olduğundan, $t(x)|\big(g(x)+h_0(x)\big)$ koşulu açıkça ortaya çıkacaktır. Bu durumda, R_{2^4} halkası üzerinde kurulan devirli kodun yapısını veren teorem aşağıdaki şekilde yazılır:

3.2.4.2. Teorem:

C kodu R_{2^4} halkası üzerinde n tek uzunluklu devirli kod olsun. Bu durumda, $a_2|a_1|g|(x^n-1)$ ve $t(x)|\big(g(x)+h_0(x)\big)$ koşullarını sağlayan $a_i(x), g(x)$ ve $t(x)\in \mathbb{F}_2[x]$ polinomları için C kodunun üreteci

$$\langle g(x)+ua_1(x)+u^2a_2(x)+vh_0(x), vt(x)\rangle$$

biçiminde yazılır.

3.2.4.3. Lemma:

$C=\langle g(x)+ua_1(x)+u^2a_2(x)+vh_0(x), vt(x)\rangle$ kodu R_{2^4} halkası üzerinde n tek uzunluklu devirli bir kod olsun. $t(x)$ monik polinom ise $der\ (h_0(x))<der\ (t(x))$ olarak alınabilir.

Kanıt:

$der\ \big(t(x)\big)\le der\ (h_0(x))$ olsun. Bu durumda, $h_0(x)=t(x)m_0(x)+r_0(x)$ eşitliğini sağlayan, $m_0(x), r_0(x)\in R_{2^4}[x]$ polinomları vardır ve burada ya $der\ \big(r_0(x)\big)<der\ (h_0(x))$ ya da $r_0(x)=0$ olacaktır. Bu duruma göre C kodunun

üreteci tekrar yazıldığında, $C = \langle g(x) + ua_1(x) + u^2a_2(x) + v(t(x)m_0(x) + r_0(x)), vt(x)\rangle$ şeklinde olacaktır. $C_1 = \langle g(x) + ua_1(x) + u^2a_2(x) + vr_0(x), vt(x)\rangle$ olsun. $C \subseteq C_1$ olduğu açıktır. $g(x) + ua_1(x) + u^2a_2(x) + vr_0(x) = g(x) + ua_1(x) + u^2a_2(x) + vt(x)m_0(x) + vr_0(x) + vt(x)m_0(x)$ biçiminde yazılırsa, $C_1 \subseteq C$ olacağı açıktır. Dolayısıyla, $C = C_1$ dir.

3.2.4.4. Sonuç:

C kodu R_{2^4} halkası üzerinde *3.2.4.2 Teorem* koşullarına uygun devirli bir kod ise R_{2^4} halkası üzerinde $(1+u^2)-$ sabit devirli kodun üreteci, $\langle g((1+u^2)x) + ua_1((1+u^2)x) + u^2a_2((1+u^2)x) + vh_0((1+u^2)x), vt((1+u^2)x)\rangle$ biçimindedir.

Kanıt:

3.2.2.1. Önerme ve *3.2.4.2 Teorem* göz önüne alındığında ispat kolaylıkla tamamlanır.

3.2.4.5. Teorem:

$C = \langle g(x) + ua_1(x) + u^2a_2(x) + vh_0(x), vt(x)\rangle$ R_{2^4} halkası üzerinde n tek uzunluklu devirli bir kod ve $der\,(g(x)) = k$ ve $der\,(t(x)) = l$ olsun. $i = 1,2$ için $g(x)$, $a_i(x)$ ve $t(x)$ monik polinomlar ise C kodunun minimum üreteç kümesi aşağıdaki şekilde verilir:

$$\{g(x) + ua_1(x) + u^2a_2(x) + vh_0(x), x(g(x) + ua_1(x) + u^2a_2(x) + vh_0(x)), \dots, x^{n-k-1}(g(x) + ua_1(x) + u^2a_2(x) + vh_0(x)), vt(x), x(vt(x)), \dots, x^{k-l-1}(vt(x))\}$$

3.2.4.6. Örnek:

R_{2^4} halkası üzerindeki 7 uzunluklu bazı devirli kodlar ve $(1+u^2)-$ sabit devirli kodların üreteçlerinin elde edilmesi için, $x^7 - 1$ polinomunun $\mathbb{F}_2[x]$ polinom halkasında çarpanlara ayrılışı göz önüne alınsın:

$$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) = f_1(x)f_2(x)f_3(x)$$

$a_2(x), a_1(x), g(x)$ ve $h_0(x)$ polinomları sırasıyla $1, f_2, f_1f_2$ ve 1 polinomlarına eşit olsun (Bu eşitlikler *3.2.4.2 Teorem* koşullarına uygun olacak şekilde yazılmalıdır). $t(x)$ polinomu *3.2.4.2 Teorem* koşunu sağlayacağından, $g(x) + h_0(x) = f_1f_2 + 1 =$

$x^4 + x^3 + x^2$ polinomunu bölmelidir. O halde, bu polinomları kullanarak R_{2^4} halkası üzerindeki bazı devirli kod üreteçleri aşağıdaki gibi yazılır:

$$C_1 = \langle x^4 + x^3 + x^2 + 1 + (x^3 + x + 1)u + u^2 + v, xv \rangle$$
$$C_2 = \langle x^4 + x^3 + x^2 + 1 + (x^3 + x + 1)u + u^2 + v, x^2v \rangle$$
$$C_3 = \langle x^4 + x^3 + x^2 + 1 + (x^3 + x + 1)u + u^2 + v, (x^2 + x + 1)v \rangle$$
$$C_4 = \langle x^4 + x^3 + x^2 + 1 + (x^3 + x + 1)u + u^2 + v, (x^3 + x^2 + x)v \rangle$$
$$C_5 = \langle x^4 + x^3 + x^2 + 1 + (x^3 + x + 1)u + u^2 + v, (x^4 + x^3 + x^2)v \rangle$$

Yukarıdaki devirli kod üreteçlerine karşılık gelen $(1 + u^2)$ −sabit devirli kodların üreteçleri *3.2.2. Bölüm* sonuçları göz önüne alınarak sırasıyla aşağıdaki gibi yazılır:

$$D_1 = \langle x^4 + (1 + u + u^2)x^3 + x^2 + ux + 1 + u + u^2 + v, xv \rangle$$
$$D_2 = \langle x^4 + (1 + u + u^2)x^3 + x^2 + ux + 1 + u + u^2 + v, x^2v \rangle$$
$$D_3 = \langle x^4 + (1 + u + u^2)x^3 + x^2 + ux + 1 + u + u^2 + v, (x^2 + x + 1)v \rangle$$
$$D_4 = \langle x^4 + (1 + u + u^2)x^3 + x^2 + ux + 1 + u + u^2 + v, (x^3 + x^2 + x)v \rangle$$
$$D_5 = \langle x^4 + (1 + u + u^2)x^3 + x^2 + ux + 1 + u + u^2 + v, (x^4 + x^3 + x^2)v \rangle$$

3.2.4.7. Örnek:

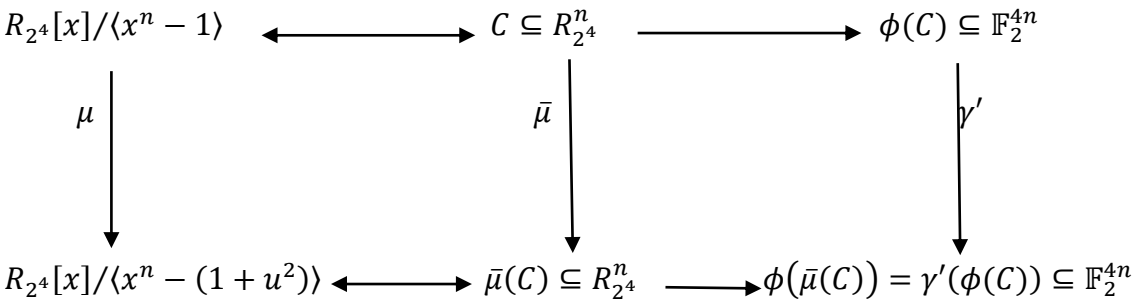
3.2.4.6. Örnek'teki C_1 devirli koduna karşılık gelen minimal üreteç kümesi $\{x^4 + (1 + u)x^3 + x^2 + ux + 1 + u + u^2 + v,\ x^5 + (1 + u)x^4 + x^3 + ux^2 + (1 + u + u^2 + v)x,\ x^6 + (1 + u)x^5 + x^4 + ux^3 + (1 + u + u^2 + v)x^2,\ vx,\ vx^2,\ vx^3\}$ biçimindedir.

3.2.5. R_{2^4} Halkası Üzerinde Tek Uzunluklu Devirli Kodlar ile $(1 + u^2) -$ Sabit Devirli Kodların Gray Görüntülerinin İlişkisi

Bu bölümde yeni R_{2^4} sonlu halkası, birimselleri ve idealleri tanıtılmıştır. Bu halka üzerinde devirli kodun üreteçlerini ve minimal üreteç kümesini veren sonuç ve teoremler ispatlanmıştır. Ayrıca $(1 + u^2) -$ birimsel elemanı seçilerek, bu halka üzerinde tek uzunluklu devirli ve $(1 + u^2) -$ sabit devirli kodların Gray görüntüleri elde edilmiştir. Elde edilen teoremler ve sonuçlar, *Şekil 3.2*'deki dönüşümlerin komütatifliğini sağlayacak şekilde verilmiştir.

Şekil 3.2'de görüldüğü gibi R_{2^4} halkası üzerindeki devirli kodlar ve $(1 + u^2) -$ sabit devirli kodlar arasındaki ilişkiyi bulabilmek için, öncelikle $R_{2^4}[x]/\langle x^n - 1 \rangle$

polinom halkası ile $R_{2^4}[x]/\langle x^n-(1+u^2)\rangle$ polinom halkası arasındaki μ izomorfizması elde edilmektedir. μ ile tanımlanan dönüşüm, n bir pozitif tek tamsayı olması durumunda izomorfizmadır. $R_{2^4}[x]/\langle x^n-1\rangle$ halkasının bir ideali, $R_{2^4}^n$ halkasının bir devirli kodu ile birebir ilişkilendirildiğinden, kodun polinom gösteriminden sıralı n'liler ile gösterim kısmına geçilirse, $R_{2^4}^n$ kümesi üzerinde μ izomorfizması yardımıyla bir $\bar{\mu}$ permütasyonu elde edilir. $R_{2^4}^n$ kümesinden $\mathbb{F}_2^{4n}$ vektör uzayına tanımlı Gray dönüşüm yardımıyla, devirli ve $(1+u^2)-$ sabit devirli kodların görüntüleri elde edilmektedir. $\phi\bar{\mu}=\gamma'\phi$ eşitliği diyagramın komütatifliğini tamamladığından, devirli ve $(1+u^2)-$ sabit devirli kodların Gray görüntülerinin $4n$ uzunluklu ve indeksi 4 olan ikili quasicyclic kodlara denk olduğu bulunmaktadır.



Şekil 3.2 R_{2^4} Halkası Üzerindeki Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı

3.3. $\mathbf{R_{p^4}}$ Sonlu Halka Sınıfı Üzerinde Devirli Kod İnşası, Devirli Kodlar ve $\boldsymbol{\lambda-}$ Sabit Devirli Kodların Gray Görüntüleri

3.3.1. R_{p^4} Kümesinin Cebirsel Yapısı

p bir asal sayı olmak üzere, $\mathbb{F}_p[u,v]/\langle u^3, v^2-v, uv\rangle = \{a+bu+cu^2+dv : a,b,c,d \in \mathbb{F}_p\}$ bölüm halkası için $u^3=0, v^2=v$ ve $uv=vu$ koşulları göz önüne alındığında *Bölüm 3.2.*'dekine benzer şekilde R_{p^4} kümesinin, adi toplama ve çarpma işlemleri ile karakteristiği p olan p^4 elemanlı değişmeli bir halka olduğu görülür.

3.3.1.1. R_{p^4} Halkasının Birimselleri

Sabit devirli kodların elde edilmesinde birimsel elemanlar önemli bir rol oynar. Bu yüzden, bu alt bölümde R_{p^4} sonlu halkasının birimsel elemanları ile ilgili özellikler araştırılmaktadır.

3.3.1.1.1. Teorem:

$a, b, c, d \in \mathbb{F}_p$ olmak üzere λ, R_{p^4} halkasının $a + bu + cu^2 + dv$ elemanı olsun. λ, R_{p^4} halkasının bir birimsel elemanı olması için gerekli ve yeterli koşul $a \neq 0$ ve $a + d \not\equiv 0 \ (mod\ p)$ olmasıdır.

Kanıt:

$\lambda = a + bu + cu^2 + dv$, R_{p^4} halkasının bir birimsel elemanı olsun. Öyleyse, $\lambda.\lambda' = 1$ eşitliğini sağlayan bir $\lambda' = a' + b'u + c'u^2 + d'v$ elemanı vardır. Bu eşitlik kullanılarak $mod\ p$'ye göre aşağıdaki denklikler elde edilir:

$$aa' \equiv 1 \quad \ldots(1)$$

$$ab' + ba' \equiv 0 \quad \ldots(2)$$

$$ac' + bb' + ca' \equiv 0 \quad \ldots(3)$$

$$ad' + da' + dd' \equiv 0 \quad \ldots(4)$$

(1) denkleminden $a' = a^{-1}$ olduğu görülür. Bu durumda, $a \in \mathbb{F}_p$ bir birimsel eleman olduğundan $a \neq 0$ bulunur. $a + d \not\equiv 0 \ (modp)$ olduğunu gösterebilmek için $d = 0$ ve $d \neq 0$ durumları incelenmelidir. $d = 0$ durumunda $a \neq 0$ olduğu için $a + d \neq 0$ olacaktır. $d \neq 0$ olduğu durumda ise, (4) denklemi kullanılarak, $(a + d)d' = -da'$ eşitliği elde edilir. Eşitliğin sağ tarafı sıfırdan farklı olduğundan, $a + d \neq 0$.

İspatın tersi için, $a \neq 0$ ve $a + d \neq 0$ olsun. Bu durumda, $a^{-1}, (a + d)^{-1} \in \mathbb{F}_p^*$ elemanları vardır. $a' = a^{-1}, b' = b(a^{-1})^2, c' = b^2(a^{-1})^3 - c(a^{-1})^2$ ve $d' = -da^{-1}(a + d)^{-1}$ eşitliklerini sağlayan $\lambda' = a' + b'u + c'u^2 + d'v$ için, $\lambda\lambda' = 1$ eşitliği sağlanır. O halde, teorem koşullarını sağlayan λ elemanı R_{p^4} halkasının birimsel elemanıdır.

Yukarıdaki teoreme göre R_{p^4} halkasındaki bir birimsel elemanın formunun sabit terime ve v'li terimin katsayısına bağlı olduğu görülür. Sabit terim $\mathbb{F}_p$ cisminde sıfırdan farklı olacak şekilde $p-1$ farklı değer alırken, v'li terimin katsayısı sabit terim ile toplandığında sıfırdan farklı olacak şekilde yine $p-1$ farklı değer alacaktır. Diğer u'lu ve u^2'li katsayılar koşulsuz olduğundan her biri p farklı değer alacaktır. Dolayısıyla aşağıdaki sonuç elde edilir:

3.3.1.1.2. Sonuç:

R_{p^4} halkasının birimsel elemanlarının sayısı, $p^2(p-1)^2$ sayısına eşittir.

3.3.1.1.3. Önerme:

$p \neq 2$ asal sayı olmak üzere, $\lambda = a + bu + cu^2 + dv \in R_{p^4}$ birimsel ise $\lambda^{p(p-1)} = 1$ eşitliği sağlanır.

Özellikle, $\lambda = a + bu + cu^2 + dv$ birimsel ise, aşağıdaki sınıflandırma sağlanır:

(i) $a = 1$ ve $d = 0$ ise $\lambda^p = 1$.

(ii) $b = 0$ ve $c = 0$ ise $\lambda^s = 1$ sağlayan $p-1$ sayısının bir s böleni vardır.

(iii) Diğer tüm durumlarda, $\lambda^{p(p-1)} = 1$.

Kanıt:

$\lambda = 1 + bu + cu^2$ olsun. $\lambda^p = (1 + bu + cu^2)^p = (1 + u(b + cu))^p$ eşitliğinin son düzenlenmiş kısmında binom açılımı uygulanırsa,

$$\lambda^p = \binom{p}{0} 1^p (u(b+cu))^0 + \binom{p}{1} 1^{p-1} (u(b+cu))^1 + \binom{p}{2} 1^{p-2} (u(b+cu))^2 + \cdots + \binom{p}{p} 1^0 (u(b+cu))^p$$

eşitliği elde edilir. Açılımın ilk terimi 1, ikinci terimi $mod\ p$'ye göre 0, üçüncü ve daha sonraki terimler $mod\ u^3$'e göre 0 olacağından ilk durum için $\lambda^p = 1$ olduğu görülür.

İkinci durumun ispatı için, $\lambda = a + dv$ olsun. Aşağıdaki eşitliğin 1 olduğu gösterilecektir:

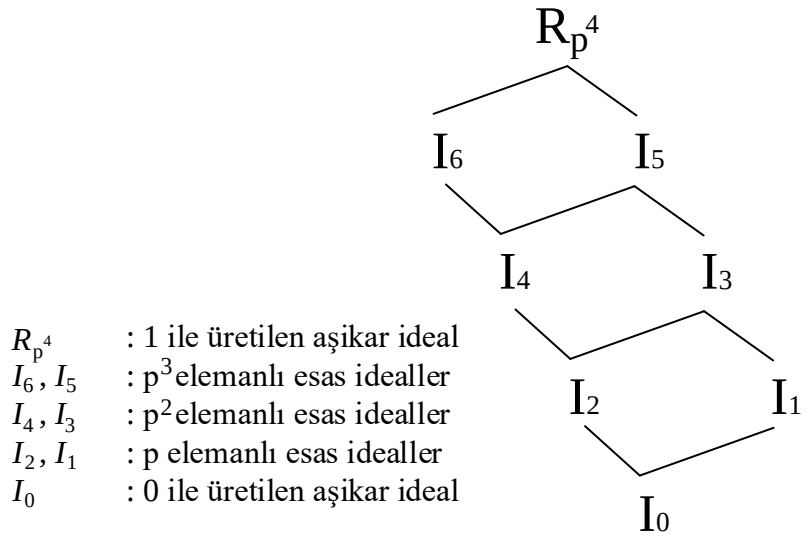
$$\lambda^{p-1} = (a + dv)^{p-1} = a^{p-1}(1 + a^{-1}dv)^{p-1}$$

a sayısı p ile aralarında asal olduğundan, $a^{p-1} \equiv 1\ (mod\ p)$ sağlanır. Ayrıca, $(1 + a^{-1}dv)^{p-1}$ ifadesinin binom açılımı $v^2 = v$ kullanılarak düzenlendiğinde $1 + v\ (-a^{-1}d + (a^{-1}d)^2 - (a^{-1}d)^3 + \cdots - (a^{-1}d)^{p-2} + (a^{-1}d)^{p-1})\ (mod\ p)$ bulunur. v parantezi içinde kalan kısım $x^p + 1 = (x + 1)(x^{p-1} - x^{p-2} + \cdots + x^2 - x + 1)$ özdeşliğinden yararlanılarak düzenlenir ve $(a^{-1}d)^{p-1} \equiv 1\ (mod\ p)$ denkliği kullanılırsa, $-a^{-1}d + (a^{-1}d)^2 - \cdots - (a^{-1}d)^{p-2} + (a^{-1}d)^{p-1} \equiv 0\ (mod\ p)$ bulunur. O halde, $\lambda^{p-1} = 1$ elde edilir.

Son durum için, $\lambda = a + bu + cu^2 + dv$ olsun. $\lambda^p = (a + bu + cu^2 + dv)^p$ eşitliğinde binom uygulanırsa, $\lambda^p \equiv (bu + cu^2)^p + (a + dv)^p\ (mod\ p)$ elde edilir. $p \neq 2$ asal sayı ve $u^3 = 0$ olduğu gerçeği kullanılırsa $\lambda^p \equiv (a + dv)^p\ (mod\ p)$ denkliği elde edilir. İkinci durumdan, $(a + dv)^{p-1} \equiv 1\ (mod\ p)$ olduğu kullanılarak, $\lambda^p \equiv a + dv\ (mod\ p)$ denkliği elde edilir. Bu denkliğin tekrar $(p - 1)$. kuvveti alınırsa, yine ikinci durumdan, $\lambda^{p(p-1)} = (a + dv)^{p-1} \equiv 1\ (mod\ p)$ bulunur.

