T.C

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BELİRLİ HALKALAR ÜZERİNDEKİ KODLAMA TEORİSİ

GÖKHAN GÖKGÖZ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

Tez Danışmanı: Prof. Dr. M. HÜLYA İŞCAN

EDİRNE-2019

GÖKHAN GÖKGÖZ'ün hazırladığı "BELİRLİ HALKALAR ÜZERİNDEKİ KODLAMA TEORİSİ" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Matematik Anabilim Dalında bir Yüksek Lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri	İmza
Prof. Dr. M. Hülya İŞCAN	
Prof. Dr. Neşet AYDIN	
Doç. Dr. Yasemin Çengellenmiş	

Tez Savunma Tarihi 11/01/2019

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Prof. Dr. M. Hülya İŞCAN

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

Prof. Dr. Murat YURTCAN

Fen Bilimleri Enstitüsü Müdürü

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK YÜKSEK LİSANS 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.

06./02./2019

Gökhan GÖKGÖZ

Yüksek Lisans Tezi

Belirli Halkalar Üzerindeki Kodlama Teorisi

T.Ü. Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

ÖZET

Cebirsel Kodlama Teorisinin amaçlarından biri sonlu cisimler veya sonlu halkalar üzerinde yeni ve iyi kodlar yazmaktır. Bilinen iyi kodlar kullanılarak yeni halkalar üzerinde iyi kodlar elde edilmesi önemlidir. Bu tezde belirli halkalar üzerinde iyi kodlar yazmak amaçlanmışır.

Bu tez çalışmasında öncelikle lineer kodlar, cyclic kodlarla ilgili temel bilgiler verilmiştir. 3. Bölümde $u^2 = u$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2$ halkasından $\mathbb{F}_2$ cismi üzerine tanımlanan bir Gray dönüşümü kullanılarak $\mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerindeki bir cyclic kodun Gray dönüşümü altındaki görüntüsü $\mathbb{F}_2$ cismi üzerinde tanımlanan iki cyclic kodun direkt çarpımı olarak yazılmıştır. $\mathbb{F}_2$ cismi üzerindeki bu iki cyclic kodun üreteç matrisleri, üreteç polinomları, idempotent üreteçleri kullanılarak $\mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerindeki cyclic kodun üreteç matrisi, üreteç polinomu ve idempotent üreteci elde edilmişbtir.

3. Bölümde daha sonra $u^2 = 0$ ya da $u^2 = 1$ durumunda elde edilen $\mathbb{F}_2 + u\mathbb{F}_2$ halkalarının birbirine izomorf olduğu gösterilmiştir. Sonra $u^2 = 0$ durumunda $\mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerindeki farklı kodlar belirlenmiştir. 4. Bölümde bu sonuçlar p bir asal sayı,

k bir doğal sayı ve $u^2 = 0$ olmak üzere $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ halkası üzerine genelleştirilmiştir. $u^2 = 0$ durumunda $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ halkası üzerinde p^s uzunluklu constacyclic kodlar incelenmiştir.

5. Bölümde $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ halkası üzerindeki cyclic, $(1-u^2)-$constacyclic veya quasi-cyclic kodlar

i. $p = 2$, $u^3 = 0$

ii. $p = 3$, $u^3 = 0$

iii. $p = 3$, $u^3 = 1$ durumlarında belirlenmiştir.

Yıl : 2018

Sayfa Sayısı : 119

Anahtar Kelimeler : Lineer Kod, Cyclic Kod, Constacyclic Kod, Quasi-Cyclic Kod, Gray Dönüşümü, Hamming Uzaklığı, Lee Uzaklığı, Üreteç Matrisi, Galois Halkası, Galois Cismi

Post GraduateThesis

Coding Theory On The Certain Rings

Trakya University Institute of Natural Sciences

Department of Mathematics

ABSTRACT

The aim of Algebraic Coding Theory is to write new and good codes over finite fields or finite rings. It is important to write good codes over the new rings using known good codes. To write good codes over the certain rings is aimed in this thesis.

Firstly basic knowledge on lineer codes, cyclic codes have been given in this thesis. In chapter 3. a Gray image of a cyclic code over $\mathbb{F}_2 + u\mathbb{F}_2$ has been written as a direct product of two codes over $\mathbb{F}_2$ by using the Gray map from the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = u$ to the field $\mathbb{F}_2$. The generator matrix, generator polynomial and idempotent generator of cyclic code over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ has been obtained by using the generator matrices, generator polynomials, idempotent generators of these two cyclic codes that are defined over the field $\mathbb{F}_2$.

In chapter 3. afterwards it has been proved that the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ and the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with are isomorphic. Then different codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ have been determined. In chapter 4. These results have been

generalized to the ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ where p is a prime number, k is a natural number. The constacyclic codes of length p^s over the ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ have been studied.

In chapter 5. the cyclic, $\left(1-u^2\right)-$constacyclic, quasi-cyclic codes over the ring $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ with $u^2 = 0$ have been determined for the following cases.

i. $p = 2$, $u^3 = 0$

ii. $p = 3$, $u^3 = 0$

iii. $p = 3$, $u^3 = 1$

Year : 2018

Number of Pages : 119

Keywords : Linear Code, Cyclic Code, Constacyclic Code, Quasi-Cyclic Code, Gray Map, Hamming Distance, Lee Distance, Generator Matrix, Galois Rings, Galois Field

ÖNSÖZ

Öğrencisi olmakla kendimi şanslı hissettiğim, bugünlere gelmemde hakkını ödeyemeyeceğim değerli hocam Prof. Dr. M. Hülya İŞCAN'a üzerimdeki tüm emekleri için çok teşekkür ederim.

Çalışmamda desteğini ve güvenini asla esirgemeyen, çalışmam için gerekli ortamı sağlayan eşim Çiler GÖKGÖZ'e ve bu süreçte bizimle daha çok ilgilenen annem Fatma SATIRLI'ya teşekkür ederim.

Çabamın hep arkasında olan manevi desteklerini her zaman yanımda hissettiğim babam İbrahim GÖKGÖZ, annem Yaşar GÖKGÖZ ve kardeşim Özkan GÖKGÖZ'e teşekkür ederim.

Lisansüstü öğrenimime devam edebilmem için ders programımın düzenlenmesine imkân sağlayan Milli Eğitim Bakanlığı ve ilgili personellerine teşekkür ederim.

Dolaylı olarak başarımda katkısı olan beni yetiştiren Dokuz Eylül Üniversitesi İlköğretim Matematik Öğretmenliği programı hocalarına teşekkür ederim.

Çalışmamın sonunda tezimi tekrar tekrar okuyarak eleştirileriyle yol gösteren değerli hocam Doç. Dr. Yasemin ÇENGELLENMİŞ'e teşekkür ederim.

Bu çalışma eşim Çiler GÖKGÖZ ve kızım Zeynep Bilge GÖKGÖZ'e ithaf olunur…

İÇİNDEKİLER

ÖZET i

ABSTRACT iii

ÖNSÖZ v

İÇİNDEKİLER vi

SİMGELER VE KISALTMALAR DİZİNİ viii

BÖLÜM 1

GİRİŞ 1

BÖLÜM 2

ÖN BİLGİLER

2.1. Lineer Kodlar 4

2.2. Cyclic Kodlar 9

BÖLÜM 3

$\mathbb{F}_2 + u\mathbb{F}_2$ HALKASI ÜZERİNDEKİ CYCLIC VE CONSTACYCLIC KODLAR

3.1. $\mathbb{F}_2 + u\mathbb{F}_2\left(u^2 = u\right)$ Halkası Üzerindeki Cyclic Kodlar İle $\mathbb{F}_2$ Cismi Üzerindeki Cyclic Kodlar Arasındaki İlişki 15

3.2. $\mathbb{F}_2 + u\mathbb{F}_2\left(u^2 = 0 \text{ ya da } u^2 = 1\right)$ Halkaları Üzerindeki Cyclic ve $(1+u)-$ Constacyclic Kodlar 47

BÖLÜM 4

$\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ HALKASI ÜZERİNDEKİ CYCLIC VE CONSTACYCLIC KODLAR

4.1. $u^2 = 0$ Durumunda $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ Halkası Üzerindeki Cyclic Kodlar İle $\mathbb{F}_{p^k}$ Cismi Üzerindeki Cyclic Kodlar Arasındaki İlişki 62

4.2. $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ $\left(u^2 = 0\right)$ Halkası Üzerindeki p^s Uzunluklu Constacyclic Kodlar 80

BÖLÜM 5

$\mathbb{F}_P + u\mathbb{F}_P + u^2\mathbb{F}_P$ HALKASI ÜZERİNDEKİ CYCLIC VE $\left(1-u^2\right)-$ CONSTACYCLIC KODLAR

5.1. $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ Halkası Üzerindeki $\left(1-u^2\right)-$Constacyclic Kodlar 96

5.2. $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ $\left(u^2 = 0 \text{ ya da } u^2 = 1\right)$ Halkaları Üzerindeki Cyclic Kodlar 104

5.3. $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ $\left(u^2 = 0\right)$ Halkası Üzerindeki Cyclic Kodlar 109

BÖLÜM 6

SONUÇLAR VE TARTIŞMA 115

KAYNAKLAR 117

ÖZGEÇMİŞ 119

SİMGELER VE KISALTMALAR DİZİNİ

$\mathbb{F}_q = GF(q)$: q elemanlı Galois Cismi

$[n,k,d]-$ lineer kod: Uzunluğu n olan, boyutu k, uzaklığı d olan lineer kod

$\tilde{h}(x)$: $h(x)$ polinomunun reciprocal polinomu

$GR(R,r)$: Temel asal polinomunun derecesi r olan Galois Halkası

$|C|$: C kodunun eleman sayısı

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

d_H, d_L, d_{hom} : Sırasıyla Hamming, Lee ve Homogeneous uzaklık fonksiyonları

w_H, w_L, w_{hom} : Sırasıyla Hamming, Lee ve Homogeneous ağırlık fonksiyonları

Φ : Gray dönüşümü

σ : Cyclic kaydırma dönüşümü

υ : Constacyclic kaydırma dönüşümü

$\sigma^{\otimes s}$: s indexli quasi-cyclic kaydırma dönüşümü

$\pi^{\otimes p^{k-1}}$: Nechaev Permütasyonu

$Tor(C)$: C kodunun torsiyon kodu

$Res(C)$: C kodunun rezidü kodu

$N(r)$: r elemanının nilpotentlik derecesi

BÖLÜM 1

GİRİŞ

Kodlama Teorisi çalışmaları elektronik iletişimde hataların belirlenmesi ve belirlenen hataların düzeltilmesi amacıyla 1950'lerde başlamıştır. See Shannon'un 1948'de yayımlanan " A mathematical theory of communication" ve R.W. Hamming'in 1950'de yayımlanan "Error detecting and error correcting codes" isimli çalışmaları Cebirsel Kodlama Teorisinin başlangıcı kabul edilir. 1990'lı yıllarda lineer olmayan kodlarla $\mathbb{Z}_4$ üzerindeki kodlar arasında ilişki kurulmuş ve halkalar üzerindeki kodların çalışılmasının önünü açılmıştır ve farklı kod alfabeleri üzerinde çalışılmaya başlanmıştır. Çalışmalar Hamming metriği olmayan metriklerde kullanılarak genişletilmiştir. Cebirsel Kodlama Teorisinin önemli problemlerinden biri yeni ve paremetreleri iyi kodlar yazmaktır. Kodun uzunluğu, kod sözcüğü sayısı ve kodun minimum uzaklığı kodun parametrelerini oluşturur. Kod uzunluğunun küçük olması kodun hızlı bir biçimde iletilmesini , kod sözcüğünün fazla olması fazla mesajın iletilmesini, kodun minimum uzaklığının büyük olması daha fazla hatanın tespitini ve çözülebilir olmasını sağlar. Bu tezde belirli halkalar üzerinde bilinen kodlar kullanılarak yeni kodların elde edilebileceği gösterilmiştir.

2. Bölümde Lineer kodlar, cyclic kodlarla ilgili genel bilgiler verilmiştir.

3.1. Bölümde $R = \mathbb{F}_2 + u\,\mathbb{F}_2 \left(u^2 = u\right)$ halkası üzerinde n uzunluklu bir C lineer kodu ve Gray dönüşümü yardımıyla $\mathbb{F}_2$ üzerinde n uzunluklu iki farklı lineer kod tanımlanmıştır. Tanımlanan bu iki kodun üreteç matrisleri, üreteç polinomları

kullanılarak sırasıyla C kodu için üreteç matrisi ve üreteç polinomu elde edilmiştir. C kodunun uzunluğunun tek olması durumunda tanımlanan iki kodun idempotent üreteçlerinden C kodu için bir idempotent üreteç elde edilmiştir. Benzer sonuçlar dual kodlar için de yazılmıştır. 3.2. Bölümde $R_1 = \mathbb{F}_2 + u\,\mathbb{F}_2 \left(u^2 = 1\right)$ halkasının $R_0 = \mathbb{F}_2 + u\,\mathbb{F}_2$ $\left(u^2 = 0\right)$halkasına izomorf olduğu gösterilmiştir. R_0 halkası üzerindeki cyclic kodlarla $\left(1+u\right)-$constacyclic kodlar arasındaki ilişki ve R_0 halkası üzerindeki $\left(1+u\right)-$ constacyclic kodlarla ikili cyclic kodlar arasındaki ilişki verilmiştir. $R_0^{\,n}$'den $\mathbb{F}_2^{\,2n}$ vektör uzayı üzerine tanımlanan Gray dönüşümü kullanılarak R_0 halkası üzerindeki n uzunluğunda bir $\left(1+u\right)-$constacyclic kodun Gray dönüşümü altındaki görüntüsünün $2\cdot n$ uzunluğunda bir cyclic kod olduğu gösterilmiştir. R_0 halkası üzerinde n uzunluğunda bir cyclic kodun Gray dönüşümü altındaki görüntüsünün ise $2\cdot n$ uzunluğunda bir cyclic koda denk kod olduğu gösterilmiştir. n sayısının tek sayı olması durumunda R_0 halkası üzerinde n uzunluğundaki bir cyclic koda karşılık bir $\left(1+u\right)-$ constacyclic kodun elde edildiği gösterilmiştir.

4.1.Bölümde 3.2. Bölümde $R_0 = \mathbb{F}_2 + u\,\mathbb{F}_2 \left(u^2 = 0\right)$ halkası üzerinde yapılan çalışmalar; p bir asal sayı, $k \in \mathbb{N}$ ve $\mathbb{F}_{p^k} = GF\left(p^k\right)$ olmak üzere; $R = \mathbb{F}_{p^k} + u\,\mathbb{F}_{p^k}$ $\left(u^2 = 0\right)$ halkasına genelleştirilmiştir. Genel durumda $p = 2$ ve $k = 1$ alındığında 3.2.Bölümdeki sonuçlar elde edilmiştir. 4.2. Bölümde; p bir asal sayı olmak üzere; $R = \mathbb{F}_{p^k} + u\,\mathbb{F}_{p^k} \left(u^2 = 0\right)$ halkası üzerindeki p^s uzunluklu constacyclic kodlar çalışılmıştır. Bu bölümde ilk olarak R üzerinde n uzunluklu bir $\lambda-$constacyclic kodun dualinin bir $\lambda^{-1}-$constacyclic kod olduğu gösterilmiştir. Ayrıca R üzerinde n uzunluklu bir C kodu için $Tor\left(C\right)$ ve $Res\left(C\right)$ kodlar tanımlanmış ve C kodunun eleman sayısıyla $Tor\left(C\right)$ ve $Res\left(C\right)$ kodların eleman sayıları arasındaki ilişki verilmiştir. Daha sonra $\mathbb{F}_{p^k}$ sonlu cismi üzerindeki p^s uzunluklu $\lambda-$constacyclic kodlar için yapılan çalışmalar R halkası üzerinde $\alpha + u\cdot\beta-$constacyclic kodlara taşınmıştır. 4.1. Bölümde $R = \mathbb{F}_{p^k} + u\,\mathbb{F}_{p^k} \left(u^2 = 0\right)$ halkası üzerinde keyfi n uzunluklu

bir cyclic koda karşılık bir $(1-u)-$constacyclic kod elde edilmiştir. Son olarak; γ, $\mathbb{F}_{p^k}$ cisminin sıfırdan farklı bir elemanı olmak üzere; R halkası üzerinde p^s uzunluklu bir cyclic koda karşılık bir $\gamma-$constacyclic kod verecek bir izomorfizma tanımlanmıştır.

5.1. Bölümde $R=\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2\ (u^3=0)$ halkasından $\mathbb{F}_2$ cismi üzerine uygun bir Gray dönüşümü tanımlanmış ve daha önceki bölümlerde tanımmlanan $\sigma,\upsilon,\mu,\bar{\mu},\sigma^{p^k-1}$ dönüşümlere benzer dönüşümler R halkası ve $\mathbb{F}_2^{\,4}$ vektör uzayı üzerinde tanımlanmıştır. 3.2. ve 4.1. Bölümdeki Nechaev permütasyonu kullanılanarak $\pi^{\otimes 2}$ permütasyonu tanımlanmıştır. 3.2. ve 4.1. Bölümdeki sonuçlar bu dönüşümler kullanılarak R halkası üzerine genelleştirilmiştir. 5.2. Bölümde $R=\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$ $(u^3=1)$halkasından $\mathbb{F}_3^{\,3}$ vektör uzayına yeni bir Gray dönüşümü tanımlanmış ve bu Gray dönüşümü kullanılarak R halkası üzerinde n uzunluklu bir cyclic kodun bu dönüşüm altındaki görüntüsünün indexi 3 olan bir quasi-cyclic kod olduğu gösterilmiştir. $S=\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3\ (u^3=0)$ halkasının R halkasına izomorf olduğu gösterilmiş ayrıca S halkası üzerinde n uzunluklu bir lineer koda permütasyon denk bir kod için üreteç matrisi elde edilmiştir. Daha sonra R ve S halkaları üzerindeki izomorfizma kullanılarak R halkası üzerindeki n uzunluklu bir lineer koda permütasyon denk bir kod için üreteç matrisi verilmiştir. 5.3. Bölümde $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ $(u^3=0)$ halkası üzerinde yapılan çalışmalar p bir asal olmak üzere $R=\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p\ (u^3=0)$halkası üzerine genelleştirilmiştir.

BÖLÜM 2

ÖN BİLGİLER

2.1. Lineer Kodlar

2.1.1.Tanım: Alfabe olarak adlandırılan $A=\{a_1,a_2,\ldots,a_r\}$ sonlu kümesinden alınan elemanların oluşturduğu sonlu dizilerin kümesine $r-$**ary kod** denir. $A^n=\{(x_1,x_2,\ldots,x_n)\mid x_i\in A,\ i=1,2,\ldots,n\}$ kümesinin elemanlarına **sözcük** denir. A^n kümesinin herhangi bir C alt kümesine n uzunluğunda bir $r-$ary kod ve C kodunun elemanlarına da **kod sözcüğü** denir. (Ling, Xing, 2004, s.5)

2.1.2.Tanım: $\mathbb{F}_q{}^n$**,** $\mathbb{F}_q$ sonlu cismi üzerinde n boyutlu vektör uzayı olsun. $\mathbb{F}_q{}^n$ vektör uzayının M elemanlı bir C alt kümesine bir $(n,M)-$**kod** denir. (Ling, Xing, 2004, s.5) □

$\mathbb{F}_2$, $\mathbb{F}_3$ ve $\mathbb{F}_4$ cisimleri üzerindeki kodlara sırasıyla ikili (binary), üçlü (ternary) ve dörtlü (quaternary) kodlar denir (Huffman & Pless, 2003, s.3).

2.1.3.Tanım: $\mathbb{F}_q{}^n$ vektör uzayının boyutu k olan bir C alt vektör uzayına $\mathbb{F}_q$ üzerinde bir $[n,k]-$**lineer kod** denir. (Roman, 1992, s.197)

2.1.4.Tanım: Sonlu, değişmeli, birimli, yerel ve p asal olmak üzere maksimal ideali (p) olan bir R halkasına **Galois halkası** denir. (Holdman, 2016) □

Eğer R halkasının idealleri küme kapsama bağıntısına göre tam sıralı ise R halkasına bir zincir halkası denir. Bir zincir halkasının tek maximal ideali tüm nilpotent elemanları içerir. Bir R zincir halkasının tüm idealleri esas idealdir. Bir sonlu zincir halkasının üreteci u olan $\langle u \rangle$ maximal ideali düşünülsün. R sonlu olduğundan $\cdots \subsetneq \langle u^j \rangle \subsetneq \cdots \subsetneq \langle u^2 \rangle \subsetneq \langle u^1 \rangle \subsetneq \langle u^0 \rangle = R$ zinciri bir sonlu zincirdir. Bu durumda öyle bir j için $\langle u^j \rangle = \langle 0 \rangle$ sağlanır. $\langle u^j \rangle = \langle 0 \rangle$ koşulunu sağlayan en küçük doğal sayı t ise t sayısına u elemanının nilpotentlik derecesi denir. Bu durumda p bir asal sayı olmak üzere rezidü cismi $\mathbb{F} = R/\langle u \rangle$ $q = p^t$ tane eleman içerir ve $Char\mathbb{F} = p$ sağlanır. Galois halkaları veya $\mathbb{F}_q[u]/\langle u^i \rangle$ biçimindeki halkalar esas ideal halkalarıdır. (Flaut, 2000)

p bir asal sayı olmak üzere $\mathbb{F}_p$ p elemanlı sonlu cisim olsun. m pozitif bir tam sayı ve u bir değişken olmak üzere; $R = \mathbb{F}_p[u]/\langle u^m \rangle = \left\{ \overline{r_0 + r_1 u + r_2 u^2 + \cdots + r_{m-1} u^{m-1}} \,\middle|\, u^m = 0, 0 \le i \le m-1 \text{ için } r_i \in \mathbb{F}_p \right\}$ halkası düşünülsün. R halkası $u^m = 0$ koşuluyla halka olan $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + \cdots + u^{m-1}\mathbb{F}_p$ halkasına izomorftur. R bölüm halkası $\langle u \rangle$ maksimal idealli bir yerel halkadır. $f(x) \in R[x]$ elemanının modülo u indirgenmiş polinomu $\overline{f(x)}$ olmak üzere $\overline{f(x)}$ polinomu $\mathbb{F}_p[x]$ polinom halkasında indirgenemez ise $f(x)$ polinomuna **temel asal polinom** denir. $h(x) \in R[x]$ temel asal bir polinom ve $d^o h = r$ olmak üzere $GR(R,r) = R[x]/\langle h(x) \rangle$ bölüm halkası bir Galois halkasıdır. $GR(R,r)$ Galois halkası $\langle u \rangle$ maksimal idealli ve $\mathbb{F}_{p^r}$ rezidü cisimli yerel halkadır. (Kai, Zhu, Li, 2010)

2.1.5.Tanım: R bir Galois halkası olmak üzere R^m kümesi bir $R-$modüldür. R^m 'nin bir C alt modülüne R **halkası üzerinde bir lineer kod** denir. (Holdman, 2016, s.47)

2.1.6.Tanım: $(R,+,\cdot)$ bir halka , A bir $R-$modül ve X A'nın bir tabanı olsun. Bu durumda A $R-$modülüne X kümesi üzerinde bir **serbest** $R-$**modül** denir. (Hungerford, 1974, s.181)

R birimli, sonlu ve değişmeli bir halka olsun. R halkası üzerinde n uzunluğunda bir C lineer kodu R^n 'in bir $R-$alt modülüdür. Bir alt modülün bir serbest modül olması gerekmez. (Flaut, 2000)

2.1.7.Tanım: C $\mathbb{F}_q$ üzerinde n uzunluğunda bir lineer kod olsun.

i. $\mathbb{F}_q^{\,n}$ vektör uzayının C alt uzayının ortagonal tümleyenine C kodunun dual kodu denir ve $C^{\perp}$ biçiminde gösterilir.

ii. C kodunun $\mathbb{F}_q$ üzerinde bir vektör uzayı olarak boyutuna C lineer kodunun boyutu denir ve $boy(C)$ biçiminde gösterilir. (Ling, Xing, 2004, s.45)

2.1.1.Lemma: C $\mathbb{F}_q$ cismi üzerinde bir $[n,k]-$lineer kod ise $C^{\perp}$ kodu $\mathbb{F}_q$ cismi üzerinde bir $[n,n-k]-$lineer koddur. (Hill, 1986, s.68)

2.1.1.Teorem: C, $\mathbb{F}_q$ üzerinde n uzunluğunda bir lineer kod ise

i. $|C|=q^{boy(C)}$ sağlanır.

ii. $C^{\perp}$ lineer kod ve $boy(C)+boy(C^{\perp})=n$ sağlanır.

iii. $(C^{\perp})^{\perp}=C$ sağlanır. (Ling, Xing, 2004, s.45)

2.1.1.Örnek: $\mathbb{F}_2$ cismi üzerinde 4 uzunluklu

$C=\{(0,0,0,0),(1,0,1,0),(0,1,0,1),(1,1,1,1)\}$ lineer kodu düşünülsün.

$C^{\perp}=\{(0,0,0,0),(1,0,1,0),(0,1,0,1),(1,1,1,1)\}=C$ olduğunu görmek kolaydır. Ayrıca $boy(C)=boy(C^{\perp})=2$ sağlanır. (Ling, Xing, 2004, s.46)

2.1.2.Örnek: $\mathbb{F}_3=\{0,1,\omega\}\,(\omega^{-1}=\omega)$ cismi üzerinde 3 uzunluklu

$C=\{(0,0,0),(0,0,1),(0,0,\omega),(0,1,0),(0,\omega,0),(0,1,1),(0,1,\omega),(0,\omega,1),(0,\omega,\omega)\}$

lineer kodu düşünülsün. Bu durumda $C^{\perp}=\{(0,0,0),(1,0,0),(\omega,0,0)\}$ elde edilir. $boy(C)=2$ ve $boy(C^{\perp})=1$ olduğundan $boy(C)+boy(C^{\perp})=3$ sağlanır. (Ling, Xing, 2004, s.46)

2.1.8.Tanım: x ve y bir A alfabesinin n uzunluklu iki sözcüğü olsun. x ve y sözcüklerinin birbirinden farklı koordinatların sayısına x ve y sözcükleri arasındaki Hamming uzaklığı denir ve $d_H(x,y)$ olarak gösterilir. (Ling, Xing, 2004, s.9)

$$d_H : A^n \times A^n \to \mathbb{N} \cup \{0\}$$
$$(x,y)=((x_1,x_2,\ldots,x_n),(y_1,y_2,\ldots,y_n)) \mapsto d_H(x,y)=\left|\{i \mid x_i \neq y_i\}\right|$$

biçiminde tanımlanan fonksiyon Hamming uzaklık fonksiyonudur ve A^n kümesi üzerinde bir metriktir. (Ling, Xing, 2004, s.9)

2.1.9.Tanım: $\mathbb{F}_q{}^n$ vektör uzayının herhangi bir x elemanının Hamming ağırlığı onun sıfırdan farklı koordinatlarının sayısı olarak tanımlanır ve $w_H(x)$ olarak gösterilir. (Ling, Xing, 2004, s.46)

2.1.10.Tanım: Herhangi bir $c=(c_0,c_1,\ldots,c_{n-1}) \in \mathbb{F}_q{}^n$ kod sözcüğünün Hamming ağırlığı $w_H(c)=\sum_{i=1}^{n-1} w_H(c_i)$ 'dir. (Ling, Xing, 2004, s.47)

Bu durumda; $0=(0,0,\ldots,0) \in \mathbb{F}_q{}^n$ olmak üzere $w_H(x)=d_H(x,0)$ sağlanır. (Ling, Xing, 2004, s.46)

2.1.11.Tanım: $\mathbb{F}_q$ cismi üzerinde n uzunluğunda bir C kodunun farklı kod sözcükleri arasındaki uzaklıkların en küçüğüne C kodunun **minimum uzaklığı** veya sadece **uzaklığı** denir ve $d_H(C)$ biçiminde gösterilir. (Huffman, Pless, 2003, s.8)

2.1.12.Tanım: C $\mathbb{F}_q$ cismi üzerinde tanımlı n uzunluğunda bir kod (lineer olması gerekmez) bir kod olsun. C kodunun sıfırdan farklı elemanlarının Hamming ağırlıklarının en küçüğüne C kodunun minimum Hamming ağırlığı denir ve $w_H(C)$ biçiminde gösterilir. (Ling, Xing, 2004, s.48)

2.1.2.Lemma: Eğer $x, y \in \mathbb{F}_q^{\,n}$ ise $d_H(x,y) = w_H(x-y)$ sağlanır. (Huffman, Pless, 2003, s.8)

2.1.2.Lemma bir lineer kodunun minimum uzaklığının kodun minimum ağırlığına eşit olduğu sonucunu verir.