3.3.1.2. R_{p^4} Halkasının İdealleri

Bu alt bölümde, R_{p^4} halkasının cebirsel yapısının ortaya çıkarılması için, halkanın ideal yapısı araştırılmaktadır. Bu araştırmalara dayanarak, herhangi bir p asalı için R_{p^4} halkasının ideallerinin tek şekilde bir ideal kafesi oluşturduğu görülmektedir. *Şekil 3.3*'de görüldüğü gibi R_{p^4} halkasının maksimal idealleri (p^3 elemanlı idealleri) ve diğer idealleri iki farklı tipte olacak şekilde dallanmaktadır. Aşağıdaki önermede bu ideallerin üreteçlerinin sayıları ve tipleri üzerinde durulmaktadır.



Şekil 3.3 R_{p^4} Halkasının İdealleri

3.3.1.2.1. Önerme:

R_{p^4} halkasının tek eleman ile üretilen tüm ideallerinin tipleri ve sayıları aşağıdaki gibidir:

(i) p^3 elemanlı, tek elemanla üretilen iki farklı maksimal ideal vardır. Birinci tip maksimal idealin üreteci: $a \neq 0$ ve $a + d \equiv 0 \,(mod\, p)$ koşullarını sağlamaktadır. O halde, birinci tip maksimal idealin üreteç sayısı $p^2(p - 1)$. İkinci tip maksimal idealin üreteci: $a = 0, b \neq 0$ ve $d \neq 0$ koşullarını sağlamaktadır. Böylece, ikinci tip maksimal idealin üreteç sayısı $(p - 1)^2 p$ dir.

(ii) p^2 elemanlı, tek elemanla üretilen iki farklı ideal vardır. Birinci tip p^2 elemanlı esas idealin üreteci: $a = 0, b \neq 0$ ve $d = 0$ koşullarını sağlamaktadır. Bu durumda, birinci tip p^2 elemanlı esas idealin üreteç sayısı $p(p - 1)$. İkinci tip p^2 elemanlı esas idealin üreteci: $a = 0, b = 0, c \neq 0$ ve $d \neq 0$ koşullarını sağlamaktadır. O halde, ikinci tip maksimal idealin üreteç sayısı $(p - 1)^2$ dir.

(iii) p elemanlı, tek elemanla üretilen iki farklı ideal vardır. Üreteçlerden biri $a = b = d = 0$ ve $c \neq 0$ koşullarını, diğeri $a = b = c = 0$ ve $d \neq 0$

koşullarını sağlamaktadır. O halde, bu iki tip p elemanlı esas idealin üreteç sayısı $p-1$ dir.

Bu önerme doğrultusunda aşağıdaki önemli sonuç elde edilir:

3.3.1.2.2. Sonuç:

R_{p^4} bir esas ideal halkasıdır.

Kanıt:

3.3.1.2.1 Önerme'deki tek eleman ile üretilen ideallerin üreteç tipleri göz önüne alınsın. $\lambda_1 = b_1u + c_1u^2$ ve $\lambda_2 = c_2u^2 + d_2v$ üreteçleri için $\langle \lambda_1, \lambda_2 \rangle$ iki elemanla üretilen ideali, üreteci $bu + cu^2 + dv$ tipinde olan bir esas ideale eşit olacaktır. $\lambda_1 = c_1u^2$ ve $\lambda_2 = d_2v$ üreteçleri için $\langle \lambda_1, \lambda_2 \rangle$ iki elemanla üretilen ideali, üreteci $cu^2 + dv$ biçiminde olan tek elemanla üretilen bir ideale eşit olacaktır. Son olarak, $\lambda_1 = b_1u + c_1u^2$ ve $\lambda_2 = d_2v$ üreteç çifti kullanılarak elde edilen $\langle \lambda_1, \lambda_2 \rangle$ ideali yine $\langle cu^2 + dv \rangle$ esas idealine eşit olacaktır. Halkanın herhangi iki tipteki elemanı ile üretilen tüm idealler bir esas ideale karşı geleceğinden, R_{p^4} halkasının tüm idealleri esas idealdir.

3.3.1.2.3. Not:

R_{p^4} halkasının iki maksimal ideali olduğundan R_{p^4} halkası yarı yerel halkadır. $soc(R_{p^4})$ kümesi R_{p^4} halkasının p^2 elemanlı bir ideali ve ayrıca R_{p^4} halkasının minimal ideallerinin toplamı da p^2 elemanlı idealidir. Dolayısıyla, $|R_{p^4}/socR_{p^4}| = p^2$. Buradan, R_{p^4} halkasının Frobenious halkası olduğu görülür.

3.3.2. $kp-1$ Uzunluklu $\lambda-$ Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki

Bu bölümde, R_{p^4} halkasının üzerindeki sabit devirli kodların elde edilmesi için $(1+u)$ ve $(1-u+u^2)$ birimsel elemanları ile çalışılmaktadır. $(1+u)$ ve $(1-u+u^2)$ birimsel elemanları için, *3.3.1.1.3 Önerme*'deki sınıflandırmaya göre $(1+u)^p = 1$ ve $(1-u+u^2)^p = 1$. Bu eşitlikler R_{p^4} halkasının üzerindeki devirli ve sabit devirli kodlar arasındaki izomorfizmanın elde edilmesi için, k bir pozitif tam sayı olmak üzere,

uzunluğun $kp-1$ biçiminde olmasını gerektirir. Bu kısıtlama altında, aşağıdaki önerme ve sonuçlar elde edilir:

3.3.2.1. Önerme:

$\lambda = 1+u$ veya $\lambda = 1-u+u^2$ olsun. $n = kp-1$ olmak üzere μ dönüşümü $R_{p^4}[x]/\langle x^n-1\rangle$ bölüm halkasından $R_{p^4}[x]/\langle x^n-\lambda\rangle$ bölüm halkasına $\mu(\overline{f(x)}) = \overline{f(\lambda x)}$ biçiminde tanımlı ise μ bir halka izomorfizmasıdır.

Kanıt:

μ'nün iyi tanımlılığı aşağıdaki gibi gösterilir:

$f(x) \equiv g(x)\ (mod\ x^n-1)$ olsun. Bu durumda, $\overline{f(x)} - \overline{g(x)} = \overline{h(x)(x^n-1)}$ sağlayan en az bir $\overline{h(x)} \in R_{p^4}[x]/\langle x^n-1\rangle$ polinomu vardır. Eşitlikte, x yerine λx yazılırsa, $\overline{f(\lambda x)} - \overline{g(\lambda x)} = \overline{h(\lambda x)(\lambda^n x^n-1)}$ eşitliği elde edilir. $n = kp-1$ olduğundan, $\lambda^n = \lambda^{kp-1}$ ve $\lambda^{kp} = 1$. Bu gerçekler ve μ dönüşümünün tanımı kullanıldığında, son eşitlik $\mu(\overline{f(x)}) - \mu(\overline{g(x)}) = \overline{h(\lambda x)\lambda^{kp-1}(x^n-\lambda)}$ biçiminde yazılır. Bunun anlamı, $\mu(f(x)) \equiv \mu(g(x))\ (mod\ x^n-\lambda)$ olmasıdır. Bu işlemler tersine de sağlanacağından, μ dönüşümü birebir dönüşümdür. μ dönüşümünün örten olduğu açıktır.

Kanıtı tamamlamak için μ dönüşümünün homomorfizma olduğunu göstermek yetecektir. Herhangi bir $\overline{f(x)}, \overline{g(x)} \in R_{p^4}[x]/\langle x^n-1\rangle$ için, μ dönüşümünün tanımı ve fonksiyonlarda toplama ve çarpmanın tanımı kullanılarak μ dönüşümünün bir halka homomorfizması olduğu görülür. O halde, μ dönüşümü bir halka izomorfizmasıdır.

Yukarıdaki önerme kullanılarak μ dönüşümünün izomorf kıldığı bu iki bölüm halkasının idealleri arasında birebir bir eşleme olduğu, aşağıdaki sonuç ile verilir:

3.3.2.2. Sonuç:

$\lambda = 1+u$ veya $\lambda = 1-u+u^2$ olsun. $n = kp-1$ ise I kümesinin $R_{p^4}[x]/\langle x^n-1\rangle$ bölüm halkasının bir ideali olması için gerekli ve yeterli koşul $\mu(I)$ kümesinin $R_{p^4}[x]/\langle x^n-\lambda\rangle$ bölüm halkasının bir ideali olmasıdır.

Kanıt:

3.2.2.2 Sonuç'un kanıtına benzer şekilde elde edilir.

3.3.2.3. Sonuç:

$\lambda = 1 + u$ veya $\lambda = 1 - u + u^2$ olmak üzere, $n = kp - 1$ ve C kümesi $R_{p^4}^n$ kümesinin bir alt kümesi olsun. $\bar{\mu}$ permütasyonu $R_{p^4}^n$ kümesi üzerinde aşağıdaki şekilde tanımlı olsun:

$$\bar{\mu}(c_0, c_1, \dots, c_{n-1}) = (c_0, \lambda c_1, \dots, \lambda^i c_i, \dots, \lambda^{n-1} c_{n-1}) \ (mod\ p)$$

Bu durumda, C'nin devirli kod olması için gerekli ve yeterli koşul $\bar{\mu}(C)$'nin $\lambda -$ sabit devirli kod olmasıdır.

Kanıt:

C devirli bir kod olsun. C'nin polinom gösterimi yine C ile gösterilsin. Bu durumda, C kümesi $R_{p^4}[x]/\langle x^n - 1\rangle$ bölüm halkasının bir idealidir. Bir önceki sonuç sağlandığından, $\mu(C)$ kümesi $R_{p^4}[x]/\langle x^n - \lambda\rangle$ bölüm halkasının bir ideali olur. Bu durumda, $\bar{\mu}(C)$ kodu $\lambda -$ sabit devirli koddur.

3.3.3. R_{p^4} Halkası Üzerinde Devirli Kodların İnşası

S halkası, $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ olsun. φ dönüşümü, R_{p^4} halkasından S halkasına $\varphi(a + bu + cu^2 + dv) = a + bu + cu^2\ (mod\ v)$ şeklinde tanımlı homomorfizma olsun. φ homomorfizması Ψ homomorfizmasına aşağıdaki şekilde genelleştirilsin:

$$\Psi: R_{p^4}[x]/\langle x^n - 1\rangle \to S[x]/\langle x^n - 1\rangle$$

$$\Psi(z_0 + z_1 x + \cdots + z_{n-1}x^{n-1}) = \varphi(z_0) + \varphi(z_1)x + \cdots + \varphi(z_{n-1})x^{n-1}$$

Ψ homomorfizmasının çekirdek kümesi aşağıdaki şekildedir:

$$çek(\Psi) = \{vp(x) | p(x) \in \mathbb{F}_p[x]/\langle x^n - 1\rangle\}$$

J kümesi, $J = \{p(x) | vp(x) \in çek(\Psi)\}$ biçiminde tanımlansın. J kümesi $\mathbb{F}_p[x]/\langle x^n - 1\rangle$ bölüm halkasının idealidir. Bu durumda, J kümesi $\mathbb{F}_p[x]/\langle x^n - 1\rangle$ kümesinde

bir devirli koddur. Buradan, $J = \langle t(x) \rangle$ olacak şekilde $mod\ p$'ye göre, $x^n - 1$ polinomunun bir $t(x)$ monik böleni vardır. O halde, Ψ homomorfizmasının çekirdek kümesi tek eleman ile üretilen $\langle vt(x) \rangle$ ideali olarak yazılır. Diğer yandan, Ψ homomorfizmasının görüntü kümesi de $S[x]/\langle x^n - 1 \rangle$ halkasının bir idealidir. Bu durumda, $Im(\Psi)$ kümesi S^n kümesinde devirli bir koddur. $p \nmid n$ olması durumunda, S sonlu zincir halkasında devirli kodun üreteç ideali, $g_2|g_1|g_0|(x^n - 1)$ olmak üzere, $\langle g_0(x), ug_1(x), u^2 g_2(x) \rangle$ şeklinde verilmiştir (Qian, vd., 2005). Buraya kadar yapılan işlemler göz önüne alındığında, *çek-gör fikri* kullanılarak R_{p^4} halkası üzerindeki devirli kodların üreteç ideali, $\langle g_0(x) + vh_0(x), ug_1(x) + vh_1(x), u^2 g_2(x) + vh_2(x), vt(x) \rangle$ olarak bulunur. R_{p^4} halkası üzerinde inşa edilen devirli kodun üreteç idealinin dört parçalı bileşenlerinin her biri için sağladıkları özellikler incelendiğinde, $v(g_0(x) + vh_0(x)) = v(g_0(x) + h_0(x)) \in \langle vt(x) \rangle = çek(\Psi)$, $v(ug_1(x) + vh_1(x)) = vh_1(x) \in \langle vt(x) \rangle = çek(\Psi)$ ve $v(u^2 g_2(x) + vh_2(x)) = vh_2(x) \in \langle vt(x) \rangle = çek(\Psi)$ ilişkileri elde edilir. Bu ilişkilerden yararlanılarak, $t(x)|g_0(x) + h_0(x)$, $t(x)|h_1(x)$ ve $t(x)|h_2(x)$ tam bölünebilme koşulları elde edilir. $t(x)$ polinomunun tam böldüğü bu polinomlar göz önüne alındığında, R_{p^4} halkası üzerinde önerilen devirli kodun üreteç ideali aşağıdaki teoremde verildiği gibi sadeleştirilebilir:

3.3.3.1. Teorem:

$p \nmid n$ sağlayan n sayısı için C, R_{p^4} halkası üzerinde n uzunluklu devirli bir kod olsun. Bu durumda, $i = 0, 1, 2$ olmak üzere, $g_i(x), h_0(x), t(x) \in \mathbb{F}_p[x]$ polinomları için $g_2|g_1|g_0|(x^n - 1)$ ve $t(x)|(g_0(x) + h_0(x))$ koşullarını sağlayan C kodunun üreteci $C = \langle g_0(x) + vh_0(x), ug_1(x), u^2 g_2(x), vt(x) \rangle$ biçimindedir.

3.3.3.2. Lemma:

$C = \langle g_0(x) + vh_0(x), ug_1(x), u^2 g_2(x), vt(x) \rangle$, R_{p^4} halkası üzerinde tanımlı devirli bir kod olsun. $t(x)$ monik polinom ise $der\,(h_0(x)) < der\,(t(x))$ olarak alınabilir.

Kanıt:

$der\left(t(x)\right) \leq der(h_0(x))$ olsun. Bu durumda, $h_0(x) = t(x)m_0(x) + r_0(x)$ eşitliğini sağlayan, $m_0(x)$, $r_0(x) \in R_{p^4}[x]$ polinomları vardır ve burada ya $der\left(r_0(x)\right) < der\,(h_0(x))$ ya da $r_0(x) = 0$ olacaktır. Bu duruma göre C kodu tekrar yazıldığında, $C = \langle g_0(x) + v(t(x)m_0(x) + r_0(x)), ug_1(x), u^2g_2(x), vt(x)\rangle$ şeklinde olacaktır. $C_1 = \langle g_0(x) + vr_0(x), ug_1(x), u^2g_2(x), vt(x)\rangle$ olsun. $C \subseteq C_1$ olduğu açıktır. $g_0(x) + vr_0(x) = g_0(x) + vt(x)m_0(x) + vr_0(x) + v(p-1)t(x)m_0(x)$ biçiminde yazılırsa, $C_1 \subseteq C$ olacağı açıktır. Dolayısıyla, $C = C_1$ bulunur.

3.3.3.3. Teorem:

$C = \langle g_0(x) + vh_0(x), ug_1(x), u^2g_2(x), vt(x)\rangle$, R_{p^4} halkası üzerinde n uzunluklu devirli bir kod olsun. $i = 0, 1, 2$ için $der(g_i(x)) = k_i$ ve $der(t(x)) = l$ olsun. $g_i(x)$ ve $t(x)$ monik polinomlar ise C kodunun minimal üreteç kümesi aşağıdaki şekilde verilir:

$$\{g_0(x) + vh_0(x), x(g_0(x) + vh_0(x)), \dots, x^{n-k_0-1}(g_0(x) + vh_0(x)), ug_1(x), x(ug_1(x)), \dots, x^{k_0-k_1-1}(ug_1(x)), u^2g_2(x), x(u^2g_2(x)), \dots, x^{k_1-k_2-1}(u^2g_2(x)), vt(x), x(vt(x)), \dots, x^{k_2-l-1}(vt(x))\}$$

3.3.3.4. Örnek:

Bu örnekte, R_{3^4} sonlu halkası üzerindeki devirli kodlar göz önüne alınsın. Burada, $n = kp - 1 = 3.3 - 1 = 8$ uzunluklu bazı devirli kodların üreteçleri ve ilişkili $(1 + u)-$ sabit devirli kodların üreteçleri elde edilecektir. $n = 8$ olmak üzere, $\mathbb{F}_3$ sonlu cisminde $x^8 - 1$ polinomunun çarpanlara ayrılışı aşağıdaki gibidir:

$$\begin{aligned} x^8 - 1 &= (x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2) \\ &= f_1(x)f_2(x)f_3(x)f_4(x)f_5(x) \end{aligned}$$

3.3.3.1 Teorem'deki devirli kodun üretecindeki $g_2(x)$, $g_1(x)$, $g_0(x)$ ve $h_0(x)$ polinomları sırasıyla $f_1, f_1f_2, f_1f_2f_3$ ve 1 olsun. *3.3.3.1 Teorem* gereği $t(x)$ polinomu $g_0(x) + h_0(x) = f_1f_2f_3 + 1 = x^4$ polinomunun bir tam böleni olmalıdır. O halde, bu koşulları sağlayan 8 uzunluklu bazı devirli kodların üreteçleri aşağıdaki gibi yazılır:

$$C_1 = \langle x^4 + 2 + v, u(x^2+2), u^2(x+1), vx\rangle$$

$$C_2 = \langle x^4 + 2 + v, u(x^2 + 2), u^2(x + 1), vx^2 \rangle$$

$$C_3 = \langle x^4 + 2 + v, u(x^2 + 2), u^2(x + 1), vx^3 \rangle$$

$$C_4 = \langle x^4 + 2 + v, u(x^2 + 2), u^2(x + 1), vx^4 \rangle$$

3.3.2.1. Önerme'deki μ izomorfizması göz önüne alındığında, C_1, C_2, C_3, C_4 devirli kodlarına ilişkin, D_1, D_2, D_3, D_4 $(1 + u) -$ sabit devirli kodların üreteçleri sırasıyla aşağıdaki gibidir:

$$D_1 = \langle (1 + u)x^4 + 2 + v, (u + 2u^2)x^2 + 2u, u^2(x + 1), vx \rangle$$

$$D_2 = \langle (1 + u)x^4 + 2 + v, (u + 2u^2)x^2 + 2u, u^2(x + 1), vx^2 \rangle$$

$$D_3 = \langle (1 + u)x^4 + 2 + v, (u + 2u^2)x^2 + 2u, u^2(x + 1), vx^3 \rangle$$

$$D_4 = \langle (1 + u)x^4 + 2 + v, (u + 2u^2)x^2 + 2u, u^2(x + 1), vx^4 \rangle$$

3.3.3.5. Örnek:

R_{5^4} halkası göz önüne alınsın. $k = 2$ olarak seçilirse, $n = kp - 1 = 2.5 - 1 = 9$ uzunluğu için $\mathbb{F}_5$ sonlu cisminde $x^9 - 1$ polinomunun çarpanlara ayrılışı aşağıdaki gibidir:

$$x^9 - 1 = (x + 4)(x^2 + x + 1)(x^6 + x^3 + 1) = f_1(x)f_2(x)f_3(x)$$

$g_2(x), g_1(x), g_0(x)$ ve $h_0(x)$ polinomları sırasıyla $1, f_2, f_1f_2$ ve 1 olsun. Bu durumda, $t(x)$ polinomu $g_0(x) + h_0(x) = f_1f_2 + 1 = x^3$ polinomunu tam böler. Bu gerçekler göz önüne alınarak, $\mathbb{F}_5$ sonlu cisminde 9 uzunluklu bazı devirli kodların üreteçleri aşağıdaki şekilde yazılır:

$$C_1 = \langle x^3 + 4 + v, u(x^2 + x + 1), u^2, vx \rangle$$

$$C_2 = \langle x^3 + 4 + v, u(x^2 + x + 1), u^2, vx^2 \rangle$$

$$C_3 = \langle x^3 + 4 + v, u(x^2 + x + 1), u^2, vx^3 \rangle$$

Bu polinomlarla ilişkili $(1 + u) -$ sabit devirli kod üreteçleri sırasıyla aşağıdaki gibidir:

$$D_1 = \langle (1+3u+3u^2)x^3 + 4 + v, (u+2u^2)x^2 + (u+u^2)x + u, u^2, vx \rangle$$

$$D_2 = \langle (1+3u+3u^2)x^3 + 4 + v, (u+2u^2)x^2 + (u+u^2)x + u, u^2, vx^2 \rangle$$

$$D_3 = \langle (1+3u+3u^2)x^3 + 4 + v, (u+2u^2)x^2 + (u+u^2)x + u, u^2, vx^3 \rangle$$

3.3.4. R_{p^4} Halkası Üzerinde Tanımlı Gray Dönüşüm

Bu bölümde, $p \neq 2$ asal sayısı için ϕ_{p^4} Gray dönüşümü aşağıdaki şekilde tanımlanmaktadır:

$\phi_{p^4}: R_{p^4} \to \mathbb{F}_p^{p+1}$

$\phi_{p^4}(a + bu + cu^2 + dv) = (s_0, s_1, \dots, s_p)$

Burada, $s_k = a_k a + b_k b + c_k c + d_k d$ olmak üzere, a_k, b_k, c_k ve d_k katsayıları aşağıdaki şekilde tanımlıdır:

$k = 0$ iken $a_0 = b_0 = c_0 = 0$ ve $d_0 = 1$.