Bir alfabe üzerinde birçok metrik tanımlanabilir. Hamming metriği bir alfabe üzerinde tanımlanabilecek metriklerden sadece biridir. Hamming metriği için yapılan tanımlar benzer biçimde tanımlanacak yeni metrik için de yapılır.

2.1.1.Not: n uzunluklu, d minimum uzaklıklı ve M tane elemanı olan bir C kodu $(n, M, d)-$kod ve uzunluğu n, boyutu k, minimum uzaklığı d olan bir C lineer kodu ise $[n, k, d]-$kod ile gösterilir. (Roman, 1992, s.145)

C bir $[n, k, d]-$kod olsun. C kodunun eleman sayısı büyüdükçe karşılık gelen mesaj sayısı da artar. Minimum uzaklık büyüdükçe daha çok hata düzeltilebilir. Bunların yanı sıra kodun eleman sayısının büyümesi minimum uzaklığının küçülmesine neden olur. (Çengellenmiş, 2005, s.24)

2.1.13.Tanım: Satırları bir C $[n, k]-$lineer kodu için taban olan $k \times n$ boyutlu G matrisine C kodu için bir üreteç matrisi denir. (Huffman, Pless, 2003, s.4)

2.1.3.Örnek: Üreteç matrisi $G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ olan $\mathbb{F}_2$ üzerinde 4 uzunluklu bir C $[4,3]-$lineer kodu düşünülsün. C kodunun 2^3 tane elemanı olduğundan 2^3 tane mesajı kodlamada kullanılır. Mesajlar $\mathbb{F}_2^{\,3}$ vektör uzayının elemanlarıyla tanımlanır. Bir mesaja karşı gelen vektör $(x_1, x_2, x_3) \in \mathbb{F}_2^{\,3}$ vektörü olsun. Mesaj vektörünün belirttiği $[x_1 \; x_2 \; x_3]$ satır matrisi ile C kodunun G üreteç matrisinin çarpılmasıyla elde edilen

$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = \begin{bmatrix} x_1 + x_3 & x_1 + x_2 & x_2 + x_3 & x_2 \end{bmatrix}$ satır matrisinin belirttiği $(x_1 + x_3, x_1 + x_2, x_2 + x_3, x_2)$ vektör mesajın kodlanmış hâlidir ve C koduna ait kod sözcüğüdür. (Roman, 1992, s.198)

2.1.14.Tanım: Bir C lineer kodunun $C^{\perp}$ dual kodunun H üreteç matrisine C kodu için bir **parity check matrisi** denir. (Ling, Xing, 2004, s.52)

2.1.3.Lemma: Bir C $[n,k]-$kodu için standart formdaki bir üreteç matrisi $G = (I_k | X)$ ise $H = (-X^T | I_{n-k})$ matrisi C kodu için bir parity-check matrisidir. (Ling, Xing, 2004, s.55)

2.1.15.Tanım: C_1 ve C_2 iki lineer kod olsun. Bir kodun kod sözcüklerinin bileşenlerine bir permütasyon uygulandığında diğer kodun kod sözcükleri elde ediliyorsa C_1 ve C_2 kodlarına **permütasyon denk kod** denir. (Huffman, Pless, 2003, s.19)

2.1.4.Örnek: $\mathbb{F}_2$ cismi üzerinde uzunluğu 4 olan $C_1 = \{(0,0,0,0),(0,1,0,1),(0,0,1,0),(0,1,1,1)\}$ kodunun kod sözcüklerinin koordinatlarına $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ permütasyonu uygulanmasıyla C_1 koduna permütasyon denk $C_2 = \{(0,0,0,0),(1,1,0,0),(0,0,0,1),(1,1,0,1)\}$ kodu elde edilir. (Ling, Xing, 2004, s.56)

2.2.Cyclic Kodlar

2.2.1.Tanım: λ R sonlu halkasının tersi olan bir elemanı ve C R üzerinde n uzunluğunda bir kod olsun. Eğer

$$\tau_\lambda : R^n \to R^n$$
$$x = (x_0, x_1, x_2, \ldots, x_{n-1}) \mapsto \tau_\lambda(x) = (\lambda \cdot x_{n-1}, x_0, x_1, \ldots, x_{n-2})$$

dönüşümü için $\tau_\lambda(C) = C$ sağlanıyorsa C koduna bir $\lambda-$**constacyclic kod** denir.

$\lambda = 1$ ise bu koda **cyclic kod**, $\lambda = -1$ ise bu koda **negacyclic kod** denir. (Dinh, 2010)

2.2.1.Teorem: R sonlu bir halka olmak üzere,

$$\pi : R^n \to R[x] \Big/ \langle x^n - \lambda \rangle$$
$$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto \pi(c) = \overline{c_0 + c_1 \cdot x + \ldots + c_{n-1} \cdot x^{n-1}}$$

dönüşümü tanımlansın. C R üzerinde n uzunluğunda bir lineer kod olsun. C kodu bir $\lambda -$ constacyclic kod ise $\pi(C)$ kümesi $R[x] \Big/ \langle x^n - \lambda \rangle$ halkasının bir idealidir. Bu ifadenin tersi de doğrudur. (Dinh, 2010)

2.2.1.Örnek: $\mathbb{F}_3 = \{0, 1, \omega\} \left(\omega^{-1} = \omega\right)$ cismi üzerinde 3 uzunluğundaki $C = \{(0,0,0), (1,1,1), (\omega, \omega, \omega)\}$ cyclic kodu için $\pi(C) = \left\{\bar{0}, \overline{1 + x + x^2}, \overline{\omega + \omega \cdot x + \omega \cdot x^2}\right\}$ kümesi $\mathbb{F}_3[x] \Big/ \langle x^3 - 1 \rangle$ halkasının bir idealidir. (Ling, Xing, 2004, s.137)

2.2.1.Lemma: $\mathbb{F}_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının her $I \neq \{\bar{0}\}$ ideali içinde tek türlü belirli minimum dereceli monik bir polinom vardır. (Ling, Xing, 2004, s.138)

2.2.2.Teorem: $\mathbb{F}_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının bir $I \neq \{\bar{0}\}$ ideali ve $\overline{g(x)}$ I idealinin minimum dereceli, sıfır olmayan monik bir polinomu ise $\overline{g(x)}$ elemanı I idealinin bir üreteci ve $g(x)$ polinomu $x^n - 1$ polinomunun bir bölenidir. (Ling, Xing, 2004, s.136)

2.2.2.Tanım: $\mathbb{F}_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının $I \neq \{\bar{0}\}$ ideali içinde tek türlü belirli minimum dereceli monik polinoma I idealinin üreteç polinomu denir. (Ling, Xing, 2004, s.138)

2.2.3.Tanım: $\mathbb{F}_q$ cismi üzerindeki bir C cyclic kodu için $\pi(C)$ idealinin üreteç polinomuna C cyclic kodunun **üreteç polinomu** denir. (Huffman, Pless, 2003, s.126)

2.2.1.Önerme: $x^n-1\in\mathbb{F}_q[x]$ polinomunun herhangi bir monik $f(x)$ böleni için $\overline{f(x)}\in \mathbb{F}_q[x]\Big/\langle x^n-1\rangle$ elemanı $\mathbb{F}_q$ cismi üzerinde n uzunluğundaki bir cyclic kodun üreteç polinomudur. (Ling, Xing, 2004, s.138)

2.2.1.Sonuç: $\mathbb{F}_q$ cismi üzerinde n uzunluğundaki cyclic kodlarla $x^n-1\in\mathbb{F}_q[x]$ polinomunun monik bölenleri arasında birebir eşleme vardır. (Ling, Xing, 2004, s.138)

2.2.3.Teorem: $p_1(x), p_2(x),\ldots, p_r(x)$ birbirinden farklı, monik, $\mathbb{F}_q$ üzerinde asal polinomlar ve her $i=1,2,\ldots,r$ için $e_i\geq 1$ olmak üzere $x^n-1\in\mathbb{F}_q[x]$ polinomu $x^n-1=\prod_{i=1}^{r} p_i^{e_i}(x)$ biçiminde çarpanlara ayrılsın. Bu durumda $\mathbb{F}_q$ üzerinde n uzunluğunda $\prod_{i=1}^{r}(e_i+1)$ tane cyclic kod vardır. (Ling, Xing, 2004, s.139)

2.2.2.Örnek: $\mathbb{F}_2$ cismi üzerinde 7 uzunluğundaki cyclic kodlar için x^7-1 polinomu $x^7-1=(x+1)\cdot(x^3+x+1)\cdot(x^3+x^2+1)\in\mathbb{F}_2[x]$ biçiminde monik asal polinomların çarpımı biçiminde yazılır. Bu durumda 1, $x+1$, x^3+x+1 , x^3+x^2+1, $x^4+x^3+x^2+1$, $x^4+x^2+x+1, x^6+x^5+x^4+x^3+x^2+x+1$, x^7+1 polinomlarını üreteç polinomu kabul eden $\mathbb{F}_2$ cismi üzerinde 7 uzunluğunda 8 tane cyclic kod vardır. (Ling, Xing, 2004, s.140)

2.2.2.Önerme: C $\mathbb{F}_q$ cismi üzerinde n uzunluğunda bir cyclic kod olsun.

i. C cyclic kodunun üreteç polinomu $g(x)$ ve $d^\circ(g(x))=r$ ise $boy(C)=n-r$ 'dir.

ii. C cyclic kodunun üreteç polinomu $g(x)=g_0+g_1x+\cdots+g_rx^r$ ise $g_0\neq 0$ 'dır. C kodunun üreteç matrisi

$$G=\begin{pmatrix} g_0 & g_1 & g_2 & \cdots & & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & & g_r & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & & g_r \end{pmatrix}_{(n-r)\times n}$$

Biçimindedir. (Roman, 1992, s.321)

2.2.4.Tanım: C $\mathbb{F}_q$ cismi üzerinde cyclic $[n,n-r]-$kod olsun. C kodunun üreteç polinomu $g(x)$, x^n-1 polinomun bir böleni olduğundan $x^n-1=g(x)\cdot h(x)$ olacak biçimde derecesi $n-r$ olan bir $h(x)\in\mathbb{F}_q[x]$ vardır. Bu koşulu sağlayan $h(x)$ polinomuna C kodunun **check polinomu** denir. (Roman, 1992, s.325)

2.2.3.Önerme: $h(x)$ polinomu $\mathbb{F}_q$ cismi üzerinde n uzunluğundaki bir cyclic C kodunun check polinomu olsun.

i. Eğer $h(x)=h_0+h_1x+\cdots+h_{n-r}x^{n-r}$ ise

$$H=\begin{pmatrix} h_{n-r} & \cdots & & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & & h_0 & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & & h_0 \end{pmatrix}$$

matrisi C cyclic kodunun bir parity-check matrisidir.

ii. $C^{\perp}$ dual kodu r boyutlu ve

$h^{\perp}(x)=h_0^{-1}x^{n-r}\ h(x^{-1})=h_0^{-1}(h_0x^{n-r}+h_1x^{n-r-1}+\cdots+h_{n-r})$ üreteç polinomlu cyclic koddur. (Roman, 1992, s.325)

2.2.3.Örnek: x^9-1polinomunun $\mathbb{F}_2$ cismi üzerinde

$$x^9-1=(x^3)^3-1=(x^3-1)\cdot(x^6+x^3+1)=(x-1)\cdot(x^2+x+1)\cdot(x^6+x^3+1)\in\mathbb{F}_2[x]$$

biçiminde asal çarpanlarına ayrılır. Bu durumda $\mathbb{F}_2$ cismi üzerinde 9 uzunluğunda 8 tane cyclic kod vardır.

Üreteç polinomu x^6+x^3+1 olan $\mathbb{F}_2$ cismi üzerinde 9 uzunluğundaki C cyclic kodunun boyutu 3 ve üreteç matrisi $G=\begin{pmatrix}1&0&0&1&0&0&1&0&0\\0&1&0&0&1&0&0&1&0\\0&0&1&0&0&1&0&0&1\end{pmatrix}$ matrisidir. $h(x)=(x-1)\cdot(x^2+x+1)=x^3-1$ polinomu C cyclic kodunun check polinomudur. Bu durumda $h^{\perp}(x)=x^3\cdot(x^{-3}-1)=x^3+1$ polinomu $C^{\perp}$ dual kodunun üreteç polinomu ve $H=\begin{pmatrix}1&0&0&1&0&0&0&0&0\\0&1&0&0&1&0&0&0&0\\0&0&1&0&0&1&0&0&0\\0&0&0&1&0&0&1&0&0\\0&0&0&0&1&0&0&1&0\\0&0&0&0&0&1&0&0&1\end{pmatrix}$ matrisi C cyclic kodunun parity-check matrisidir . (Roman, 1992, s.326)

Üreteç polinomlarının yanı sıra bir cyclic kodu üretmekte kullanılabilecek bir çok polinom vardır. Bu polinomlardan biri idempotent üreteç olarak isimlendirilen özel bir polinomdur.

2.2.5.Tanım: $\overline{e(x)}\in \mathbb{F}_q[x]/\langle x^n-1\rangle$ için $\overline{e(x)}^2=\overline{e(x)}$ oluyorsa $\overline{e(x)}$ elemanına bir **idempotent eleman** denir. (Huffman & Pless, 2003, s.132) □

2.2.2.Lemma: $\mathbb{F}_q$ halkası üzerindeki herhangi bir C cyclic kodu için $\mathbb{F}_q[x]/\langle x^n-1\rangle$ halkasının $\pi(C)$ idealinin tek türlü belirli idempotent bir üreteci vardır. (Huffman, Pless, 2003, s.132)

2.2.6.Tanım: $\mathbb{F}_q$ halkası üzerindeki herhangi bir C cyclic kodu için $\pi(C)$ idealinin idempotent üretecine C cyclic kodun **idempotent üreteci** denir. (Huffman, Pless, 2003, s.132)

2.2.4.Önerme: C $\mathbb{F}_q$ üzerinde idempotent üreteci $\overline{e(x)}$ olan bir cyclic kod olsun. Bu durumda $g(x)=\left(e(x),x^n-1\right)_{EBOB}\in\mathbb{F}_q[x]$ polinomu C kodunun üreteç polinomudur. (Huffman, Pless, 2003, s.133)

2.2.4.Önerme $\mathbb{F}_q$ üzerindeki bir cyclic kodun idempotent üretecinden üreteç polinomunun elde edilişini gösteriyor.

2.2.4.Örnek: $\mathbb{F}_2$ üzerinde 7 uzunluklu, $g_i(x)$ üreteç polinomlu, $\overline{e_i(x)}$ idempotent üreteçli tüm C_i cyclic kodlar aşağıdaki tablodaki gibi verilir.

i	$boy(C_i)$	$g_i(x)$	$\overline{e_i(x)}$
0	0	$1+x^7$	$\bar{0}$
1	1	$1+x+x^2+\cdots+x^6$	$\overline{1+x+x^2+\cdots+x^6}$
2	3	$1+x^2+x^3+x^4$	$\overline{1+x^3+x^5+x^6}$
3	3	$1+x+x^2+x^4$	$\overline{1+x+x^2+x^4}$
4	4	$1+x+x^3$	$\overline{x+x^2+x^4}$
5	4	$1+x^2+x^3$	$\overline{x^3+x^5+x^6}$
6	6	$1+x$	$\overline{x+x^2+\cdots+x^6}$
7	7	1	$\bar{1}$

BÖLÜM 3

$\mathbb{F}_2 + u\mathbb{F}_2$ HALKASI ÜZERİNDEKİ CYCLIC VE CONSTACYCLIC KODLAR

Bu bölümde $u^2 = 0$, $u^2 = 1$, $u^2 = u$ farklı durumlarındaki $R = \mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerindeki cyclic ve constacyclic kodlar incelenmiştir.

3.1. $\mathbb{F}_2 + u\mathbb{F}_2 (u^2 = u)$ Halkası Üzerindeki Cyclic Kodlar İle $\mathbb{F}_2$ Cismi Üzerindeki Cyclic Kodlar Arasındaki İlişki

Bu bölümde $R = \mathbb{F}_2 + u\mathbb{F}_2 (u^2 = u)$ halkası üzerindeki cyclic kodlarla ikili cyclic kodlar arasındaki ilişki verilmiştir.

$R = \mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u\}$ kümesi $u^2 = u$ koşulu ile bir halkadır. Bu durumda $R \cong \mathbb{F}_2[u]/(u^2 - u)$ sağlanır. Bu alt bölüm boyunca R halkası denildiğinde $\mathbb{F}_2 + u\mathbb{F}_2 (u^2 = u)$ halkası anlatılmaktadır.

Bu bölümde R^n'den $\mathbb{F}_2^{2\cdot n}$'e tanımlı bir Gray dönüşümü yardımıyla R üzerinde tanımlı n uzunluklu bir C lineer kodu, $\mathbb{F}_2$ cismi üzerinde n uzunluklu iki farklı lineer koda bağlı olarak tanımlanmıştır. Tanımlanan bu iki kodun üreteç matrisleri, üreteç polinomları kullanılarak sırasıyla C kodu için üreteç matrisi ve üreteç polinomu elde edilmiştir. C kodunun uzunluğunun tek olması durumunda tanımlanan iki kodunun

idempotent üreteçlerinden C kodu için bir idempotent üreteç elde edilmiştir. Benzer sonuçlar dual kodlar için de yazılmıştır.

3.1.1.Teorem: $\begin{array}{l}\Phi : R \to \mathbb{F}_2^{\,2} \\ a+u\cdot b \mapsto \Phi(a+u\cdot b)=(a,a+b)\end{array}$ biçiminde tanımlanan Φ Gray dönüşümü bir izomorfizmadır. (Zhu, Wang & Shi, 2010)

Kanıt: Φ dönüşümünün "+" ve "·" işlemlerini koruduğu ve birebir fonksiyon olduğu kolaylıkla gösterilebilir. Ayrıca her $(x,y)\in\mathbb{F}_2^{\,2}$ için $\Phi\left(x+u\cdot(y-x)\right)=\left(x,x+(y-x)\right)=(x,y)\in\mathbb{F}_2^{\,2}$ olacak şekilde en az bir tane $x+u\cdot(y-x)\in R$ vardır.

O halde Φ örtendir.

O halde Φ izomorfizmadır. □

Φ dönüşümü

$$\Phi : R^n \to \mathbb{F}_2^{\,2\cdot n}$$
$$x=(r_1+u\cdot q_1, r_2+u\cdot q_2,\ldots,r_n+u\cdot q_n)\mapsto \Phi(x)=(r_1,r_2,\ldots,r_n,r_1+q_1,r_2+q_2,\ldots,r_n+q_n)$$

biçiminde R^n'e genişletilir. (Zhu vd., 2010)

3.1.1.Önerme: R halkası üzerinde uzunluğu n olan bir lineer kod C kodu olsun. Bu durumda $C_1=\left\{x\in\mathbb{F}_2^{\,n}\,\middle|\,\exists y\in\mathbb{F}_2^{\,n}\ için\ x+u\,y\in C\right\}$,

$C_2=\left\{x+y\in\mathbb{F}_2^{\,n}\,\middle|\,\exists x,y\in\mathbb{F}_2^{\,n}\ için\ x+u\,y\in C\right\}$ biçiminde tanımlanan C_1 ve C_2 $\mathbb{F}_2$ üzerinde tanımlı iki lineer koddur. (Zhu vd., 2010)

Kanıt: C, $R=\mathbb{F}_2+u\cdot\mathbb{F}_2\left(u^2=u\right)$ halkası üzerinde n uzunluklu bir lineer kod ise C, R^n'nin bir $R-$ alt modülüdür.

C_1'in $\mathbb{F}_2^{\,n}$'nin alt vektör uzayı olduğu gösterilecektir.

Herhangi iki $x_1,x_2\in C_1$ için $x_1+u\,y_1\in C$ ve $x_2+u\,y_2\in C$ olacak biçimde en az bir tane $y_1,y_2\in\mathbb{F}_2^{\,n}$ vardır.

$\underset{\substack{(C,+)\\ Abel\ Grup}}{\Rightarrow}\left(x_1+u\cdot y_1\right)+\left(x_2+u\cdot y_2\right)\in C$

$\underset{\substack{(C,+)\\ Abel\ Grup}}{\Rightarrow}\left(x_1+x_2\right)+u\left(y_1+y_2\right)\in C$ olacak şekilde en az bir $y_1+y_2\in C$ vardır.

$\underset{\substack{C_1\text{'in}\\ \text{tanımı}}}{\Rightarrow} x_1 + x_2 \in C_1$ sağlanır.

Her $\lambda \in \mathbb{F}_2$ ve her $x \in C_1$ için $x + u\,y \in C$ olacak şekilde en az bir tane $y \in \mathbb{F}_2^{\,n}$ vardır.

$$\underset{\substack{C \subseteq R^n\\ R-\text{alt}\\ \text{modül}\\ \lambda \in R}}{\Rightarrow} \lambda \cdot (x + u\,y) \in C$$

$$\underset{\substack{C \subseteq R^n\\ R-\text{alt}\\ \text{modül}}}{\Rightarrow} \lambda \cdot x + (\lambda \cdot y)u \in C \text{ olacak şekilde en az bir tane } \lambda \cdot y \in \mathbb{F}_2^{\,n} \text{ vardır.}$$

$$\underset{\substack{C_1\text{'in}\\ \text{tanımı}}}{\Rightarrow} \lambda \cdot x \in C_1 \text{ sağlanır.}$$

O halde C_1 $\mathbb{F}_2^{\,n}$'nin alt vektör uzayıdır.

Herhangi iki $x_1 + y_1$ ve $x_2 + y_2 \in C_2$ için $x_1 + u\,y_1 \in C$ ve $x_2 + u\,y_2 \in C$ olacak şekilde en az iki $x_1, y_1 \in \mathbb{F}_2^{\,n}$ ve $x_2, y_2 \in \mathbb{F}_2^{\,n}$ elemanları vardır.

$$\underset{\substack{(C,+)\\ \text{Abel Grup}}}{\Rightarrow} \text{En az bir } (x_1 + x_2), (y_1 + y_2) \in \mathbb{F}_2^{\,n} \text{ için } (x_1 + x_2) + u(y_1 + y_2) \in C \text{ dir.}$$

$$\underset{\substack{C_2\text{'nin}\\ \text{tanımı}}}{\Rightarrow} (x_1 + x_2) + (y_1 + y_2) \in C_2$$

$$\underset{\substack{+\text{'nın değ.}\\ \text{ve bir. özlğ.}}}{\Rightarrow} (x_1 + y_1) + (x_2 + y_2) \in C_2 \text{ sağlanır.}$$

Her $\lambda \in \mathbb{F}_2$ ve her $x + y \in C_2$ için $x + u\,y \in C$ olacak şekilde en az bir $x, y \in \mathbb{F}_2^{\,n}$ vardır.

$$\underset{\substack{C \subseteq R^n\\ R-\text{alt}\\ \text{modül}\\ \lambda \in R}}{\Rightarrow} \lambda \cdot (x + u\,y) \in C$$

$$\underset{\substack{C \subseteq R^n\\ R-\text{alt}\\ \text{modül}}}{\Rightarrow} (\lambda \cdot x) + (\lambda \cdot y)u \in C \text{ olacak biçimde en az bir } \lambda \cdot x, \lambda \cdot y \in \mathbb{F}_2^{\,n} \text{ vardır.}$$

$$\underset{\substack{C_2\text{'nin}\\ \text{tanımı}}}{\Rightarrow} (\lambda \cdot x) + (\lambda \cdot y) \in C_2$$

$$\Rightarrow \lambda \cdot (x + y) \in C_2 \text{ sağlanır.}$$

O halde C_2 $\mathbb{F}_2^{\,n}$'nin alt vektör uzayıdır.□

3.1.1.Not: 3.1. Bölüm boyunca C, C_1 ve C_2 lineer kodları denildiğinde 3.1.1.Önerme'de tanımlanan kodlar düşünülecektir.

3.1.1.Gösterim: A kümesinin elemanları sıralı m'liler, B kümesinin elemanları sıralı n'liler olmak üzere

$A \otimes B = \left\{ (\omega_1, \omega_2, \ldots \omega_m, \xi_1, \xi_2, \ldots, \xi_n) \middle| (\omega_1, \omega_2, \ldots \omega_m) \in A, (\xi_1, \xi_2, \ldots, \xi_n) \in B \right\}$ 'dir.

3.1.2.Teorem: C, R halkası üzerinde n uzunluğunda bir lineer kod olmak üzere $\Phi(C) = C_1 \otimes C_2$ ve $|C| = |C_1| \cdot |C_2|$ sağlanır. (Zhu vd., 2010)

Kanıt:

$\Phi(C)$ kümesinin herhangi bir elemanı $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n)$ olsun.

Her $i = 1, 2, \ldots, n$ için $c_i = r_i + u \cdot (r_i + q_i) \in R = \mathbb{F}_2 + u\,\mathbb{F}_2$ elemanları ele alınsın. Bu durumda

$$c = (c_1, c_2, \ldots, c_n) = (r_1 + u \cdot (r_1 + q_1), r_2 + u \cdot (r_2 + q_2), \ldots, r_n + u \cdot (r_n + q_n)) \in R^n$$

$$\Rightarrow \Phi(c) = (r_1, r_2, \ldots, r_n, r_1 + (r_1 + q_1), r_2 + (r_2 + q_2), \ldots, r_n + (r_n + q_n))$$

$$\Rightarrow \Phi(c) = (r_1, r_2, \ldots, r_n, 2 \cdot r_1 + q_1, 2 \cdot r_2 + q_2, \ldots, 2 \cdot r_n + q_n)$$

$$\Rightarrow \Phi(c) = (r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in \Phi(C)$$

O halde $c \in C$'dir. Ayrıca Φ birebir olduğundan böyle bir c bir tanedir.

$C_1 = \left\{ x \in \mathbb{F}_2^{\,n} \middle| \exists y \in \mathbb{F}_2^{\,n} \text{ için } x + u \cdot y \in C \right\}$ 'idi.

Öyle bir $(r_1 + q_1, r_2 + q_2, \ldots, r_n + q_n) \in \mathbb{F}_2^{\,n}$ için

$(r_1 + u \cdot (r_1 + q_1), r_2 + u \cdot (r_2 + q_2), \ldots, r_n + u \cdot (r_n + q_n)) \in C$ olduğundan $(r_1, r_2, \ldots, r_n) \in C_1$ 'dir. $\cdots (i)$

Diğer taraftan $C_2 = \left\{ x + y \in \mathbb{F}_2^{\,n} \middle| \exists x, y \in \mathbb{F}_2^{\,n} \text{ için } x + u \cdot y \in C \right\}$ 'idi

Öyle bir $(r_1, r_2, \ldots, r_n), (r_1 + q_1, r_2 + q_2, \ldots, r_n + q_n) \in \mathbb{F}_2^{\,n}$ için

$(r_1 + u \cdot (r_1 + q_1), r_2 + u \cdot (r_2 + q_2), \ldots, r_n + u \cdot (r_n + q_n)) \in C$ olduğundan

$(r_1 + r_1 + q_1, r_2 + r_2 + q_2, \ldots, r_n + r_n + q_n) \in C$

$= (2 \cdot r_1 + q_1, 2 \cdot r_2 + q_2, \ldots, 2 \cdot r_n + q_n) \in C$

$= (q_1, q_2, \ldots, q_n) \in C_2$ dir. $\cdots (ii)$

i ve ii'den $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in C_1 \otimes C_2$ dir.

O halde $\Phi(C) \subseteq C_1 \otimes C_2 \cdots (\mathrm{I})$

$C_1 \otimes C_2$ kümesinin herhangi bir $(r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n)$ elemanı için

$(r_1, r_2, \ldots, r_n) \in C_1$ *ve* $(q_1, q_2, \ldots, q_n) \in C_2$'dir.

$\underset{C_1 \text{ve } C_2\text{'nin tanımından}}{\Rightarrow} a = (a_1, a_2, \ldots, a_n) \in C$ ve $(b_1, b_2, \ldots, b_n) \in C$ olacak şekilde $1 \le i \le n$ ve $m_i, n_i \in \mathbb{F}_2$ için öyle bir $a_i = r_i + u \cdot m_i$ ve $b_i = q_i + (1+u) \cdot n_i \in \mathbb{F}_2 + u \cdot \mathbb{F}_2 \left(u^2 = u\right)$ vardır

$$\left.\begin{array}{l} (1+u) \in R \text{ ve } a \in C \underset{\substack{C \\ \text{Alt Modül}} \subseteq R^n}{\Rightarrow} (1+u) \cdot a \in C \\ u \in R \text{ ve } b \in C \underset{\substack{C \\ \text{Alt Modül}} \subseteq R^n}{\Rightarrow} u \cdot b \in C \end{array}\right\} \Rightarrow c = (1+u) \cdot a + u \cdot b \in C$$

$$\Rightarrow \Phi(c) = (r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in \Phi(C)$$

O halde $C_1 \otimes C_2 \subseteq \Phi(C)$'dir.$\cdots(\mathrm{II})$

O halde (I) ve (II)'den; $\Phi(C) = C_1 \otimes C_2$'dir.

Diğer taraftan $\Phi(C)$ ve $C_1 \otimes C_2$ sonlu kümeler olduklarından $\Phi(C)$ ve $C_1 \otimes C_2$ kümelerinin eleman sayıları eşittir. Ayrıca C_1 ve C_2 sonlu olduklarından $C_1 \otimes C_2$ kümesinin eleman sayısı C_1 ve C_2 kümelerinin eleman sayılarının çarpımına eşittir. C kümesinin sonlu bir küme ve Φ dönüşümünün homomorfizma olduğu göz önüne alındığında $\Phi(C)$ kümesinin eleman sayısı da C kümesinin eleman sayısına eşittir. Bu durumda $|C| = |C_1| \cdot |C_2|$ sağlanır.

3.1.3.Teorem: $\begin{array}{l} \Phi : R \to \mathbb{F}_2^{\,2} \\ a + u \cdot b \mapsto \Phi(a + u\,b) = (a, a+b) \end{array}$ biçiminde tanımlanan Φ dönüşümünün ters dönüşümü $\begin{array}{l} \Phi^{-1} : \mathbb{F}_2^{\,2} \to R \\ (x, y) \mapsto x + u(y - x) \end{array}$ biçimindedir.

Kanıt: $\Phi \circ \Phi^{-1} = \mathrm{I}_{\mathbb{F}_2^{\,2}}$ olduğu gösterilecektir.

Her $(x, y) \in \mathbb{F}_2^{\,2}$ için

$$\Phi \circ \Phi^{-1}(x, y) = \Phi\left(\Phi^{-1}(x, y)\right) = \Phi\left(x + u(y - x)\right) = \left(x, x + (y - x)\right) = (x, y) \ldots (i)$$

$$\mathrm{I}_{\mathbb{F}_2^{\,2}}(x, y) = (x, y) \ldots (ii)$$

O halde i ve ii'den $\Phi \circ \Phi^{-1}(x,y) = \mathrm{I}_{\mathbb{F}_2{}^2}(x,y)$'dir.□

3.1.4.Teorem: $\mathbb{F}_2{}^{2n}$ vektör uzayı üzerine

$$\Phi^{-1} : \mathbb{F}_2{}^{2\cdot n} \to R^n$$
$$x = (r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_n) \in \mathbb{F}_2{}^{2\cdot n} \mapsto \Phi^{-1}(x) = \left(r_1 + u(q_1 - r_1), r_2 + u(q_2 - r_2), \ldots, r_n + u(q_n - r_n)\right)$$

biçiminde genişletilen Φ^{-1} dönüşümü bir $\mathbb{F}_2$ – homomorfizmadır.

Kanıt: Φ^{-1} dönüşümünün toplama ve skalerle çarpma işlemlerini koruduğu kolaylıkla gösterilir.

3.1.2.Gösterim: Bu tez boyunca bileşenleri matris olan $\begin{pmatrix} G_{11}\ G_{12}\ \cdots G_{1n} \\ G_{21}\ G_{22}\ \cdots G_{2n} \\ \vdots \\ G_{m1}\ G_{m2}\ \cdots G_{mn} \end{pmatrix}$ matrisi $1 \le i \le m$ ve $1 \le j \le n$ olmak üzere G_{ij} matrislerini oluşturan elemanların satır ve sütun sıraları korunarak bu elemanların oluşturduğu matris olarak düşünülecektir.

3.1.5.Teorem: C_1 ve C_2 lineer kodlarının üreteç matrisleri sırasıyla G_1 ve G_2 ise $\Phi(C) = C_1 \otimes C_2$ lineer kodunun üreteç matirisi $\begin{pmatrix} G_1\ 0 \\ 0\ G_2 \end{pmatrix}$'dir. (Zhu vd., 2010)

Kanıt: $G_1 = \begin{pmatrix} a_{11}\, a_{12} \ldots a_{1n} \\ a_{21}\, a_{22} \ldots a_{2n} \\ \vdots \\ a_{m1}\, a_{m2} \ldots a_{mn} \end{pmatrix}_{m\times n}$ matrisi $C_1 \subseteq \mathbb{F}_2{}^n$ lineer kodunun

$G_2 = \begin{pmatrix} b_{11}\, b_{12} \ldots b_{1n} \\ b_{21}\, b_{22} \ldots b_{2n} \\ \vdots \\ b_{k1}\, b_{k2} \ldots b_{kn} \end{pmatrix}_{k\times n}$ matrisi $C_2 \subseteq \mathbb{F}_2{}^n$ lineer kodunun üreteç matrisleri olsun. Bu durumda $U = \{(a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})\}$ C_1 lineer kodunun,

$V = \{(b_{11}, b_{12}, \ldots, b_{1n}), (b_{21}, b_{22}, \ldots, b_{2n}), \ldots, (b_{k1}, b_{k2}, \ldots, b_{kn})\}$ C_2 lineer kodunun bir tabanıdır.

$W=\{(a_{11},a_{12},\ldots,a_{1n},0,0,\ldots,0),(a_{21},a_{22},\ldots,a_{2n},0,0,\ldots,0),\ldots,(a_{m1},a_{m2},\ldots,a_{mn},0,0,\ldots,0),$
$(0,0,\ldots,0,b_{11},b_{12},\ldots,b_{1n}),(0,0,\ldots,0,b_{21},b_{22},\ldots,b_{2n}),\ldots,(0,0,\ldots,0,b_{k1},b_{k2},\ldots,b_{kn})\}\subseteq \mathbb{F}_2^{\,2n}$

kümesi tanımlansın. W kümesi $\Phi(C)=C_1\otimes C_2$ lineer kodu için bir taban olduğu gösterilecektir.

Her $\lambda_i\in\mathbb{F}_2$ $(i=0,1,\ldots,k+l)$ için

$$\lambda_1\cdot(a_{11},a_{12},\ldots,a_{1n},0,0,\ldots,0)+\lambda_2\cdot(a_{21},a_{22},\ldots,a_{2n},0,0,\ldots,0)+\ldots+\lambda_m\cdot(a_{m1},a_{m2},\ldots,a_{mn},0,0,\ldots,0)$$
$$+\lambda_{m+1}\cdot(0,0,\ldots,0,b_{11},b_{12},\ldots,b_{1n})+\lambda_{m+2}\cdot(,b_{21},b_{22},\ldots,b_{2n})+\ldots+\lambda_n\cdot(0,0,\ldots,0,b_{k1},b_{k2},\ldots,b_{kn})$$
$$=\underset{(2n\ tane)}{(0,0,\ldots,0)}$$

$$\Rightarrow \lambda_1\cdot(a_{11},a_{12},\ldots,a_{1n})+\lambda_2\cdot(a_{21},a_{22},\ldots,a_{2n})+\cdots+\lambda_m\cdot(a_{m1},a_{m2},\ldots,a_{mn})=\underset{(n\,tane)}{(0,0,\ldots,0)}\ \text{ve}$$
$$\lambda_{m+1}\cdot(,b_{11},b_{12},\ldots,b_{1n})+\lambda_{m+2}\cdot(b_{21},b_{22},\ldots,b_{2n})+\ldots+\lambda_n\cdot(b_{k1},b_{k2},\ldots,b_{kn})=\underset{(n\ tane)}{(0,0,\ldots,0)}$$

$$\underset{U\ ve\ V\ taban}{\Rightarrow}\lambda_1=\lambda_2=\cdots=\lambda_m=0\ \text{ve}\ \lambda_{m+1}=\lambda_{m+2}=\cdots=\lambda_n=0$$

$\Rightarrow$ Her $i=1,2,\ldots,n$ için $\lambda_i=0$ 'dır.$\ldots..(i)$

Her $(c_1,c_2,\ldots,c_n,c_{n+1},c_{n+2},\ldots,c_{2n})\in\Phi(C)=C_1\otimes C_2$ için

$(c_1,c_2,\ldots,c_n)\in C_1$ ve $(c_{n+1},c_{n+2},\ldots,c_{2n})\in C_2$ 'dir.

$\underset{\substack{G_1\ C_1\text{'in}\\ G_2\ C_2\text{'nin}\\ tabanı}}{\Rightarrow}$ Öyle bir $\lambda_1,\lambda_2,\ldots,\lambda_m\in\mathbb{F}_2$ için

$(c_1,c_2,\ldots,c_n)=\lambda_1\cdot(a_{11},a_{12},\ldots,a_{1n})+\lambda_2\cdot(a_{21},a_{22},\ldots,a_{2n})+\cdots+\lambda_m\cdot(a_{m1},a_{m2},\ldots,a_{mn})$ ve

Öyle bir $\lambda_{m+1},\lambda_{m+2},\ldots,\lambda_{m+k}=\lambda_n\in\mathbb{F}_2$ için

$(c_{n+1},c_{n+2},\ldots,c_{2n})=\lambda_{m+1}\cdot(,b_{11},b_{12},\ldots,b_{1n})+\lambda_{m+2}\cdot(b_{21},b_{22},\ldots,b_{2n})+\ldots+\lambda_n\cdot(b_{k1},b_{k2},\ldots,b_{kn})$

'dir.

$\underset{\substack{C_1\otimes C_2\text{'nin}\\ tanımı}}{\Rightarrow}$ Öyle bir $\lambda_1,\lambda_2,\ldots,\lambda_m,\lambda_{m+1},\lambda_{m+2},\ldots,\lambda_n\in\mathbb{F}_2$ için

$$(c_1,c_2,\ldots,c_n,c_{n+1},c_{n+2},\ldots,c_{2n})=\lambda_1\cdot(a_{11},a_{12},\ldots,a_{1n},0,0,\ldots,0)+\lambda_2\cdot(a_{21},a_{22},\ldots,a_{2n},0,0,\ldots,0)+\ldots$$
$$+\lambda_m\cdot(a_{m1},a_{m2},\ldots,a_{mn},0,0,\ldots,0)+\lambda_{m+1}\cdot(0,0,\ldots,0,b_{11},b_{12},\ldots,b_{1n})+\lambda_{m+2}\cdot(0,0,\ldots,0,b_{21},b_{22},\ldots,b_{2n})+\ldots$$
$$+\lambda_n\cdot(0,0,\ldots,0,b_{k1},b_{k2},\ldots,b_{kn})\text{'dir.}\cdots(ii)$$

O halde i ve ii 'den W kümesi $\Phi(C)=C_1\otimes C_2$ lineer kodu için bir tabandır.

Bir lineer kodun üreteç matrisinin tanımından $\Phi(C)=C_1\otimes C_2$ lineer kodunun üreteç matrisi

$$G=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & b_{1n} \\ 0 & 0 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & & & & & & & \\ 0 & 0 & \dots & 0 & b_{k1} & b_{k2} & \dots & b_{kn} \end{pmatrix}_{(m+k)\times 2n} = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}_{(m+k)\times 2n}$$ matrisidir. □

3.1.2.Önerme: $\Phi(C)=C_1\otimes C_2$ lineer kodunun $\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$ üreteç matrisinin belirttiği taban W ise $\Phi^{-1}(W)$ kümesinin elemanlarını satır kabul eden matris $\begin{pmatrix} (1+u)\cdot G_1 \\ u\cdot G_2 \end{pmatrix}$ matrisidir.

Kanıt: $\Phi(C)=C_1\otimes C_2$ lineer kodunun üreteç matrisi

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}_{(m+k)\times 2n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & b_{1n} \\ 0 & 0 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & & & & & & & \\ 0 & 0 & \dots & 0 & b_{k1} & b_{k2} & \dots & b_{kn} \end{pmatrix}_{(m+k)\times 2n}$$ ve bu matrisin belirttiği taban

$$W=\{(a_{11},a_{12},\dots,a_{1n},0,0,\dots,0),(a_{21},a_{22},\dots,a_{2n},0,0,\dots,0),\dots,(a_{m1},a_{m2},\dots,a_{mn},0,0,\dots,0),$$
$$(0,0,\dots,0,b_{11},b_{12},\dots,b_{1n}),(0,0,\dots,0,b_{21},b_{22},\dots,b_{2n}),\dots,(0,0,\dots,0,b_{k1},b_{k2},\dots,b_{kn})\}\subseteq \mathbb{F}_2^{\,2n}$$

$$\Rightarrow \Phi^{-1}(W)=\{\Phi^{-1}(a_{11},a_{12},\dots,a_{1n},0,0,\dots,0),\Phi^{-1}(a_{21},a_{22},\dots,a_{2n},0,0,\dots,0),$$
$$\dots,\Phi^{-1}(a_{m1},a_{m2},\dots,a_{mn},0,0,\dots,0),\Phi^{-1}(0,0,\dots,0,b_{11},b_{12},\dots,b_{1n}),\Phi^{-1}(0,0,\dots,0,b_{21},b_{22},\dots,b_{2n}),\dots,\Phi^{-1}(0,0,\dots,0,b_{k1},b_{k2},\dots,b_{kn})\}$$

$$=((a_{11}+u\cdot(0-a_{11}),a_{12}+u\cdot(0-a_{12}),\dots,a_{1n}+u\cdot(0-a_{1n})),(a_{21}+u\cdot(0-a_{21}),a_{22}+u\cdot(0-a_{22}),\dots,a_{2n}+u\cdot(0-a_{2n}))$$
$$\dots,(a_{m1}+u\cdot(0-a_{m1}),a_{m2}+u\cdot(0-a_{m2}),\dots,a_{mn}+u\cdot(0-a_{mn})),(0+u\cdot(b_{11}-0),0+u\cdot(b_{12}-0),\dots,0+u\cdot(b_{1n}-0)),$$
$$(0+u\cdot(b_{21}-0),0+u\cdot(b_{22}-0),\dots,0+u\cdot(b_{2n}-0)),\dots,(0+u\cdot(b_{k1}-0),0+u\cdot(b_{k2}-0),\dots,0+u\cdot(b_{kn}-0)))$$

$$=\Big(\big((1+u)\cdot a_{11},(1+u)\cdot a_{12},\ldots,(1+u)\cdot a_{1n}\big),\big((1+u)\cdot a_{21},(1+u)\cdot a_{22},\ldots,(1+u)\cdot a_{2n}\big),\ldots,\big((1+u)\cdot a_{m1},(1+u)\cdot a_{m2},\ldots,(1+u)\cdot a_{mn}\big),$$
$$\big(u\cdot b_{11},u\cdot b_{12},\ldots,u\cdot b_{1n}\big),\big(u\cdot b_{21},u\cdot b_{22},\ldots,u\cdot b_{2n}\big),\ldots,\big(u\cdot b_{k1},u\cdot b_{k2},\ldots,u\cdot b_{kn}\big)\Big)$$

$$=\Big(\big(1+u\big)\cdot\big(a_{11},a_{12},\ldots,a_{1n}\big),\big(1+u\big)\cdot\big(a_{21},a_{22},\ldots,a_{2n}\big),\ldots,\big(1+u\big)\cdot\big(a_{m1},a_{m2},\ldots,a_{mn}\big),u\cdot\big(b_{11},b_{12},\ldots,b_{1n}\big),u\cdot\big(b_{21},b_{22},\ldots,b_{2n}\big),\ldots,$$
$$u\cdot\big(b_{k1},b_{k2},\ldots,b_{kn}\big)\Big)$$

Bu durumda $\Phi^{-1}(W)$ kümesinin elemanlarını satır kabul eden matris

$$\begin{pmatrix}(1+u)\cdot a_{11} & (1+u)\cdot a_{12} & \ldots & (1+u)\cdot a_{1n}\\ (1+u)\cdot a_{21} & (1+u)\cdot a_{22} & \ldots & (1+u)\cdot a_{2n}\\ \vdots & & & \\ (1+u)\cdot a_{m1} & (1+u)\cdot a_{m2} & \ldots & (1+u)\cdot a_{mn}\\ u\cdot b_{11} & u\cdot b_{12} & \ldots & u\cdot b_{1n}\\ u\cdot b_{21} & u\cdot b_{22} & \ldots & u\cdot b_{2n}\\ \vdots & & & \\ u\cdot b_{k1} & u\cdot b_{k2} & \ldots & u\cdot b_{kn}\end{pmatrix}_{(m+k)\times n} = \begin{pmatrix}(1+u)\cdot G_1\\ u\cdot G_2\end{pmatrix} \text{ matrisidir. } \square$$

3.1.1.Lemma: S, $\mathbb{F}_q^{\,n}$ vektör uzayının boş kümeden farklı bir alt kümesi ve A S kümesinin elemanlarını satır kabul eden matris olsun. A matrisine uygulanacak elementer satır işlemleriyle elde edilen A matrisinin Echelon formunun tamamı sıfır olmayan satırlarının belirttiği küme S kümesinin ürettiği alt vektör uzayı için bir tabandır. (Ling, Xing, 2004, s.49)

3.1.3.Önerme: C_1 ve C_2 lineer kodlarının üreteç matrisleri sırasıyla G_1 ve G_2 olsun. $\Phi(C)=C_1\otimes C_2$ lineer kodunun üreteç matrisi $\begin{pmatrix}G_1 & 0\\ 0 & G_2\end{pmatrix}$ matrisinin belirttiği taban W olsun. $G_1=G_2$ ise $\Phi^{-1}(W)$ kümesinin ürettiği lineer kodun tabanının elemanlarını satır kabul eden matris $G_1=G_2$ matrisidir.

Kanıt: $\Phi(C)=C_1\otimes C_2$ lineer kodunun üreteç matrisi $\begin{pmatrix}G_1 & 0\\ 0 & G_2\end{pmatrix}$ matrisinin belirttiği taban W ve $G_1=G_2=\begin{pmatrix}a_{11}\,a_{12}\ldots a_{1n}\\ a_{21}\,a_{22}\ldots a_{2n}\\ \vdots\\ a_{m1}\,a_{m2}\ldots a_{mn}\end{pmatrix}_{m\times n}$

$\underset{\text{3.1.2.Önerme}}{\Rightarrow}$ $\Phi^{-1}(W)$ kümesinin elemanlarını satır kabul eden matris

$$\begin{pmatrix}(1+u)\cdot G_1\\ u\cdot G_2\end{pmatrix}=\begin{pmatrix}(1+u)\cdot a_{11} & (1+u)\cdot a_{12} & \dots & (1+u)\cdot a_{1n}\\ (1+u)\cdot a_{21} & (1+u)\cdot a_{22} & \dots & (1+u)\cdot a_{2n}\\ \vdots & & & \\ (1+u)\cdot a_{m1} & (1+u)\cdot a_{m2} & \dots & (1+u)\cdot a_{mn}\\ u\cdot a_{11} & u\cdot a_{12} & \dots & u\cdot a_{1n}\\ u\cdot a_{21} & u\cdot a_{22} & \dots & u\cdot a_{2n}\\ \vdots & & & \\ u\cdot a_{m1} & u\cdot a_{m2} & \dots & u\cdot a_{mn}\end{pmatrix}_{(2m)\times n}$$ matrisidir.

Bu matrisin $(m+1).$ satırının $1.$satıra, $(m+2).$ satırının $2.$ satıra,…, $(m+i).$satırının $i.$satıra $(1\le i\le m)$ eklenmesiyle

$$\begin{pmatrix}(1+u)\cdot a_{11}+u\cdot a_{11} & (1+u)\cdot a_{12}+u\cdot a_{12} & \dots & (1+u)\cdot a_{1n}+u\cdot a_{1n}\\ (1+u)\cdot a_{21}+u\cdot a_{21} & (1+u)\cdot a_{22}+u\cdot a_{22} & \dots & (1+u)\cdot a_{2n}+u\cdot a_{2n}\\ \vdots & & & \\ (1+u)\cdot a_{m1}+u\cdot a_{m1} & (1+u)\cdot a_{m2}+u\cdot a_{m2} & \dots & (1+u)\cdot a_{mn}+u\cdot a_{mn}\\ u\cdot a_{11} & u\cdot a_{12} & \dots & u\cdot a_{1n}\\ u\cdot a_{21} & u\cdot a_{22} & \dots & u\cdot a_{2n}\\ \vdots & & & \\ u\cdot a_{m1} & u\cdot a_{m2} & \dots & u\cdot a_{mn}\end{pmatrix}$$

$$=\begin{pmatrix}a_{11} & a_{12} & \dots & a_{1n}\\ a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn}\\ u\cdot a_{11} & u\cdot a_{12} & \dots & u\cdot a_{1n}\\ u\cdot a_{21} & u\cdot a_{22} & \dots & u\cdot a_{2n}\\ \vdots & & & \\ u\cdot a_{m1} & u\cdot a_{m2} & \dots & u\cdot a_{mn}\end{pmatrix}_{(2m)\times n}$$ matrisi elde edilir. Bu matrisin $1.$ satırının u ile çarpılıp $(m+1).$satıra, $2.$satırın u ile çarpılıp $(m+2).$ satıra ,…, $i.$ satırın u ile çarpılıp $(m+i).$satıra $(1\le i\le m)$ eklenmesiyle

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \\ u\cdot a_{11}+u\cdot a_{11} & u\cdot a_{12}+u\cdot a_{12} & \dots & u\cdot a_{1n}+u\cdot a_{1n} \\ u\cdot a_{21}+u\cdot a_{21} & u\cdot a_{22}+u\cdot a_{22} & \dots & u\cdot a_{2n}+u\cdot a_{2n} \\ \vdots & & & \\ u\cdot a_{m1}+u\cdot a_{m1} & u\cdot a_{m2}+u\cdot a_{m2} & \dots & u\cdot a_{mn}+u\cdot a_{mn} \end{pmatrix}_{(2m)\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & 0 \end{pmatrix}_{(2m)\times n}$$

matrisi elde edilir.

$\underset{\text{3.1.1.Lemma'dan}}{\Rightarrow} \Phi^{-1}(W)$ kümesinin ürettiği lineer kodun tabanının elemanlarını satır kabul eden matris

$$G = \begin{pmatrix} a_{11}\, a_{12} \dots a_{1n} \\ a_{21}\, a_{22} \dots a_{2n} \\ \vdots \\ a_{m1}\, a_{m2} \dots a_{mn} \end{pmatrix}_{m\times n} = G_1 = G_2 \ \square$$

3.1.1.Sonuç: C_1 ve C_2 lineer kodlarının üreteç matrisleri sırasıyla G_1 ve G_2 matrisleri olsun. Bu durumda C lineer kodunu üreteç matrisi:

$G = \begin{pmatrix} (1+u)\cdot G_1 \\ u\cdot G_2 \end{pmatrix}$[1]matrisidir. Ayrıca $G_1 = G_2$ ise $G = G_1$'dir. (Zhu vd., 2010)$\square$

Eğer G matrisinin satırları lineer bağımsız değilse, G matrisine uygulanacak elementer satır işlemleri sonucunda elde edilen yeni matriste tamamı sıfır olmayan satırların oluşturduğu matris üreteç matrisi olacaktır.

3.1.2.Sonuç: Eğer $\Phi(C) = C_1 \otimes C_2$ ise $C = (1+u)\cdot C_1 \oplus u\cdot C_2$'dir. (Zhu vd., 2010)

[1] Bu gösterimde G_1 ve G_2 matrislerinin sırasıyla $(1+u)$ ve u skalerleriyle çarpılması sonucu elde edilen $(1+u)\cdot G_1$ ve $u\cdot G_2$ matrislerinin satırlarını satır kabul eden, $(1+u)\cdot G_1$ matrisinin satırlarının altına $u\cdot G_2$ matrisinin satırlarının yazılmasıyla elde edilen yeni matris anlatılmaktadır.