$0 < k \leq p$ iken $a_k \equiv \frac{(k-2)(k-1)}{2} \ (mod\ p)$, $b_k = k - 1, c_k = 1$ ve $d_k = 0$.

Yukarıda tanımlı ϕ_{p^4} Gray dönüşümü $R_{p^4}^n$ halkasına aşağıdaki şekilde genişletilir:

$$\phi_{p^4}: R_{p^4}^n \to \mathbb{F}_p^{(p+1)n}$$

$$\phi_{p^4}(z_0, z_1, \dots, z_{n-1}) = (s_{00}, \dots, s_{0(n-1)}, s_{10}, \dots, s_{1(n-1)}, \dots, s_{p0}, \dots, s_{p(n-1)})$$

Burada, her $0 \leq i \leq n-1$ sağlayan i ve her $0 \leq k \leq p$ sağlayan k için $a_i, b_i, c_i, d_i \in \mathbb{F}_p$ olmak üzere, $z_i = a_i + b_i u + c_i u^2 + d_i v$ ve $s_{ki} = a_k a_i + b_k b_i + c_k c_i + d_k d_i$ biçiminde tanımlıdır. s_{ki}'nin a_k, b_k, c_k ve d_k katsayıları yukarıda tanımlı olduğu gibi alınacaktır.

3.3.4.1. Örnek:

Yukarıda tanımlanan Gray dönüşümü $p = 13$ asal sayısı için aşağıdaki şekilde yazılır:

$\phi_{13^4}: R_{13^4} \to \mathbb{F}_{13}^{14}$

$$\phi_{13^4}(a+bu+cu^2+dv) = (s_0, s_1, \dots, s_{13})$$
$$= (d, c, b+c, a+2b+c, 3a+3b+c, 6a+4b+c, 10a+5b$$
$$+c, 2a+6b+c, 8a+7b+c, 2a+8b+c, 10a+9b+c, 6a$$
$$+10b+c, 3a+11b+c, a+12b+c)$$

3.3.4.2. R_{p^4} Halkası Üzerinde $(1+u)-$ Sabit Devirli Kodlar

Bu alt bölümde, R_{p^4} halkası üzerindeki devirli kodların ve $(1+u)-$ sabit devirli kodların Gray görüntüleri araştırılmaktadır.

3.3.4.2.1. Önerme:

$\nu, (1+u)-$ sabit devirli öteleme ve $\sigma^{\otimes(p+1)}$, $p+1$ indeksli quasicyclic öteleme olsun. $\{0,1,\dots,pn+n-1\}$ kümesi üzerindeki π_{p^4} permütasyonu, $\pi_{p^4} = (n, pn)(pn, (p-1)n) \dots (4n, 3n)(3n, 2n)$ şeklinde tanımlı olmak üzere, $\phi_{p^4}\nu = \pi_{p^4}\sigma^{\otimes(p+1)}\phi_{p^4}$ eşitliği sağlanır.

Kanıt:

Her $z = (z_0, z_1, \dots, z_{n-1}) \in R_{p^4}$ alınsın. Her $0 \le i \le n-1$ sağlayan i için $a_i, b_i, c_i, d_i \in \mathbb{F}_p$ olmak üzere, $z_i = a_i + b_i u + c_i u^2 + d_i v$. Bu durumda, $\nu(z) = ((1+u)z_{n-1}, z_0, z_1, \dots, z_{n-2})$. Gray dönüşümün tanımından, $(\phi_{p^4}(\nu))(z) = (d_{n-1}, d_0, \dots, d_{n-2}, b_{n-1}+c_{n-1}, c_0, \dots, c_{n-2}, a_{n-1}+2b_{n-1}+c_{n-1}, b_0+c_0, b_1+c_1, \dots, b_{n-2}+c_{n-2}, 3a_{n-1}+3b_{n-1}+c_{n-1}, a_0+2b_0+c_0, \dots, a_{n-2}+2b_{n-2}+c_{n-2}, \dots, \dots, c_{n-1}, a_0+(p-1)b_0+c_0, \dots, a_{n-2}+(p-1)b_{n-2}+c_{n-2})$ elde edilir. Diğer yandan, $\phi_{p^4}(z) = (d_0, \dots, d_{n-1}, c_0, \dots, c_{n-1}, b_0+c_0, \dots, b_{n-1}+c_{n-1}, a_0+2b_0+c_0, \dots, a_{n-1}+2b_{n-1}+c_{n-1}, \dots, \dots, a_0+(p-1)b_0+c_0, \dots, a_{n-1}+(p-1)b_{n-1}+c_{n-1})$ eşitliğinin her iki yanına, $\sigma^{\otimes(p+1)}$ dönüşümü uygulanırsa, $\sigma^{\otimes(p+1)}(\phi_{p^4}(z)) = (d_{n-1}, d_0, \dots, d_{n-2}, c_{n-1}, c_0, \dots, c_{n-2}, b_{n-1}+c_{n-1}, b_0+c_0, \dots, b_{n-2}+c_{n-2}, a_{n-1}+2b_{n-1}+c_{n-1}, a_0+2b_0+c_0, \dots, a_{n-2}+2b_{n-2}+c_{n-2}, \dots, \dots, a_{n-1}+(p-1)b_{n-1}+c_{n-1}, a_0+(p-1)b_0+c_0, \dots, a_{n-2}+(p-1)b_{n-2}+c_{n-2})$ eşitliği elde edilir. Elde edilen bu son eşitliğe, önermede tanımlanan π_{p^4} permütasyonu uygulanırsa,

$(\pi_{p^4}(\sigma^{\otimes(p+1)})(\phi_{p^4}(z)))) = (d_{n-1}, d_0, \dots, d_{n-2}, b_{n-1} + c_{n-1}, c_0, \dots, c_{n-2}, a_{n-1} + 2b_{n-1} + c_{n-1}, b_0 + c_0, b_1 + c_1, \dots, b_{n-2} + c_{n-2}, 3a_{n-1} + 3b_{n-1} + c_{n-1}, a_0 + 2b_0 + c_0, \dots, a_{n-2} + 2b_{n-2} + c_{n-2}, \dots, \dots, c_{n-1}, a_0 + (p-1)b_0 + c_0, \dots, a_{n-2} + (p-1)b_{n-2} + c_{n-2})$ elde edilir. O halde, $\phi_{p^4}\nu = \pi_{p^4}\sigma^{\otimes(p+1)}\phi_{p^4}$ eşitliği sağlanır.

3.3.4.2.2. Teorem:

R_{p^4} halkası üzerindeki n uzunluklu $(1+u)-$ sabit devirli kodların Gray görüntüleri, $\mathbb{F}_p$ sonlu cismi üzerinde $(p+1)n$ uzunluklu ve indeksi $(p+1)$ olan quasicyclic koda denktir.

Kanıt:

C, R_{p^4} halkası üzerinde n uzunluklu $(1+u)-$ sabit devirli kod olsun. Öyleyse, $\nu(C) = C$ olur. Bu eşitliğin her iki yanının Gray dönüşüm altındaki görüntüsü alınırsa, $\phi_{p^4}(\nu(C)) = \phi_{p^4}(C)$ elde edilir. *3.3.4.2.1 Önerme* kullanılarak, $\phi_{p^4}(C) = \pi_{p^4}\left(\sigma^{\otimes(p+1)}\left(\phi_{p^4}(C)\right)\right)$ bulunur. Bunun anlamı, $\phi_{p^4}(C)$ kodu $\mathbb{F}_p$ üzerinde $(p+1)n$ uzunluklu ve indeksi $(p+1)$ olan quasicyclic koda denktir.

3.3.4.2.3. Önerme:

$\bar{\mu}$ dönüşümü *3.3.2.3 Sonuç*'ta tanımlı permütasyon olsun. k pozitif bir tam sayı ve $n = kp - 1$ ise γ_{p^4} permütasyonu $\{0,1, \dots, (p+1)(kp-1)-1\}$ kümesi üzerinde $\xi_{i,j}$, p uzunluklu devrinimlerinin bileşkesi (devrinimler ayrık olduğundan bileşke değişmeli olacaktır ve sıra bakmaksızın bileşke alınabilir) biçiminde tanımlı olmak üzere, $\gamma'(z_0, z_1, \dots, z_{(p+1)(kp-1)-1}) = (z_{\gamma_{p^4}(0)}, z_{\gamma_{p^4}(1)}, \dots, z_{\gamma_{p^4}((p+1)(kp-1)-1)})$ permütasyonu ile $\phi_{p^4}\bar{\mu} = \gamma'\phi_{p^4}$ eşitliği sağlanır. Burada, $i = 1,2, \dots, p-1$, $j = 0,1, \dots, k-1$ ve $t = 2, \dots, p$ için $a_{1t} = p + 2 - t$ ve $a_{it} \equiv a_{(i-1)t} + 1 - t \ (mod\ p)$ katsayıları için $\xi_{i,j}$ devrinimleri,

$$\xi_{i,j} = \left(n + i + jp, a_{i2}.n + i + jp, a_{i3}.n + i + jp, \dots, a_{i(p-1)}.n + i + jp, a_{ip}.n + i + jp\right)$$

biçiminde tanımlıdır (Ayrıca $i = p-1$ ve $j = k-1$ için $\xi_{p-1,k-1}$ devrinimi tanımlı değildir ve $a_{it} \equiv 0\ (mod\ p)$ durumunda $a_{it} = p$ alınır).

Kanıt:

$z = (z_0, z_1, \dots, z_{kp-2}) \in R_{p^4}^n$ olsun. Her $0 \le i \le kp-2$ sağlayan i için $a_i, b_i, c_i, d_i \in \mathbb{F}_p$ olmak üzere, $z_i = a_i + b_i u + c_i u^2 + d_i v$ olsun. $\bar{\mu}$ permütasyonu uygulayarak, $\bar{\mu}(z_0, z_1, \dots, z_{kp-2}) = (z_0, (1+u)z_1, \dots, (1+u)^{kp-2} z_{kp-2})$ eşitliği bulunur. $(1+u)^{-1} = 1 - u + u^2$ ve $(1+u)^{kp} \equiv 1 \ (mod\ p)$ eşitlikleri kullanıldığında, $\bar{\mu}(z)$'nin Gray görüntüsünün yukarıdaki şekilde tanımlı γ' permütasyonu için $\gamma'\left(\phi_{p^4}(z)\right)$ bileşkesine eşit olduğu görülür.

3.3.4.2.4. Teorem:

γ', *3.3.4.2.3. Önerme*'de tanımlı permütasyon olsun. $n = kp - 1$ olmak üzere, Δ, R_{p^4} halkası üzerinde bir devirli kodun Gray görüntüsü ise $\gamma'(\Delta)$ kodu, $(kp-1)(p+1)$ uzunluklu $\mathbb{F}_p$ üzerinde indeksi $p+1$ olan quasicyclic koda denktir.

Kanıt:

$\Delta = \phi_{p^4}(C)$, R_{p^4} halkası üzerinde bir C devirli kodunun Gray görüntüsü olsun. *3.3.4.2.3 Önerme*'den $\phi_{p^4}(\bar{\mu}(C)) = \gamma'(\phi_{p^4}(C)) = \gamma'(\Delta)$ olduğu görülür.

3.3.4.2.5. Sonuç:

R_{p^4} halkası üzerinde $kp-1$ uzunluklu devirli bir kodun Gray görüntüsü, $\mathbb{F}_p$ üzerinde $(kp-1)(p+1)$ uzunluklu ve indeksi $p+1$ olan bir quasicyclic koda denktir.

3.3.4.3. R_{p^4} Halkası Üzerinde $(1 - u + u^2)$ − Sabit Devirli Kodlar

Bu alt bölümde, R_{p^4} halkası üzerindeki devirli kodların ve $(1 - u + u^2)$ − sabit devirli kodların Gray görüntüleri araştırılacaktır. ϕ_{p^4} Gray dönüşümü ile elde edilebilecek sabit devirli kodların Gray görüntüleri sadece $(1+u)$ ve $(1 - u + u^2)$ birimsel elemanları için geçerli olmaktadır.

3.3.4.3.1. Önerme:

$\nu, (1-u+u^2)-$ sabit devirli öteleme ve $\sigma^{\otimes(p+1)}$, $p+1$ indeksli quasicyclic öteleme olsun. $\{0,1,\dots,pn+n-1\}$ kümesi üzerindeki π_{p^4} permütasyonu, $\pi_{p^4} = (n,2n)(2n,3n)\dots((p-1)n,pn)$ şeklinde tanımlı olmak üzere, $\phi_{p^4}\nu = \pi_{p^4}\sigma^{\otimes(p+1)}\phi_{p^4}$ eşitliği sağlanır.

Kanıt:

Her $z=(z_0,z_1,\dots,z_{n-1}) \in R_{p^4}^n$ alınsın. Her $0 \le i \le n-1$ sağlayan i için $a_i,b_i,c_i,d_i \in \mathbb{F}_p$ olmak üzere, $z_i = a_i + b_iu + c_iu^2 + d_iv$. Bu durumda, $\nu(z) = ((1-u+u^2)z_{n-1}, z_0, z_1, \dots, z_{n-2})$. ϕ_{p^4} Gray dönüşümünün tanımından, $(\phi_{p^4}(\nu))(z) = (d_{n-1}, d_0, \dots, d_{n-2}, a_{n-1}+(p-1)b_{n-1}+c_{n-1}, c_0, \dots, c_{n-2}, c_{n-1}, b_0+c_0, b_1+c_1, \dots, b_{n-2}+c_{n-2}, b_{n-1}+c_{n-1}, a_0+2b_0+c_0, \dots, a_{n-2}+2b_{n-2}+c_{n-2}, \dots, \dots, a_0+(p-1)b_0+c_0, \dots, a_{n-2}+(p-1)b_{n-2}+c_{n-2})$ elde edilir. Diğer yandan, $\phi_{p^4}(z) = (d_0, \dots, d_{n-1}, c_0, \dots, c_{n-1}, b_0+c_0, \dots, b_{n-1}+c_{n-1}, a_0+2b_0+c_0, \dots a_{n-1}+2b_{n-1}+c_{n-1}, \dots, \dots, a_0+(p-1)b_0+c_0, \dots, a_{n-1}+(p-1)b_{n-1}+c_{n-1})$ eşitliğinin her iki yanına, $\sigma^{\otimes(p+1)}$ dönüşümü uygulanırsa, $\sigma^{\otimes(p+1)}(\phi_{p^4}(z)) = (d_{n-1}, d_0, \dots, d_{n-2}, c_{n-1}, c_0, \dots, c_{n-2}, b_{n-1}+c_{n-1}, b_0+c_0, \dots, b_{n-2}+c_{n-2}, a_{n-1}+2b_{n-1}+c_{n-1}, a_0+2b_0+c_0, \dots, a_{n-2}+2b_{n-2}+c_{n-2}, \dots, \dots, a_{n-1}+(p-1)b_{n-1}+c_{n-1}, a_0+(p-1)b_0+c_0, \dots, a_{n-2}+(p-1)b_{n-2}+c_{n-2})$ eşitliği elde edilir. Elde edilen bu son eşitliğe, önermede tanımlanan π_{p^4} permütasyonu uygulanırsa, $(\pi_{p^4}(\sigma^{\otimes(p+1)}(\phi_{p^4}(z)))) = (d_{n-1}, d_0, \dots, d_{n-2}, a_{n-1}+(p-1)b_{n-1}+c_{n-1}, c_0, \dots, c_{n-2}, c_{n-1}, b_0+c_0, b_1+c_1, \dots, b_{n-2}+c_{n-2}, b_{n-1}+c_{n-1}, a_0+2b_0+c_0, \dots, a_{n-2}+2b_{n-2}+c_{n-2}, \dots, \dots, a_0+(p-1)b_0+c_0, \dots, a_{n-2}+(p-1)b_{n-2}+c_{n-2})$ elde edilir. O halde, $\phi_{p^4}\nu = \pi_{p^4}\sigma^{\otimes(p+1)}\phi_{p^4}$ eşitliği sağlanır.

3.3.4.3.2. Teorem:

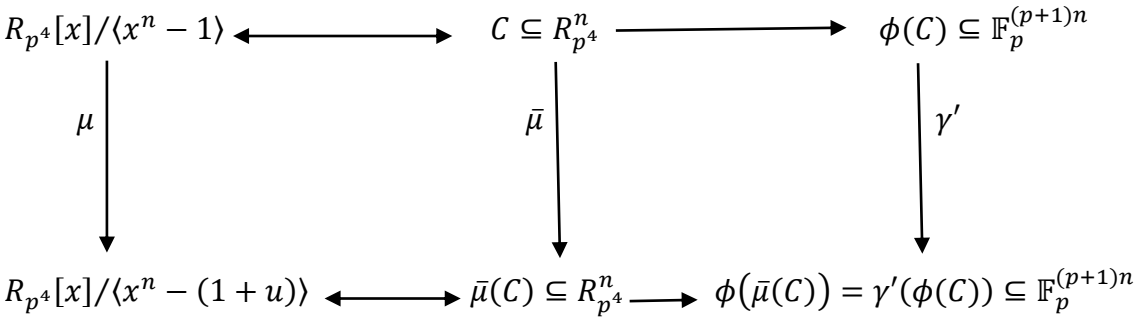
R_{p^4} halkası üzerindeki n uzunluklu $(1-u+u^2)-$ sabit devirli kodların Gray görüntüleri, $\mathbb{F}_p$ üzerinde $(p+1)n$ uzunluklu ve indeksi $(p+1)$ olan quasicyclic koda denktir.

Kanıt:

C, R_{p^4} halkası üzerinde n uzunluklu $(1+u)-$ sabit devirli kod olsun. O halde, $\nu(C)=C$ olur. Bu eşitliğin her iki tarafının Gray dönüşüm altındaki görüntüsü alınırsa, $\phi_{p^4}(\nu(C))=\phi_{p^4}(C)$ olur. *3.3.4.3.1 Önerme* kullanılarak, $\phi_{p^4}(C)=\pi_{p^4}\sigma^{\otimes(p+1)}\phi_{p^4}(C)$ elde edilir. Böylece, $\phi_{p^4}(C)$ kodu $(p+1)n$ uzunluklu indeksi $(p+1)$ olan $p-ary$ quasicyclic koda denk olduğu görülür.

3.3.5. R_{p^4} Halkası Üzerindeki $kp-1$ Uzunluklu Devirli Kodlar ile $(1+u)-$ Sabit Devirli Kodların Gray Görüntülerinin İlişkisi

Şekil 3.4.'de görüldüğü gibi bu bölümde, R_{p^4} halkası üzerinde devirli ve $(1+u)-$ sabit devirli kodları tanımlamak için, ilk olarak elde edilen bölüm halkalarını ilişkilendiren ve μ ile gösterilen izomorfizma verilmiştir. Daha sonra bu izomorfizma yardımıyla $\bar{\mu}$ permütasyonu tanımlanmıştır. Bu izomorfizma ve permütasyon, k pozitif tamsayı olmak üzere uzunluğun $kp-1$ olması durumunda sağlanacağı ifade edilmiştir. Son olarak, bu halka üzerinde tanımlanan devirli ve sabit devirli kodların Gray görüntülerinin $\mathbb{F}_p$ üzerinde bir quasicyclic koda denk olmasını sağlayan γ' ve π_{p^4} permütasyonları elde edilmiştir. Bu permütasyonlar yardımıyla, Şekil 3.4 diyagram komutatifliğini sağlayan, $\phi_{p^4}\nu=\pi_{p^4}\sigma^{\otimes(p+1)}\phi_{p^4}$ ve $\phi_{p^4}\bar{\mu}=\gamma'\phi_{p^4}$ eşitlikleri elde edilmiştir.