Kanıt: $G_1 = \begin{pmatrix} a_{11}\, a_{12} \ldots a_{1n} \\ a_{21}\, a_{22} \ldots a_{2n} \\ \vdots \\ a_{m1}\, a_{m2} \ldots a_{mn} \end{pmatrix}_{m \times n}$ matrisi $C_1 \subseteq \mathbb{F}_2^{\,n}$ lineer kodunun

$G_2 = \begin{pmatrix} b_{11}\, b_{12} \ldots b_{1n} \\ b_{21}\, b_{22} \ldots b_{2n} \\ \vdots \\ b_{k1}\, b_{k2} \ldots b_{kn} \end{pmatrix}_{k \times n}$ matrisi $C_2 \subseteq \mathbb{F}_2^{\,n}$ lineer kodunun üreteç matrisleri

$\Rightarrow U = \{(a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})\}$ C_1 lineer kodunun,

$V = \{(b_{11}, b_{12}, \ldots, b_{1n}), (b_{21}, b_{22}, \ldots, b_{2n}), \ldots, (b_{k1}, b_{k2}, \ldots, b_{kn})\}$ C_2 lineer kodunun bir tabanıdır.

$\underset{\text{3.1.1 Sonuçtan}}{\Rightarrow}$ C lineer kodunu üreteç matrisi:

$$G = \begin{pmatrix} (1+u)\cdot G_1 \\ u \cdot G_2 \end{pmatrix} = \begin{pmatrix} (1+u)\cdot a_{11} & (1+u)\cdot a_{12} & \ldots & (1+u)\cdot a_{1n} \\ (1+u)\cdot a_{21} & (1+u)\cdot a_{22} & \ldots & (1+u)\cdot a_{2n} \\ \vdots & & & \\ (1+u)\cdot a_{m1} & (1+u)\cdot a_{m2} & \ldots & (1+u)\cdot a_{mn} \\ u\cdot b_{11} & u\cdot b_{12} & \ldots & u\cdot b_{1n} \\ u\cdot b_{21} & u\cdot b_{22} & \ldots & u\cdot b_{2n} \\ \vdots & & & \\ u\cdot b_{k1} & u\cdot b_{k2} & \ldots & u\cdot b_{kn} \end{pmatrix}_{(m+k)\times n}$$ matrisidir.

$\Rightarrow W = \{((1+u)\cdot a_{11}, (1+u)\cdot a_{12}, \ldots, (1+u)\cdot a_{1n}), ((1+u)\cdot a_{21}, (1+u)\cdot a_{22}, \ldots, (1+u)\cdot a_{2n}),$
$\ldots, ((1+u)\cdot a_{m1}, (1+u)\cdot a_{m2}, \ldots, (1+u)\cdot a_{mn}), (u\cdot b_{11}, u\cdot b_{12}, \ldots, u\cdot b_{1n}), (u\cdot b_{21}, u\cdot b_{22}, \ldots, u\cdot b_{2n}),$
$\ldots (u\cdot b_{k1}, u\cdot b_{k2}, \ldots, u\cdot b_{kn})\}$ C lineer kodunun bir tabanıdır.

$\Rightarrow$: Herhangi bir $(x_1 + u\cdot y_1, x_2 + u\cdot y_2, \ldots, x_n + u\cdot y_n) \in C$ alınsın.

$(x_1 + u\cdot y_1, x_2 + u\cdot y_2, \ldots, x_n + u\cdot y_n)$
$\underset{\substack{W\ C'nin \\ Tabanı}}{=} (\lambda_1 + u\cdot\beta_1)\cdot((1+u)\cdot a_{11}, (1+u)\cdot a_{12}, \ldots, (1+u)\cdot a_{1n}) +$
$(\lambda_2 + u\cdot\beta_2)\cdot((1+u)\cdot a_{21}, (1+u)\cdot a_{22}, \ldots, (1+u)\cdot a_{2n}) + \cdots + (\lambda_m + u\cdot\beta_m)((1+u)\cdot a_{m1}, (1+u)\cdot a_{m2}, \ldots, (1+u)\cdot a_{mn}) +$
$(\lambda_{m+1} + u\cdot\beta_{m+1})\cdot(u\cdot b_{11}, u\cdot b_{12}, \ldots, u\cdot b_{1n}) + (\lambda_{m+2} + u\cdot\beta_{m+2})\cdot(u\cdot b_{21}, u\cdot b_{22}, \ldots, u\cdot b_{2n}) +$
$\cdots + (\lambda_{m+k} + u\cdot\beta_{m+k})\cdot(u\cdot b_{k1}, u\cdot b_{k2}, \ldots, u\cdot b_{kn})$

$$=(1+u)\cdot\lambda_1\cdot(a_{11},a_{12},\ldots,a_{1n})+(1+u)\cdot\lambda_2\cdot(a_{21},a_{22},\ldots,a_{2n})+\cdots+(1+u)\cdot\lambda_m\cdot(a_{m1},a_{m2},\ldots,a_{mn})+$$
$$u\cdot(\lambda_{m+1}+\beta_{m+1})\cdot(b_{11},b_{12},\ldots,b_{1n})+u\cdot(\lambda_{m+2}+\beta_{m+2})\cdot(b_{21},b_{22},\ldots,b_{2n})+\cdots+u\cdot(\lambda_{m+k}+\beta_{m+k})\cdot(b_{k1},b_{k2},\ldots,b_{kn})$$
$$=(1+u)\cdot\underbrace{\left[\lambda_1\cdot(a_{11},a_{12},\ldots,a_{1n})+\lambda_2\cdot(a_{21},a_{22},\ldots,a_{2n})+\cdots+\lambda_m\cdot(a_{m1},a_{m2},\ldots,a_{mn})\right]}_{\in C_1}+$$
$$u\cdot\underbrace{\left[(\lambda_{m+1}+\beta_{m+1})\cdot(b_{11},b_{12},\ldots,b_{1n})+(\lambda_{m+2}+\beta_{m+2})\cdot(b_{21},b_{22},\ldots,b_{2n})+\cdots+(\lambda_{m+k}+\beta_{m+k})\cdot(b_{k1},b_{k2},\ldots,b_{kn})\right]}_{\in C_2}\in(1+u)\cdot C_1\oplus u\cdot C_2$$

olacak biçimde öyle bir $\lambda_1+u\beta_1,\lambda_2+u\beta_2,\ldots,\lambda_n+u\beta_n\in R=\mathbb{F}_2+u\mathbb{F}_2(u^2=u)$ vardır.

O halde $C\subseteq(1+u)\cdot C_1\oplus u\cdot C_2$'dir.$\ldots(i)$

$\Leftarrow$: Herhangi bir $(1+u)\cdot(c_1,c_2,\ldots,c_n)+u\cdot(d_1,d_2,\ldots,d_n)\in(1+u)\cdot C_1\oplus u\cdot C_2$ alınsın.

U C_1'in, V C_2'nin tabanı olduğundan

$$(1+u)\cdot(c_1,c_2,\ldots,c_n)+u\cdot(d_1,d_2,\ldots,d_n)$$
$$=(1+u)\cdot\left[\lambda_1\cdot(a_{11},a_{12},\ldots,a_{1n})+\lambda_2\cdot(a_{21},a_{22},\ldots,a_{2n})+\cdots+\lambda_m\cdot(a_{m1},a_{m2},\ldots,a_{mn})\right]$$
$$+u\cdot\left[(\lambda_{m+1})\cdot(b_{11},b_{12},\ldots,b_{1n})+(\lambda_{m+2})\cdot(b_{21},b_{22},\ldots,b_{2n})+\cdots+(\lambda_{m+k})\cdot(b_{k1},b_{k2},\ldots,b_{kn})\right]$$
$$=\lambda_1\cdot((1+u)\cdot a_{11},(1+u)\cdot a_{12},\ldots,(1+u)\cdot a_{1n})+\lambda_2\cdot((1+u)\cdot a_{21},(1+u)\cdot a_{22},\ldots,(1+u)\cdot a_{2n})$$
$$+\cdots+\lambda_m\cdot((1+u)\cdot a_{m1},(1+u)\cdot a_{m2},\ldots,(1+u)\cdot a_{mn})+\lambda_{m+1}\cdot(u\cdot b_{11},u\cdot b_{12},\ldots,u\cdot b_{1n})$$
$$+\lambda_{m+2}\cdot(u\cdot b_{21},u\cdot b_{22},\ldots,u\cdot b_{2n})+\cdots+\lambda_{m+k}\cdot(u\cdot b_{k1},u\cdot b_{k2},\ldots,u\cdot b_{kn})\underset{\substack{W\ C'nin\\ Tabanı}}{\in} C$$

olacak biçimde $\lambda_1,\lambda_2,\ldots,\lambda_{m+k}\in\mathbb{F}_2\subseteq R=\mathbb{F}_2+u\mathbb{F}_2(u^2=u)$ vardır.

O halde $(1+u)\cdot C_1\oplus u\cdot C_2\subseteq C$'dir.$\ldots(ii)$

O halde i ve ii'den $C=(1+u)\cdot C_1\oplus u\cdot C_2$'dir.

3.1.2.Lemma: R üzerinde n uzunluklu C lineer kodunun dual kodu $C^{\perp}$ ise $\Phi(C^{\perp})=\Phi(C)^{\perp}$ sağlanır. (Zhu vd., 2010)

Kanıt: $\Phi(C^{\perp})\subseteq\Phi(C)^{\perp}$ olduğu aşağıdaki şekilde gösterilir.

Herhangi bir $\Phi(a)\in\Phi(C^{\perp})$ alınsın.

$\Rightarrow a\in C^{\perp}$

$\Rightarrow C$ kodunun herhangi bir b elemanı için $a\cdot b=0$'dır.

$$\underset{\Phi\ izom.}{\Rightarrow}\Phi(a\cdot b)=\Phi(a)\cdot\underset{\in\Phi(C)}{\Phi(b)}=0$$

$\underset{\substack{\Phi(C)^{\perp}\text{'nin}\\ \text{Tanımı}}}{\Rightarrow} \Phi(a)\ \Phi(C)^{\perp}$ kümesinin bir elemanıdır.

O halde $\Phi(C^{\perp}) \subseteq \Phi(C)^{\perp} \cdots (i)$

$\Phi(C)^{\perp} \subseteq \Phi(C^{\perp})$ olduğu aşağıdaki şekilde gösterilir.

Herhangi bir $y \in \Phi(C)^{\perp} \subseteq \mathbb{F}_2^{2n}$ alınsın. R^n'den $\mathbb{F}_2^{2n}$'e tanımlanan Φ Gray dönüşümü örten olduğundan $\Phi(x) = y$ olacak biçimde en az bir $x \in R^n$ vardır. O halde $\Phi(C)^{\perp}$ kümesinin herhangi bir elemanı R^n kümesindeki bir elemanın Φ dönüşümü altındaki görüntüsü olarak yazılabilir.

$\Leftarrow$: Herhangi bir $\Phi(x) \in \Phi(C)^{\perp}$ alınsın. Bu durumda her $\Phi(z) \in \Phi(C)$ için $\Phi(x) \cdot \Phi(z) = 0$

$\underset{\Phi\,izom.}{\Rightarrow}$ Her $z \in C$ için $\Phi(x \cdot z) = 0$

$\underset{\Phi\,izom.}{\Rightarrow}$ Her $z \in C$ için $x \cdot z = 0$

$\underset{\substack{C^{\perp}\text{'nin}\\ \text{tanımı}}}{\Rightarrow} z \in C^{\perp}$

$\Rightarrow \Phi(z) \in \Phi(C^{\perp})$

O halde $\Phi(C)^{\perp}$ kümesi $\Phi(C^{\perp})$ kümesinin bir alt kümesidir. $\cdots (ii)$

O halde (i) ve (ii)'den $\Phi(C)^{\perp} = \Phi(C^{\perp})$'dir. □

3.1.2.Lemma kullanılarak elde edilen aşağıdaki diyagram

$$\begin{array}{ccc} C & \to & \Phi(C) \\ \downarrow & \circlearrowright & \downarrow \\ C^{\perp} & \to & \Phi(C^{\perp}) \end{array}$$

R üzerinde n uzunluklu C lineer kodlarının Gray dönüşümü altındaki $\Phi(C)$ görüntüleri ile C lineer kodların dual kodları $C^{\perp}$ 'lerin Gray dönüşümü altındaki görüntüleri olan $\Phi(C^{\perp})$ kodları arasında bire bir eşleme olduğunu göstermektedir.

3.1.6.Teorem: C R üzerinde n uzunluklu bir lineer kod ve $\Phi(C) = C_1 \otimes C_2$ ise $\Phi(C^{\perp}) = C_1^{\perp} \otimes C_2^{\perp}$ 'dir. (Zhu vd., 2010)

Kanıt: 3.1.2 Lemma'dan $\Phi(C^{\perp})$ kümesi $\Phi(C)^{\perp}$ kümesine , 3.1.2.Teorem'den de - $\Phi(C)^{\perp}$ kümesi $(C_1 \otimes C_2)^{\perp}$ kümesine eşittir. Bu durumda $(C_1 \otimes C_2)^{\perp} = C_1^{\perp} \otimes C_2^{\perp}$ gösterilmesi yeterlidir.

$\Rightarrow$: Herhangi bir $(z,t) \in C_1^{\perp} \otimes C_2^{\perp}$ alınsın.

$(z,t) \in C_1^{\perp} \otimes C_2^{\perp}$

$\Rightarrow z \in C_1^{\perp}$ ve $t \in C_2^{\perp}$

$\Rightarrow$ Her $x \in C_1$ için $x \cdot z = 0$ ve her $w \in C_2$ için $w \cdot t = 0$

$\Rightarrow$ Her $(x,w) \in C_1 \otimes C_2$ için $(x,w) \cdot (z,t) = 0$

$\Rightarrow (z,t) \in (C_1 \otimes C_2)^{\perp}$ 'dir.

O halde $C_1^{\perp} \otimes C_2^{\perp} \subseteq (C_1 \otimes C_2)^{\perp} \ldots (i)$

$\Leftarrow$: C_1 ve C_2 sırasıyla $[n,m]$ ve $[n,k]$ ikili lineer kodlar olsunlar. Bu durumda;

$|C_1^{\perp} \otimes C_2^{\perp}| = |C_1^{\perp}| \cdot |C_2^{\perp}| = |(C_1 \otimes C_2)^{\perp}| = 2^{2n-m-k}$ olur.

Yani sayılabilir sonlu tane elemanı olan $C_1^{\perp} \otimes C_2^{\perp}$ ve $(C_1 \otimes C_2)^{\perp}$ kümelerinin eleman sayıları eşittir.$\ldots (ii)$

O halde i ve ii 'den $(C_1 \otimes C_2)^{\perp} = C_1^{\perp} \otimes C_2^{\perp}$ 'dir.□

3.1.3.Sonuç: C R üzerinde n uzunluklu bir lineer kod ve $\Phi(C) = C_1 \otimes C_2$ ise $C^{\perp} = (1+u) \cdot C_1^{\perp} \oplus u \cdot C_2^{\perp}$ 'dir. (Zhu vd., 2010)

Kanıt: C R üzerinde n uzunluklu bir lineer kod ve $\Phi(C)=C_1\otimes C_2$

$\underset{3.1.6.Teorem}{\Rightarrow} \Phi\left(C^{\perp}\right)=C_1^{\perp}\otimes C_2^{\perp} \underset{3.1.2.\,Sonuç}{\Rightarrow} C^{\perp}=(1+u)\cdot C_1^{\perp}\oplus u\cdot C_2^{\perp}$ □

3.1.3.Gösterim: $i=1,2,\ldots,k\left(2\le k,k\in\mathbb{N}\right)$ ve $n_i\in\mathbb{N}\setminus\{0\}$ için

$x_1=\left(\rho_{11},\rho_{12},\ldots,\rho_{1n_1}\right), x_2=\left(\rho_{21},\rho_{22},\ldots,\rho_{2n_2}\right),\ldots,x_k=\left(\rho_{k1},\rho_{k2},\ldots,\rho_{kn_k}\right)$ sıralıları

düşünülsün $\left(x_1|x_2|,\ldots,|x_k\right)=\left(\rho_{11},\rho_{12},\ldots,\rho_{1n_1},\rho_{21},\rho_{22},\ldots,\rho_{2n_2},\ldots,\rho_{k1},\rho_{k2},\ldots,\rho_{kn_k}\right)$'dir.

Yani sıralılar arasına " | " işareti konması, sıralıların parantezlerinin kaldırılıp, bileşenlerinin sıraları korunarak tek bir tane sıralı yazma anlamına gelmektedir.

3.1.7.Teorem: $C=(1+u)\cdot C_1\oplus u\cdot C_2$ R üzerinde n uzunluklu bir lineer kod ve C lineer kodu R üzerinde cyclic kod olsun. Bu durumda C_1 ve C_2 lineer kodları cyclic koddur. Bu ifadenin tersi de doğrudur. (Zhu vd., 2010)

Kanıt: $\Rightarrow$: Her $r=\left(r_0,r_1,\ldots,r_{n-1}\right)\in C_1$ ve $q=\left(q_0,q_1,\ldots,q_{n-1}\right)\in C_2$

$\Rightarrow i=0,1,\ldots,n-1$ için $c_i=r_i+u\cdot\left(r_i+q_i\right)$ olmak üzere $c=\left(c_0,c_1,\ldots,c_{n-1}\right)\in C$'dir.

$\underset{\substack{C\subseteq R^n\\ cyclic}}{\Rightarrow}\sigma(c)\in C$

$\Rightarrow\Phi\left(\sigma(c)\right)=\Phi\left(r_{n-1}+u\cdot\left(r_{n-1}+q_{n-1}\right),r_0+u\cdot\left(r_0+q_0\right),\ldots,r_{n-2}+u\cdot\left(r_{n-2}+q_{n-2}\right)\right)$

$=\left(r_{n-1},r_0,\ldots,r_{n-2},r_{n-1}+r_{n-1}+q_{n-1},r_0+r_0+q_0,\ldots,r_{n-2}+r_{n-2}+q_{n-2}\right)$

$=\left(r_{n-1},r_0,\ldots,r_{n-2},q_{n-1},q_0,\ldots,q_{n-2}\right)$

$=\left(\sigma(r)|\sigma(q)\right)\underset{i'\text{den}}{\in} C_1\otimes C_2\quad\left(\Phi\left(\sigma(c)\right)\in\Phi\left(\sigma(C)\right)\underset{C\text{ cylic}}{=}\Phi(C)\underset{3.1.2.\text{Teorem}}{=}C_1\otimes C_2\right)\cdots(i)$

$\Rightarrow\sigma(r)\in C_1$ ve $\sigma(q)\in C_2$'dir.

$\Rightarrow C_1$ ve C_2 cyclic kodlardır.

$\Leftarrow$: Her $i=0,1,\ldots,n-1$, $c_i=r_i+u\cdot q_i$ olmak üzere $\left(c_0,c_1,\ldots,c_{n-1}\right)\in C$

$$\left(\begin{array}{l}\underset{\substack{C_1\text{ ve }C_2\\ \text{Tanımı}}}{\Rightarrow} r=\left(r_0,r_1,\ldots,r_{n-1}\right)\text{ ve }q=\left(q_0,q_1,\ldots,q_{n-1}\right)\text{ olmak üzere }r\in C_1\text{ ve }r+q\in C_2\text{'dir.}\\ \underset{\substack{C_1\text{ ve }C_2\\ \text{cylic}}}{\Rightarrow}\sigma(r)\in C_1\text{ ve }\sigma(r+q)\in C_2\text{'dir.}\end{array}\right)\cdots(ii)$$

$\Rightarrow\sigma(c)=\sigma\left(c_0,c_1,\ldots,c_{n-1}\right)$

$$= \sigma\left(r_0 + u\cdot q_0, r_1 + u\cdot q_1, \ldots, r_{n-1} + u\cdot q_{n-1}\right)$$

$$= \left(r_{n-1} + u\cdot q_{n-1}, r_0 + u\cdot q_0, \ldots, r_{n-2} + u\cdot q_{n-2}\right)$$

$$= (1+u)\cdot\left(r_{n-1}, r_0, \ldots, r_{n-2}\right) + u\cdot\left(r_{n-1} + q_{n-1}, r_0 + q_0, \ldots, r_{n-2} + q_{n-2}\right)$$

$$= (1+u)\cdot\sigma(r) + u\cdot\sigma(r+q) \underset{ii'\text{den}}{\in} (1+u)\cdot C_1 \oplus u\cdot C_2 \underset{\text{Varsayım}}{=} C$$

O halde C cyclictir.□

3.1.1.Tanım: $\sigma : \mathbb{F}_2^{\,n} \to \mathbb{F}_2^{\,n}$
$\left(a_1, a_2, \ldots, a_n\right) \mapsto \sigma\left(a_1, a_2, \ldots, a_n\right) = \left(a_n, a_1, \ldots, a_{n-1}\right)$ cyclic kaydırma dönüşümü olsun. $i = 1, 2, \ldots, s$ için

$a^{(1)} = \left(a_1, a_2, \ldots, a_n\right) \in \mathbb{F}_2^{\,n}$

$a^{(2)} = \left(a_{n+1}, a_{n+2}, \ldots, a_{2n}\right) \in \mathbb{F}_2^{\,n}$

$a^{(3)} = \left(a_{2n+1}, a_{2n+2}, \ldots, a_{3n}\right) \in \mathbb{F}_2^{\,n}$

$\vdots$

$a^{(i)} = \left(a_{(i-1)\cdot n+1}, a_{(i-1)\cdot n+2}, \ldots, a_{i\cdot n}\right) \in \mathbb{F}_2^{\,n}$ olmak üzere;

Her $a = \left(a_1, a_2, \ldots, a_{n\cdot s}\right) \in \mathbb{F}_2^{\,n\cdot s}$ elemanı $a = \left(a^{(1)} \middle| a^{(2)} \middle| \ldots \middle| a^{(s)}\right) \in \mathbb{F}_2^{\,n\cdot s}$ gösterimiyle yazıldığı düşünülürse

$$\sigma^{\otimes s} : \mathbb{F}_2^{\,n\cdot s} \to \mathbb{F}_2^{\,n\cdot s}$$

$$a = \left(a_1, a_2, \ldots, a_{n\cdot s}\right) \mapsto \sigma^{\otimes s}(a) = \sigma^{\otimes s}\left(a^{(1)} \middle| a^{(2)} \middle| \ldots \middle| a^{(s)}\right) = \left(\sigma\left(a^{(1)}\right) \middle| \sigma\left(a^{(2)}\right) \middle| \ldots \middle| \sigma\left(a^{(s)}\right)\right)$$

biçiminde tanımlanan $\sigma^{\otimes s}$ dönüşümüne bir quasi-cyclic dönüşümü denir. (Zhu vd., 2010)

3.1.2.Tanım: $\sigma^{\otimes s}$ dönüşümü quasi-cyclic bir dönüşüm olmak üzere bir $C \subseteq \mathbb{F}_2^{\,n\cdot s}$ kodu için eğer $\sigma^{\otimes s}(C) = C$ oluyorsa C koduna indexi s uzunluğu $n\cdot s$ olan bir quasi-cyclic kod denir. (Zhu vd., 2010)

3.1.8.Teorem: Eğer C R üzerinde n uzunluklu bir cyclic kod ise $\Phi(C)$ indexi 2 uzunluğu $2\cdot n$ olan bir ikili quasi-cyclic koddur. (Zhu vd., 2010)

Kanıt: $\sigma : \mathbb{F}_2^{\,n} \to \mathbb{F}_2^{\,n}$ cyclic kaydırma dönüşümü ve

$a^{(1)} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^{\,n}$

$a^{(2)} = (a_{n+1}, a_{n+2}, \ldots, a_{2\cdot n}) \in \mathbb{F}_2^{\,n}$ olmak üzere;

Herhangi bir $a = (a_1, a_2, \ldots, a_{2\cdot n}) \in \mathbb{F}_2^{\,2\cdot n}$ elemanı $a = \left(a^{(1)} \middle| a^{(2)}\right)$ gösterimiyle yazılırsa $\mathbb{F}_2$ üzerinde $2\cdot n$ uzunluklu, 2 indexli quasi-cyclic dönüşümü

$$\sigma^{\otimes 2} : \mathbb{F}_2^{\,2\cdot n} \to \mathbb{F}_2^{\,2\cdot n}$$

$a = (a_1, a_2, \ldots, a_{2n}) \mapsto \sigma^{\otimes 2}(a) = \sigma^{\otimes s}\left(a^{(1)} \middle| a^{(2)}\right) = \left(\sigma\left(a^{(1)}\right) \middle| \sigma\left(a^{(2)}\right)\right)$ biçimindedir.

Ayrıca R^n üzerindeki cyclic kaydırma dönüşümü

$$\sigma : R^n \to R^n$$

$x = (x_0, x_1, \ldots, x_{n-1}) \mapsto \sigma(x) = (x_{n-1}, x_0, \ldots, x_{n-1})$ verilsin.

$\left(\sigma^{\otimes 2}(\Phi(C)) \underset{?}{=} \Phi(C) \Leftrightarrow \text{Herhangi bir } a = (a_1, a_2, \ldots, a_{2\cdot n}) \in \Phi(C) \text{ için; } \sigma^{\otimes 2}(a) \underset{?}{\in} \Phi(C)\right)$

$\Rightarrow$: Herhangi bir $a = (a_1, a_2, \ldots, a_n, a_{n+1}, a_{n+2}, \ldots, a_{2\cdot n}) \in \Phi(C)$

$\Rightarrow (a_n, a_1, a_2, \ldots, a_{n-1}, a_{2\cdot n}, a_{n+1}, a_{n+2}, \ldots, a_{2\cdot n-1}) \in \Phi(C)$

$\Rightarrow \sigma^{\otimes 2}(a) \in \Phi(C)$

O halde $\Phi(C) \subseteq \mathbb{F}_2^{\,2\cdot n}$ 2 indexli bir quasi-cyclic koddur. □

$\mathbb{F}_2$ üzerinde n uzunluklu herhangi bir C cyclic kodu $\mathbb{F}_2[x] \Big/ \langle x^n - 1 \rangle$ bölüm halkasının bir idealidir.

3.1.9.Teorem:

$$\pi : R^n \to R[x] \Big/ \left(x^n - 1\right)$$

$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto \pi(c) = \overline{c_0 + c_1 \cdot x + \cdots + c_{n-1} \cdot x^{n-1}} = c_0 + c_1 \cdot x + \cdots + c_{n-1} \cdot x^{n-1} + \left(x^n - 1\right)$

biçiminde tanımlanan π dönüşümü bir $R-$homomorfizmadır.

Kanıt: $(R, +, \cdot)$ bir halka R^n ve $R[x] \Big/ \left(x^n - 1\right)$ birer $R-$modüldür. π dönüşümünün toplama ve skalerle çarpma işlemlerini koruduğu kolaylıkla gösterilir.

3.1.4.Sonuç: 3.1.9.Teoremde $R=\mathbb{F}_2$ alınarak benzer biçimde π dönüşümü $\mathbb{F}_2^{\,n}$ vektör uzayı üzerinde tanımlanır ve π bir $\mathbb{F}_2-$homomorfizmadır.