Şekil 3.4 R_{p^4} Halka Sınıfı Üzerindeki $kp-1$ Uzunluklu Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı

BÖLÜM 4

R_{2^5} HALKASI VE $R_{(2^k)^4}$ HALKA SINIFI ÜZERİNDE DEVİRLİ VE SABİT DEVİRLİ KODLARIN GRAY GÖRÜNTÜLERİ

4.1. Giriş

Bir lineer kodu temsil ederken uzunluk, boyut ve minimum uzaklık olmak üzere üç parametre kullanılır. Minimum uzaklık en önemli parametrelerinden biridir. Bir kodun minimum uzaklık parametresinin büyük olması, kodun hata düzeltme kapasitesini arttıracağından, minimum uzaklıkları büyük kodlar elde etmek önemlidir. Çeşitli sonlu halkalar kullanılarak devirli ve sabit devirli kodların, sonlu cisimler üzerinde görüntüleri elde edilerek minimum uzaklık parametresi büyük ve yeni kodlar elde edilen çalışmalar yapılmıştır. Bu çalışmalar, halkalar üzerinde tanımlanan kodlar ile cisimler üzerinde tanımlı kodlar arasındaki ilişkiyi bulmaya yönelik yöntemler içermektedir. Bu ilişki Gray dönüşüm isimli uzaklık koruyan, bir lineer dönüşüm yardımıyla kurulmaktadır.

Son yıllarda, pek çok makale Gray görüntü yöntemini içermektedir. İlk olarak, Qian 2006 yılında yaptığı çalışmalarda bu yöntemi kullanmıştır (Qian, vd., 2006a; Qian, vd., 2006b; Qian, vd., 2005). Ardından, Amarra, Çengellenmiş, Zhu, Dougherty, Kai, Yu gibi araştırmacılar aynı yöntemi farklı sonlu halkalar seçerek çalışmışlardır (Amarra, vd., 2008; Cengellenmis, 2009a; Cengellenmis, 2009b; Dougherty, vd., 2011; Kai, Zhu, Wang, 2012; Yu, vd., 2014; Zhu, Wang, 2010). Bu çalışmalarda, yöntem aynı olmasına rağmen, sonlu halkalar ve üzerlerinde tanımlanan Gray dönüşümler birbirinden farklıdır. Bu çalışmalardaki sonlu halkalar, bölüm halkalarından elde edilen halkalardır. Bölüm

halkasının üst kısmına yazılan polinom halkasının katsayıları değiştikçe ya da bölüm halkasının paydasına yazılan koşullar değiştikçe, yeni sonlu halkalar elde etmek mümkündür. Bu durumda, eleman sayıları aynı olsa bile cebirsel yapıları ve sahip olduğu özellikleri bakımından farklı sonlu halkalar elde edilir. Eleman sayıları eşit olan cisimler birbirlerine izomorf olduğu için, eleman sayıları aynı olan cisimlerde bu farklılığı ve doğal olarak bu çeşitliliği yakalamak mümkün değildir.

Son yıllarda artan Gray görüntü yöntemini bulunduran çalışmalardaki sonlu halkalar çeşitli cebirsel özelliklere sahiptir; örneğin, sonlu zincir halkaları (Cengellenmis, 2009a; Ding, vd., 2015; Qian, vd., 2006a; Qian, vd., 2006b; Qian, vd., 2005), Frobenious halkaları (Karadeniz, Yıldız, 2011; Liao, Tang, 2012), esas ideal halkaları, yerel halkalar (Aydın, Cengellenmis, Dertli, 2018; Dougherty, Salturk, submitted), yarı yerel (semilocal) halkalar (Liao, vd., 2012; Zhu, vd., 2011) gibi. Bu çalışmalardaki bazı halkalar tek değişkenli (Cengellenmis, 2009b; Udomkavanich, vd., 2009) iken bazıları birden fazla değişken (Dertli, Cengellenmis, 2016; Gao, 2015; Kai, vd., 2012; Yıldız, vd., 2011) yardımıyla tanımlanmıştır.

Bu bölümde, yeni bir sonlu halka ve sonlu halka sınıfı tanıtılmaktadır. Bu sonlu halkaların cebirsel yapısı araştırılmaktadır. Her bir sonlu halka ve sonlu halka sınıfı üzerinde yeni bir Gray dönüşüm tanımlanarak, devirli ve bazı sabit devirli kodların Gray görüntüleri elde edilmektedir.

4.2. $R_{(2^k)^4}$ Sonlu Halka Sınıfı Üzerinde Devirli ve $(1+u)-$ Sabit Devirli Kodların Gray Görüntüleri

4.2.1. $R_{(2^k)^4}$ Kümesinin Cebirsel Yapısı

k pozitif tamsayı olmak üzere, $\mathbb{F}_{2^k}[u,v]/\langle u^3, v^2-v, uv\rangle = \{a+bu+cu^2+dv : a,b,c,d \in \mathbb{F}_{2^k}\}$ bölüm halkası için $u^3=0, v^2=v$ ve $uv=vu$ koşulları göz önüne alındığında *Bölüm 3.2.*'dekine benzer şekilde $R_{(2^k)^4}$ kümesinin, adi toplama ve çarpma işlemleri ile karakteristiği 2 olan 2^{4k} elemanlı değişmeli bir halka olduğu görülür.

4.2.1.1. $R_{(2^k)^4}$ Halkasının Birimselleri

Bu alt bölümde, $R_{(2^k)^4}$ halkası üzerinde sabit devirli kodların elde edilmesi için birim elemanları araştırılmaktadır. Birimsel elemanların genel formu ve sayısını veren formüller aşağıdaki teoremlerle ifade edilmektedir.

4.2.1.1.1. Teorem:

$a, b, c, d \in \mathbb{F}_{2^k}$ olmak üzere, $\lambda = a + bu + cu^2 + dv$ elemanın $R_{(2^k)^4}$ halkasının bir birimsel elemanı olması için gerekli ve yeterli koşul $a \neq 0$ ve $a + d \not\equiv 0 \ (mod\ 2)$ olmasıdır.

Kanıt:

$\lambda = a + bu + cu^2 + dv$, $R_{(2^k)^4}$ halkasında bir birimsel olsun. Bu durumda, $\lambda.\lambda' = 1$ eşitliğini sağlayan bir $\lambda' \in R_{(2^k)^4}$ elemanı vardır. Bu eşitlik kullanılarak $mod\ 2$'ye göre aşağıdaki denklikler elde edilir:

$$aa' \equiv 1 \tag{1}$$

$$ab' + ba' \equiv 0 \tag{2}$$

$$ac' + bb' + ca' \equiv 0 \tag{3}$$

$$ad' + da' + dd' \equiv 0 \tag{4}$$

(1) denkleminden $a' = a^{-1}$ elde edilir. Dolayısıyla, $a \in \mathbb{F}_{2^k}$ bir birimsel eleman olduğundan $a \neq 0$. Bu durumda, $d = 0$ ise $a + d \not\equiv 0 \ (mod\ 2)$. $d \neq 0$ olduğu durumda ise, (4) denklemi kullanılarak $(a + d)d' = -da' \neq 0$ eşitliği ile $a + d \not\equiv 0$ bulunur.

İspatın tersi için, $a \neq 0$ ve $a + d \not\equiv 0 \ (mod\ 2)$ olsun. Bu durumda, $a^{-1}, (a + d)^{-1} \in \mathbb{F}_{2^k}^*$ elemanları vardır. $\lambda' = a^{-1} - b(a^{-1})^2u + (b^2(a^{-1})^3 - c(a^{-1})^2)u^2 + (-da^{-1}(a + d)^{-1})v$ elemanı için $\lambda.\lambda' = 1$ eşitliği sağlandığından, λ elemanı $R_{(2^k)^4}$ halkasının birimsel elemanıdır.

4.2.1.1.2. Sonuç:

$R_{(2^k)^4}$ halkasının birim elemanlarının sayısı $2^{2k}(2^k - 1)^2$ sayısına eşittir.

Kanıt:

$a + bu + cu^2 + dv$ birimsel eleman olsun. *4.2.1.1.1 Teorem*'i gereği $R_{(2^k)^4}$ halkasındaki bir birimsel elemanın $a \neq 0$ ve $a + d \not\equiv 0\ (mod\ 2)$ koşullarını sağlayan a sabit teriminin ve d katsayısının her biri için seçim sayısı $2^k - 1$ tanedir. b ve c katsayıları için bir kısıtlama olmadığından, bu elemanların seçim sayıları 2^k tanedir. O halde, $a + bu + cu^2 + dv$ birimsel elemanlarının sayısı $2^{2k}(2^k - 1)^2$ tanedir.

4.2.1.2. $R_{(2^k)^4}$ Halkasının İdealleri

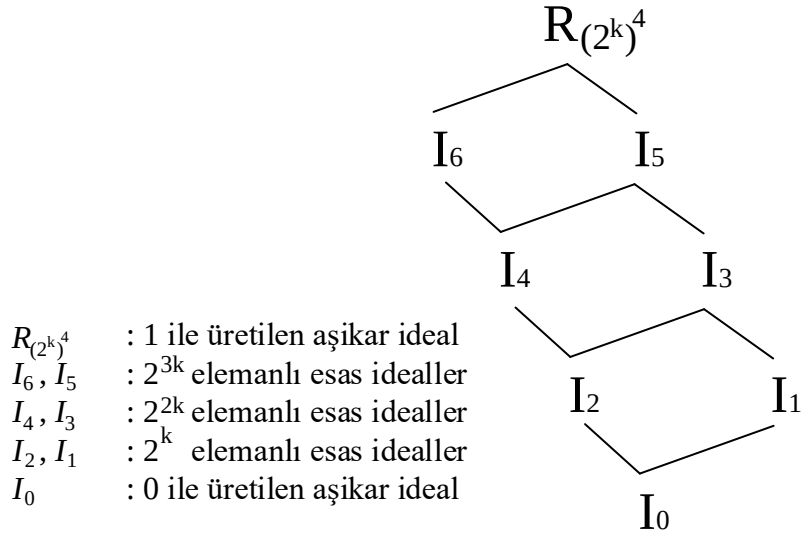
4.2.1.2.1. Önerme:

$R_{(2^k)^4}$ halkasının $a + bu + cu^2 + dv$ elemanı ile üretilen tüm ideallerinin tipleri ve sayıları aşağıdaki gibidir:

(i) 2^{3k} elemanlı iki farklı maksimal ideali vardır. 2^{3k} elemanlı ilk ideal tipinin üreteci, $a \neq 0$ ve $a + d \equiv 0\ (mod 2)$ koşullarını sağlar. Bu idealin üreteçlerinin sayısı $2^{2k}(2^k - 1)$ olur. 2^{3k} elemanlı ikinci ideal tipinin üreteci, $a = 0, b \neq 0$ ve $d \neq 0$ koşullarını sağlar. Bu idealin üreteçlerinin sayısı $2^k(2^k - 1)^2$ dir.

(ii) 2^{2k} elemanlı iki farklı ideali vardır. 2^{2k} elemanlı ilk ideal tipinin üreteci, $a = 0, b \neq 0$ ve $d = 0$ koşullarını sağlar. Bu idealin üreteçlerinin sayısı $2^k(2^k - 1)$ olur. 2^{2k} elemanlı ikinci ideal tipinin üreteci, $a = 0, b = 0, c \neq 0$ ve $d \neq 0$ koşullarını sağlar. Bu idealin üreteçlerinin sayısı $(2^k - 1)^2$ dir.

(iii) 2^k elemanlı iki farklı ideali vardır. Üreteçlerden biri, $a = b = d = 0$ ve $c \neq 0$ koşulları ile, diğeri $a = b = c = 0$ ve $d \neq 0$ koşulları ile yazılır. Bu iki tipin üreteçlerinin sayısı $2^k - 1$ dir.



Şekil 4.1 $R_{(2^k)^4}$ Halkasının İdealleri

4.2.1.2.2. Sonuç:

$R_{(2^k)^4}$ bir esas ideal halkasıdır.

Kanıt:

4.2.1.2.1 Önerme'deki tek eleman ile üretilen ideallerin üreteç tipleri göz önüne alınsın. $\lambda_1 = b_1u + c_1u^2$ ve $\lambda_2 = c_2u^2 + d_2v$ üreteçleri için $\langle \lambda_1, \lambda_2 \rangle$ iki elemanla üretilen ideali, $\langle bu + cu^2 + dv \rangle$ esas idealine eşittir. $\lambda_1 = c_1u^2$ ve $\lambda_2 = d_2v$ üreteçleri için $\langle \lambda_1, \lambda_2 \rangle$ iki elemanla üretilen ideali, tek elemanla üretilen $\langle cu^2 + dv \rangle$ idealine eşittir. Son olarak, $\lambda_1 = b_1u + c_1u^2$ ve $\lambda_2 = d_2v$ üreteç çifti kullanılarak elde edilen $\langle \lambda_1, \lambda_2 \rangle$ ideali yine $\langle cu^2 + dv \rangle$ esas idealine eşittir. O halde, $R_{(2^k)^4}$ halkasının tüm idealleri esas idealdir.

4.2.1.2.3. Not:

$R_{(2^k)^4}$ halkasının iki maksimal ideali olduğundan, $R_{(2^k)^4}$ halkası yarı yerel halkadır. $soc\left(R_{(2^k)^4}\right)$ kümesi $R_{(2^k)^4}$ halkasının 2^{2k} elemanlı ideali ve ayrıca $R_{(2^k)^4}$ halkasının minimal ideallerinin toplamı da 2^{2k} elemanlı idealidir. Dolayısıyla, $\left|R_{(2^k)^4} \Big/ soc\left(R_{(2^k)^4}\right)\right| = 2^{2k}$. O halde, $R_{(2^k)^4}$ halkası Frobenious halkasıdır.

4.2.1.2.4. Not:

4.2.1.1.1 Teorem gereği $1+u$ elemanı $R_{(2^k)^4}$ halka sınıfında her zaman birimsel elemandır. Bu bölümde λ birimsel elemanı olarak $1+u$ elemanı alınacaktır ve $(1+u)^4 = 1$ olduğu kullanılacaktır.

4.2.2. $4s-1$ Uzunluklu $(1+u)-$ Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki

Bu bölümde $R_{(2^k)^4}$ halkası üzerinde tanımlı devirli kodlar ile $(1+u)-$ sabit devirli kodlar arasındaki ilişkiyi veren izomorfizmanın varlığı gösterilmektedir.

4.2.2.1. Önerme:

s pozitif tamsayı ve $n = 4s-1$ olmak üzere, $R_{(2^k)^4}[x]/\langle x^n-1\rangle$ bölüm halkasından $R_{(2^k)^4}[x]/\langle x^n-(1+u)\rangle$ bölüm halkasına $\mu(\overline{f(x)}) = \overline{f((1+u)x)}$ biçiminde tanımlı μ dönüşümü bir halka izomorfizmasıdır.

Kanıt:

$f(x) \equiv g(x)\ (mod\ x^n-1)$ olsun. Bu durumda, $\overline{f(x)} - \overline{g(x)} = \overline{h(x)}.\overline{(x^n-1)}$ sağlayan en az bir $\overline{h(x)} \in R_{(2^k)^4}[x]/\langle x^n-1\rangle$ polinomu vardır. Eşitlikte, x yerine $(1+u)x$ yazılırsa, $\overline{f\big((1+u)x\big)} - \overline{g\big((1+u)x\big)} = \overline{h\big((1+u)x\big)}.\overline{((1+u)^n x^n-1)}$ eşitliği elde edilir. $n = 4s-1$ ve $(1+u)^4 = 1$ olduğundan, $(1+u)^n = (1+u)^{-1}$ bulunur. Bu gerçekler ve μ dönüşümünün tanımı kullanıldığında, $\mu(\overline{f(x)}) - \mu(\overline{g(x)}) = \overline{h((1+u)x)(1+u)^{-1}(x^n-(1+u))}$ eşitliği elde edilir. Bunun anlamı, $\mu(f(x)) \equiv \mu(g(x))\ (mod\ x^n-(1+u))$ olmasıdır. O halde, μ iyi tanımlıdır. Bu işlemler tersine de yapılabileceğinden, μ dönüşümü birebir dönüşümdür. μ dönüşümünün örten olduğu açıktır.

Kanıtı tamamlamak için, μ dönüşümünün homomorfizma olduğunu göstermek yeterlidir. Herhangi bir $\overline{f(x)}, \overline{g(x)} \in R_{(2^k)^4}[x]/\langle x^n-1\rangle$ için, μ dönüşümünün tanımı ve fonksiyonlarda toplamanın tanımı kullanılarak aşağıdaki eşitlik elde edilir:

$$\mu(\overline{f(x)+g(x)}) = \mu(\overline{(f+g)(x)}) = \overline{(f+g)((1+u)x)}$$
$$= \overline{f((1+u)x)} + \overline{g((1+u)x)} = \mu(\overline{f(x)}) + \mu(\overline{g(x)})$$

Benzer işlemler, çarpma işleminin korunduğunu da göstermek için yapılırsa, μ dönüşümünün bir halka homomorfizması olduğu görülür. O halde, μ bir izomorfizmadır.

4.2.2.2. Sonuç:

s pozitif tamsayı olmak üzere, $n = 4s - 1$ ise I kümesinin $R_{(2^k)^4}[x]/\langle x^n - 1\rangle$ bölüm halkasının bir ideali olması için gerekli ve yeterli koşul $\mu(I)$ kümesinin $R_{(2^k)^4}[x]/\langle x^n - (1+u)\rangle$ bölüm halkasının bir ideali olmasıdır.

Kanıt:

*3.2.2.2 Sonuç'*un kanıtına benzer şekilde elde edilir.

4.2.2.3. Sonuç:

s pozitif tamsayı olmak üzere, $n = 4s - 1$ ve C kümesi $R_{(2^k)^4}^n$ kümesinin bir alt kümesi olsun. $\bar{\mu}$ permütasyonu $R_{(2^k)^4}^n$ kümesi üzerinde aşağıdaki şekilde tanımlı olsun:

$$\bar{\mu}(c_0, c_1, \dots, c_{n-1}) = (c_0, (1+u)c_1, \dots, (1+u)^{n-1}c_{n-1})$$

Bu durumda, C kodunun devirli kod olması için gerekli ve yeterli koşul $\bar{\mu}(C)$ kodunun $(1+u) -$ sabit devirli kod olmasıdır.

Kanıt:

C, n uzunluklu bir devirli kod olsun. C'nin polinom gösterimi yine C olsun. O halde, C kümesi $R_{(2^k)^4}[x]/\langle x^n - 1\rangle$ bölüm halkasının bir idealidir. Bir önceki sonuçtan, $\mu(C)$ kümesi $R_{(2^k)^4}[x]/\langle x^n - (1+u)\rangle$ bölüm halkasının bir ideali olacaktır. Bu durumda, $\bar{\mu}(C)$ kümesi $R_{(2^k)^4}^n$ üzerinde $(1+u) -$ sabit devirli kod olacaktır.

4.2.3. $R_{(2^k)^4}$ Halkasında Tanımlı Gray Dönüşüm, Devirli ve Sabit Devirli Kodların Gray Görüntüleri

ϕ Gray dönüşümü aşağıdaki şekilde tanımlansın:

$\phi: R_{(2^k)^4} \to \mathbb{F}_{2^k}^{12n}$

$\phi(a + bu + cu^2 + dv) = (a, b, a + b, c, a + c, b + c, a + b + c, d, c + d, a + c + d, b + c + d, a + b + c + d)$

$0 \leq i \leq n - 1$ ve $a_i, b_i, c_i, d_i \in \mathbb{F}_{2^k}$ olmak üzere, her $z_i = a_i + b_i u + c_i u^2 + d_i v$ elemanı için yukarıdaki ϕ Gray dönüşümünün $R_{(2^k)^4}^n$ kümesine genişletilmiş hali aşağıdaki gibi olacaktır:

$\phi: R_{(2^k)^4}^n \to \mathbb{F}_{2^k}^{12n}$

$$\begin{aligned}(z_0, z_1, \dots, z_{n-1}) \mapsto \phi(z_0, z_1, \dots, z_{n-1}) \\ = (a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1}, a_0 + b_0, \dots, a_{n-1} \\ + b_{n-1}, c_0, \dots, c_{n-1}, a_0 + c_0, \dots, a_{n-1} + c_{n-1}, b_0 + c_0, \dots, b_{n-1} \\ + c_{n-1}, a_0 + b_0 + c_0, \dots, a_{n-1} + b_{n-1} + c_{n-1}, d_0, \dots, d_{n-1}, c_0 \\ + d_0, \dots, c_{n-1} + d_{n-1}, a_0 + c_0 + d_0, \dots, a_{n-1} + c_{n-1} + d_{n-1}, b_0 \\ + c_0 + d_0, \dots, b_{n-1} + c_{n-1} + d_{n-1}, a_0 + b_0 + c_0 + d_0, \dots, a_{n-1} \\ + b_{n-1} + c_{n-1} + d_{n-1})\end{aligned}$$

4.2.3.1. Önerme:

$(R_{(2^k)^4}^n, d_G)$ kümesinden $(\mathbb{F}_{2^k}^{12n}, d_H)$ kümesine tanımlı ϕ Gray dönüşümü bir lineer ve uzaklık koruyan dönüşümdür.

Kanıt:

3.2.3.2 Önerme'nin kanıtına benzer şekilde elde edilir.

4.2.3.2. Teorem:

C kodu $R_{(2^k)^4}$ halkası üzerinde bir (n, M, d_G) lineer kod ise $d_G = d_H$ olmak üzere, $\phi(C)$ kodu $\mathbb{F}_{2^k}$ sonlu cismi üzerinde bir $(12n, M, d_H)$ lineer koddur.

4.2.3.3. Önerme:

σ ve ν sırasıyla, $R_{(2^k)^4}^n$ kümesi üzerinde devirli ve $(1 + u) -$ sabit devirli ötelemeler olsun. $\{0,1, \dots, 12n - 1\}$ kümesi üzerindeki π permütasyonu $\pi =$

$(n, 2n)(3n, 6n)(6n, 4n)(4n, 5n)(8n, 11n)(11n, 9n)(9n, 10n)$ olmak üzere, $\phi \circ \nu = \pi \circ \sigma^{\otimes 12} \circ \phi$ biçimindedir.

Kanıt:

3.2.3.4 Önerme'nin kanıtına benzer şekilde yapılır.

4.2.3.4. Teorem:

$R_{(2^k)^4}$ halkası üzerinde, n uzunluklu $(1+u)-$ sabit devirli kodun Gray görüntüsü, $\mathbb{F}_{2^k}$ sonlu cismi üzerinde $12n$ uzunluklu ve indeksi 12 olan bir quasicyclic koda denktir.

Kanıt:

$C, R_{(2^k)^4}$ halkası üzerinde n uzunluklu $(1+u)-$ sabit devirli kod olsun. Bu durumda, $\nu(C) = C$. Bu eşitliğin Gray görüntüsü alınırsa, $\phi(\nu(C)) = \phi(C)$ bulunur. Son eşitlik ve *4.2.3.3 Önerme* kullanılırsa, $\phi(C) = \pi(\sigma^{\otimes 12}(\phi(C)))$ olduğu görülür. O halde $\phi(C)$ kodu $\mathbb{F}_{2^k}$ sonlu cismi üzerinde $12n$ uzunluklu indeksi 12 olan bir quasicyclic koda denktir.

4.2.3.5. Önerme:

s pozitif tamsayı olmak üzere, $n = 4s - 1$ *ve* $\bar{\mu}$ permütasyonu *4.2.2.3 Sonuç*'taki gibi olsun. Bu durumda, $\phi\bar{\mu} = \gamma'\phi$ eşitliğini sağlayan bir $\gamma'(z_0, z_1, \dots, z_{4n-1}) = (z_{\gamma(0)}, z_{\gamma(1)}, \dots, z_{\gamma(4n-1)})$ permütasyonu vardır. Burada, $\{0,1, \dots, 12(4s-1)-1\}$ kümesi üzerindeki γ permütasyonu $j = 1,2, \dots, 2s-1$, $t = 1,2, \dots, s$ ve $l = 1,2, \dots, s-1$ için $n_j = 2j-1$, $n_t = 4t-3$, $n_l = 4l-1$ ve $m_t = 4t-2$ olmak üzere aşağıdaki $\xi_1, \xi_2, \xi_3, \xi_4$ permütasyonlarının bileşkesi $\gamma = \xi_1\xi_2\xi_3\xi_4$ biçimindedir:

$$\xi_1 = (n+1, 2n+1)(n+3, 2n+3) \dots (n+n_j, 2n+n_j)$$

$$\begin{aligned}\xi_2 = (&3n+1, 6n+1, 4n+1, 5n+1)(3n+5, 6n+5, 4n+5, 5n+5) \dots (3n \\ &+ n_t, 6n+n_t, 4n+n_t, 5n+n_t)(8n+1, 11n+1, 9n+1, 10n \\ &+ 1)(8n+5, 11n+5, 9n+5, 10n \\ &+ 5) \dots (8n+n_t, 11n+n_t, 9n+n_t, 10n+n_t)\end{aligned}$$

$$\xi_3 = (3n+3,5n+3,4n+3,6n+3)(3n+7,5n+7,4n+7,6n+7)\dots(3n+n_l,5n+n_l,4n+n_l,6n+n_l)(8n+3,10n+3,9n+3,11n+3)(8n+7,10n+7,9n+7,11n+7)\dots(8n+n_l,10n+n_l,9n+n_l,11n+n_l)$$

$$\xi_4 = (3n+2,4n+2)(3n+6,4n+6)\dots(3n+m_t,4n+m_t)(5n+2,6n+2)(5n+6,6n+6)\dots(5n+m_t,6n+m_t)(8n+2,9n+2)(8n+6,9n+6)\dots(8n+m_t,9n+m_t)(10n+2,11n+2)(10n+6,11n+6)\dots(10n+m_t,11n+m_t)$$

Kanıt:

$0 \le i \le 4s-2$ için $z_i = a_i + b_i u + c_i u^2 + d_i v$ olmak üzere, $a_i, b_i, c_i, d_i \in \mathbb{F}_{2^k}$ olsun. Herhangi bir $z = (z_0, z_1, \dots, z_{4s-2}) \in R^n_{(2^k)^4}$ elemanı için, $\bar{\mu}(z) = \bar{\mu}(z_0, z_1, \dots, z_{4s-2}) = (z_0, (1+u)z_1, (1+u)^2 z_2, \dots, (1+u)^{4s-2} z_{4s-2})$ ifadesinde $(1+u)^{-1} \equiv 1-u+u^2$ ve $(1+u)^4 \equiv 1\ (mod\ 2)$ denklikleri kullanılarak, γ' permütasyonu yukarıda tanımlandığı gibi olmak üzere $\bar{\mu}(z)$ elemanının Gray görüntüsü $\gamma'(\phi(z))$ elemanına eşit olacaktır.

4.2.3.6. Teorem:

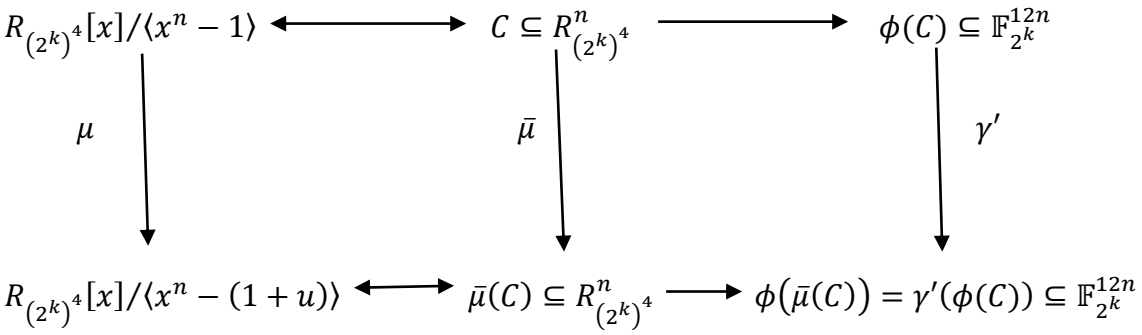
$n = 4s-1$ ve Δ, $R_{(2^k)^4}$ halkası üzerinde devirli bir kodun Gray görüntüsü ise $\gamma'(\Delta)$ kodu $\mathbb{F}_{2^k}$ sonlu cismi üzerinde $12n$ uzunluklu ve indeksi 12 olan bir quasicyclic koda denktir.

Kanıt:

C'nin $R_{(2^k)^4}$ halkası üzerinde Gray görüntüsü $\Delta = \phi(C)$ olsun. *4.2.3.5 Önerme*'den $\phi(\bar{\mu}(C)) = \gamma'(\phi(C)) = \gamma'(\Delta)$ eşitliği elde edilir. *4.2.2.3 Sonuç* göz önüne alınarak $\bar{\mu}(C)$'nin R halkası üzerinde bir D, $(1+u)-$ sabit devirli koda eşit olduğu görülür. O halde, $\phi(\bar{\mu}(C)) = \phi(D)$ olacaktır. *4.2.3.4 Teorem* gereği $\phi(D)$, $\mathbb{F}_{2^k}$ cismi üzerinde $12n$ uzunluklu ve indeksi 12 olan bir quasicyclic koda denktir.

4.2.4. $R_{(2^k)^4}$ Halkası Üzerinde $4s-1$ Uzunluklu Devirli Kodlar ile $(1+u)-$ Sabit Devirli Kodlar Arasındaki İlişki

Şekil 4.1'de görüldüğü gibi $R_{(2^k)^4}$ halkası üzerindeki devirli kodlar ve $(1+u)-$ sabit devirli kodlar arasındaki ilişkiyi bulabilmek için, öncelikle $R_{(2^k)^4}[x]/\langle x^n-1\rangle$ ile $R_{(2^k)^4}[x]/\langle x^n-(1+u)\rangle$ polinom halkaları arasındaki μ izomorfizması elde edilmiştir. μ ile tanımlanan dönüşüm, s pozitif tamsayı olmak üzere $n=4s-1$ durumunda izomorfizmadır. Bu durumda, μ dönüşümü yardımıyla elde edilen tüm sonuçlar $n=4s-1$ uzunluk kısıtlaması ile verilmiştir. $R_{(2^k)^4}[x]/\langle x^n-1\rangle$ ve $R_{(2^k)^4}[x]/\langle x^n-(1+u)\rangle$ halkalarının ideallerinin polinom gösterimlerinden, $R^n_{(2^k)^4}$ halkasındaki kodların sıralı n'li ile gösterimlerine geçilip, $R^n_{(2^k)^4}$ kümesi üzerinde μ izomorfizması yardımıyla bir $\bar{\mu}$ permütasyonu elde edilmiştir. $R^n_{(2^k)^4}$ kümesinden $\mathbb{F}_{2^k}^{12n}$ vektör uzayına tanımlı Gray dönüşüm yardımıyla, devirli ve $(1+u)-$ sabit devirli kodların görüntüleri elde edilmiştir. *4.2.3.3 Önerme*'deki $\phi\circ\nu=\pi\circ\sigma^{\otimes 12}\circ\phi$ eşitliği ile *4.2.3.5 Önerme*'deki $\phi\bar{\mu}=\gamma'\phi$ eşitliği diyagramın komütatifliğini tamamladığından, devirli ve $(1+u)-$ sabit devirli kodların Gray görüntülerinin $\mathbb{F}_{2^k}$ sonlu cismi üzerinde $12n$ uzunluklu ve indeksi 12 olan bir quasicyclic kodlara denk oldukları bulunmuştur.



Şekil 4.2 $R_{(2^k)^4}$ Halkası Üzerindeki $4s-1$ Uzunluklu Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı

4.2.4.1. Sonuç:

s pozitif bir tamsayı olmak üzere, $R_{(2^k)^4}$ halkası üzerinde $4s-1$ uzunluklu devirli bir kodun Gray görüntüsü, $\mathbb{F}_{2^k}$ sonlu cismi üzerinde $12(4s-1)$ uzunluklu ve indeksi 12 olan bir quasicyclic koda denktir.

4.3. R_{2^5} Sonlu Halkası Üzerinde Devirli ve $(1+u^2+u^3)-$ Sabit Devirli Kodların Gray Görüntüleri

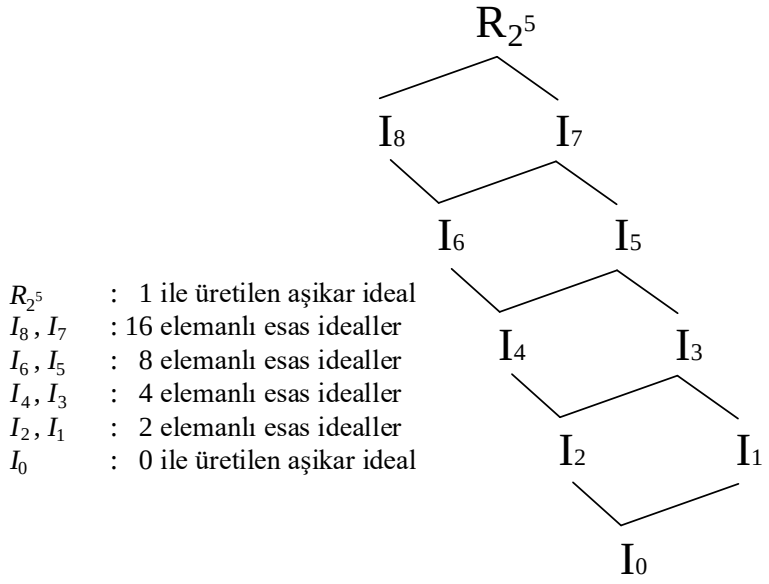
4.3.1. R_{2^5} Kümesinin Cebirsel Yapısı

R_{2^5} kümesi, $u^4=0, v^2=v$ ve $uv=vu=0$ koşulları ile $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2+v\mathbb{F}_2$ halkası olsun. R_{2^5} kümesinin *Bölüm 3.2.*'dekine benzer şekilde, $\mathbb{F}_2[u,v]/\langle u^4, v^2-v, uv\rangle$ bölüm halkasına izomorf olduğu görülür.

$R_{2^5}=\{0, u^2+v+1, u^3+v, u^3, u^2+u, u^3+u, u^3+u^2+v+1, u^2+u+1, u^3+u^2+u+1, u^3, u^2+u+v, u^3+u^2, u^3+u^2+u+v+1, u^3+u^2+u+v, 1, u^3+v+1, u+v+1, u^3+u+v+1, u^3+u+1, v+1, u^3+u^2+1, v, u, u+1, u^2+1, u^3+u+v, u^3+1, u^3+u^2+v, u^2+u+v+1, u^3+u^2+u, u+v, u^2+v\}$ halkası karakteristiği 2 olan değişmeli bir halkadır.

Halkanın birimsel elemanları, $1, 1+u, 1+u^2, 1+u+u^2, 1+u^3, 1+u+u^3, 1+u+u^2+u^3, 1+u^2+u^3$ şeklindedir.

Halkanın idealleri: $\langle 0\rangle, \langle v\rangle, \langle u^3\rangle, \langle u^2\rangle, \langle u\rangle, \langle u^3+v\rangle, \langle u^2+v\rangle, \langle u+v\rangle, \langle 1+v\rangle, \langle 1\rangle$. Maksimal idealler $\langle u+v\rangle, \langle 1+v\rangle$ olduğundan, R_{2^5} halkası yarı yerel halkadır. R_{2^5} halkasının tüm idealleri esas ideal olduğundan, R_{2^5} bir esas ideal halkasıdır. *Şekil 4.3*'te bu halkanın idealler kafesi gösterilmektedir.



Şekil 4.3 R_{2^5} Halkasının İdealleri

Bu bölümde, sabit devirli kodların elde edilmesinde kullanılan λ birimsel elemanı $1 + u^2 + u^3$ olarak seçilecektir. Bu birimsel elemanın çift kuvvetleri 1 olduğundan , R_{2^5} sonlu halkası üzerinde elde edilecek sabit devirli kodların uzunluklarının tek uzunlukta çalışılabileceği sonucunu ortaya çıkacaktır.

4.3.2. R_{2^5} Halkası Üzerinde Tek Uzunluklu $\lambda -$ Sabit Devirli Kodlar

$\lambda = 1 + u^2 + u^3$ birimsel elemanı göz önüne alınsın. n tek tamsayı iken $\lambda^n = \lambda$ ve n çift tamsayı iken $\lambda^n = 1$'dir.

4.3.2.1. Önerme:

$\lambda = 1 + u^2 + u^3$ ve n tek tamsayı olmak üzere, $R_{2^5}[x]/\langle x^n - 1\rangle$ bölüm halkasından $R_{2^5}[x]/\langle x^n - \lambda\rangle$ bölüm halkasına $\mu(\overline{f(x)}) = \overline{f(\lambda x)}$ biçiminde tanımlanan μ dönüşümü bir halka izomorfizmasıdır.

Kanıt:

3.2.2.1 Önerme'deki kanıta benzer olarak gösterilir.

4.3.2.2. Sonuç:

n pozitif tek tamsayı ve $\lambda = 1 + u^2 + u^3$ ise I kümesinin $R_{2^5}[x]/\langle x^n - 1\rangle$ bölüm halkasının bir ideali olması için gerekli ve yeterli koşul $\mu(I)$ kümesinin $R_{2^5}[x]/\langle x^n - \lambda\rangle$ bölüm halkasının bir ideali olmasıdır.

Kanıt:

3.2.2.2 Sonuç ile benzer şekilde gösterilir.

4.3.2.3. Sonuç:

n tek tamsayı, C kümesi $R_{2^5}^n$ kümesinin bir alt kümesi ve $\lambda = 1 + u^2 + u^3$ olsun. $\bar{\mu}$ permütasyonu $R_{2^5}^n$ kümesi üzerinde aşağıdaki şekilde tanımlı olsun:

$$\bar{\mu}(c_0, c_1, \dots, c_{n-1}) = (c_0, \lambda c_1, \lambda^2 c_2 \dots, \lambda^{n-1} c_{n-1})$$

Bu durumda, C kodunun devirli kod olması için gerekli ve yeterli koşul $\bar{\mu}(C)$ kodunun $\lambda -$ sabit devirli kod olmasıdır.

Kanıt:

3.2.2.3 Sonuç ile benzer şekilde gösterilir.

4.3.3. R_{2^5} Halkası Üzerinde Tanımlı Gray Dönüşüm, $\lambda -$ Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri

ϕ Gray dönüşümü;

$\phi: R_{2^5} \to \mathbb{F}_2^6$

$$a + bu + cu^2 + du^3 + ev \to \phi(a + bu + cu^2 + du^3 + ev) = (a + b + c + d + e, a + c + d + e, a, e, a + b + d, d)$$

biçiminde tanımlansın. $0 \le i \le n - 1$ ve $a_i, b_i, c_i, d_i, e_i \in \mathbb{F}_2$ olmak üzere, her $z_i = a_i + b_i u + c_i u^2 + d_i u^3 + e_i v$ elemanı için yukarıdaki ϕ Gray dönüşümün $R_{2^5}^n$ kümesine genişletilmiş hali aşağıdaki gibi olacaktır:

$\phi: R_{2^5}^n \to \mathbb{F}_2^{6n}$

$$(z_0, z_1, \dots, z_{n-1}) \mapsto \phi(z_0, z_1, \dots, z_{n-1})$$
$$= (a_0 + b_0 + c_0 + d_0 + e_0, \dots, a_{n-1} + b_{n-1} + c_{n-1} + d_{n-1}$$
$$+ e_{n-1}, a_0 + c_0 + d_0 + e_0, \dots, a_{n-1} + c_{n-1} + d_{n-1}$$
$$+ e_{n-1}, a_0, \dots, a_{n-1}, e_0, \dots, e_{n-1}, a_0 + b_0 + d_0, \dots, a_{n-1} + b_{n-1}$$
$$+ d_{n-1}, d_0, \dots, d_{n-1})$$

R_{2^5} kümesindeki bir x elemanının Gray ağırlığı, x elemanının Gray görüntüsünün Hamming ağırlığı ile bulunur ve aşağıdaki şekilde yazılır:

$$w_G(x) = \begin{cases} 0 & x = 0 \\ 1 & x = u^2 + v \\ 2 & x = \begin{matrix} u^2, u^2 + u, u^3 + u, u^2 + u + 1, u^3 + u^2, \\ u^2 + 1, u^3 + 1, u^3 + u^2 + u, u + 1, u \end{matrix} \\ 3 & x = \begin{matrix} u^3 + v, u^3 + u^2 + v + 1, u^2 + u + v, u^3 + u^2 + u + v, u + v, \\ u + v + 1, v + 1, v, u^3 + u + v, u^2 + u + v + 1 \end{matrix} \\ 4 & x = u^3 + u^2 + u + 1, u^3, 1, u^3 + u + 1, u^3 + u^2 + 1 \\ 5 & x = \begin{matrix} u^2 + v + 1, u^3 + u^2 + u + v + 1, \\ u^3 + v + 1, u^3 + u + v + 1, u^3 + u^2 + v \end{matrix} \end{cases}$$

C, R_{2^5} halkası üzerinde n uzunluklu lineer bir kod olsun. Herhangi bir $c = (c_0, c_1, \dots, c_{n-1})$ kod sözcüğü için c elemanının Gray ağırlığı, $w_G(C) = \sum_{i=0}^{n-1} w_G(c_i)$ biçiminde tanımlıdır.