3.1.4.Gösterim: $R[x]\Big/\left(x^n-1\right)$ bölüm halkası R_n olarak gösterilecektir. □

$c=\left(c_0,c_1,\ldots,c_{n-1}\right)\in R^n$ için $\pi(c)=\overline{c_0+c_1\cdot x+\cdots+c_{n-1}\cdot x^{n-1}}\in R[x]\Big/\left(x^n-1\right)$ elemanına c elemanının polinom temsili denir. (Ling, Xing, 2004, s.138)

Özel olarak $R=\mathbb{F}_2$ alınırsa $c=\left(c_0,c_1,\ldots,c_{n-1}\right)\in\mathbb{F}_2^{\,n}$ elemanının polinom temsili $\pi(c)$ benzer biçiminde tanımlanır.

3.1.10.Teorem: Bir C kodun R üzerinde n uzunluklu bir cyclic kod ise $\pi(C)$ 'nin R_n halkasının bir idealidir. Bu ifadenin tersi de doğrudur. (Zhu vd., 2010)

3.1.11.Teorem: C $\mathbb{F}_2$ üzerinde n uzunluklu bir cyclic kod ise $\pi(C)$ $\mathbb{F}_2[x]\Big/\left(x^n-1\right)$ bölüm halkasının bir idealidir. Bu ifadenin tersi de doğrudur. (Ling, Xing, 2004, s.136)

3.1.12.Teorem: Eğer $C=(1+u)\cdot C_1\oplus u\cdot C_2$ R üzerinde n uzunluğunda bir cyclic kod , $g_1(x),g_2(x)$ sırasıyla C_1 ve C_2 lineer kodlarının üreteç polinomları ise $\pi(C)=\left\langle\overline{(1+u)\cdot g_1(x)},\overrightarrow{u\cdot g_2(x)}\right\rangle$ ve $|C|=2^{2n-d^o(g_1(x))-d^o(g_2(x))}$ 'dir. (Zhu vd., 2010)

Kanıt: $\pi(C_1)=\left\langle\overline{g_1(x)}\right\rangle,\pi(C_2)=\left\langle\overline{g_2(x)}\right\rangle$ ve $C=(1+u)\cdot C_1\oplus u\cdot C_2\subseteq R^n$ bir cyclic kod olsun. $\pi(C)=(1+u)\cdot\left\langle\overline{g_1(x)}\right\rangle\oplus u\cdot\left\langle\overline{g_2(x)}\right\rangle$

$$\Rightarrow\pi(C)=\left\{\overline{c(x)}=\overline{(1+u)\cdot g_1(x)}\cdot\overline{r_1(x)}+\overline{u\cdot g_2(x)}\cdot\overline{r_2(x)}\,\middle|\,\overline{r_1(x)},\overline{r_2(x)}\in\mathbb{F}_2[x]\Big/\left\langle x^n-1\right\rangle\right\}$$

$$\Rightarrow\pi(C)\subseteq\left\langle\overline{(1+u)\cdot g_1(x)},\overrightarrow{u\cdot g_2(x)}\right\rangle\subseteq R_n\ldots(i)$$

Herhangi bir

$$\overline{(1+u)\cdot g_1(x)}\cdot\overline{k_1(x)}+\overline{u\cdot g_2(x)}\cdot\overline{k_2(x)}\in\left\langle\overline{(1+u)\cdot g_1(x)},\overline{u\cdot g_2(x)}\right\rangle\left(\overline{k_1(x)},\overline{k_2(x)}\in R_n\right)$$

alınsın.

$$\left.\begin{array}{l}(1+u)\cdot(1+u)=1+u+u+u^2 \underset{u^2=u}{=} 1+2\cdot u+u \underset{CharR=2}{=} 1+u=(1+u)\cdot \underset{\in\mathbb{F}_2}{1}\\ (1+u)\cdot u=u+u^2 \underset{u^2=u}{=} u+u=2\cdot u \underset{CharR=2}{=} 0=(1+u)\cdot \underset{\in\mathbb{F}_2}{0}\\ (1+u)\cdot 1=(1+u)\cdot \underset{\in\mathbb{F}_2}{1}\\ (1+u)\cdot 0=(1+u)\cdot \underset{\in\mathbb{F}_2}{0}\end{array}\right\}\ldots(ii)$$

$$\left.\begin{array}{l}u\cdot(1+u)=u+u^2 \underset{u^2=u}{=} u+u=2\cdot u \underset{CharR=2}{=} 0=u\cdot \underset{\in\mathbb{F}_2}{0}\\ u\cdot u=u^2 \underset{u^2=u}{=} u=u\cdot \underset{\in\mathbb{F}_2}{1}\\ u\cdot 1=u\cdot \underset{\in\mathbb{F}_2}{1}\\ u\cdot 0=u\cdot \underset{\in\mathbb{F}_2}{0}\end{array}\right\}\cdots(iii)$$

ii ve *iii*'de verilen çarpma işlemlerinden dolayı katsayıları R halkasında olan $k_1(x)$ ve $k_2(x)$ polinomları sırasıyla katsayıları $\mathbb{F}_2$ cisminde olan uygun $r_1(x)$ ve $r_2(x)$ polinomları olarak yazılabilir. Bu durumda $(1+u)\cdot \underset{\in R[x]}{k_1(x)}=(1+u)\cdot r_1(x)$ ve

$u\cdot \underset{\in R[x]}{k_2(x)}=u\cdot r_2(x)$ olacak biçimde öyle bir $r_1(x), r_2(x)\in\mathbb{F}_2[x]$ vardır.

O halde $\left\langle \overline{(1+u)\cdot g_1(x)}, \overline{u\cdot g_2(x)}\right\rangle \subseteq \pi(C)\ldots(iv)$

O halde *i* ve *iv*'den $\pi(C)=\left\langle \overline{(1+u)\cdot g_1(x)}, \overline{u\cdot g_2(x)}\right\rangle$'dir.

Ayrıca

$$\left.\begin{array}{l}\pi(C_1)=\left\langle \overline{g_1(x)}\right\rangle \Rightarrow |C_1|=2^{n-d^o(g_1(x))}\\ \pi(C_2)=\left\langle \overline{g_2(x)}\right\rangle \Rightarrow |C_2|=2^{n-d^o(g_2(x))}\end{array}\right\} \underset{|C|=|C_1|\cdot|C_2|}{\Rightarrow} |C|=2^{2n-d^o(g_1(x))-d^o(g_2(x))} \text{ olur.}$$

3.1.13.Teorem: $g_1(x)$, $g_2(x)$ sırasıyla, $\mathbb{F}_2$ üzerinde tanımlı C_1 ve C_2 lineer kodlarının üreteç polinomları olmak üzere C R üzerinde n uzunluğunda bir cyclic kod olsun. Bu durumda $\pi(C)=\left\langle \overline{g(x)}\right\rangle$ olacak biçimde tek türlü tanımlı $g(x)$ polinomu vardır. $g(x)=g_1(x)+u\cdot(g_1(x)+g_2(x))$ biçiminde ise $g(x)$ polinomu

$\left(x^n-1\right)$ polinomunun bir bölenidir. Özellikle $g_1(x)=g_2(x)$ ise $g(x)=g_1(x)$'dir. (Zhu vd., 2010)

Kanıt: 3.1.12.Teorem'den $\pi(C)=\left\langle \overline{(1+u)\cdot g_1(x)}, \overline{u\cdot g_2(x)} \right\rangle$'dir.

Her $\left(\overline{(1+u)\cdot g_1(x)}+\overline{u\cdot g_2(x)}\right)\cdot \overline{r(x)} \in \left\langle \overline{g(x)} \right\rangle = \left\langle \overline{(1+u)\cdot g_1(x)+u\cdot g_2(x)} \right\rangle$ için $\overline{(1+u)\cdot g_1(x)}\cdot\overline{r(x)}+\overline{u\cdot g_2(x)}\cdot\overline{r(x)} \in \pi(C)=\left\langle \overline{(1+u)\cdot g_1(x)}, \overline{u\cdot g_2(x)} \right\rangle$ sağlanır.

O halde $\left\langle g(x)\right\rangle \subseteq \pi(C) \ldots (i)$

$$\left.\begin{array}{l} g(x)=(1+u)\cdot g_1(x)+u\cdot g_2(x) \\ \Rightarrow (1+u)\cdot g(x)=(1+u)\cdot\left((1+u)\cdot g_1(x)+u\cdot g_2(x)\right) \\ \Rightarrow (1+u)\cdot g(x)=(1+u)\cdot(1+u)\cdot g_1(x)+(1+u)\cdot u\cdot g_2(x) \\ \Rightarrow (1+u)\cdot g(x) \underset{\substack{(1+u)\cdot(1+u)=(1+u)\\ (1+u)\cdot u=0}}{=} (1+u)\cdot g_1(x) \end{array}\right\} \ldots (ii)$$

$$\left.\begin{array}{l} g(x)=(1+u)\cdot g_1(x)+u\cdot g_2(x) \\ \Rightarrow u\cdot g(x)=u\cdot\left((1+u)\cdot g_1(x)+u\cdot g_2(x)\right) \\ \Rightarrow u\cdot g(x)=u\cdot(1+u)\cdot g_1(x)+u\cdot u\cdot g_2(x) \\ \Rightarrow u\cdot g(x) \underset{\substack{u^2=u\\ (1+u)\cdot u=0}}{=} u\cdot g_2(x) \end{array}\right\} \ldots (iii)$$

Herhangi bir $\overline{(1+u)\cdot g_1(x)}\cdot\overline{r_1(x)}+\overline{u\cdot g_2(x)}\cdot\overline{r_2(x)} \in \pi(C)=\left\langle \overline{(1+u)\cdot g_1(x)}, \overline{u\cdot g_2(x)} \right\rangle$ alınsın.

ii ve *iii*'den

$$\overline{(1+u)\cdot g_1(x)\cdot r_1(x)+u\cdot g_2(x)\cdot r_2(x)}=\overline{(1+u)\cdot g(x)\cdot r_1(x)+u\cdot g(x)\cdot r_2(x)}$$

$$=\overline{g(x)}\underbrace{\left(\overline{(1+u)\cdot r_1(x)+u\cdot r_2(x)}\right)}_{\in R_n} \in \left\langle \overline{g(x)} \right\rangle \text{ sağlanır. } \ldots (iv)$$

O halde i ve iv'den $\pi(C)=\left\langle \overline{g(x)} \right\rangle$'dir.

$g(x)\left| x^n-1 \right.$ sağlandığı aşağıdaki biçimde gösterilir.

$\pi(C_1)=\left\langle \overline{g_1(x)} \right\rangle \Rightarrow g_1(x)\left| x^n-1 \right. \Rightarrow x^n-1=g_1(x)\cdot r_1(x)$ olacak biçimde öyle bir $r_1(x)\in \mathbb{F}_2[x]$ vardır. Ayrıca

$\pi(C_2)=\langle\overline{g_2(x)}\rangle \Rightarrow g_2(x)\,|\,x^n-1 \Rightarrow x^n-1=g_2(x)\cdot r_2(x)$ olacak biçimde öyle bir $r_2(x)\in\mathbb{F}_2[x]$ vardır. ….(v)

$\Rightarrow x^n-1=(1+u)\cdot(x^n-1)+u\cdot(x^n-1)$

$\Rightarrow x^n-1 \underset{v'den}{=} (1+u)\cdot g_1(x)\cdot r_1(x)+u\cdot g_2(x)\cdot r_2(x)$

$\Rightarrow x^n-1 \underset{ii \text{ ve } iii'den}{=} (1+u)\cdot g(x)\cdot r_1(x)+u\cdot g(x)\cdot r_2(x)$

$\Rightarrow x^n-1=g(x)\cdot\big((1+u)\cdot r_1(x)+u\cdot r_2(x)\big) \Rightarrow g(x)\,|\,x^n-1$'dir.

Şimdi de $g_1(x)=g_2(x)$

$$\underset{3.1.12.Teorem}{\Rightarrow} \pi(C)=\langle\overline{(1+u)\cdot g_1(x)},\overline{u\cdot g_2(x)}\rangle$$

$$\underset{\substack{g_1(x)=g_2(x)\\ \text{Varsayım}}}{=} \langle\overline{(1+u)\cdot g_1(x)},\overline{u\cdot g_1(x)}\rangle$$

$$=\left\{\overline{(1+u)\cdot g_1(x)}\cdot\overline{r_1(x)}+\overline{u\cdot g_1(x)}\cdot\overline{r_2(x)}\,\middle|\,\overrightarrow{r_1(x)},\overline{r_2(x)}\in R_n\right\}$$

$$=\left\{\overline{g_1(x)}\cdot\overline{\big((1+u)\cdot r_1(x)+u\cdot r_2(x)\big)}\,\middle|\,\overline{r_1(x)},\overline{r_2(x)}\in R_n\right\}$$

$$\underset{\substack{\overline{r_3(x)}=\overline{(1+u)\cdot r_1(x)+u\cdot r_2(x)}\\ \text{olacak biçimde öyle bir}\\ \overline{r_3(x)}\in R_n \text{ vardır.}}}{=} \left\{\overline{g_1(x)}\cdot\overline{r_3(x)}\,\middle|\,\overline{r_3(x)}\in R_n\right\}=\langle\overline{g_1(x)}\rangle$$

Diğer taraftan $\pi(C)=\langle\overline{g(x)}\rangle$ idi.

O halde $g(x)=g_1(x)$'dir.□

3.1.3.Tanım: $\tilde{h}(x)=x^{d^o(h(x))}\cdot h(x^{-1})$ biçiminde tanımlanan $\tilde{h}(x)$ polinomuna $h(x)$ polinomunun **reciprocal polinomu** denir. (Huffman & Pless, 2003, s.116)

3.1.3.Lemma: C $\mathbb{F}_q$ üzerinde, $g(x)$ üreteç polinomlu bir $[n,k]-$kod ve $h(x)=\dfrac{(x^n-1)}{g(x)}$ olsun. Bu durumda $C^{\perp}$ kodunun üreteç polinomu $\dfrac{x^k}{h(0)}\cdot h(x^{-1})$ polinomudur. Ayrıca $h(x)$ monik ise $C^{\perp}$ kodunun üreteç polinomu $\tilde{h}(x)$ polinomu olur. (Zhu vd., 2010)

3.1.5.Sonuç: $g_1(x)$ C_1'in ve $g_2(x)$ C_2'nin üreteç polinomları ,

$h_1(x)=\dfrac{x^n-1}{g_1(x)}$, $h_2(x)=\dfrac{x^n-1}{g_2(x)}$ ve $\Phi(C)=C_1\otimes C_2$ olmak üzere

$C=(1+u)\cdot C_1\oplus u\cdot C_2$ kodu R üzerinde n uzunluklu bir cyclic kod ise

$\pi(C^{\perp})=\left\langle\overline{(1+u)\cdot\tilde{h}_1(x)+u\cdot\tilde{h}_2(x)}\right\rangle$ ve $|C^{\perp}|=2^{d^o(g_1(x))+d^o(g_2(x))}$'dir. (Zhu vd., 2010)

Kanıt: $\Phi(C)=C_1\otimes C_2$ ve $C=(1+u)\cdot C_1\oplus u\cdot C_2$ R üzerinde tanımlı n uzunluğunda bir cyclic kod

$\underset{\text{3.1.3.}Sonuç}{\Rightarrow} C^{\perp}=(1+u)\cdot C_1^{\perp}\oplus u\cdot C_2^{\perp}$'dir.

$\underset{\substack{\tilde{h}_1(x);\ C_1^{\perp}\text{'in}\\ \tilde{h}_2(x);\ C_2^{\perp}\text{'in}\\ \text{üreteç polinomları}\\ \text{ve}\\ \text{3.1.13.Teorem'den}}}{\Rightarrow}$ $\pi(C^{\perp})=\left\langle\overline{(1+u)\cdot\tilde{h}_1(x)+u\cdot\tilde{h}_2(x)}\right\rangle$'dir.

3.1.14.Teorem: n tek doğal sayı olmak üzere C R üzerinde n uzunluklu bir cyclic kod olsun. C cyclic kodu için $\pi(C)=\left\langle\overline{e(x)}\right\rangle$ olacak şekilde tek türlü belirli idempotent $\overline{e(x)}\in\pi(C)$ elemanı vardır. (Zhu vd., 2010)

Kanıt: $\pi(C_1)\subseteq\mathbb{F}_2[x]/(x^n-1)$ $\underset{\text{2.2.2.}Lemma}{\Rightarrow}$ $\pi(C_1)=\left\langle\overline{e_1(x)}\right\rangle$ olacak şekilde $\exists!\overline{e_1(x)}\in\pi(C_1)$ idempotent elemanı vardır. Benzer şekilde; $\pi(C_2)\subseteq\mathbb{F}_2[x]/(x^n-1)$ $\underset{\text{2.2.2.}Lemma}{\Rightarrow}$ $\pi(C_2)=\left\langle\overline{e_2(x)}\right\rangle$ olacak şekilde $\exists!\,\overline{e_2(x)}\in\pi(C_2)$ idempotent elemanı vardır

$$e(x)=(1+u)\cdot e_1(x)+u\cdot e_2(x)=e_1(x)+u\cdot(e_1(x)+e_2(x))$$

$\underset{\text{3.1.13.Teorem}}{\Rightarrow}$ $\pi(C)=\left\langle\overline{(1+u)\cdot e_1(x)+u\cdot e_2(x)}\right\rangle$

$\overline{e(x)}\in\pi(C)$ idempotent olduğu gösterilecektir.

$$\left(\overline{e(x)}\right)^2 = \left(\overline{(1+u)\cdot e_1(x)+u\cdot e_2(x)}\right)^2$$

$$= \overline{(1+u)^2\cdot\left(e_1(x)\right)^2 + u^2\cdot\left(e_2(x)\right)^2 + \underbrace{2\cdot(1+u)\cdot e_1(x)\cdot u\cdot e_2(x)}_{=0(CharR_n=2)}}$$

$$\underset{\substack{e_1(x) \text{ ve } e_2(x) \\ \text{idempotent,} \\ u^2=u}}{=} \overline{(1+u)\cdot e_1(x)+u\cdot e_2(x) = e(x)}$$

O halde $\overline{e(x)} \in \pi(C)$ idempotenttir.

$\overline{e(x)} \in \pi(C)$ tek şekilde tanımlı olduğu gösterilecektir.

$\overline{d(x)} \in \pi(C), \pi(C) = \langle \overline{d(x)} \rangle$ ve $\left(\overline{d(x)}\right)^2 = \overline{d(x)}$ olsun.

$\overline{d(x)} \in \pi(C) = \langle \overline{e(x)} \rangle \Rightarrow \overline{d(x)} = \overline{a(x)}\cdot\overline{e(x)}$ olacak biçimde $\overline{a(x)} \in R_n$ vardır. $\cdots(i)$

$$\Rightarrow \overline{e(x)}\cdot\overline{d(x)} = \left(\overline{e(x)}\right)^2\cdot\overline{a(x)}$$

$$\underset{\substack{\overline{e(x)} \\ \text{idempotent}}}{\Rightarrow} \overline{e(x)}\cdot\overline{d(x)} = \overline{e(x)}\cdot\overline{a(x)}$$

$$\underset{i'den}{\Rightarrow} \overline{e(x)}\cdot\overline{d(x)} = \overline{d(x)} \ldots (ii)$$

$\overline{e(x)} \in \pi(C) = \langle \overline{d(x)} \rangle \Rightarrow \overline{e(x)} = \overline{b(x)}\cdot\overline{d(x)}$ olacak biçimde en az bir $\overline{b(x)} \in R_n$ vardır. $\cdots(iii)$

$$\Rightarrow \overline{e(x)}\cdot\overline{d(x)} = \overline{b(x)}\cdot\left(\overline{d(x)}\right)^2$$

$$\underset{\substack{d(x) \\ \text{idempotent}}}{\Rightarrow} \overline{e(x)}\cdot\overline{d(x)} = \overline{b(x)}\cdot\overline{d(x)}$$

$$\underset{iii'den}{\Rightarrow} \overline{e(x)}\cdot\overline{d(x)} = \overline{e(x)} \ldots (iv)$$

O halde ii ve iv'den $\overline{e(x)} = \overline{d(x)}$'dir

O halde $\overline{e(x)}$ tek türlüdür.

3.1.15.Teorem: n tek sayı, C R üzerinde n uzunluklu bir cyclic kod, $e(x)$ polinomu C cyclic kodunun idempotent üreteci ise $C^{\perp}$ kodunun idempotent üreteci $1-e(x^{-1})$ polinomudur. (Zhu vd., 2010)

Kanıt: n tek doğal sayı, $C \subseteq R^n$ cyclic kod ve $\pi(C) = \left\langle \overline{e(x)} \right\rangle$,

$e(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 \cdots + a_{n-2} \cdot x^{n-2} + a_{n-1} \cdot x^{n-1}$

$\Rightarrow (a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1}) \in C \subseteq R^n$ 'dir.

$(1-a_0, -a_{n-1}, -a_{n-2}, \ldots, -a_2, -a_1) \in R^n$ elemanı alınsın.

$\underset{i'den}{\Rightarrow} (1-a_0, -a_{n-1}, -a_{n-2}, \ldots, -a_2, -a_1) = (1+a_0, a_{n-1}, a_{n-2}, \ldots, a_2, a_1)$

$$\left.\begin{array}{l} R \text{ halkası üzerindeki toplama işlemine bakıldığında;} \\ (1+u)+(1+u) = 0 \Rightarrow -(1+u) = (1+u) \\ u+u = 0 \Rightarrow -u = u \\ 1+1 = 0 \Rightarrow -1 = 1 \\ 0+0 = 0 \Rightarrow -0 = 0 \text{ olduğu görülür.} \end{array}\right\} \ldots(i)$$

$$\left.\begin{array}{l} a_o = 0 \Rightarrow a_0 + (a_0)^2 = 0 + 0^2 = 0 + 0 = 0 \\ a_o = 1 \Rightarrow a_0 + (a_0)^2 = 1 + 1^2 = 1 + 1 = 2 \cdot 1 \underset{CharR=2}{=} 0 \\ a_o = u \Rightarrow a_0 + (a_0)^2 = u + u^2 \underset{u^2=u}{=} u + u = 2 \cdot u \underset{CharR=2}{=} 0 \\ a_o = 1+u \Rightarrow a_0 + (a_0)^2 = (1+u) + (1+u)^2 = (1+u) + (1+u) = 2 \cdot (1+u) \underset{CharR=2}{=} 0 \end{array}\right\} \cdots(ii)$$

$(a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1}) \cdot (1+a_0, a_{n-1}, a_{n-2}, \ldots, a_2, a_1)$

$= a_0 \cdot (1+a_0) + \underbrace{a_1 \cdot a_{n-1} + a_2 \cdot a_{n-2} + \cdots + a_{n-2} \cdot a_2 + a_{n-1} \cdot a_1}_{n \text{ tek olduğundan çift sayıda terim vardır.}}$

$= a_0 \cdot (1+a_0) + 2 \cdot \left(a_1 \cdot a_{n-1} + a_2 \cdot a_{n-2} + \cdots + a_{\frac{n-1}{2}} \cdot a_{\frac{n+1}{2}} \right)$

$\underset{CharR=2}{=} a_0 \cdot (1+a_0) + 0 = a_0 + (a_0)^2 \underset{ii}{=} 0$

$\pi(1-a_0, -a_{n-1}, -a_{n-2}, \ldots, -a_2, -a_1) = \overline{(1-a_0) - a_{n-1} \cdot x - a_{n-2} \cdot x^2 - \cdots - a_2 \cdot x^{n-2} - a_1 \cdot x^{n-1}}$

$\underset{\substack{x^n \equiv 1 \bmod (x^n-1) \\ \Rightarrow x^{-n} \equiv 1 \bmod (x^n-1)}}{=} \overline{(1-a_0) - a_{n-1} \cdot x \cdot x^{-n} - a_{n-2} \cdot x^2 \cdot x^{-n} - \cdots - a_2 \cdot x^{n-2} \cdot x^{-n} - a_1 \cdot x^{n-1} \cdot x^{-n}}$

$= \overline{(1-a_0) - a_{n-1} \cdot x^{1-n} - a_{n-2} \cdot x^{2-n} - \cdots - a_2 \cdot x^{n-2-n} - a_1 \cdot x^{n-1-n}}$

$= \overline{1 - a_0 - a_{n-1} \cdot (x^{-1})^{n-1} - a_{n-2} \cdot (x^{-1})^{n-2} - \cdots - a_2 \cdot (x^{-1})^2 - a_1 \cdot x^{-1}}$

$= \overline{1 - \left(a_0 + a_1 \cdot x^{-1} + a_2 \cdot (x^{-1})^2 + \cdots + a_{n-2} \cdot (x^{-1})^{n-2} + a_{n-1} \cdot (x^{-1})^{n-1} \right)}$

$= \overline{1-e\left(x^{-1}\right)} \in \pi\left(C^{\perp}\right) \subseteq R_n$

O halde $\left(1+a_0, a_{n-1}, a_{n-2}, \ldots, a_2, a_1\right) = \left(1-a_0, -a_{n-1}, -a_{n-2}, \ldots, -a_2, -a_1\right) \in C^{\perp}$

$\overline{1-e\left(x^{-1}\right)} \in \pi\left(C^{\perp}\right)$ elemanının bir idempotent eleman olduğu gösterilecektir.

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

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

$$\underset{Char R_n = 2}{=} \overline{1+\left(e\left(x^{-1}\right)\right)^2}$$

$$\underset{\substack{e(x)\text{ idempotent}\\ \left(e\left(x^{-1}\right)\right)^2 = e\left(x^{-1}\right)}}{=} \overline{1+e\left(x^{-1}\right)}$$

O halde $\overline{1-e\left(x^{-1}\right)} \in \pi\left(C^{\perp}\right)$ idempotent elemandır.□

3.1.16.Teorem: $x^n-1 \in \mathbb{F}_2[x]$ polinomu $i=1,2,\ldots,r$ için $p_i(x)$ $\mathbb{F}_2$ üzerinde aralarında asal, sıfırdan farklı polinomlar olmak üzere $x^n-1 = \prod_{i=1}^{r} p_i^{s_i}(x)$ biçiminde tek türlü çarpanlara ayrılır ise R halkası üzerinde n uzunluklu cyclic kodların sayısı $\left(\prod_{i=1}^{r}(s_i+1)\right)^2$'dir. (Zhu vd., 2010)

Kanıt: $x^n-1 \in \mathbb{F}_2[x]$ polinomu $i=1,2,\ldots,r$ için $p_i(x)$ $\mathbb{F}_2$ üzerinde aralarında asal, sıfırdan farklı polinomlar olmak üzere $x^n-1 = \prod_{i=1}^{r} p_i^{s_i}(x)$ biçiminde çarpanlara ayrılsın.

$\underset{2.2.3.Teorem}{\Rightarrow}$ $\mathbb{F}_2$ üzerinde n uzunluğunda $\prod_{i=1}^{r}(s_i+1)$ tane cyclic kod yazılabilir.

$\Rightarrow \mathbb{F}_2$ üzerinde n uzunluğundaki C_1 ve C_2 cyclic kodlarının her birinden $\prod_{i=1}^{r}(s_i+1)$ tane yazılır.