Herhangi bir $c' \in C$ ve $c \neq c'$ için $d_G(c, c') = w_G(c - c')$ olmak üzere C kümesinin minimum Gray uzaklığı $d_G(C) = min\{d_G(c, c') : c, c' \in C, c \neq c'\}$ şeklinde tanımlanır.

4.3.3.1. Önerme:

$(R_{2^5}^n, d_G)$ kümesinden $(\mathbb{F}_2^{6n}, d_H)$ kümesine tanımlı ϕ Gray dönüşümü bir lineer ve uzaklık koruyan dönüşümdür.

Kanıt:

3.2.3.2 Önerme'deki şekilde kanıtlanır.

4.3.3.2. Teorem:

C kodu R_{2^5} halkası üzerinde bir (n, M, d_G) lineer kod ise $d_G = d_H$ olmak üzere, $\phi(C)$ kodu bir ikili $(6n, M, d_H)$ lineer koddur.

4.3.3.3. Önerme:

$\lambda = 1 + u^2 + u^3$ olmak üzere σ ve ν sırasıyla, $R_{2^5}^n$ halkası üzerinde devirli ve $\lambda -$ sabit devirli öteleme olsun. $\{0,1, \dots, 6n-1\}$ kümesi üzerindeki π permütasyonu $\pi = (0, n)(4n, 5n)$ biçiminde olmak üzere, $\phi \circ \nu = \pi \circ \sigma^{\otimes 6} \circ \phi$ eşitliği sağlanır.

Kanıt:

3.2.3.4 Önerme'deki ispat tekniği kullanılarak sonuç elde edilir.

4.3.3.4. Teorem:

$\lambda = 1 + u^2 + u^3$ olsun. R_{2^5} halkası üzerinde n uzunluklu $\lambda -$ sabit devirli kodun Gray görüntüsü, $6n$ uzunluklu ve indeksi 6 olan bir ikili quasicyclic koda denktir.

Kanıt:

3.2.3.5 Teorem'in ispatına benzer şekilde yapılır.

4.3.3.5. Önerme:

n pozitif tek tamsayı ve $\bar{\mu}$ permütasyonu *4.3.2.3 Sonuç*'taki gibi olsun. Bu durumda, $\{0,1, \dots, 6n-1\}$ kümesi üzerindeki γ permütasyonu, $\xi_1 = (1, n+1)(3, n+3) \dots (n-2, 2n-2)$ ve $\xi_2 = (4n+1, 5n+1)(4n+3, 5n+3) \dots (4n+(n-2), 5n+(n-2))$ permütasyonlarının bileşkesi $\gamma = \xi_1 \xi_2$ biçiminde tanımlı olmak üzere, $\phi\bar{\mu} = \gamma'\phi$ eşitliğini sağlayan bir $\gamma'(z_0, z_1, \dots, z_{4n-1}) = (z_{\gamma(0)}, z_{\gamma(1)}, \dots, z_{\gamma(6n-1)})$ permütasyonu vardır.

Kanıt:

3.2.3.6 Önerme'deki ispat tekniği kullanılarak istenilen sonuç elde edilir.

4.3.3.6. Teorem:

n tek tamsayı ve Δ kodu, R_{2^5} halkası üzerinde bir devirli kodun Gray görüntüsü ise $\gamma'(\Delta)$ kodu $6n$ uzunluklu ve indeksi 6 olan bir ikili quasicyclic koda denktir.

Kanıt:

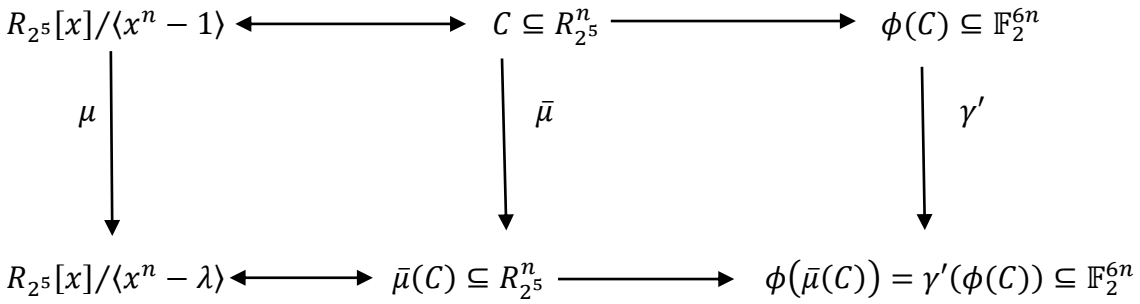
3.2.3.7 Teorem'in ispatına benzer şekilde yapılır.

4.3.3.7. Sonuç:

R_{2^5} halkası üzerinde tek uzunluklu devirli bir kodun Gray görüntüsü, $6n$ uzunluklu ve indeksi 6 olan bir ikili quasicyclic koda denktir.

4.3.4. R_{2^5} Halkası Üzerinde Tanımlı Tek Uzunluklu Devirli Kodlar ile λ − Sabit devirli Kodlar Arasındaki İlişki

Bölüm 3.2, *Bölüm 3.3* ve *Bölüm 4.2*'de bulunan sonuçlardakilere benzer olarak, *4.3.3.3 Önerme*'deki $\phi \circ \nu = \pi \circ \sigma^{\otimes 6} \circ \phi$ eşitliği ile *4.3.3.5 Önerme*'deki $\phi\bar{\mu} = \gamma'\phi$ eşitliği kullanılarak *Şekil 4.4*'deki diyagramın komütatifliği elde edilmiştir.



Şekil 4.4 R_{2^5} Halkası Üzerindeki Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Komütatif Diyagramı

BÖLÜM 5

$\mathbb{F}_{2^m}$ SONLU CİSMİ ÜZERİNE MDS ÖZELLİKLİ İNVOLUTİF MATRİSLER

5.1. Giriş

MDS kodlardan elde edilen Maksimum Uzaklık Ayrılabilir (Maksimum Distance Seperable – MDS) matrisleri, C. Shannon tarafından sunulan iki önemli kriptografik özellikten birisi olan maksimum yayılımı (diffusion) sağladıkları için, blok şifreler ve Hash fonksiyonlar gibi kriptografik yapıların tasarımında doğrusal dönüşüm katmanı veya bu katmanın ana bileşeni olarak kullanılmaktadırlar (Shannon, 1949). MDS matrisler, kriptografik yapıların çığ karakteristiklerini geliştirir. Bu matrisler yerdeğiştirme katmanı (substitution layer) veya bir doğrusal olmayan katmanın kullanımıyla birlikte diferansiyel (Bilham, Shamir, 1990) ve doğrusal kriptanalize (Matsui, 1994) karşı güvenlik sağlamaya yardımcı olur. Aynı modül tarafından uygulanacak bir blok şifresi üreten involutif yayılım katmanları (veya involutif MDS matrisleri), şifreleme ve şifre çözme işlemlerinde aynı uygulama maliyetini sağladıkları için blok şifreleme tasarımında avantajlara sahiptir. Bu nedenle, düşük maliyetli uygulama özelliklerine sahip involutif MDS matrislerin tasarımı (lightweight) blok şifrelerin tasarımında ilginç ve açık bir araştırma alanıdır.

Literatürde MDS matrisler; dairesel (circulant) matrisler, Hadamard matrisler, Cauchy matrisler (Youssef, Mister, Tavares, 1997), Vandermonde matrisler (Lacan, vd., 2004; Sajadieh, vd., 2012), eş (companion) matrisler (Gupta, vd., 2013; Guo, Peyrin, Poschmann, 2011) ve Toeplitz matrisler (Sarkar, Sim, 2016; Sarkar, Syed, 2016) gibi bazı

özel matris tiplerinden elde edilmektedir. Son zamanlarda, $GL\,(4;\,\mathbb{F}_2)$ ve $GL\,(8;\,\mathbb{F}_2)$ uzayları üzerinde dairesel özellikli involutif MDS matrisler önerilmiştir (Li, vd., 2016) ve dairesel matrislerin genelleştirilmesi (devirli matrisler olarak adlandırılan yeni bir form) (Liu, vd., 2016) çalışmasında verilmiştir. $\mathbb{F}_{2^m}$ üzerine involutif MDS matrislerinin tasarımı için yapılan çalışmalar, temel olarak involutif matrisleri kolayca oluşturmayı sağlayan Hadamard matrisine dayanmaktadır. (Pehlivanoğlu, vd., 2018) çalışmasında, yeni tip $k \times k$ ($k = 2^t$) MDS (veya involutif MDS) matrislerini etkin bir şekilde üreten ve Genelleştirilmiş Hadamard (GHadamard) matrisi olarak adlandırılan yeni bir matris tipi önerilmiştir. Bu fikir, $2^s \neq k$ biçiminde olmak üzere, $k \times k$ MDS (veya involutif MDS) matrislerine de uygulanabilir. Literatürde verilen MDS matrislerinin tasarım yöntemleri, esas olarak Vandermonde matrisleri ve Cauchy matrislerine dayalı yöntemler (doğrudan elde etme yöntemi) haricinde arama tabanlıdır. Diğer taraftan GHadamard matris tipi, MDS (veya involutif MDS) matrislerinin elde edilmesinde doğrudan elde etme ve arama tabanlı teknikleri birleştirdiği için melez bir yöntemdir.

Singleton Sınırı, $\mathbb{F}_q = GF(q)$ sonlu cismi üzerinde (n, M, d) parametreli bir kodun eleman sayısı olan M'nin alacağı en büyük değer $A_q(n, d)$ olmak üzere $A_q(n, d) \leq q^n - d + 1$ eşitsizliğinin sağlanmasıdır. Bir $\mathbb{F}_q$ cismi üzerinde $[n, k, d]$ lineer kodunun eleman sayısı q^k olduğundan, *2.2.3.2 Teorem*'deki Singleton sınırı kullanılarak $k \leq n - d + 1$ eşitsizliği elde edilir. Bu eşitsizliğin eşitlik durumunu sağlayan kodlara *MDS kod* denir. Bu kodlara ait üreteç matrisin standart formu $[\,I \mid A\,]$ olmak üzere, A matrisine *MDS matris* denir.

Tezin bu bölümünde, maksimum hata düzelten kodlar olan MDS kodlardan elde edilen MDS matrislerin kriptolojideki uygulama alanından faydalanılarak, elemanları $\mathbb{F}_{2^m}$ genişletilmiş cisminden alınan 2×2 ve 3×3 boyutlarındaki tüm involutif MDS matrislerin elde edilmesi için yeni bir matris formu geliştirilmektedir. Geliştirilen matris formu yardımıyla elemanları $\mathbb{F}_{2^m}$ sonlu cisminde olan 3×3 boyutunda tüm involutif ve MDS matris sayısını veren formül elde edilmektetir. Ayrıca elde edilen form kullanılarak, katsayıları $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ sonlu cisimlerinden alınan 3×3 boyutunda en hafif (leightweight) MDS ve involutif matrisler Magma (Bosma, Cannon, Playoust, 1997) kullanılarak üretilmektedir.

5.2. Bileşenleri $\mathbb{F}_{2^m}$ Sonlu Cisminden Alınan 2×2 Boyutlu MDS İnvolutif Matrisler

5.2.1. Teorem:

$M_{2\times2}(GF(2^m))$, bileşenleri $GF(2^m)$ cisminden alınan 2×2 boyutlu matris uzayı ve $a_{11} \neq 0$ olmak üzere, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in M_{2\times2}(GF(2^m))$ matrisi involutif ise $a_{11} = a_{22}$, ve $a_{12} = (1 + a_{11})b_0$, $a_{21} = (1 + a_{11}){b_0}^{-1}$ olacak şekilde bir $b_0 \in GF(2^m)^*$ elemanı vardır. Bu durumda, A matrisi aşağıdaki gibidir.

$$A = \begin{bmatrix} a_{11} & (1 + a_{11})b_0 \\ (1 + a_{11}){b_0}^{-1} & a_{11} \end{bmatrix}$$

Ayrıca, $GF(2^m)$ cisminde 2×2'lik involutif matris sayısı $(2^m - 2).(2^m - 1)$ adettir.

Kanıt:

$a_{11} \neq 0$ olmak üzere, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ matrisi involutif olsun.

$A^2 = I$ olacağından aşağıdaki denklemler sağlanır:

$${a_{11}}^2 + a_{12}a_{21} = 1 \quad (1)$$

$$a_{11}a_{12} + a_{12}a_{22} = 0 \quad (2)$$

$$a_{21}a_{11} + a_{22}a_{21} = 0 \quad (3)$$

$$a_{21}a_{12} + {a_{22}}^2 = 1 \quad (4)$$

(1) ve (4) denklemleri taraf tarafa toplandığında ${a_{11}}^2 = {a_{22}}^2$ elde edilir. Bu durumda, $a_{11} = a_{22}$ olur. Ayrıca, (1) denkleminden elde edilen $a_{12}a_{21} = 1 - {a_{11}}^2 = (1 + a_{11})^2$ eşitliğinden genelliği bozmaksızın en az bir $b_0 \in GF(2^m)^*$ elemanı için $a_{12} = (1 + a_{11})b_0$ ve $a_{21} = (1 + a_{11}){b_0}^{-1}$elde edilir.

5.2.2. Sonuç:

$a_{11} = 1$ olması durumunda a_{12} ve a_{21} değerleri $(1 + a_{11})$ çarpanından dolayı 0'a eşittir. Bu durumda elde edilen matris, b_0 elemanının seçilişinden bağımsız olarak birim matristir.

Birim matris dışındaki involutif matrislerin sayısı için $a_{11} \neq 0$ ve $a_{11} \neq 1$ olacağından a_{11} elemanının seçim sayısı $(2^m - 2)$'dir. a_{11} elemanın $(2^m - 2)$ seçimine karşılık $2^m - 1$ adet b_0 elemanı vardır. a_{12} ve a_{21} değerleri a_{11}ve b_0 elemanların seçimine bağlı olduğundan bu koşulları sağlayan involutif matris sayısı $(2^m - 2).(2^m - 1)$ tanedir.

Buradaki involutif matris formunun ürettiği matrisler MDS matristir.

5.3. Bileşenleri $\mathbb{F}_{2^m}$ Sonlu Cisminden Alınan Tüm 3×3 İnvolutif MDS Matrisleri Üreten Yeni Bir Matris Formu

Literatürde etkili uygulama özelliklerine sahip $2^t \times 2^t$ boyutunda MDS matrisler ile ilgili çeşitli çalışmalar bulunmaktadır. Diğer boyutlar için (involutif) MDS matrislerin elde edilmesine yönelik derinlemesine çalışmalar bulunmamaktadır. (Liu, vd., 2016) çalışmasında, elemenları $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ sonlu cisimlerinden alınan 3×3 boyutunda en hafif (lightweight) involutif MDS matrisler verilmiştir. Daha büyük boyutlu MDS matrisler için bu özellikler kullanılabileceğinden, 3×3 boyutunda bir matrisin involutif MDS olma gerekliliklerinin belirlenmesi önemli bir problemdir. 3×3 MDS (veya involutif MDS) matrisleri, (hafif) blok şifrelemelerin ve ayrıca sıra dışı blok ve anahtar boyutlarına sahip karma fonksiyonların tasarımında kullanılabilir. Örneğin, (Barreto, 2007) çalışmasında Curupira adlı kısıtlı platformlar için yinelenen bir blok şifresi önerilmiştir. Curupira blok şifresinde, 96, 144 veya 192 bit anahtarlarla 96 bit düz metin blokları kullanılır. Düz metin, alt anahtarlar ve ayrıca şifreli metinler, $3 \times N$ boyutlu bir bayt matrisinde oluşturulur ve burada N, $24-$ bitlik kelimelerin sayısıdır. Curupira'nın yayılım tabakası, elemanları $\mathbb{F}_{2^8}$ sonlu cisminden alınan bir 3×3 MDS matrisidir. Çalışmanın bu bölümündeki katkılar aşağıdaki gibidir:

- Herhangi bir ikili cisim genişlemesi üzerinde 3×3 boyutunda involutif MDS matrislerinin elde edilmesi için yeni bir yol tanımlanmaktadır.
- Elemanları $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ sonlu cisimlerinden alınan 3×3 boyutunda involutif MDS matrislerinin sayısı hesaplanmaktadır.
- 3×3 boyutunda involutif MDS matrislerdeki maksimum 1 sayısını sağlayan ve (Junod, Vaudenay, 2005) çalışmasında verilen 1'lerin üst sınırı 6'dan 3'e geliştirilmektedir.
- (Liu, vd., 2016)'de verilen sonuçlar önemli ölçüde geliştirilmektedir ve $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ sonlu cisimleri üzerine en hafif 3×3 boyutunda involutif MDS matrisler elde edilmektedir.

5.3.1. Yeni 3×3 İnvolutif MDS Matris Formu

Bu bölümde, bileşenleri $\mathbb{F}_{2^m}$ sonlu cisminden alınan tüm 3×3 involutif ve MDS matrisleri üreten yeni bir matris formu tanımlanmaktatır. Ayrıca, $\mathbb{F}_{2^m}$ sonlu cismi üzerinde tüm 3×3 involutif ve MDS matrislerin sayısının $(2^m - 1)^2(2^m - 2)(2^m - 4)$ olduğu gösterilmektedir. Önerilen matris formu kullanılarak $\mathbb{F}_{2^8}$ sonlu cismi üzerine, literatürde de verilen iki 3×3 involutif ve MDS matris örneği sunulmaktadır. *5.3.2.1 Teorem*'de, $\mathbb{F}_{2^m}$ sonlu cismi üzerine tüm 3×3 involutif matrisleri üreten yeni bir matris formu verilmektedir.

5.3.1.1. Teorem:

$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ elemanları $\mathbb{F}_{2^m}$ sonlu cisminde 3×3 boyutlu bir matris olsun. Eğer, A matrisi involutif ise A'nın elemanları A'nın köşegen elemanları olan a_{11} ve a_{22} elemanları ile aşağıdaki şekilde ifade edilir. $a_{11} \neq a_{22}$ ve $b_0, b_1 \in \mathbb{F}_{2^m}^*$ olmak üzere, $a_{12} = (a_{11} + 1)b_0$, $a_{13} = (a_{11} + 1)b_1$, $a_{21} = (a_{22} + 1)b_0^{-1}$, $a_{23} = (a_{22} + 1)b_0^{-1}b_1$, $a_{31} = (a_{11} + a_{22})b_1^{-1}$, $a_{32} = (a_{11} + a_{22})b_1^{-1}b_0$, $a_{33} = a_{11} + a_{22} + 1$.

Burada, önerilen 3×3 involutif matris formu $(IM)_{3\times3}$ aşağıdaki formda yazılır:

$$(IM)_{3\times3} = \begin{pmatrix} a_{11} & (a_{11} + 1)b_0 & (a_{11} + 1)b_1 \\ (a_{22} + 1)b_0^{-1} & a_{22} & (a_{22} + 1)b_0^{-1}b_1 \\ (a_{11} + a_{22})b_1^{-1} & (a_{11} + a_{22})b_1^{-1}b_0 & a_{11} + a_{22} + 1 \end{pmatrix}$$

Kanıt:

$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ matrisi involutif olsun ve $j = 1, 2, 3$ için A^2 matrisinin elemanları $c_{ij} = \sum_{k=1}^{3} a_{ik}a_{kj}$ ile gösterilsin. Bu durumda, I matrisi 3×3 boyutlu birim matrisi olmak üzere $A^2 = I$ olacaktır. $i = j$ ise, $c_{ij} = 1$. Diğer durumlarda, $c_{ij} = 0$ olur. O halde, aşağıdaki denklemler elde edilir:

$$a_{11}{}^2 + a_{12}a_{21} + a_{13}a_{31} = 1 \quad (1)$$

$$a_{21}a_{12} + a_{22}{}^2 + a_{23}a_{32} = 1 \quad (2)$$

$$a_{31}a_{13} + a_{32}a_{23} + a_{33}{}^2 = 1 \quad (3)$$

$$a_{11}a_{12} + a_{12}a_{22} + a_{13}a_{32} = 0 \quad (4)$$

$$a_{11}a_{13} + a_{12}a_{23} + a_{13}a_{33} = 0 \quad (5)$$

$$a_{21}a_{11} + a_{22}a_{21} + a_{23}a_{31} = 0 \quad (6)$$

$$a_{21}a_{13} + a_{22}a_{23} + a_{23}a_{33} = 0 \quad (7)$$

$$a_{31}a_{11} + a_{32}a_{21} + a_{33}a_{31} = 0 \quad (8)$$

$$a_{31}a_{12} + a_{32}a_{22} + a_{33}a_{32} = 0 \quad (9)$$

(1), (2) ve (3) denklemleri taraf tarafa toplanırsa, $a_{11}{}^2 + a_{22}{}^2 + a_{33}{}^2 = 1$ eşitliği elde edilir. $\mathbb{F}_{2^m}$ sonlu cisminde,

$$a_{11} + a_{22} + a_{33} = 1 \quad (10)$$

elde edilir. (4), (5), (6), (7), (8) ve (9) denklemlerinden aşağıdaki denklemler elde edilir:

$$a_{12}(a_{11} + a_{22}) = a_{13}a_{32} \quad (11)$$

$$a_{13}(a_{11} + a_{33}) = a_{12}a_{23} \quad (12)$$

$$a_{21}(a_{11} + a_{22}) = a_{23}a_{31} \quad (13)$$

$$a_{23}(a_{22} + a_{33}) = a_{21}a_{13} \quad (14)$$

$$a_{31}(a_{11} + a_{33}) = a_{32}a_{21} \tag{15}$$

$$a_{32}(a_{22} + a_{33}) = a_{31}a_{12} \tag{16}$$

(11) ile (13) denklemleri, (12) ile (15) denklemleri ve (14) ile (16) denklemleri çarpıldığında sırasıyla aşağıdaki denklemler elde edilir:

$$a_{12}a_{21}(a_{11} + a_{22})^2 = a_{13}a_{31}a_{32}a_{23} \tag{17}$$

$$a_{13}a_{31}(a_{11} + a_{33})^2 = a_{12}a_{21}a_{32}a_{23} \tag{18}$$

$$a_{23}a_{32}(a_{22}+a_{33})^2 = a_{21}a_{12}a_{13}a_{31} \tag{19}$$

(18) ve (19) denklemleri taraf tarafa çarpılarak, $(a_{11} + a_{33})^2(a_{22} + a_{33})^2 = (a_{12}a_{21})^2$ denklemi elde edilir. $mod\ 2$'ye göre bu denklem, $(a_{11} + a_{33})(a_{22} + a_{33}) = a_{12}a_{21}$ şeklinde sadeleştirilir. (10) denklemi kullanılarak, bir $b_0 \in \mathbb{F}_{2^m} - \{0\}$ elemanı için $a_{12} = (a_{11} + 1)b_0$ ve $a_{21} = (a_{22} + 1){b_0}^{-1}$ eşitlikleri elde edilir. $a_{11} \neq a_{22}$ kısıtlaması kullanılarak, $a_{11} + a_{22} \neq 0$ sonucu elde edilir. Bu durumda, ikili cisim genişlemesinde çalışıldığından, (11) ve (13) denklemlerinin sağ tarafları sıfırdan farklıdır. Bu gerçekler göz önüne alınarak, (17) ve (19) denklemleri taraf tarafa çarpıldığında, bir $b_1 \in F_{2^m} - \{0\}$ elemanı için $a_{13} = (a_{11} + 1)b_1$, $a_{31} = (a_{22} + 1){b_1}^{-1}$ sonuçları elde edilir. Yukarıda yapılan işlemlere benzer olarak, (17) ve (18) denklemleri taraf tarafa çarpıldığında, (10) ve (14) denklemlerini kullanarak $a_{23} = (a_{22} + 1){b_0}^{-1}b_1$ sonucu ile (10) ve (16) denklemlerini kullanarak $a_{32} = (a_{11} + a_{22}){b_1}^{-1}b_0$ sonucu elde edilir.

5.3.1.2. Not:

5.3.1.1 Teorem'de önerilen $(IM)_{3\times3}$ matris formu, $a_{11} = a_{22}$ koşulu ile elde edilen involutif matrisler dışındaki tüm involutif matrisleri üretir. Ayrıca, $a_{11} = a_{22}$ koşulu ile elde edilen involutif matrislerin MDS olmadığı açıktır. *5.3.1.3 Önerme*'de $(IM)_{3\times3}$ matrisine bazı ek koşullar ekleyerek, tüm 3×3 involutif MDS matrisleri elde edilmektedir.

5.3.1.3. Önerme:

$(IM)_{3\times3}$ matris formu *5.3.2.1 Teorem*'de tanımlandığı gibi olsun. Bu durumda, $\mathbb{F}_{2^m}$ üzerinde $(IM)_{3\times3}$ ile üretilen ve $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 0$, $a_{11}, a_{22} \neq 1$ ve $a_{11} +$

$a_{22} \neq 1$ koşullarını sağlayan tüm 3×3 involutif matrisler MDS'dir. Böylece, $\mathbb{F}_{2^m}$ üzerinde tüm involutif MDS matrislerinin sayısı, $m > 2$ olmak üzere $(2^m - 1)^2(2^m - 2)(2^m - 4)$ sayısına eşittir.

Kanıt:

2.2.3.5 Teorem'den bir matrisin MDS olması için gerekli ve yeterli koşul tüm kare alt matrisleri terslenebilir olmasıdır. Bu bağlamda, *5.3.1.1 Teorem*'de verilen matrisin tüm kare alt matrislerinin sıfırdan farklı olduğu gösterilmelidir. *5.3.1.1 Teorem*'de verilen $(IM)_{3\times3}$ matrisi $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 0$, $a_{11}, a_{22} \neq 1$ ve $a_{11} + a_{22} \neq 1$ koşullarını sağladığından, 1×1 boyutlu tüm kare alt matrisleri sıfırdan farklıdır. 2×2 boyutlu tüm kare alt matrislerin determinantının sıfırdan farklı olduğu aşağıdaki gibi gösterilir:

$$\begin{vmatrix} a_{11} & (a_{11}+1)b_0 \\ (a_{22}+1){b_0}^{-1} & a_{22} \end{vmatrix} = a_{11} + a_{22} + 1 \neq 0$$

$$\begin{vmatrix} a_{11} & (a_{11}+1)b_1 \\ (a_{22}+1){b_0}^{-1} & (a_{22}+1){b_0}^{-1}b_1 \end{vmatrix} = {b_0}^{-1}b_1(a_{22}+1) \neq 0$$

$$\begin{vmatrix} (a_{11}+1)b_0 & (a_{11}+1)b_1 \\ a_{22} & (a_{22}+1){b_0}^{-1}b_1 \end{vmatrix} = b_1(a_{11}+1) \neq 0$$

$$\begin{vmatrix} a_{11} & (a_{11}+1)b_0 \\ (a_{11}+a_{22}){b_1}^{-1} & (a_{11}+a_{22}){b_1}^{-1}b_0 \end{vmatrix} = {b_1}^{-1}b_0(a_{11}+a_{22}) \neq 0$$

$$\begin{vmatrix} a_{11} & (a_{11}+1)b_1 \\ (a_{11}+a_{22}){b_1}^{-1} & a_{11}+a_{22}+1 \end{vmatrix} = a_{22} \neq 0$$

$$\begin{vmatrix} (a_{11}+1)b_0 & (a_{11}+1)b_1 \\ (a_{11}+a_{22}){b_1}^{-1}b_0 & a_{11}+a_{22}+1 \end{vmatrix} = b_0(a_{11}+1) \neq 0$$

$$\begin{vmatrix} (a_{22}+1){b_0}^{-1} & a_{22} \\ (a_{11}+a_{22}){b_1}^{-1} & (a_{11}+a_{22}){b_1}^{-1}b_0 \end{vmatrix} = {b_1}^{-1}(a_{11}+a_{22}) \neq 0$$

$$\begin{vmatrix} (a_{22}+1){b_0}^{-1} & (a_{22}+1){b_0}^{-1}b_1 \\ (a_{11}+a_{22}){b_1}^{-1} & a_{11}+a_{22}+1 \end{vmatrix} = {b_0}^{-1}(a_{22}+1) \neq 0$$

$$\begin{vmatrix} a_{22} & (a_{22}+1){b_0}^{-1}b_1 \\ (a_{11}+a_{22}){b_1}^{-1}b_0 & a_{11}+a_{22}+1 \end{vmatrix} = a_{11} \neq 0$$

Kısıtlamalar ile verilen $(IM)_{3\times3}$ matris formu, herhangi bir $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$ elemanları ve a_{11}, a_{22} köşegen elemanları ile ifade edilir. Bu yüzden, b_0, b_1 elemanlarının seçim sayısı $(2^m - 1)^2$. Verilen kısıtlamalar doğrultusunda, a_{11} elemanı 0 ve 1'e eşit olamaz. Bu durumda, a_{11} elemanının seçim sayısı, $2^m - 2$'dir. Ayrıca, köşegenleri birbirinden farklı ve toplamları 1 olan elemanları seçmek için, a_{22} elemanı a_{11} ve $a_{11} + 1$ elemanlarından farklı olmalıdır. Bu durumda, a_{22} elemanının seçim sayısı $m > 2$ için $2^m - 4$ olur. O halde, $\mathbb{F}_{2^m}$ sonlu cismi üzerine tüm 3×3 boyutlu involutif ve MDS matris sayısı, $m > 2$ için $(2^m - 1)^2(2^m - 2)(2^m - 4)$ ile verilir.

5.3.1.1 Teorem ve *5.3.1.3 Önerme*'yi kullanarak, 3×3 boyutlu involutif MDS matrislerini daha kolay göstermek için aşağıdaki tanım verilmiştir:

5.3.1.4. Tanım:

$\mathbb{F}_{2^m}$ sonlu cismi üzerinde tüm 3×3 boyutunda involutif ve MDS matrisleri üretmek için $IM_{3\times3}(a_{11}, a_{22}, b_0, b_1)$ matris formu aşağıdaki şekilde tanımlanır:

$$(IM)_{3\times3} = \begin{pmatrix} a_{11} & (a_{11}+1)b_0 & (a_{11}+1)b_1 \\ (a_{22}+1){b_0}^{-1} & a_{22} & (a_{22}+1){b_0}^{-1}b_1 \\ (a_{11}+a_{22}){b_1}^{-1} & (a_{11}+a_{22}){b_1}^{-1}b_0 & a_{11}+a_{22}+1 \end{pmatrix}$$

Burada $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 0$, $a_{11}, a_{22} \neq 1$, $a_{11} + a_{22} \neq 1$ ve $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$.

(Sajadieh, vd., 2012) çalışmasında Vandermonde matrisinden elde edilen ve önerilen matris formu kullanılarak $\mathbb{F}_{2^8}$ üzerine bir 3×3 boyutunda involutif MDS matris *5.3.1.5 Örnek*'te üretilmektedir.

5.3.1.5. Örnek:

$\mathbb{F}_{2^8}$, $0 \times 11d$ ilkel polinomunun bir kökü olan α ilkel (primitive) elemanı ile üretilsin. $\mathbb{F}_{2^8}/0 \times 11d$ sonlu cismi üzerine $IM_{3\times3}(\alpha, \alpha^{26}, \alpha^{173}, \alpha^{232})$ matrisi göz önüne alınsın.

$$IM_{3\times3}(\alpha, \alpha^{26}, \alpha^{173}, \alpha^{232}) = \begin{bmatrix} \alpha & \alpha^{198} & \alpha^2 \\ \alpha^{25} & \alpha^{26} & \alpha^2 \\ \alpha^{25} & \alpha^{198} & \alpha^{50} \end{bmatrix} = \begin{bmatrix} 0\times02 & 0\times07 & 0\times04 \\ 0\times03 & 0\times06 & 0\times04 \\ 0\times03 & 0\times07 & 0\times05 \end{bmatrix}$$

matrisi elamanları $\mathbb{F}_{2^8}/0 \times 11d$ sonlu cisminden alınan bir involutif MDS matristir.

(Liu, vd., 2016) çalışmasında bir dairesel matristen elde edilen ve önerilen matris formu kullanılarak $\mathbb{F}_{2^8}$ sonlu cismi üzerine bir 3×3 boyutlu involutif MDS matris *5.3.1.6 Örnek*'te üretilmektedir:

5.3.1.6. Örnek:

$\mathbb{F}_{2^8}$ sonlu cismi, 0×169 ilkel polinomunun bir kökü olan α ilkel elemanı ile üretilsin. Elemanları $\mathbb{F}_{2^8}/0 \times 169$ sonlu cisminden alınan $IM_{3\times3}(\alpha^{253}, \alpha^{250}, \alpha^{3}, \alpha^{220})$ matrisi göz önüne alınsın. Bu matris aşağıdaki gibi ifade edilir:

$$IM_{3\times3}(\alpha^{253}, \alpha^{250}, \alpha^{3}, \alpha^{220}) = \begin{bmatrix} \alpha^{253} & \alpha^{33} & \alpha^{250} \\ \alpha^{33} & \alpha^{250} & \alpha^{253} \\ \alpha^{250} & \alpha^{253} & \alpha^{33} \end{bmatrix} = \begin{bmatrix} 0 \times 5a & 0 \times 0a & 0 \times 51 \\ 0 \times 0a & 0 \times 51 & 0 \times 5a \\ 0 \times 51 & 0 \times 5a & 0 \times 0a \end{bmatrix}$$

$\alpha^{253}, \alpha^{33}$ ve α^{250} elemanlarının XOR sayısı sırasıyla 6,11 ve 13 olduğundan bu matris $138(= 90 + 3.2.8)$ XOR sayılı involutif MDS matristir.

Bu iki örnekten de görüleceği üzere, önerilen form daha önceki çalışmalardaki yöntemleri (Vandermonde ve left circulant matrisleri) kapsayan daha genel bir yöntemdir.

5.3.2. En Hafif 3×3 İnvolutif ve MDS Matrisler İçin Deneysel Sonuçlar

Bu bölümde $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ cisimleri üzerine tanımlı en hafif 3×3 boyutunda involutif MDS matrisler elde edilmektedir. *5.3.1.3 Önerme*'sinden $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ cisimleri üzerinde sırasıyla 1176, 37800 ve $\approx 2^{31.95}$ adet 3×3 boyutunda involutif MDS matrisin var olduğu gösterilebilir. Tez çalışmasında $\mathbb{F}_{2^3}/0 \times b$, $\mathbb{F}_{2^4}/0 \times 13$ ve $\mathbb{F}_{2^8}/0 \times 1c3$ üzerindeki tüm 3×3 boyutunda involutif MDS matrisler üretilmekte ve minimum XOR sayısına sahip olanlar kontrol edilmektedir. $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ cisimleri üzerine XOR sayısı metriği açısından sırasıyla en hafif 24, 12 ve 24 adet 3×3 boyutunda involutif MDS matris belirlenmektedir. $0 \times 1c3$ ilkel polinomundan başka ilkel polinomlar ile de $\mathbb{F}_{2^8}$ üzerinde daha iyi matrisler elde edilebileceği unutulmamalıdır.

5.3.2.1 Örnek'te, önerilen matris formu kullanılarak $\mathbb{F}_{2^4}$ sonlu cismi üzerine en hafif 3×3 boyutunda involutif MDS matrisler verilmektedir.

5.3.2.1. Örnek:

$\mathbb{F}_{2^4}$ sonlu cismi, 0×13 ilkel polinomunun bir α ilkel kökü ile üretilsin. Elemanları $\mathbb{F}_{2^4}/0 \times 13$ sonlu cisminden alınan $IM_{3\times3}(\alpha^3, \alpha^6, 1, \alpha^2)$ matrisi aşağıdaki gibi gösterilir:

$$IM_{3\times3}(\alpha^3, \alpha^6, 1, \alpha^2) = \begin{bmatrix} \alpha^3 & \alpha^{14} & \alpha \\ \alpha^{13} & \alpha^6 & 1 \\ 1 & 1 & \alpha^8 \end{bmatrix} = \begin{bmatrix} 0\times8 & 0\times9 & 0\times2 \\ 0\times d & 0\times c & 0\times1 \\ 0\times1 & 0\times1 & 0\times5 \end{bmatrix}$$

$1, \alpha, \alpha^3, \alpha^6, \alpha^8, \alpha^{13}$ ve α^{14} elemanlarının XOR sayıları sırasıyla $0, 1, 3, 5, 6, 3$ ve 1 olduğundan bu matrisin XOR sayısı $43(= 19 + 3.2.4)$'tür. *Çizelge 5.1*'de de görüldüğü gibi literatürdeki sonuç olan 60 XOR sayısı, 43 XOR sayısına kadar düşmektedir.

Önerilen matris formu kullanılarak, $\mathbb{F}_{2^8}/0 \times 1c3$ üzerine en hafif 3×3 involutif MDS matrislerden birisi verilmiştir.

5.3.2.2. Örnek:

$\mathbb{F}_{2^8}$ sonlu cismi, $0 \times 1c3$ ilkel polinomunun ilkel bir α kökü ile üretilsin. Elemanları $\mathbb{F}_{2^8}/0 \times 1c3$ sonlu cisminden alınan $IM_{3\times3}(\alpha^{150}, \alpha^{156}, 1, \alpha)$ matrisi aşağıdaki gibi gösterilir:

$$IM_{3\times3}(\alpha^{150}, \alpha^{156}, 1, \alpha) = \begin{bmatrix} \alpha^{150} & \alpha^{58} & \alpha^{59} \\ \alpha^{254} & \alpha^{156} & 1 \\ 1 & 1 & \alpha^{157} \end{bmatrix} = \begin{bmatrix} 0\times e2 & 0\times e3 & 0\times05 \\ 0\times e1 & 0\times e0 & 0\times01 \\ 0\times01 & 0\times01 & 0\times03 \end{bmatrix}$$

$1, \alpha^{58}, \alpha^{59}, \alpha^{150}, \alpha^{156}, \alpha^{157}$ ve α^{254} elemanlarının XOR sayıları sırasıyla $0, 12, 11, 16, 9, 9$ ve 3 olduğundan bu matrisin XOR sayısı $108(= 60 + 3.2.8)$'dir. *Çizelge 5.1*'de de görüldüğü gibi literatürdeki sonuç olan 138 XOR sayısı, 108 XOR sayısına kadar düşmektedir.

Çizelge 5.1'de literatürdeki çalışmalar ile bu çalışmada önerilen matris formundan elde edilen sonuçlar karşılaştırılmaktadır.

Çizelge 5.1 En Hafif 3x3 MDS ve İnvolutif Matrisler İçin Karşılaştırma

	$\mathbb{F}_{2^3}$	**Poly.**	$\mathbb{F}_{2^4}$	**Poly.**	$\mathbb{F}_{2^8}$	**Poly.**
Mevcut	-	-	60 (Liu, vd., 2016)	0x1f	138 (Liu, vd., 2016)	0x169
IM Form	31	0xb	43	0x13	108	0x1c3

Çizelge 5.2'de bu çalışmada önerilen $IM_{3\times3}(a_{11}, a_{22}, b_0, b_1)$ involutif, MDS formu kullanılarak $\mathbb{F}_{2^3}, \mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ ikili genişletilmiş cisimlerindeki Magma hesaplamaları sonucu elde edilen en hafif involutif MDS matrisleri verilmektedir.