$\underset{\text{3.1.7.}Teorem}{\Rightarrow}$ R üzerinde n uzunluklu $\left(\prod_{i=1}^{r}(s_i+1)\right)\cdot\left(\prod_{i=1}^{r}(s_i+1)\right)=\left(\prod_{i=1}^{r}(s_i+1)\right)^2$ tane $C=(1+u)\cdot C_1\oplus u\cdot C_2$ cyclic kodu yazılır.

$\underset{\substack{R \text{ üzerinde herhangi bir } C \text{ cylic kodu } C=(1+u)\cdot C_1\oplus u\cdot C_2 \text{ biçiminde yazılabilir.}}}{\Rightarrow}$ R halkası üzerinde n uzunluklu cyclic kodların sayısı $\left(\prod_{i=1}^{r}(s_i+1)\right)^2$ 'dir.

3.1.1.Örnek: $x^3-1\in\mathbb{F}_2[x]$ polinomunun $\mathbb{F}_2$ üzerindeki çarpanlara ayrılışı $x^3-1=(1+x)\cdot(1+x+x^2)\in\mathbb{F}_2[x]$'dir. 3.1.16.Teoremden R halkası üzerinde $n=3$ uzunluğunda $((1+1)\cdot(1+1))^2=16$ tane cyclic kod vardır. Bu cyclic kodlardan biri sıfır $\{(0,0,0)\}\subseteq R^3$ cyclic kodu olacağından R halkası üzerinde $n=3$ uzunluğunda 15 tane sıfır olmayan cyclic kod vardır. $i=1,2,\ldots,15$ olmak üzere bu kodlar A_i olarak isimlendirilirse A_i cyclic kodların üreteç polinomları, üreteç matrisleri ve idempotent elemanları aşağıdaki tablodaki gibi verilir.

Kod	Üreteç Matrisi	Üreteç Polinomu	İdempotent Elemanı
A_1	$(1\ \ 1\ \ 1)$	$1+x+x^2$	$1+x+x^2$
A_2	$(u\ \ u\ \ u)$	$u+u\cdot x+u\cdot x^2$	$u+u\cdot x+u\cdot x^2$
A_3	$(1+u\ \ 1+u\ \ 1+u)$	$(1+u)\cdot(1+x+x^2)$	$(1+u)\cdot(1+x+x^2)$
A_4	$\begin{pmatrix}1&1&0\\0&1&1\end{pmatrix}$	$1+x$	$x+x^2$
A_5	$\begin{pmatrix}u&0&u\\0&u&u\end{pmatrix}$	$u+u\cdot x$	$u\cdot x+u\cdot x^2$
A_6	$\begin{pmatrix}1+u&0&1+u\\0&1+u&1+u\end{pmatrix}$	$(1+u)+(1+u)\cdot x$	$(1+u)\cdot x+(1+u)\cdot x^2$

A_7	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	1	1
A_8	$\begin{pmatrix}u&0&0\\0&u&0\\0&0&u\end{pmatrix}$	u	u
A_9	$\begin{pmatrix}1+u&0&0\\0&1+u&0\\0&0&1+u\end{pmatrix}$	$1+u$	$1+u$
A_{10}	$\begin{pmatrix}1&1&1+u\\0&u&u\end{pmatrix}$	$1+x+(1+u)\cdot x^2$	$(1+u)+x+x^2$
A_{11}	$\begin{pmatrix}1&1&u\\0&1+u&1+u\end{pmatrix}$	$1+x+u\cdot x^2$	$u+x+x^2$
A_{12}	$\begin{pmatrix}1&1&1\\0&u&0\\0&0&u\end{pmatrix}$	$1+(1+u)\cdot x+(1+u)\cdot x^2$	$1+(1+u)\cdot x+(1+u)\cdot x^2$
A_{13}	$\begin{pmatrix}1&1&1\\0&1+u&0\\0&0&1+u\end{pmatrix}$	$1+u\cdot x+u\cdot x^2$	$1+u\cdot x+u\cdot x^2$
A_{14}	$\begin{pmatrix}1&0&1\\0&1&1\\0&0&u\end{pmatrix}$	$1+(1+u)\cdot x$	$u+(1+u)\cdot x+(1+u)\cdot x^2$
A_{15}	$\begin{pmatrix}1&0&1\\0&1&1\\0&0&1+u\end{pmatrix}$	$1+u\cdot x$	$(1+u)+u\cdot x+u\cdot x^2$

(Zhu vd., 2010)

Bu tablo şu adımlar uygulanarak elde edilmiştir.

I. $x^3-1=(1+x)\cdot(1+x+x^2)\in\mathbb{F}_2[x]$ Çarpanlara ayrılışından elde edilen $\{1,1+x,1+x+x^2,1+x^3\}$ kümesinden keyfi olarak C_1 ve C_2 lineer kodları için sırasıyla $g_1(x)$ ve $g_2(x)$ üreteç polinomları seçilir.

II. 2.2.2.Önerme'den $g_1(x)$ ve $g_2(x)$ üreteç polinomları kullanılarak sırasıyla C_1 cyclic kodu için G_1, C_2 cyclic kodu için G_2 üreteç matrisi elde edilir.

III. 3.1.1.Sonuç'tan $C \subseteq R^3$ cyclic kodu için $G = \begin{pmatrix} (1+u)\cdot G_1 \\ u \cdot G_2 \end{pmatrix}$ matrisi yazılır.

IV. Ayrıca 3.1.13.Teorem'den $C \subseteq R^3$ cyclic kodu için bir üreteç polinomu olan $g(x) = g_1(x) + u \cdot (g_1(x) + g_2(x))$ polinomu elde edilir.

V. $\pi(C) = \langle \overline{g(x)} \rangle = \left\{ \overline{r(x)} \cdot \overline{g(x)} \middle| \overline{r(x)} \in R_n \right\}$ kümesinin idempotent elemanı yazılır.

Tablodaki kodların üreteç polinomları, üreteç matrisleri ve idempotent elemanların bulunmasıyla ilgili örnek verilmek istenirse:

I.Örnek: Tablodaki A_4 kodunun üreteç polinomu ve üreteç matrisi şu şekilde elde edilmiştir: $C_1 \subseteq \mathbb{F}_2^{\,3}$ cyclic kodunun üreteç polinomu $g_1(x) = 1+x$ seçilsin. Yani; $\pi(C_1) = \langle \overline{1+x} \rangle$ 'dir. $C_2 \subseteq \mathbb{F}_2^{\,3}$ cyclic kodunun üreteç polinomu $g_2(x) = 1+x$ seçilsin. Yani; $\pi(C_2) = \langle \overline{1+x} \rangle$ 'dir. 2.2.2.Önermeden $G_1 = G_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$'dir. 3.1.1.Sonuçtan A_4 cyclic kodunun üreteç matrisi $G = G_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ elde edilir. Ayrıca 3.1.13.Teoremden A_4 cyclic kodunun üreteç polinomu

$g(x) = g_1(x) + u \cdot (g_1(x) + g_2(x)) = 1 + x + u \cdot (1 + x + 1 + x) \underset{Char R_n = 2}{=} 1 + x$ elde edilir.

$\pi(A_4) = \langle \overline{1+x} \rangle = \left\{ \overline{r(x)} \cdot \overline{1+x} \middle| \overline{r(x)} \in R_3 \right\}$ kümesinin idempotent elemanı $\overline{x+x^2} \in \pi(A_4)$'dir. Gerçekten de;

$$\overline{x+x^2} \cdot \overline{x+x^2} = \overline{(x+x^2)\cdot(x+x^2)} = \overline{x^2+x^3+x^3+x^4} = \overline{x^2+2\cdot x^3+x^4} \underset{\substack{Char R_n = 2 \text{ ve} \\ \text{"+"nın değişme} \\ \text{özelliği}}}{=} \overline{x^4+x^2}$$

$$\underset{x^4 = x (\bmod x^3 - 1)}{=} \overline{x+x^2}$$ olur. Bu durumda $A_4 \subseteq R^3$ cyclic kodunun idempotent polinomu $x+x^2$ polinomudur.

II.Örnek: Tablodaki A_{11} kodunun üreteç polinomu ve üreteç matrisi şu şekilde elde edilmiştir: $C_1 \subseteq \mathbb{F}_2^{\,3}$ cyclic kodunun üreteç polinomu $g_1(x)=1+x$, $C_2 \subseteq \mathbb{F}_2^{\,3}$ cyclic kodunun üreteç polinomu $g_2(x)=1+x+x^2$ seçilsin. 2.2.2.Önerme'den $d^o\left(g_1(x)\right)=1 \Rightarrow boy(C_1)=3-1=2$ ve $d^o\left(g_2(x)\right)=2 \Rightarrow boy(C_2)=3-2=1$'dir. Bu durumda; C_1 lineer kodunun üreteç matrisi G_1'in satır sayısı 2 C_2 lineer kodunun üreteç matrisi G_2'nin satır sayısı 1 olur. 2.2.2.Önerme'den $G_1=\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}$ ve $G_2=\begin{pmatrix}1 & 1 & 1\end{pmatrix}$'dir. 3.1.1.Sonuç'tan $G=\begin{pmatrix}(1+u)\cdot G_1\\ u\cdot G_2\end{pmatrix}=\begin{pmatrix}1+u & 1+u & 0\\ 0 & 1+u & 1+u\\ u & u & u\end{pmatrix}$ olur.

Fakat G matrisinin satırlarını eleman kabul eden ; $U=\{(1+u,1+u,0),(0,1+u,1+u),(u,u,u)\}$ kümesi A_{11} cyclic kodu için bir taban değildir. Çünkü $\lambda_1,\lambda_2,\lambda_3 \in R$ olmak üzere $\lambda_1\cdot(1+u,1+u,0)+\lambda_2\cdot(0,1+u,1+u)+\lambda_3\cdot(u,u,u)=(0,0,0)$ eşitliği $\lambda_1=u,\lambda_2=u,\lambda_3=1+u$ değerleri için doğrudur. Yani; $U \subseteq R^3$ kümesi lineer bağımsız değildir. G matrisine sırasıyla; 3. satırın 1. satıra eklenmesi ve 3. satırın u skaleriyle çarpılması elementer satır işlemleri uygulanırsa; A_{11} cyclic kodunun üreteç matrisi $G=\begin{pmatrix}1 & 1 & u\\ 0 & 1+u & 1+u\end{pmatrix}$ elde edilir.

3.1.13.Teoremden; A_{11} cyclic kodunun üreteç polinomu

$g(x)=g_1(x)+u\cdot\left(g_1(x)+g_2(x)\right)=1+x+u\cdot\left(1+x+1+x+x^2\right)\underset{CharR_n=2}{=}1+x+u\cdot x^2$'dir.

$\pi(A_{11})=\left\langle\overline{1+x+u\cdot x^2}\right\rangle=\left\{\overline{r(x)}\cdot\overline{1+x+u\cdot x^2}\,\middle|\,\overline{r(x)}\in R_3\right\}$ kümesinin idempotent elemanı $\overline{u+x+x^2}\in\pi(A_{11})$'dir. Gerçekten de;

$\overline{\left(u+x+x^2\right)}\cdot\overline{\left(u+x+x^2\right)}=\overline{u^2+u\cdot x+u\cdot x^2+u\cdot x+x^2+x^3+u\cdot x^2+x^3+x^4}$

$=\overline{u^2+2\cdot u\cdot x+2\cdot u\cdot x^2+2\cdot x^3+x^2+x^4}\underset{\substack{u^2=u\\ x^4=x(\mathrm{mod}\,x^3-1)\\ CharR_n=2}}{=}\overline{u+x+x^2}$ olur.

Bu durumda; $A_{11} \subseteq R^3$ cyclic kodunun idempotent polinomu $u + x + x^2$ polinomudur.

3.1.2.Örnek: $x^4 - 1 \in \mathbb{F}_2[x]$ polinomunun $\mathbb{F}_2$ üzerindeki çarpanlara ayrılışı $x^4 - 1 = (1+x)^4 \in \mathbb{F}_2[x]$ biçimindedir. 3.1.16.Teoremden R halkası üzerinde $n = 4$ uzunluğunda $((4+1))^2 = 25$ tane cyclic kod vardır. Bu cyclic kodlardan biri sıfır $\{(0,0,0,0)\} \subseteq R^4$ cyclic kodu olacağından R halkası üzerinde $n = 4$ uzunluğunda 24 tane sıfır olmayan cyclic kod vardır. $i = 1, 2, \ldots, 24$ olmak üzere bu kodlar B_i olarak isimlendirilirse $B_i \subseteq R^3$ cyclic kodlar için üreteç polinomları aşağıdaki gibi listelenir.

Kod	Üreteç Polinomu	Kod	Üreteç Polinomu
B_1	$1+x+x^2+x^3$	B_{13}	$1+x+u\cdot x^2+u\cdot x^3$
B_2	$1+x$	B_{14}	$1+u\cdot x+x^2+u\cdot x^3$
B_3	1	B_{15}	$(1+u)$
B_4	$1+x^2$	B_{16}	$(1+u)+(1+u)\cdot x$
B_5	u	B_{17}	$(1+u)+(1+u)\cdot x^2$
B_6	$u+u\cdot x$	B_{18}	$(1+u)+(1+u)\cdot x+(1+u)\cdot x^2+(1+u)\cdot x^3$
B_7	$u+u\cdot x^2$	B_{19}	$1+(1+u)\cdot x$
B_8	$u+u\cdot x+u\cdot x^2+u\cdot x^3$	B_{20}	$1+(1+u)\cdot x^2$
B_9	$1+u\cdot x$	B_{21}	$1+(1+u)\cdot x+(1+u)\cdot x^2+(1+u)\cdot x^3$
B_{10}	$1+u\cdot x^2$	B_{22}	$1+(1+u)\cdot x+(1+u)\cdot x^2$
B_{11}	$1+u\cdot x+u\cdot x^2+u\cdot x^3$	B_{23}	$1+x+(1+u)\cdot x^2+(1+u)\cdot x^3$
B_{12}	$1+u\cdot x+(1+u)\cdot x^2$	B_{24}	$1+(1+u)\cdot x+x^2+(1+u)\cdot x^3$

(Zhu vd., 2010)

3.1.3.Örnek: $n=7$ için $x^7-1\in\mathbb{F}_2[x]$ polinomunun $\mathbb{F}_2$ üzerindeki çarpanlara ayrılışı $x^7-1=(1+x)\cdot(1+x+x^3)\cdot(1+x^2+x^3)\in\mathbb{F}_2[x]$ biçimindedir. 3.1.16.Teoremden R halkası üzerinde $n=7$ uzunluğunda $((1+1)\cdot(1+1)\cdot(1+1))^2=64$ tane cyclic kod vardır. Bu cyclic kodlardan biri sıfır $\{(0,0,0,0,0,0,0)\}\subseteq R^7$ cyclic kodu olacağından R halkası üzerinde $n=7$ uzunluğunda 63 tane sıfır olmayan cyclic kod vardır. Eğer $g_1(x)=(1+x)$, $g_2(x)=(1+x+x^3)$ ve $g_3(x)=1+x^2+x^3$ denilirse R üzerinde 7 uzunluğundaki tüm cyclic kodların π dönüşümü altındaki görüntüleri üreteç polinomları cinsinden aşağıdaki gibi listelenir:

$\langle\bar{1}\rangle,\langle\bar{u}\rangle,\langle\overline{1+u}\rangle$
$i=1,2,3$ için; $\langle\overline{g_i}\rangle,\langle\overline{u\cdot g_i}\rangle,\langle\overline{(1+u)\cdot g_i}\rangle$
$i=1,2,3$ için; $\langle\overline{(1+u)+u\cdot g_i}\rangle,\langle\overline{(1+u)\cdot g_i+u}\rangle$
$i,j=1,2,3$ ve $i\neq j$ için; $\langle\overline{(1+u)\cdot g_i+u\cdot g_j}\rangle$
$i,j=1,2,3$ ve $i\neq j$ için; $\langle\overline{g_i\cdot g_j}\rangle,\langle\overline{u\cdot g_i\cdot g_j}\rangle,\langle\overline{(1+u)\cdot g_i\cdot g_j}\rangle$
$i,j=1,2,3$ ve $i\neq j$ için; $\langle\overline{(1+u)+u\cdot g_i\cdot g_j}\rangle,\langle\overline{(1+u)\cdot g_i\cdot g_j+u}\rangle$
$i,j,k=1,2,3$ ve $i\neq j$ için; $\langle\overline{(1+u)\cdot g_i\cdot g_j+ug_k}\rangle$
$i,j,k=1,2,3$ ve $i\neq j$ için; $\langle\overline{(1+u)\cdot g_k+u\cdot g_i\cdot g_j}\rangle$
$i,j,k=1,2,3$ ve $i\neq j$, $i\neq k$, $j\neq k$ için; $\langle\overline{(1+u)\cdot g_i\cdot g_j+u\cdot g_i\cdot g_k}\rangle$

(Zhu vd., 2010)

3.2. $\mathbb{F}_2+u\mathbb{F}_2\,(u^2=0)$, $\mathbb{F}_2+u\mathbb{F}_2\,(u^2=1)$ Halkaları Üzerindeki Cyclic ve $(1+u)-$Constacyclic Kodlar

Bu bölümde $R_1=\mathbb{F}_2+u\,\mathbb{F}_2\left(u^2=1\right)$ halkasının $R_0=\mathbb{F}_2+u\,\mathbb{F}_2\left(u^2=0\right)$ halkasına izomorf olduğu gösterilmiştir. R_0 halkası üzerindeki cyclic kodlarla $(1+u)-$ constacyclic kodlar arasındaki ilişki ve R_0 halkası üzerindeki $(1+u)-$constacyclic kodlarla ikili cyclic kodlar arasındaki ilişki verilmiştir.

$\mathbb{F}_2+u\mathbb{F}_2=\{0,1,u,1+u\}$ kümesi $u^2=0$ ya da $u^2=1$ koşulları ile birer halkadır. $u^2=0$ koşuluyla elde edilen halka R_0, $u^2=1$ koşuluyla elde edilen halka R_1 ile gösterilirse $R_0\cong \mathbb{F}_2[u]/\langle u^2\rangle$ ve $R_1\cong \mathbb{F}_2[u]/\langle u^2-1\rangle$ sağlanır.

Bu bölümde $R_0\cong R_1$ olduğu gösterilmiştir. $R_0{}^n$'den $\mathbb{F}_2{}^{2\cdot n}$ vektör uzayı üzerine bir Gray dönüşümü tanımlanmıştır. R_0 halkası üzerinde n uzunluğunda bir $(1+u)-$ constacyclic kodun Gray dönüşümü altındaki görüntüsünün $2\cdot n$ uzunluğunda bir cyclic kod olduğu gösterilmiştir. R_0 halkası üzerinde n uzunluğunda bir cyclic kodun Gray dönüşümü altındaki görüntüsünün ise $2\cdot n$ uzunluğunda bir cyclic koda denk kod olduğu gösterilmiştir. n tek olmak üzere R_0 halkası üzerinde n uzunluğunda bir cyclic koda karşılık bir $(1+u)-$constacyclic kodun elde edildiği gösterilmiştir.

3.2.1.Teorem: $f:\left(\mathbb{F}_2[u]/\langle u^2-1\rangle,+,\cdot\right)\to\left(\mathbb{F}_2[u]/\langle u^2\rangle,+,\cdot\right)$ biçiminde

$$\overline{a+bu}\mapsto f\left(\overline{a+bu}\right)=\overline{(a+b)+bu}$$

tanımlanan f dönüşümü bir halka izomorfizmasıdır. (Çengellenmiş, 2009a)

Kanıt: f dönüşümünün tanımı, $\mathbb{F}_2[u]/\langle u^2\rangle$ bölüm halkasında çarpma ve toplama işleminin özellikleri göz önüne alındığında f dönüşümünün toplamayı koruduğu kolaylıkla gösterilir. Benzer bir biçimde $u^2=0$ ve $Char\mathbb{F}_2=2$ özellikleri kullanılarak f dönüşümünün çarpmayı koruduğu da kolaylıkla gösterilir.

f fonksiyonunun birebir olduğu gösterilecektir.

Her $\overline{a_1+b_1u}, \overline{a_2+b_2u} \in \mathbb{F}_2[u]/\langle u^2-1\rangle$ için $f\left(\overline{a_1+b_1u}\right) = f\left(\overline{a_2+b_2u}\right)$

$\Rightarrow \overline{(a_1+b_1)+b_1u} = \overline{(a_2+b_2)+b_2u} \in \mathbb{F}_2[u]/\langle u^2\rangle$

$\underset{\substack{Temsilciler\\ Denktir}}{\Rightarrow} ((a_1+b_1)+b_1u)-((a_2+b_2)+b_2u) \in \langle u^2\rangle$

$\Rightarrow (a_1+b_1-a_2-b_2)+(b_1-b_2)u \in \langle u^2\rangle$

$\Rightarrow (a_1+b_1-a_2-b_2)+(b_1-b_2)u = u^2\, g(u)$ olacak biçimde en az bir $g(u) \in \mathbb{F}_2[u]$ vardır.

$\Rightarrow a_1+b_1-a_2-b_2 = 0$ ve $b_1-b_2 = 0 \Rightarrow (a_1-a_2)+(b_1-b_2) = 0$ ve $b_1 = b_2$

$\underset{b_1=b_2}{\Rightarrow} a_1 = a_2$ ve $b_1 = b_2 \Rightarrow \overline{a_1+b_1u} = \overline{a_2+b_2u}$

O halde f birebir bir fonksiyondur.

f fonksiyonunun örten olduğu gösterilecektir.

Herhangi bir $\overline{a+bu} \in \mathbb{F}_2[u]/\langle u^2\rangle$ için

$f\left(\overline{(a-b)+b\cdot u}\right) = \overline{(a-b+b)+b\cdot u} = a+b\cdot u \in \mathbb{F}_2[u]/\langle u^2\rangle$ olacak biçimde en az bir

$\overline{(a-b)+bu} \in \mathbb{F}_2[u]/\langle u^2-1\rangle$ vardır.

O halde f örten bir fonksiyondur.

O halde f bir halka izomorfizmasıdır. □

Bu durumda sırasıyla $\mathbb{F}_2[u]/\langle u^2-1\rangle$ ve $\mathbb{F}_2[u]/\langle u^2\rangle$ bölüm halkalarına izomorf olan R_1 ve R_0 halkaları için $\begin{array}{l}\psi : R_1 \to R_0 \\ a+bu \mapsto \psi(a+bu) = (a+b)+bu\end{array}$ biçiminde tanımlanan ψ dönüşümü bir halka izomorfizmasıdır. ψ dönüşümünün R_1^n'den R_0^n'e genişletilmesi

$$\psi : R_1^{\,n} \to R_0^{\,n}$$

$$c = (a_0 + b_0 u, \ldots, a_{n-1} + b_{n-1} u) \mapsto \psi(c) = ((a_0 + b_0) + b_0 u, \ldots, (a_{n-1} + b_{n-1}) + b_{n-1} u)$$

biçimindedir. (Çengellenmiş, 2009a)□

$j = 0,1$ olmak üzere R_j üzerinde n uzunluklu bir C lineer kodu $R_j^{\,n}$'nin bir R_j − alt modülüdür. (Çengellenmiş, 2009a)

3.2.1.Tanım:

$$w_H : \mathbb{F}_2 \to \{0,1\} \subseteq \mathbb{Z}$$
$$0 \mapsto w_H(0) = 0$$
$$1 \mapsto w_H(1) = 1$$

biçiminde tanımlanan fonksiyona w_H Hamming ağırlık fonksiyonu denir. (Ling, Xing, 2004, s.46)

3.2.2.Tanım: $j = 0,1$ için

$$w_L : R_j \to \{0,1,2\} \subseteq \mathbb{Z}$$
$$1 \mapsto w_L(1) = 1$$
$$0 \mapsto w_L(0) = 0$$
$$u \mapsto w_L(u) = 2$$
$$1 + u \mapsto w_L(1 + u) = 1$$

biçiminde tanımlanan w_L fonksiyonuna R_j üzerinde **Lee ağırlık fonksiyonu** denir. (Dougherty & Shiromoto, 2001)

3.2.3.Tanım: $j = 0,1$ için herhangi bir $x = (x_0, x_1, \ldots, x_{n-1}) \in R_j^{\,n}$ elemanının Lee ağırlığı; $w_L(x) = \sum_{i=0}^{n-1} w_L(x_i)$'dir. (Dougherty & Shiromoto, 2001)

3.2.4.Tanım: $j = 0,1$ için R_j'nin herhangi iki x ve y elemanları için $x - y$ elemanının Lee ağırlığına x ve y elemanları arasındaki Lee uzaklığı denir ve $d_L(x, y)$ biçiminde gösterilir. Yani; $d_L(x, y) = w_L(x - y)$'dir. (Çengellenmiş, 2009a)

3.2.1.Örnek: $R_0 = \mathbb{F}_2 + u\,\mathbb{F}_2 \left(u^2 = 0\right)$ halkası üzerinde 3 uzunluklu $C = \{(0,0,0),(0,1,u),(0,u,0),(0,1+u,u)\}$ lineer kodu düşünülsün. C lineer kodunun kod sözcüklerinin Lee ağırlıkları şu şekildedir;

$w_L(0,0,0) = w_L(0) + w_L(0) + w_L(0) = 0+0+0 = 0$

$w_L(0,1,0) = w_L(0) + w_L(1) + w_L(0) = 0+1+0 = 1$

$w_L(0,u,0) = w_L(0) + w_L(u) + w_L(0) = 0+2+0 = 2$

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

$(0,1,u),(0,u,0),(0,1+u,u) \in C$ elemanlarının birbirine olan Lee uzaklıkları ise şu şekildedir;

$d_L((0,1,0),(0,u,0)) = w_L((0,1,0)-(0,u,0)) = w_L(0,1+u,0) = 0+1+0 = 1$

$d_L((0,1,0),(0,1+u,u)) = w_L((0,1,0)-(0,1+u,u)) = w_L(0,u,u) = 0+2+2 = 4$

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

3.2.2.Teorem: $j = 0,1$ için

$$P_j : R_j^{\,n} \to R_j[x] \Big/ \langle x^n - 1 \rangle$$
$$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto P_j(c) = \overline{c_0 + c_1 \cdot x + \cdots + c_{n-1} \cdot x^{n-1}}$$
$$= c_0 + c_1 \cdot x + \cdots + c_{n-1} \cdot x^{n-1} + \langle x^n - 1 \rangle$$

biçiminde tanımlanan P_j dönüşümü bir R_j − homomorfizmadır.

3.2.5.Tanım: $j = 0,1$ için her $c = (c_0, c_1, \ldots, c_{n-1}) \in R_j^{\,n}$ kod sözcüğünün $P_j(c)$ elemanına c kod sözcüğünün polinom temsili denir.

3.2.3.Teorem: $j = 0,1$ için $R_j^{\,n}$'nin boş kümeden farklı bir C alt kümesi R_j üzerinde n uzunluğunda bir lineer cyclic kod ise $P_j(C)$ kümesi $R_j[x] \Big/ \langle x^n - 1 \rangle$ bölüm halkasının bir idealidir. Bu ifadenin tersi de doğrudur. (Çengellenmiş, 2009a)

3.2.6.Tanım: n tek olmak üzere; $\{0,1,2,\ldots,2\cdot n-1\}$ kümesi üzerinde τ permütasyonu; $\tau=(1,n+1)(3,n+3)\cdots(2\cdot i+1,n+2\cdot i+1)\cdots(n-2,2\cdot n-2)$ biçiminde tanımlansın. Bu permütasyon kullanılarak

$$\pi:\mathbb{F}_2^{\,2\cdot n}\to\mathbb{F}_2^{\,2\cdot n}$$
$$c=(c_0,c_1,\ldots,c_{2\cdot n-1})\mapsto\pi(c)=\left(c_{\tau(0)},c_{\tau(1)},\ldots,c_{\tau(2\cdot n-1)}\right)$$

biçiminde tanımlanan π dönüşümüne; $\mathbb{F}_2^{\,2\cdot n}$ üzerinde **Nechaev Permütasyonu** denir. (Çengellenmiş, 2009a)

Bu kısımda π dönüşümü; $\mathbb{F}_2^{\,2\cdot n}$ üzerinde tanımlı Nechaev Permütasyonu olarak kullanılacaktır.

3.2.1.Önerme:

$$\varphi:{R_1[x]}\Big/{\langle x^n-1\rangle}\to{R_0[x]}\Big/{\langle x^n-1\rangle}$$
$$\overline{c(x)}=\overline{c_0+c_1\cdot x+\cdots+c_{n-1}\cdot x^{n-1}}\mapsto\varphi\left(\overline{c(x)}\right)=\overline{\sum_{i=0}^{n-1}\psi(c_i)\cdot x^i}$$

biçiminde tanımlanan φ dönüşümü bir izomorfizmadır. (Çengellenmiş, 2009a)

Kanıt: ψ dönüşümünün tanımlanışı düşünülerek φ dönüşümünün izomorfizma olduğu kolaylıkla gösterilir.

3.2.1.Sonuç: ${R_1[x]}\Big/{\langle x^n-1\rangle}$ bölüm halkasının boş kümeden farklı bir I alt kümesinin bir ideal olması için gerekli ve yeterli koşul $\varphi(I)$ kümesinin ${R_0[x]}\Big/{\langle x^n-1\rangle}$ bölüm halkasının bir ideali olmasıdır.

3.2.2.Önerme: $P_0\circ\psi=\varphi\circ P_1$'dir. (Çengellenmiş, 2009a)

Kanıt: P_0,P_1,ψ ve φ dönüşümlerinden şu diyagram elde edilir:

$$\begin{array}{ccc} R_1^{\,n} & \xrightarrow{P_1} & R_1[x]\Big/\langle x^n-1\rangle \\ \psi\downarrow & \circlearrowright & \downarrow\varphi \\ R_0^{\,n} & \xrightarrow{P_0} & R_0[x]\Big/\langle x^n-1\rangle \end{array}$$

Her $c=(a_0+b_0u, a_1+b_1u, \ldots, a_{n-1}+b_{n-1}u)\in R_1^{\,n}$

$$\Rightarrow \psi(c)=((a_0+b_0)+b_0u,(a_1+b_1)+b_1u,\ldots,(a_{n-1}+b_{n-1})+b_{n-1}u)\in R_0^{\,n}$$

$$\Rightarrow P_0(\psi(c))=\overline{(a_0+b_0)+b_0u,(a_1+b_1)+b_1u,\ldots,(a_{n-1}+b_{n-1})+b_{n-1}u}\in R_0[x]\Big/\langle x^n-1\rangle \cdots (i)$$

Diğer taraftan her $c=(a_0+b_0u, a_1+b_1u, \ldots, a_{n-1}+b_{n-1}u)\in R_1^{\,n}$ için;

$$P_1(c)=\overline{a_0+b_0u+(a_1+b_1u)\cdot x+\ldots+(a_{n-1}+b_{n-1}u)\cdot x^{n-1}}\in R_1[x]\Big/\langle x^n-1\rangle$$

$$\psi(P_1(c))=\overline{\psi(a_0+b_0u)+\psi(a_1+b_1u)\cdot x+\ldots+\psi(a_{n-1}+b_{n-1}u)\cdot x^{n-1}}\in R_0[x]\Big/\langle x^n-1\rangle$$

$$=\overline{(a_0+b_0)+b_0u,(a_1+b_1)+b_1u,\ldots,(a_{n-1}+b_{n-1})+b_{n-1}u}\in R_0[x]\Big/\langle x^n-1\rangle \cdots (ii)$$

O halde i ve ii'den; $P_0\circ\psi=\varphi\circ P_1$ olur.

3.2.2.Sonuç: $R_1^{\,n}$'nin boş kümeden farklı bir C alt kümesi R_1 üzerinde n uzunluğunda bir lineer cyclic kod ise $\psi(C)$ kümesi R_0 üzerinde aynı uzunluklu bir lineer cyclic koddur. Bu ifadenin tersi de doğrudur.□

R_0 halkası üzerindeki cyclic ve constacyclic kodlar için yapılan çalışmalar R_0 ve R_1 halkaları arasındaki ψ izomorfizması kullanılarak R_1 halkası üzerindeki cyclic ve constacyclic kodlar üzerine taşınabilir. Bu alt bölümün devamında sadece R_0 üzerindeki cyclic ve $(1+u)-$constacyclic kodlar incelenecektir.

3.2.3.Önerme:

$$\Phi : R_0 \to \mathbb{F}_2^{\,2}$$
$$z = r + q \cdot u \mapsto \Phi(z) = (q, q + r)$$

biçiminde tanımlanan Φ dönüşümü $R_0^{\,n}$'den $\mathbb{F}_2^{\,2\cdot n}$ vektör uzayına

$$\Phi : R_0^{\,n} \to \mathbb{F}_2^{\,2\cdot n}$$
$$z = (r_1 + q_1 u, r_2 + q_2 u, \ldots, r_n + q_n u) \mapsto \Phi(z) = (q_1, q_2, \ldots, q_n, q_1 + r_1, q_2 + r_2, \ldots, q_n + r_n)$$

biçiminde genelleştirilir. Tanımlanan Φ dönüşümü birebir, örten bir $\mathbb{F}_2-$ homomorfizmadır. (Çengellenmiş, 2009a)

Bu bölüm boyunca $R_0^{\,n}$ üzerinde Φ Gray dönüşümü denildiğinde bu dönüşüm anlatılmaktadır.

3.2.7.Tanım: $$\upsilon : R_0^{\,n} \to R_0^{\,n}$$
$$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto \upsilon(c) = ((1+u)c_{n-1}, c_0, c_1, \ldots, c_{n-2})$$ biçiminde bir υ dönüşümü tanımlansın. R_0 üzerinde n uzunluğunda bir C kodu için $\upsilon(C) = C$ oluyorsa C koduna R_0 üzerinde n uzunluğunda bir $(1+u)-$constacyclic kod denir. (Qian, Zhang & Zhu, 2006)

3.2.4.Teorem:

$$P_2 : R_0^{\,n} \to R_0[x] \Big/ \langle x^n - (1+u) \rangle$$
$$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto P_2(c) = \overline{c_0 + c_1 \cdot x + \ldots + c_{n-1} \cdot x^{n-1}} = c_0 + c_1 \cdot x + \ldots + c_{n-1} \cdot x^{n-1} + \langle x^n - (1+u) \rangle$$

biçiminde tanımlanan P_2 dönüşümü bir R_0-homomorfizmadır.

Kanıt: $R_0[x] \Big/ \langle x^n - (1+u) \rangle$ bölüm homomorfizmasının bir R_0-modül olduğu gösterilir. Daha sonra P_2 dönüşümün bir R_0-homomorfizma olduğu kolaylıkla gösterilir.

3.2.5.Teorem: $R_0^{\,n}$'nin boş kümeden farklı bir C alt kümesinin R_0 üzerinde n uzunluğunda bir $(1+u)-$constacyclic kod ise $P_2(C)$ kümesi $R_0[x]\Big/\langle x^n-(1+u)\rangle$ bölüm halkasının bir idealidir. Bu ifadenin tersi de doğrudur. (Qian vd., 2006)

3.2.4.Önerme: $1+u\in R_0$ için n tek bir doğal sayı ise $(1+u)^n=1+u$, n çift bir doğal sayı ise $(1+u)^n=1$'dir. (Qian vd., 2006)

Kanıt: $(1+u)\cdot(1+u)=1+2u+u^2 \underset{\substack{Char R_0=2\\ u^2=0}}{=} 1$ dir. $\cdots(i)$

n tek bir doğal sayı $\Rightarrow n=2\cdot k+1$ olacak biçimde öyle bir $k\in\mathbb{N}$ vardır.

$\Rightarrow (1+u)^n=(1+u)^{2\cdot k+1}=\left((1+u)^2\right)^k\cdot(1+u)\underset{i'\text{den}}{=}1^k\cdot(1+u)=(1+u)$ olur.

n çift bir doğal sayı $\Rightarrow n=2\cdot k$ olacak biçimde öyle bir $k\in\mathbb{N}$ vardır.

$\Rightarrow (1+u)^n=(1+u)^{2\cdot k}=\left((1+u)^2\right)^k\underset{i'\text{den}}{=}1^k=1$ olur.□

Bu bölümün devamında sadece R_0 üzerindeki tek uzunluklu $(1+u)-$ constacyclic kodlar çalışılmıştır.

3.2.5.Önerme: $\mu: R_0[x]\Big/\langle x^n-1\rangle \to R_0[x]\Big/\langle x^n-(1+u)\rangle$, $\overline{c(x)}\mapsto \mu\left(\overline{c(x)}\right)=\overline{c\left((1+u)x\right)}$ biçiminde tanımlanan μ dönüşümü n tek ise bir halka izomorfizmasıdır. (Qian vd., 2006)

Kanıt: μ dönüşümünün tanımlanışından toplama ve çarpma işlemlerini koruduğu kolaylıkla gösterilir.

μ dönüşümünün birebir olduğu gösterilecektir.

Her $\overline{a(x)}=\overline{a_0+a_1\cdot x+\cdots+a_{n-1}\cdot x^{n-1}}, \overline{b(x)}=\overline{b_0+b_1\cdot x+\cdots+b_{n-1}\cdot x^{n-1}}\in R_0[x]\Big/\langle x^n-1\rangle$ için; $\mu\left(\overline{a(x)}\right)=\mu\left(\overline{b(x)}\right)$

$$\Rightarrow \overline{a_0 + a_1(1+u)x + a_2\left((1+u)x\right)^2 \cdots + a_{n-1}\left((1+u)x\right)^{n-1}}$$
$$= \overline{b_0 + b_1(1+u)x + b_2\left((1+u)x\right)^2 \cdots + b_{n-1}\left((1+u)x\right)^{n-1}}$$

$$\Rightarrow \left(b_0 + b_1(1+u)x + b_2\left((1+u)x\right)^2 \cdots + b_{n-1}\left((1+u)x\right)^{n-1}\right)$$
$$-\left(a_0 + a_1(1+u)x + a_2\left((1+u)x\right)^2 \cdots + a_{n-1}\left((1+u)x\right)^{n-1}\right) \in \left\langle x^n - (1+u)\right\rangle$$

$\Rightarrow$ Öyle bir $f(x) \in R_0[x]$ için

$$(b_0 - a_0) + (b_1 - a_1)\cdot(1+u)x + (b_2 - a_2)\cdot\left((1+u)\cdot x\right)^2 \cdots + (b_{n-1} - a_{n-1})\cdot\left((1+u)\cdot x\right)^{n-1}$$
$$= f(x)\cdot\left(x^n - (1+u)\right)$$

$$\Rightarrow a_0 = b_0, a_1 = b_1, \ldots, a_{n-1} = b_{n-1}$$

$$\Rightarrow \overline{a_0 + a_1 \cdot x + \cdots + a_{n-1}\cdot x^{n-1}} = \overline{b_0 + b_1 \cdot x + \cdots + b_{n-1}\cdot x^{n-1}} \Rightarrow \overline{a(x)} = \overline{b(x)}$$

O halde μ birebir bir fonksiyondur.

μ dönüşümünün örten dönüşüm olduğu gösterilecektir.Herhangi bir

$\overline{a(x)} = \overline{a_0 + a_1 \cdot x + \cdots + a_{n-1}\cdot x^{n-1}} \in R_0[x] \Big/ \left\langle x^n - (1+u)\right\rangle$ için

$\mu\left(\overline{b_0 + b_1 \cdot x + \cdots + b_{n-1}\cdot x^{n-1}}\right) = \overline{a_0 + a_1 \cdot x + \cdots + a_{n-1}\cdot x^{n-1}}$ olacak biçimde $0 \le i \le n-1$

için; $b_i = \begin{cases} (1+u)\cdot a_i; & i \text{ tek ise} \\ a_i: & i \text{ çift ise} \end{cases}$ olmak üzere öyle bir

$\overline{b_0 + b_1 \cdot x + \cdots + b_{n-1}\cdot x^{n-1}} \in R_0[x] \Big/ \left\langle x^n - 1\right\rangle$ vardır.

O halde μ örten bir fonksiyondur.

O halde μ bir halka izomorfizmasıdır.

3.2.3.Sonuç: n tek sayı olmak üzere $R_0[x] \Big/ \left\langle x^n - 1\right\rangle$ bölüm halkasının boş kümeden farklı bir I alt kümesi $R_0[x] \Big/ \left\langle x^n - 1\right\rangle$ bölüm halkasının bir ideali ise $\mu(I)$ kümesi $R_0[x] \Big/ \left\langle x^n - (1+u)\right\rangle$ bölüm halkasının bir idealidir. Bu ifadenin tersi de doğrudur. (Qian vd., 2006)

3.2.6.Teorem: n tek sayı olmak üzere;

$$\overline{\mu}: R_0^{\,n} \to R_0^{\,n}$$

$$c=(c_0,c_1,\ldots,c_{n-1}) \mapsto \overline{\mu}(c)=\left(c_0,(1+u)c_1,(1+u)^2 c_2,\ldots,(1+u)^i c_i,\ldots,(1+u)^{n-1} c_{n-1}\right)$$

biçiminde bir $\overline{\mu}$ permütasyonu tanımlansın. $R_0^{\,n}$'nin boş kümeden farklı bir D alt kümesi lineer cyclic kod ise $\overline{\mu}(D)$ kümesi bir lineer $(1+u)-$constacyclic koddur. Bu ifadenin tersi de doğrudur. (Qian vd., 2006)

Kanıt: $\Rightarrow$: n tek doğal sayı ve D, R_0 halkası üzerinde n uzunluğunda bir lineer cyclic kod olsun. Herhangi bir

$$\left(x_0,(1+u)\cdot x_1,(1+u)^2\cdot x_2,(1+u)^3\cdot x_3,\ldots,(1+u)^{n-3}\cdot x_{n-3},(1+u)^{n-2}\cdot x_{n-2},(1+u)^{n-1}\cdot x_{n-1}\right)\in\overline{\mu}(D)$$

alınsın.

$$\underset{\substack{k\in\mathbb{N}\text{ olm. üzr.}\\ (1+u)^{2\cdot k+1}=1+u\\ (1+u)^{2\cdot k}=1}}{\Rightarrow} \left(x_0,(1+u)\cdot x_1,x_2,(1+u)\cdot x_3,\ldots,x_{n-3},(1+u)\cdot x_{n-2},x_{n-1}\right)\in\overline{\mu}(D)$$

$$\underset{\substack{\mu\text{ permütasyon}\\ \mu\text{ birebir ve örten}}}{\Rightarrow} \left(x_0,x_1,x_2,x_3,\ldots,x_{n-3},x_{n-2},x_{n-1}\right)\in D$$

$$\underset{D\text{ cylic kod}}{\Rightarrow} \left(x_{n-1},x_0,x_1,x_2,x_3,\ldots,x_{n-3},x_{n-2}\right)\in D$$

$$\underset{\substack{D\text{ lineer cylic}\\ \text{olduğundan}\\ \text{bir } R_0-\text{modül}}}{\Rightarrow} (1+u)\cdot\left(x_{n-1},x_0,x_1,x_2,x_3,\ldots,x_{n-3},x_{n-2}\right)\in D$$

$$\Rightarrow\left((1+u)\cdot x_{n-1},(1+u)\cdot x_0,(1+u)\cdot x_1,(1+u)\cdot x_2,(1+u)\cdot x_3,\ldots,(1+u)\cdot x_{n-3},(1+u)\cdot x_{n-2}\right)\in D$$

$$\Rightarrow\overline{\mu}\left((1+u)\cdot x_{n-1},(1+u)\cdot x_0,(1+u)\cdot x_1,(1+u)\cdot x_2,(1+u)\cdot x_3,\ldots,(1+u)\cdot x_{n-3},(1+u)\cdot x_{n-2}\right)$$

$$=\left((1+u)\cdot x_{n-1},(1+u)\cdot(1+u)\cdot x_0,(1+u)^2\cdot(1+u)\cdot x_1,(1+u)^3\cdot(1+u)\cdot x_2,\ldots,(1+u)^{n-2}\cdot(1+u)\cdot x_{n-3},(1+u)^{n-1}\cdot(1+u)\cdot x_{n-2}\right)$$

$$\underset{\substack{k\in\mathbb{N}\text{ olm. üzr.}\\ (1+u)^{2\cdot k+1}=1+u\\ (1+u)^{2\cdot k}=1}}{\Rightarrow} \left((1+u)\cdot x_{n-1},x_0,(1+u)\cdot x_1,x_2,(1+u)\cdot x_3,\ldots,x_{n-3},(1+u)\cdot x_{n-2}\right)\in\overline{\mu}(D)$$

O halde $\overline{\mu}(D)\subseteq R_0^{\,n}$ bir $(1+u)-$constacyclic koddur.

$\Leftarrow$: n tek doğal sayı ve $\overline{\mu}(D)$ R_0 halkası üzerinde n uzunluğunda bir lineer $(1+u)-$constacyclic kod olsun. Herhangi bir $(x_0,x_1,\ldots,x_{n-1})\in D$

$$\Rightarrow\overline{\mu}(x_0,x_1,\ldots,x_{n-1})=\left(x_0,(1+u)\cdot x_1,(1+u)^2\cdot x_2,(1+u)^3\cdot x_3,\ldots,(1+u)^{n-2}\cdot x_{n-2},(1+u)^{n-1}\cdot x_{n-1}\right)\in\overline{\mu}(D)$$

$$\underset{\substack{\bar{\mu}(D);\\ (1+u)-\text{constacylic}\\ \text{kod}}}{\Rightarrow} \left((1+u)\cdot(1+u)^{n-1}\cdot x_{n-1}, x_0, (1+u)\cdot x_1, (1+u)^2\cdot x_2, (1+u)^3\cdot x_3, \ldots, (1+u)^{n-2}\cdot x_{n-2}\right) \in \bar{\mu}(D)$$

$$\underset{\substack{\bar{\mu}(D);(1+u)-\text{constacylic}\\ \text{kod olduğundan bir}\\ R_0-\text{modüldür.}}}{\Rightarrow} \left((1+u)^{n+1}\cdot x_{n-1}, (1+u)\cdot x_0, (1+u)^2\cdot x_1, (1+u)^3\cdot x_2, (1+u)^4\cdot x_3, \ldots, (1+u)^{n-1}\cdot x_{n-2}\right) \in \bar{\mu}(D)$$

$$\underset{\substack{\bar{\mu}\text{ bir permütasyon}\\ \text{olduğundan birebirdir.}\\ k\in\mathbb{N}\text{ olmak üzere}\\ (1+u)^{2\cdot k+1}=1+u\\ (1+u)^{2\cdot k}=1}}{\Rightarrow} \left(x_{n-1}, x_0, x_1, \ldots, x_{n-2}\right) \in \bar{\mu}(D)$$

O halde $D \subseteq R_0^{\,n}$ cyclic bir koddur.

3.2.6.Önerme: $\Phi \circ \upsilon = \sigma \circ \Phi$ sağlanır. (Qian vd., 2006)

Kanıt: υ, σ ve Φ dönüşümleri düşünüldüğünde aşağıdaki diyagram elde edilir:

$$\begin{array}{ccc} R_0^{\,n} & \xrightarrow{\Phi} & \mathbb{F}_2^{\,2\cdot n} \\ \upsilon\downarrow & \circlearrowright & \downarrow\sigma \\ R_0^{\,n} & \xrightarrow{\Phi} & \mathbb{F}_2^{\,2\cdot n} \end{array}$$

Her $r = \left(r_0 + q_0 u, r_1 + q_1 u, \ldots, r_{n-1} + q_{n-1} u\right) \in R_0^{\,n}$ alınsın.

$$\Phi\left(\upsilon(r)\right) = \Phi\left((1+u)\cdot\left(r_{n-1} + q_{n-1} u\right), r_0 + q_0 u, r_1 + q_1 u, \ldots, r_{n-2} + q_{n-2} u\right)$$

$$\left.\begin{array}{l} (1+u)\cdot\left(r_{n-1} + q_{n-1} u\right) \\ = r_{n-1} + q_{n-1} u + r_{n-1} u + q_{n-1} u^2 \\ \underset{u^2=0}{=} r_{n-1} + \left(r_{n-1} + q_{n-1}\right) u \end{array}\right\} \cdots (i)$$

$$\underset{i\text{'den}}{=} \Phi\left(r_{n-1} + \left(r_{n-1} + q_{n-1}\right) u, r_0 + q_0 u, r_1 + q_1 u, \ldots, r_{n-2} + q_{n-2} u\right)$$

$$= \left(r_{n-1} + q_{n-1}, q_0, q_1, \ldots, q_{n-2}, r_{n-1} + q_{n-1} + r_{n-1}, q_0 + r_0, \ldots, q_{n-2} + r_{n-2}\right)$$

$$\underset{\substack{+\text{'nın değişme}\\ \text{özelliği ve Char}\mathbb{F}_2=2}}{=} \left(r_{n-1} + q_{n-1}, q_0, q_1, \ldots, q_{n-2}, q_{n-1}, q_0 + r_0, \ldots, q_{n-2} + r_{n-2}\right) \cdots (ii)$$

Diğer taraftan;

$$\sigma\left(\Phi(r)\right) = \sigma\left(q_0, q_1, \ldots, q_{n-1}, q_0 + r_0, q_1 + r_1, \ldots, q_{n-1} + r_{n-1}\right)$$

$$= \left(q_{n-1} + r_{n-1}, q_0, q_1, \ldots, q_{n-1}, q_0 + r_0, q_1 + r_1, \ldots, q_{n-2} + r_{n-2}\right) \cdots (iii)$$

O halde ii ve iii 'den $\Phi \circ \upsilon = \sigma \circ \Phi$ olur.

3.2.4.Sonuç: C R_0 üzerinde n uzunluğunda bir $(1+u)-$constacyclic kod ise $\Phi(C)$ $\mathbb{F}_2$ üzerinde $2\cdot n$ uzunluğunda bir cyclic koddur. (Qian vd., 2006)

Kanıt: $C \subseteq R_0^{\,n}$ bir cyclic kod

$$\underset{\text{3.2.6.Önerme}}{\Rightarrow} \Phi(\upsilon(C)) = \sigma(\Phi(C))$$

$$\underset{\substack{C\ (1+u)-\text{constacylic}\\ \text{kod olduğundan;}\\ \upsilon(C)=C\text{'dir.}}}{\Rightarrow} \Phi(C) = \sigma(\Phi(C))$$

$\Rightarrow \Phi(C) \subseteq \mathbb{F}_2^{\,2\cdot n}$ cyclic koddur.

3.2.7.Önerme: n tek bir doğal sayı olmak üzere $\Phi \circ \overline{\mu} = \pi \circ \Phi$ sağlanır. (Qian vd., 2006)

Kanıt: $\overline{\mu}, \pi$ ve Φ dönüşümleri düşünüldüğünde aşağıdaki diyagram elde edilir:

$$\begin{array}{ccc} R_0^{\,n} & \xrightarrow{\Phi} & \mathbb{F}_2^{\,2\cdot n} \\ \overline{\mu}\downarrow & \circlearrowright & \downarrow \pi \\ R_0^{\,n} & \xrightarrow{\Phi} & \mathbb{F}_2^{\,2\cdot n} \end{array}$$

Herhangi bir $r = (r_0 + q_0 \cdot u, r_1 + q_1 \cdot u, \ldots, r_{n-1} + q_{n-1} \cdot u) \in R_0^{\,n}$ alınsın.

$$\Rightarrow \Phi(\overline{\mu}(r)) = \Phi\left(r_0 + q_0 u, (1+u)\cdot(r_1 + q_1 u), (1+u)^2 \cdot (r_2 + q_2 u), \ldots, (1+u)^{n-1} \cdot (r_{n-1} + q_{n-1} u)\right)$$

$$\underset{\substack{k\in\mathbb{N}\text{ olm. üzr.}\\ (1+u)^{2k+1}=1+u\\ (1+u)^{2k}=1}}{=} \Phi\left(r_0 + q_0 u, (1+u)\cdot(r_1 + q_1 u), r_2 + q_2 u, (1+u)\cdot(r_3 + q_3 u) \ldots, (1+u)\cdot(r_{n-2} + q_{n-2} u) r_{n-1} + q_{n-1} u\right)$$

$$\left(i = 1,3,5,\ldots,n-2 \text{ için; } (1+u)\cdot(r_i + q_i u) = r_i + (r_i + q_i)u\right) \ldots (i)$$

$$\underset{i'den}{=} \Phi\left(r_0 + q_0 u, r_1 + (r_1 + q_1)u, r_2 + q_2 u, r_3 + (r_3 + q_3)u, \ldots, r_{n-2} + (r_{n-2} + q_{n-2})u, r_{n-1} + q_{n-1} u\right)$$

$$= (q_0, r_1 + q_1, q_2, r_3 + q_3, \ldots, r_{n-2} + q_{n-2}, q_{n-1}, r_0 + q_0, r_1 + r_1 + q_1, r_2 + q_2, r_3 + r_3 + q_3, \ldots, r_{n-2} + r_{n-2} + q_{n-2}, r_{n-1} + q_{n-1})$$

$$\underset{Char\mathbb{F}_2=2}{=} (q_0, r_1 + q_1, q_2, r_3 + q_3, \ldots, r_{n-2} + q_{n-2}, q_{n-1}, r_0 + q_0, q_1, r_2 + q_2, q_3, \ldots, q_{n-2}, r_{n-1} + q_{n-1}) \ldots (ii)$$

Diğer taraftan;

$$\pi(\Phi(r)) = \pi(q_0, q_1, q_2, q_3 \ldots, q_{n-3}, q_{n-2}, q_{n-1}, q_0 + r_0, q_1 + r_1, q_2 + r_2, \ldots, q_{n-2} + r_{n-2}, q_{n-1} + r_{n-1})$$

$c_0 = q_0, c_1 = q_1, c_2 = q_2, c_3 = q_3, \ldots, c_{n-3} = q_{n-3}, c_{n-2} = q_{n-2}, c_{n-1} = q_{n-1}, c_n = r_0 + q_0, c_{n+1} = r_1 + q_1,$ $c_{n+2} = r_2 + q_2, \ldots, c_{2\cdot n-1} = r_{n-1} + q_{n-1}$ olmak üzere;

3.2.6.Tanımdan;

$$\pi\left(\Phi\left(r\right)\right)=\left(c_{\tau(0)},c_{\tau(1)},c_{\tau(2)},c_{\tau(3)},\ldots,c_{\tau(n-3)},c_{\tau(n-2)},c_{\tau(n-1)},c_{\tau(n)},c_{\tau(n+1)},c_{\tau(n+2)}c_{\tau(2\cdot n-1)}\right)$$

$$=\left(c_0,c_{n+1},c_2,c_{n+3},\ldots,c_{n-3},c_{2\cdot n-2},c_{n-1},c_n,c_1,c_{n+2},c_3,\ldots,c_{n-2},c_{2\cdot n-1}\right)$$

$$=\left(q_0,r_1+q_1,q_2,r_3+q_3,\ldots,r_{n-2}+q_{n-2},q_{n-1},r_0+q_0,q_1,r_2+q_2,q_3,\ldots,q_{n-2},r_{n-1}+q_{n-1}\right)\ldots\left(iii\right)$$

O halde ii ve iii'den; $\Phi\circ\overline{\mu}=\pi\circ\Phi$ olur.□

3.2.5.Sonuç: n tek sayı ve C R_0 üzerinde n uzunluğunda bir cyclic kod ise $\pi\left(\Phi\left(C\right)\right)$ bir cyclic koddur. (Qian vd., 2006)

Kanıt: n tek bir doğal sayı ve $C\subseteq R_0^{\,n}$ bir cyclic kod

$\underset{\text{3.2.6.Teorem}}{\Rightarrow}$ $\overline{\mu}(C)$ bir$\left(1+u\right)-$constacyclic koddur.