Çizelge 5.2 Bileşenleri $\mathbb{F}_{2^3}, \mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^8}$ Cisimlerinden Alınan En Hafif İnvolutif MDS Matrisleri

$\mathbb{F}_{2^3}/0xb$			
a_{11}	a_{22}	b_0	b_1
α	α^2	α^4	α^4
α	α^2	α^6	α^4
α	α^4	α^4	α^6
α	α^4	α^5	1
α	α^4	α^4	α^4
α	α^5	α^4	α^6
α	α^6	1	α^5
α	α^6	α^6	α^4
α^2	α	α	α^5
α^2	α	α^3	1
α^2	α^5	1	α^3
α^2	α^5	α^5	α

$\mathbb{F}_{2^3}/0xb$			
a_{11}	a_{22}	b_0	b_1
α^4	α	α^2	α^2
α^4	α	α^3	α^2
α^4	α^6	α^2	α^2
α^4	α^6	α^2	α^3
α^5	α	α^3	1
α^5	α	α^3	α^2
α^5	α^2	1	α^3
α^5	α^2	α^2	α^3
α	α	1	α^5
α^6	α	α	α^5
α^6	α^4	α^5	1
α^6	α^4	α^5	α

$\mathbb{F}_{2^4}/0x13$			
a_{11}	a_{22}	b_0	b_1
α^3	α^6	1	α^2
α^3	α^6	α^{14}	α
α^3	α^8	α	α^{14}
α^3	α^8	α^2	1
α^6	α^3	1	α^2
α^6	α^3	α	α^2
α^6	α^8	α^2	1
α^6	α^8	α^2	α
α^8	α^3	α^{13}	α^{13}
α^8	α^3	α^{14}	α^{13}
α^8	α^6	α^{13}	α^{13}
α^8	α^6	α^{13}	α^{14}

$\mathbb{F}_{2^8}/0x1c3$			
a_{11}	a_{22}	b_0	b_1
α^{150}	α^{156}	1	α
α^{150}	α^{156}	α^{196}	α^{197}
α^{150}	α^{156}	α^{197}	α^{198}
α^{150}	α^{156}	α^{254}	1
α^{150}	α^{157}	1	α^{254}
α^{150}	α^{157}	α	1
α^{150}	α^{157}	α^{197}	α^{196}
α^{150}	α^{157}	α^{198}	α^{197}
α^{156}	α^{150}	1	α
α^{156}	α^{150}	α	α
α^{156}	α^{150}	α^{58}	α
α^{156}	α^{150}	α^{59}	α

$\mathbb{F}_{2^8}/0x1c3$			
a_{11}	a_{22}	b_0	b_1
α^{156}	α^{157}	α	1
α^{156}	α^{157}	α	α
α^{156}	α^{157}	α	α^{58}
α^{156}	α^{157}	α	α^{59}
α^{157}	α^{150}	1	α^{254}
α^{157}	α^{150}	α^{57}	α^{254}
α^{157}	α^{150}	α^{58}	α^{254}
α^{157}	α^{150}	α^{254}	α^{254}
α^{157}	α^{156}	α^{254}	1
α^{157}	α^{156}	α^{254}	α^{57}
α^{157}	α^{156}	α^{254}	α^{58}
α^{157}	α^{156}	α^{254}	α^{254}

BÖLÜM 6

SONUÇLAR VE TARTIŞMALAR

6.1. Sonuçlar

Bu çalışmada, sonlu cisimler üzerinde tanımlanan minimum uzaklık parametresi büyük kodlar elde edebilmek için yeni iki halka ve yeni iki halka sınıfı üzerinde tanımlı devirli ve sabit devirli kodlar araştırılmıştır. Elde edilen yeni sonlu halka sınıflarının, bu çalışmada tanıtılan yeni sonlu halkanın genelleştirmesi olduğu ortaya çıkarılmıştır ve ayrıca tüm yeni sonlu halka ve halka sınıflarına ait cebirsel yapılar belirlenmiştir. Bunlara ek olarak, çalışmadaki bir halka ve bir halka sınıfına ait devirli kodların inşası 3.2.4 ve 3.3.3 bölümlerinde elde edilmiştir, buna bağlı olarak devirli kodların üreteç idealleri sırasıyla 3.2.4.2 Teorem ve 3.3.3.1. Teorem'i ile, minimal üreteç kümeleri ise 3.2.4.5 Teorem ve 3.3.3.3 Teorem'i ile verilmiştir.

Bu tez çalışmasının kapsadığı halka ve halka sınıfları için, birimsel elemanlar belirlenerek sınıflandırılmıştır ve bu sınıflandırma göz önüne alınarak seçilen birimsel elemanlar yardımıyla belirli uzunluğa sahip sabit devirli kodlar ve devirli kodların arasındaki ilişkiler belirlenerek bu kodların Gray görüntüleri 4.2.3 ve 4.3.3 bölümlerinde 4.2.3.4, 4.2.3.6, 4.3.3.4 ve 4.3.3.6 Teorem'leri ile elde edilmiştir.

Çalışmada, tezin bir diğer araştırma konusu olan MDS özellikli involutif matris yapısı araştırılmıştır. Bileşenleri $\mathbb{F}_{2^m}$ sonlu cisminden alınan 2×2 ve 3×3 boyutundaki MDS ve involutif matrislerin genel formları 5.2.1 ve 5.3.1.1 Teorem'leri ile oluşturulmuştur. Bu forma ilişkin elde edilebilecek matris sayısı formülü 5.3.1.3 Önerme

ile bulunmuştur. Elde edilen genel form yardımıyla, *XOR* sayısı metriği göz önüne alınarak literatürde verilmiş MDS ve involutif matrislere (3×3 boyutunda) göre daha az maliyetli matrisler Çizelge 5.2'deki gibi elde edilmiştir.

6.2. Gelecek Çalışma

Bu tez çalışmasında verilen bu iki halka ve iki halka sınıfı üzerinde aşikar olmayan otomorfizmalar tanımlanarak, bu çalışmalar skew devirli (cyclic) kodlar üzerine taşınabilir.

Koşullar değiştirilerek ve genelleştirmeler yapılarak başka halka sınıfları oluşturulabilir ve buradaki çalışmalara benzer şekilde devirli ve sabit devirli kodlar arasındaki ilişkiler, uygun uzunluk ve Gray dönüşümleri belirlenerek bulunabilir.

Bu çalışmada tanımlanan yeni 16 elemanlı halka ve bu halka üzerinde tanımlanan devirli kodların üreteçleri kullanılarak yeni DNA devirli kodlar tanımlanabilir ve tanımlanacak olan DNA devirli kodların sıralı terslenebilen (reversible) ve sıralı terslenebilen tamamlanan (reversible complement) olması için gerek ve yeter koşullar belirlenebilir.

Bu çalışmada elde edilen farklı iki devirli kod inşasına ilişkin minimal üreteçler kullanılarak minimum uzaklık parametresi büyük olan kodlar hesaplama yoluyla elde edilebilir.

Tezin diğer çalışma konusu olan 3×3 boyutlu MDS involutif matris formu inşası, 3×3 boyutunda matris kullanmaya elverişli farklı şifreleme algoritmalarının yayılım tabakasında donanım kolaylığı ve az maliyetli olması açısından kullanılabilir.

Bu tez çalışmasında verilen 3×3 boyutlu MDS involutif matris formuna benzer bir form, bileşenleri $\mathbb{F}_{2^m}$ sonlu cisminden alınan 4×4 boyutlu involutif MDS matrislerin genel bir formunun elde edilmesi için kullanılabilir ve bu form yardımıyla elde edilecek 4×4 boyutlu involutif MDS matrisler şifre tasarımlarının düşük uygulama maliyetli elemanları olarak kullanılabilir.

KAYNAKÇA

Abualrub, T. ve Siap, I., "Cyclic Codes over The Rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$", Des. Codes Cryptogr., no. 42, pp. 273-287., 2007.

Abualrub, T. ve Siap, I., "Reversible Quaternary Cyclic Codes", Proceedings of the 9th WSEAS International Conference on Applied Mathematics, İstanbul, 2008.

Amarra, M. C. V. ve Nemenzo, F. R., "On $(1-u)-$ Cyclic Codes over $\mathbb{F}_{p^k} + u\,\mathbb{F}_{p^k}$", Appl. Math. Lett., no. 21, pp. 1129-1133, 2008.

Aydin, N., Cengellenmis Y. ve Dertli A., "On Some Constacyclic Codes over $\mathbb{Z}_4[u]/\langle u^2-1\rangle$, Their $\mathbb{Z}_4$ Images, and New Codes", Des. Codes Cryptogr., 2018.

Barreto, P. ve Jr. M. Simplicio Jr, M., Curupira, a block cipher for constrained platforms,

25th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC) 2007.

Biham, E. ve Shamir, A., "Differential Cryptanalysis of DES-like Cryptosystems", CRYPTO'90, LNCS, 1990.

Blake, I. F., "Codes over Certain Rings", Information And Control, No. 20, pp. 396-404, 1972.

Blake, I. F., "Codes over Integer Residue Rings", Inform. Contr., no. 29, pp. 295-300, 1975.

Bonnecaze, A. ve Udaya, P., "Cyclic Codes and Self-Dual Codes over $\mathbb{F}_2 + u\mathbb{F}_2$", IEEE Transactions On Information Theory, cilt 45, no. 4, pp. 1250-1255, 1999.

Bosma, W., Cannon, J., Playoust, C. 1997. “The Magma Algebra System 1: The User Language”. J. Symb. Comp. 24, 235-265.

Calderbank, A. R. ve Sloane, N. J. A., “Modular and p-adic Cyclic Codes”, Designs, Codes and Cryptography, no. 6, pp. 21-35, 1995.

Cengellenmis, Y., “On $(1 - u^2)$ −Cyclic Codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$”, Journal of Discrete Mathematical Science Cryp., cilt 12, no. 2, pp. 239-243, 2009.

Cengellenmis, Y., “On $(1 - u^m)$ −Cyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^m\mathbb{F}_2$”, International J. of Contemp. Math. Sci., no. 4, pp. 987-992, 2009.

Çallıalp, F., “Örneklerle Soyut Cebir”, İstanbul: Birsen yayınevi, 2013.

Dertli, A. ve Cengellenmis, Y., “On $(1 + u)$ −Cyclic and Cyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$”, European J. of Pure and Applied Math., no. 9, pp. 305-313, 2016.

Ding, J. ve Li, H., “The Gray Images of $(1 + u) -$ Constacyclic Codes over $\mathbb{F}_{2^m}[u]/\langle u^k \rangle$”, Journal of Applied Mathematics and Computing, cilt 49, p. 433–445, 2015.

Dinh, H. Q. ve López-Permouth, S. R., “Cyclic and Negacyclic Codes over Finite Chain Rings”, IEEE Transactions on Information Theory, cilt 5, no. 8, pp. 1728-1744, 2004.

Dougherty, S. T. ve Salturk, E., “Constacyclic Codes over Local Rings of Order 16”, submitted.

Dougherty, S. T., “Algebraic Coding Theory over Finite Commutative Rings”, PA, USA: Springer, 2017.

Dougherty, S. T., Yildiz, B. ve Karadeniz, S., “Codes over R_k, Gray Maps and Their Binary Images”, Finite Fields and Their Applications, no. 17, p. 205–219, 2011.

Forouzan B. A., Cryptography and Network Security, International Edition, McGraw-Hill Education, 2008.

FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November 26, 2001.

Gao, J., "Linear Codes and $(1+uv)$ −Constacyclic Codes over $R[v]/\langle v^2+v\rangle$", IEICE Transactions on Fundamentals, no. E98-A, pp. 1044-1048, 2015.

Green, G. G., "US Patent 3537103: Serial Digital Decoder, (NASA) Algorithm", NASA: Air Force Cambridge Research Center, Cambridge, MA., 1970.

Guo, J., Peyrin, T. ve Poschmann, A., "The PHOTON Family of Lightweight Hash Functions", CRYPTO 2011, LNCS, 2011.

Gupta, K. C. ve Ray, I. G., "On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography", CD-ARES 2013 Workshops: MoCrySEn, 2013.

Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A. ve Solé, P., "The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes", IEEE Trans. Inform. Theory, No. 40, pp. 301-318, 1994.

Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A. ve Solé, P., "On The Apparent Duality of The Kerdock and Preparata Codes Applied Algebra, Algebraic Algorithms And Error Correcting Codes", Berlin, 1993.

Hill, R., "A First Course in Coding Theory", Oxford: Clarendon Press, 1986.

Hoffman, K. ve Kunze, R., "Linear Algebra (2nd edition)", New Jersey: Prentice-Hall, Inc. , Englewood Cliffs, 1971.

Huffman, W. C., Cary, W. ve Pless, V., "Fundamentals of Error-Correcting Codes", Cambridge University Press, 2003.

Hungerford, T., "Algebra", New York: Springer-Verlag, 1973.

Jitman, S., Udomkavanich, P. ve Ling, S., "Skew Constacyclic Codes over Finite Chain Rings", Adv. Math Commun, no. 6, pp. 29-63., 2012.

Junod, P. ve Vaudenay, S., "Perfect Diffusion Primitives for Block Ciphers", Selected Areas in Cryptography (SAC 2004), LNCS, 2005.

Kai, X., Zhu, S. ve Wang, L., "A Family of Constacyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", J Sysst Sci Complex, no. 25, pp. 1032-1040, 2012.

Karadeniz, S. ve Yildiz, B., "$(1+v)$ −Constacyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", Journal of Franklin Ins., no. 348, pp. 2625-2632, 2011.

Karakaş, H. İ., "Cebir Dersleri", 2 dü., Ankara: Tüba yayınları, 2012.

Khoo, K., Peyrin, T., Poschmann, A. Y. ve Yap, H., "FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison", Cryptographic Hardware and Embedded Systems (CHES 2014), LNCS, 2014.

Lacan, J. ve Fimes, J., "Systematic MDS Erasure Codes Based on Vandermonde Matrices", IEEE Trans. Commun. Lett., cilt 8, pp. 570-572, 2004.

Li, Y. ve Wang, M., "On the Construction of Lightweight Circulant Involutory MDS Matrices", Fast Software Encryption (FSE 2016), LNCS, 2016.

Liao, D. ve Tang, Y. , "A Class of Constacyclic Codes over $R + vR$ and its Gray Image", Int. J. Commun. Network and Syst. Sci., no. 5, pp. 222-227, 2012.

Ling, S. ve Xing, C., "Coding Theory a First Course", New York: Cambridge University Press, 2004.

Liu, M. ve Sim, S. M., "Lightweight MDS Generalized Circulant Matrices", Fast Software Encryption (FSE 2016), LNCS, 2016.

MacWilliams, F. ve Sloane, N.J.A., "The Theory of Error-Correcting Codes", 1 dü., cilt 16, North-Holland Publishing Company, 1983.

Matsui, M., "Linear Cryptanalysis Method for DES Cipher", EUROCRYPT'93, LNCS, 1994.

Ozger, Z. O., Kara, U. U. ve Yildiz, B., "Linear, Cyclic and Constacyclic over $S_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$", Filomat, no. 28, pp. 897-906, 2014.

Özen, M., Uzekmek, F. Z., Aydin, N. ve Özzaim, N. T., "Cyclic and Some Constacyclic Codes over the Ring $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$", Finite Fields and Their Applications, no. 38, pp. 27-39, 2016.

Pehlivanoğlu, M. K., Sakallı, M. T., Akleylek, S., Duru, N. ve Rijmen, V., "Generalization of Hadamard Matrix to Generate Involutory MDS Matrices for Lightweight Cryprography", IET Information Security, 2018.

Pless, V. S. ve Qian, Z., "Cyclic Codes and Quadratic Residue Codes over $\mathbb{Z}_4$", IEEE Transactions on Information Theory, cilt 42, no. 5, pp. 1594-1600, 1996.

Pless, V. S., Solé, P. ve Qian, Z., "Cyclic Self-Dual $\mathbb{Z}_4$-codes", Finite Fields Their Applic., cilt 3, p. 48–69, 1997.

Prange, E., "Cyclic Error-Correcting Codes in Two Symbols", Cambridge: Air Force Cambridge Research Center-TN-57-103, 1957.

Prange, E., "Some Cyclic Error-Correcting Codes with Simple Decoding Algorithms", Cambridge: Air Force Cambridge Research Center-TN-58-156, 1958.

Preneel B., Analysis and Design of Cryptographic hash functions, Ph.D. Thesis, Katholieke Universiteit Leuven, January 1993.

Qian, J., Zang, L. ve Zhu, S., "$(1 + u)$ −Constacyclic and Cyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2$", Appl. Math. Lett, no. 19, pp. 820-823, 2006.

Qian, J., Zang, L. ve Zhu, S., "Constacyclic and Cyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$", IEICE Trans. Fund. Electron. Commun. Comput. Sci., no. E89 - A(6), pp. 1863-1865, 2006.

Qian, J., Zang, L. ve Zhu, S., "Cyclic Codes over $\mathbb{F}_p + u\mathbb{F}_p + ... + (u^k - 1)\mathbb{F}_p$", IEICE Trans. Fundamentals, no. E88 - A(3), pp. 795-797, 2005.

Sajadieh, M., Dakhilalian M., Mala H. ve Omoomi B., "On Construction of Involutory MDS Matrices from Vandermonde Matrices in $GF(2^q)$", Design, Codes and Cryptography, cilt 64, pp. 287-308, 2012.

Sarkar, S. ve Syed, H., "Analysis of Toeplitz MDS Matrices", ACISP 2017, LNCS, 2017.

Sarkar, S. ve Sim, S. M., "A Deeper Understanding of the XOR Count Distribution in the Context of Lightweight Cryptography", Afrıcacrypt 2016, LNCS, 2016.

Sarkar, S. ve Syed, H., "Lighweight Diffusion Layer: Importance of Toeplitz Matrices", IACR Transactions on Symmetric Cryptology, 2016.

Shannon, C. E., "Communication Theory of Secrecy Systems", Bell System Technical Journal, cilt 28, pp. 656-715, 1949.

Shannon, C., "A Mathematical Theory of Communication", The Bell System Technical Journal, pp. 379-423, 1948.

Sim, S. M., Khoo, K., Oggier, F. ve Peyrin, T., "Lightweight MDS Involution Matrices", Fast Software Encryption (FSE 2015), LNCS, 2015.

Singleton, R. C., “Maximum Distance q-nary Codes”, IEEE Trans. Inform. Theory, no. 10, p. 116–118, 1964.

Stinson R., Cryptography: Theory and Practice, Second Edition, CRC Press, 2002.

Taşcı, D., “Soyut Cebir”, Ankara: Alp Yayınevi, 2007.

Udomkavanich, P. ve Jitman, S., “On the Gray Image of $(1 - u^m)$ −Cyclic Codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^m\mathbb{F}_{p^m}$”, Int. J. Contemp. Math. Sciences, cilt 4, no. 26, pp. 1265 - 1272, 2009.

Yıldız, B. ve Aydın, N., “On Cyclic Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and Their $\mathbb{Z}_4 -$ Images”, Int. J. Information and Coding Theory, cilt 2, no. 4, pp. 226-237, 2014.

Yildiz, B. ve Karadeniz, S., “Cyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$”, Des. Codes Cryptogr., no. 58, pp. 221-234, 2011.

Youssef, A. M., Mister, S. ve Tavares, S. E., “On the Design of Linear Transformation for Substitution Permutation Encryption Networks”, Proceedings of Selected Areas in Cryptography (SAC'97), 1997.

Yu, H., Zhu, S. ve Kai, X., “$(1 - uv)$ −Constacyclıc Codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$”, J Syst Sci Complex, no. 27, p. 811–816, 2014.

Zhu, S. ve Wang, L., “A Class of Constacyclic Codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray Image”, Discrete Mathematics, no. 311, pp. 2677-2682, 2011.

Zhu, S., Wang, Y. ve Sji, M., “Some Results on Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$”, IEEE Transactions on Information Theory, cilt 56, no. 4, pp. 1680-1684, 2010.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : G. Gözde GÜZEL

Doğum Yeri ve Tarihi : Fatih / İSTANBUL – 1986

e-mail : ggozdeguzel@gmail.com

Eğitim Bilgileri

Lise	:	Sakıp Sabancı Anadolu Lisesi, Beşiktaş, İST	2004
Lisans	:	Matematik Bölümü, Trakya Üniversitesi, Fen Fakültesi, Edirne	2008
Y. Lisans	:	Matematik, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne	2011
Doktora	:	Hesaplamalı Bilimler, Trakya Üniversitesi, FBE, Edirne	2019

İş Deneyimleri

2008 – 2013	Sınav Dershanesi, Edirne	Matematik Öğretmeni
2013 – …	İpsala Meslek Yüksekokulu, Trakya Üniversitesi	Öğretim Görevlisi

Yabancı Diller

İngilizce

TEZ SIRASINDA YAPILAN ÇALIŞMALAR

1. G. G. Güzel, A. Dertli, Y. Çengellenmiş, "**The $(1+u^2)-$ Constacyclic and Cyclic Codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+v\mathbb{F}_2$**", Journal of Applicable Algebra in Engineering, Communication and Computing (AAECC), Springer, 2018, (submitted).
2. G. G. Güzel, A. Dertli, Y. Çengellenmiş, "**Constacyclic and Cyclic Codes over the Class of Finite Rings $\mathbb{F}_{2^k}+u\mathbb{F}_{2^k}+u^2\mathbb{F}_{2^k}+v\mathbb{F}_{2^k}$**", 24th Conference on Applications of Computer Algebra, Santiago De Compestela- İspanya, 2018.
3. G. G. Güzel, A. Dertli, Y. Çengellenmiş, **"On the $(1+u^2+u^3)-$ Constacyclic and Cyclic Codes over the Finite Ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2+v\mathbb{F}_2$",** Notes from the International Autumn School on Computational Number Theory: Izmir Institute of Technology 2017, Eds. E.Buyukasik&I.Inam, Springer/Birkhauser, 2019.
4. G. G. Güzel, M. T. Sakallı, S. Akleylek, V. Rijmen, Y. Çengellenmiş, **"A New Matrix Form to Generate All 3×3 Involutory MDS Matrices over $\mathbb{F}_{2^m}$"**, Journal of Information Processing Letters (IPL), Elsiever, 2019 (submitted).