$\underset{\text{3.2.4.Sonuç}}{\Rightarrow}$ $\Phi\left(\overline{\mu}\left(C\right)\right)\subseteq\mathbb{F}_2^{\,2\cdot n}$ bir cyclic koddur.

$\underset{\text{3.2.7.Önerme}}{\Rightarrow}$ $\Phi\left(\overline{\mu}\left(C\right)\right)=\pi\left(\Phi\left(C\right)\right)$ bir cyclic koddur.□

3.2.6.Sonuç: n tek bir doğal sayı ve C R_0 üzerinde n uzunluğunda bir cyclic kod ise $\Phi\left(C\right)$ $\mathbb{F}_2$ üzerinde $2\cdot n$ uzunluğunda bir cyclic koda permütasyon denktir. (Qian vd., 2006)

Kanıt: n tek bir doğal sayı ve C R_0 üzerinde n uzunluğunda bir cyclic kod

$\underset{\text{3.2.5.Sonuç}}{\Rightarrow}$ $\pi\left(\Phi\left(C\right)\right)\subseteq\mathbb{F}_2^{\,2\cdot n}$ cyclic koddur.

$\underset{\substack{\text{2.1.15.Tanım}\\ \text{ve } \pi \text{ permütasyonunun}\\ \text{tanımı}}}{\Rightarrow}$ $\Phi\left(C\right)\subseteq\mathbb{F}_2^{\,2n}$ kodu ile $\pi\left(\Phi\left(C\right)\right)\subseteq\mathbb{F}_2^{\,2\cdot n}$ kodu permütasyon denktir.□

Bir cyclic koda permütasyon denk olan bir kodun cyclic olması gerekmez.

3.2.2.Örnek: $\mathbb{F}_2$ cismi üzerinde 4 uzunluklu

$C_1=\left\{\left(0,0,0,0\right),\left(1,1,1,1\right),\left(1,0,1,0\right),\left(0,1,0,1\right),\left(1,1,0,1\right),\left(1,0,1,1\right),\left(1,1,1,0\right),\left(0,1,1,1\right)\right\}$

cyclic kodunun bileşenlerine

$$g:\{1,2,3,4\}\to\{1,2,3,4\}$$
$$1\mapsto g(1)=1$$
$$2\mapsto g(2)=2$$
$$3\mapsto g(3)=4$$
$$4\mapsto g(4)=3$$

biçiminde tanımlanan g permütasyonunun uygulanmasıyla elde edilen yeni kod C_2 olsun. Bu durumda;

$$C_2=\left\{\left(a_{g(1)},a_{g(2)},a_{g(3)},a_{g(4)}\right)\middle|\left(a_1,a_2,a_3,a_4\right)\in C_1\right\}$$
$$=\left\{(0,0,0,0),(1,1,1,1),(1,0,0,1),(0,1,1,0),(1,1,1,0),(1,0,1,1),(1,1,0,1),(0,1,1,1)\right\}\subseteq\mathbb{F}_2^{\,4}$$

biçimindedir.

$(1,0,0,1)\in C_2$ olmasına rağmen; $(1,1,0,0)\notin C_2$ olduğundan C_2 kodu cyclic değildir.□

3.2.3.Örnek: 2.2.1.Sonuca benzer olarak R_0 üzerinde n uzunluklu cyclic kodlarla $x^n-1\in R_0[x]$ polinomunun monik bölenleri arasında birebir eşleme vardır. $n=7$ için; x^7-1 polinomunun R_0 halkası üzerinde çarpanlara ayrılışı $x^7-1=(x-1)\cdot\left(x^3+x+1\right)\cdot\left(x^3+x^2+1\right)\in R_0[x]$ biçimindedir. R_0 halkası üzerinde 7 uzunluklu bir C cyclic polinomunun üreteç polinomu $(x-1)\cdot\left(x^3+x+1\right)$ olsun. Bu durumda $P_0(C)=\left\langle\overline{(x-1)\cdot\left(x^3+x+1\right)}\right\rangle\subseteq R_0[x]\Big/\left\langle x^7-1\right\rangle$ olur.

$$\mu\left(P_0(C)\right)=\left\langle\mu\left(\overline{(x-1)\cdot\left(x^3+x+1\right)}\right)\right\rangle\underset{iii}{=}\left\langle\overline{(x-(1+u))\cdot\left(x^3+x+1+u\right)}\right\rangle\subseteq R_0[x]\Big/\left\langle x^7-(1+u)\right\rangle$$

$$\left(\begin{array}{l}
\mu\left(\overline{(x-1)\cdot(x^3+x+1)}\right)=\mu\left(\overline{x^4+x^2+x-x^3-x-1}\right)=\mu\left(\overline{x^4+x^2-x^3-1}\right)\\
=\overline{(1+u)^4x^4+(1+u)^2x^2-(1+u)^3x^3-1}\\
\underset{\substack{k\in\mathbb{N}\text{ olm. üzr.}\\(1+u)^{2k+1}=1+u\\(1+u)^{2k}=1}}{=}\overline{x^4+x^2-(1+u)x^3-1}\cdots(i)\\
\left(\overline{x-(1+u)}\right)\cdot\left(\overline{x^3+x+1+u}\right)=\overline{x^4+x^2+x+ux-(1+u)x^3-(1+u)x-(1+u)-u-u^2}\\
=\overline{x^4+x^2-(1+u)x^3+\left((1+u)-(1+u)\right)x-1-2u-u^2}\underset{\substack{Char R_0=2\\u^2=0}}{=}\overline{x^4+x^2-(1+u)x^3+1}\cdots(ii)\\
\text{O halde } i \text{ ve } ii\text{'den; } \mu\left(\overline{(x-1)\cdot(x^3+x+1)}\right)=\overline{\left(x-(1+u)\right)\cdot\left(x^3+x+1+u\right)}\text{'dir.}\ldots(iii)
\end{array}\right)$$

3.2.3.Sonuçtan $\left\langle\overline{\left(x-(1+u)\right)\cdot\left(x^3+x+1+u\right)}\right\rangle\subseteq R_0[x]\Big/\left\langle x^7-(1+u)\right\rangle$ idealine karşılık gelen $\left(x-(1+u)\right)\cdot\left(x^3+x+1+u\right)\in R_0[x]$ üreteç polinomlu $(1+u)-$constacyclic kod $C\subseteq R_0$ olsun.

Ayrıca bu elde edilen C, $(1+u)-$constacyclic kodun Gray dönüşümü altındaki görüntüsü $\Phi(C)\subseteq\mathbb{F}_2^{14}$ bir $[14,9,4]-$koddur. (Qian vd., 2006)

BÖLÜM 4

$\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ HALKASI ÜZERİNDEKİ CYCLIC VE CONSTACYCLIC KODLAR

Bu bölümde $u^2 = 0$ durumunda halka olan $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ halkası üzerindeki cyclic ve constacyclic kodlar incelenmiştir. 4.1. Bölümde 3.2.Bölümde yapılan çalışmalar $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ $\left(u^2 = 0\right)$ halkası üzerine genelleştirilmiştir. 4.2. Bölümde de $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ $\left(u^2 = 0\right)$ halkası üzerindeki p^s uzunluklu constacyclic kodlar incelenmiştir.

4.1. $u^2 = 0$ Durumunda $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ Halkası Üzerindeki Cyclic Kodlar İle $\mathbb{F}_{p^k}$ Cismi Üzerindeki Cyclic Kodlar Arasındaki İlişki

Bu bölümde 3.2. Bölümde $R_0 = \mathbb{F}_2 + u\mathbb{F}_2\left(u^2 = 0\right)$ halkası üzerinde yapılan çalışmalar p bir asal sayı, $k \in \mathbb{N}$ ve $\mathbb{F}_{p^k} = GF(p^k)$ olmak üzere; $R = \mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\left(u^2 = 0\right)$ halkasına genelleştirilmiştir ve genel durum için verilen sonuçlarda $p = 2$ ve $k = 1$ alındığında 3.2.Bölümde verilen sonuçlar elde edilmiştir.

p bir asal sayı, $k \in \mathbb{N}$ olmak üzere $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} = \left\{a + b\,u \middle| a,b \in \mathbb{F}_{p^k}\right\}$ kümesi $u^2 = 0$ koşuluyla bir halkadır. 4.1. Bölüm boyunca aksi belirtilmedikçe bu halka R ile gösterilecektir. □

Bu durumda $R \cong {\mathbb{F}_{p^k}[u]}/{\langle u^2 \rangle}$ olur. R halkası maximal ideali $\langle u \rangle = u \cdot R$ ve rezidü cismi $\mathbb{F}_{p^k}$ olan sonlu bir zincir halkasıdır. (Amarra & Nemenzo, 2008)

3.2.2.Teoreme benzer olarak 4.1.1.Önerme yazılır.

4.1.1.Önerme:

$$P_3 : R^n \to {R[x]}/{\langle x^n - 1 \rangle}$$

$$c = (a_0, a_1, \ldots, a_{n-1}) \mapsto P_3(c) = \overline{a_0 + a_1 \cdot x + \cdots + a_{n-1} \cdot x^{n-1}}$$

$$= a_0 + a_1 \cdot x + \cdots + a_{n-1} \cdot x^{n-1} + \langle x^n - 1 \rangle$$

biçiminde tanımlanan P_3 dönüşümü bir $R-$homomorfizmadır. □

3.2.5.Tanım ve 3.2.3.Teorem P_3 dönüşümü ve R halkasına kolaylıkla taşınabileceğinden ayrıca verilmemiştir. 3.2.7.Tanıma benzer biçimde 4.1.1.Tanım verilir.

4.1.1.Tanım:

$$\upsilon : R^n \to R^n$$

$$q = (q_0, q_1, \ldots, q_{n-1}) \mapsto \upsilon(q) = \big((1-u) \cdot q_{n-1}, q_0, q_1, \ldots, q_{n-2}\big)$$

biçiminde bir υ dönüşümü tanımlansın. C R üzerinde n uzunluğunda bir kod olsun. Eğer $\upsilon(C) = C$ ise C koduna R üzerinde n uzunluğunda bir $(1-u)-$constacyclic kod denir. (Amarra & Nemenzo, 2008)

3.2.2.Tanım ve 3.2.5.Teorem R halkasına kolaylıkla taşınabileceğinden ayrıca verilmemiştir. 3.1.1.Tanıma benzer olarak 4.1.2.Tanım verilir.

4.1.2.Tanım: Herhangi bir $a = \left(a_0, a_1, \ldots, a_{p^k \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p^k \cdot n}$ elemanı için;

$a^{(0)} = \left(a_0, a_1, \ldots, a_{p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$a^{(1)} = \left(a_{p \cdot n}, a_{p \cdot n+1}, \ldots, a_{2 \cdot p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$a^{(2)} = \left(a_{2 \cdot p \cdot n}, a_{2 \cdot p \cdot n+1}, \ldots, a_{3 \cdot p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$\vdots$

$a^{(t)} = \left(a_{t \cdot p \cdot n}, a_{t \cdot p \cdot n+1}, \ldots, a_{(t+1) \cdot p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$\vdots$

$a^{\left(p^{k-1}-1\right)}=\left(a_{\left(p^{k-1}-1\right)\cdot p\cdot n},a_{\left(p^{k-1}-1\right)\cdot p\cdot n+1},\ldots,a_{p^{k-1}\cdot p\cdot n-1}\right)\in\mathbb{F}_{p^k}{}^{p\cdot n}$ olmak üzere;

$a=\left(a_0,a_1,\ldots,a_{p^k\cdot n-1}\right)=\left(a^{(0)}\middle|a^{(1)}\middle|\cdots\middle|a^{\left(p^{k-1}-1\right)}\right)$ biçiminde yazılsın. Ayrıca; $\mathbb{F}_{p^k}{}^{p\cdot n}$ vektör uzayı üzerindeki cyclic kaydırma dönüşümü;

$$\sigma:\mathbb{F}_{p^k}{}^{p\cdot n}\to\mathbb{F}_{p^k}{}^{p\cdot n}$$
$$c=\left(c_0,c_1,\ldots,c_{p\cdot n-1}\right)\mapsto\sigma(c)=\left(c_{p\cdot n-1},c_0,c_1,\ldots,c_{p\cdot n-2}\right)$$

biçiminde tanımlanan σ dönüşümü olsun.

$$\sigma^{\otimes p^{k-1}}:\mathbb{F}_{p^k}{}^{p^k\cdot n}\to\mathbb{F}_{p^k}{}^{p^k\cdot n}$$
$$a=\left(a_0,a_1,\ldots,a_{p^k\cdot n-1}\right)=\left(a^{(0)}\middle|a^{(1)}\middle|\cdots\middle|a^{\left(p^{k-1}-1\right)}\right)\mapsto\sigma^{\otimes p^{k-1}}(a)=\left(\sigma\left(a^{(0)}\right)\middle|\sigma\left(a^{(1)}\right)\middle|\cdots\middle|\sigma\left(a^{\left(p^{k-1}-1\right)}\right)\right)$$

biçiminde $\sigma^{\otimes p^{k-1}}$ dönüşümü tanımlansın.

Eğer $\mathbb{F}_{p^k}$ üzerinde $p^k\cdot n$ uzunluğundaki bir C kodu için, $\sigma^{\otimes p^{k-1}}(C)=C$ oluyorsa; C koduna $\mathbb{F}_{p^k}$ üzerinde $p^k\cdot n$ uzunluğunda p^{k-1} indeksli bir quasicyclic kod denir. (Amarra & Nemenzo, 2008)

4.1.3.Tanım:

$$w_{\text{hom}}:R\to\left\{p^k-1,p^k,0\right\}$$
$$r\mapsto w_{\text{hom}}(r)=\begin{cases}p^k-1;\ r\in R\setminus R\cdot u\text{ ise}\\ \mathrm{p}^k;\ r\in R\cdot u\setminus\{0\}\text{ ise}\\ 0;\ \text{diğer durumlarda}\end{cases}$$

biçiminde tanımlanan w_{hom} fonksiyonuna **homogenous ağırlık fonksiyonu** denir. Ayrıca; herhangi bir $r\in R$ için $w_{\text{hom}}(r)$ değerine r elemanının homogenous ağırlığı denir. (Amarra & Nemenzo, 2008)□

Yukarıdaki tanımda $p=2$, $k=1$ alındığında;

$$w_{\text{hom}} : R=\mathbb{F}_2+u\cdot\mathbb{F}_2\left(u^2=0\right)\to\left\{2^1-1,2^1,0\right\}=\left\{0,1,2\right\}\subseteq\mathbb{N}\cup\left\{0\right\}$$

$$r\mapsto w_{\text{hom}}\left(r\right)=\begin{cases}2^1-1;\ r\in R\setminus R\cdot u \text{ ise}\\ 2^1;\ r\in R\cdot u\setminus\left\{0\right\} \text{ ise}\\ 0;\ \text{diğer durumlarda}\end{cases}\underset{R\cdot u=\{0,u\}}{=}\begin{cases}1;\ r\in\left\{1,1+u\right\} \text{ ise}\\ 2;\ r=u \text{ ise}\\ 0;\ r=0 \text{ ise}\end{cases}$$

biçiminde elde edilen w_{hom} dönüşümü 3.2.2.Tanımda R_0 üzerinde tanımlanan w_L Lee ağırlık fonksiyonu ile aynıdır.

Bölüm boyunca w_H 3.2.1.Tanım ve 2.1.9.Tanım'da geçen Hamming ağırlık fonksiyonunun $\mathbb{F}_{p^k}{}^n$ üzerine genişletilmiş anlamında kullanılmıştır.

4.1.4.Tanım: $i=0,1,\ldots,k-1$ için $\gamma_{i,\varepsilon}\in\left\{0,1,2,\ldots,p-1\right\}$ olmak üzere; herhangi bir $\bar{\varepsilon}\in\mathbb{Z}_{p^k}$ elemanı için ε sayısı $\varepsilon=\gamma_{0,\varepsilon}+\gamma_{1,\varepsilon}\cdot p+\cdots+\gamma_{(k-1),\varepsilon}\cdot p^{k-1}$ biçimde tek türlü olarak yazılır. Bu yazıma ε sayısının $p-$sel gösterimi denir. (Amarra & Nemenzo, 2008)

4.1.1.Örnek: 4.1.4.Tanımda $p=2$, $k=3$ alınırsa; $i=0,1,\ldots,7$ için $\gamma_{i,\varepsilon}\in\left\{0,1\right\}$ olmak üzere; $\bar{\varepsilon}\in\mathbb{Z}_8$ elemanları için ε sayılarının $2-$sel gösterimleri şu şekildedir: $0=0+0\cdot2+0\cdot2^2$; $1=1+0\cdot2+0\cdot2^2$; $2=0+1\cdot2+0\cdot2^2$; $3=1+1\cdot2+0\cdot2^2$; $4=0+0\cdot2+1\cdot2^2$; $5=1+0\cdot2+1\cdot2^2$; $6=0+1\cdot2+1\cdot2^2$; $7=1+1\cdot2+0\cdot2^2$.

4.1.5.Tanım: Bir $GF(q)$ sonlu cisminin, çarpımsal grubunun bir üretecine bir primitif eleman denir. Diğer bir deyişle $\alpha\in GF(q)$ bir primitif eleman ise $GF(q)$ Galois cisminin sıfırdan farklı her elemanı, öyle bir i pozitif tam sayısı için α^i biçiminde yazılabilir. (Roman, 1992, s.289)□

$\alpha\in\mathbb{F}_{p^k}$ sabit bir primitif eleman ve herhangi bir $\bar{\varepsilon}\in\mathbb{Z}_{p^k}$ için ε sayısının $p-$sel gösterimi $\varepsilon=\gamma_{0,\varepsilon}+\gamma_{1,\varepsilon}\cdot p+\cdots+\gamma_{(k-1),\varepsilon}\cdot p^{k-1}$ olmak üzere ε sayısına karşılık gelen herhangi bir $\alpha_\varepsilon\in\mathbb{F}_{p^k}$ elemanı $\alpha_\varepsilon=\gamma_{0,\varepsilon}+\gamma_{1,\varepsilon}\cdot\alpha+\cdots+\gamma_{(k-1),\varepsilon}\cdot\alpha^{k-1}$ biçiminde tek türlü yazılır. Bu durumda R^n üzerindeki bir Gray Φ dönüşümü şu teoremdeki gibi tanımlanır:

4.1.1.Teorem:

$$\Phi:\left(R,d_{\text{hom}}\right)\to\left(\mathbb{F}_{p^k}{}^{p^k},d_H\right)$$
$$x+yu\mapsto\Phi\left(x+yu\right)=\left(y,\alpha_1\cdot x+y,\alpha_2\cdot x+y,\ldots,\alpha_{p^k-1}\cdot x+y\right)$$

biçiminde tanımlanan Φ dönüşümü bir izometridir. (Amarra & Nemenzo, 2008)

Kanıt: Herhangi iki $x_1+y_1u, x_2+y_2u\in R$ alınsın.

$$\left(d_{\text{hom}}\left(x_1+y_1u,x_2+y_2u\right)\underset{?}{=}d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)\right)$$

I.Durum: $x_1=x_2, y_1\neq y_2$

$$\Rightarrow d_{\text{hom}}\left(x_1+y_1u,x_2+y_2u\right)=w_{\text{hom}}\left(\left(x_1+y_1u\right)-\left(x_2+y_2u\right)\right)$$
$$=w_{\text{hom}}\left(\left(x_1-x_2\right)+\left(y_1-y_2\right)u\right)$$
$$\underset{\underset{\left(y_1-y_2\right)u\in R\cdot u\setminus\{0\}}{\underbrace{\left(y_1-y_2\right)}_{\neq 0}\cdot u}}{=}\quad w_{\text{hom}}\left(\left(y_1-y_2\right)u\right)\underset{\text{tanım}}{=}p^k\ \text{ olur.}\cdots(i)$$

Diğer taraftan;

$$d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$$
$$=d_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right),\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$
$$=w_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right)-\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$
$$=w_H\left(\left(y_1-y_2\right),\alpha_1\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\alpha_2\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\ldots,\alpha_{p^k-1}\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right)\right)$$
$$\underset{x_1-x_2=0}{=}w_H\left(\underbrace{\left(y_1-y_2\right),\left(y_1-y_2\right),\left(y_1-y_2\right),\ldots,\left(y_1-y_2\right)}_{p^k\text{ tane}}\right)$$
$$\underset{\substack{y_1\neq y_2\\ y_1-y_2\neq 0\\ w_H\text{ tanım}}}{=}p^k\ \text{ olur.}\cdots(ii)$$

O halde i ve ii'den; $d_{\text{hom}}\left(x_1+y_1u,x_2+y_2u\right)=d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$'dir.

II.Durum: $x_1=x_2, y_1=y_2$

$$\Rightarrow d_{\text{hom}}\left(x_1+y_1u, x_2+y_2u\right)=w_{\text{hom}}\left(\left(x_1+y_1u\right)-\left(x_2+y_2u\right)\right)$$
$$=w_{\text{hom}}\left(\left(x_1-x_2\right)+\left(y_1-y_2\right)u\right)$$
$$=w_{\text{hom}}\left(0\right)\underset{\substack{w_{\text{hom}}\\ \text{tanım}}}{=}0 \text{ olur.}\cdots(iii)$$

Diğer taraftan; $d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$

$$=d_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right),\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$

$$=w_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right)-\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$

$$=w_H\left(\left(y_1-y_2\right),\alpha_1\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\alpha_2\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\ldots,\alpha_{p^k-1}\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right)\right)$$

$$=w_H\left(\underbrace{0,0,0,\ldots,0}_{p^k \text{ tane}}\right)\underset{\text{Tanım}}{\overset{w_H}{=}}0 \text{ olur.}\cdots(iv)$$

O halde iii ve iv'den; $d_{\text{hom}}\left(x_1+y_1u, x_2+y_2u\right)=d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$'dir.

III.Durum: $x_1\neq x_2, y_1=y_2$

$$\Rightarrow d_{\text{hom}}\left(x_1+y_1u, x_2+y_2u\right)=w_{\text{hom}}\left(\left(x_1+y_1u\right)-\left(x_2+y_2u\right)\right)$$
$$=w_{\text{hom}}\left(\left(x_1-x_2\right)+\left(y_1-y_2\right)u\right)$$
$$\underset{\substack{x_1-x_2\neq 0\\ x_1-x_2\in R\setminus R\cdot u}}{=}w_{\text{hom}}\left(x_1-x_2\right)\underset{\substack{w_{\text{hom}}\\ \text{tanım}}}{=}p^k-1 \text{ olur.}\cdots(v)$$

Diğer taraftan; $d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$

$$=d_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right),\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$

$$=w_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right)-\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$

$$=w_H\left(\left(y_1-y_2\right),\alpha_1\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\alpha_2\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\ldots,\alpha_{p^k-1}\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right)\right)$$

$$=w_H\left(\underbrace{y_1-y_2}_{=0},\underbrace{\alpha_1\cdot\left(x_1-x_2\right),\alpha_2\cdot\left(x_1-x_2\right),\ldots,\alpha_{p^k-1}\cdot\left(x_1-x_2\right)}_{\left(p^k-1\right) \text{ tane}}\right)$$

$$\underset{\substack{vi \text{ ve } x_1-x_2\neq 0 \text{ olduğundan;}\\ i=1,2,\ldots,p^k-1 \text{ için;}\\ \alpha_i\cdot\left(x_1-x_2\right)\neq 0\text{'dır.}\\ \text{Ayrıca; } w_H \text{ tanım.}}}{=}p^k-1 \text{ olur.}\cdots(vii)$$

$$\left(\begin{array}{l}\bar{0}\in\mathbb{Z}_{p^k}\text{ elemanı için 0'ın } p-\text{sel gösterimi;}\\ 0=\gamma_{0,0}+\gamma_{1,0}\cdot p+\cdots+\gamma_{k-1,0}\cdot p^{k-1}\text{'dir.}\\ \Rightarrow \gamma_{0,0}=\gamma_{1,0}=\cdots=\gamma_{k-1,0}=0\text{'dır.}\\ \text{Bu durumda; } \bar{0}\in\mathbb{Z}_{p^k}\text{ elemanına karşılık gelen } \alpha_0\in\mathbb{F}_{p^k}\text{ elemanı;}\\ \alpha_0=\gamma_{0,0}+\gamma_{1,0}\cdot\alpha+\cdots+\gamma_{k-1,0}\cdot\alpha^{k-1}=0\text{'dır.}\\ \mathbb{Z}_{p^k}\text{ halkasının herhangi bir } \bar{\varepsilon}\text{ elemanı ile } \alpha_\varepsilon\in\mathbb{F}_{p^k}\text{ ile gösterilen } \mathbb{F}_{p^k}\text{ cisminin}\\ \text{elemanları arasında birebir eşleme olduğundan } \varepsilon\neq 0 \text{ ise } \alpha_\varepsilon\neq 0 \text{ olur.}\end{array}\right)\cdots(vi)$$

O halde *v* ve *vii* 'den; $d_{\text{hom}}\left(x_1+y_1u,x_2+y_2u\right)=d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$ 'dir.

IV.Durum: $x_1\neq x_2, y_1\neq y_2$

$$\Rightarrow d_{\text{hom}}\left(x_1+y_1u,x_2+y_2u\right)=w_{\text{hom}}\left(\left(x_1+y_1u\right)-\left(x_2+y_2u\right)\right)$$

$$=w_{\text{hom}}\left(\left(x_1-x_2\right)+\left(y_1-y_2\right)u\right)$$

$$\underset{\substack{x_1-x_2\neq 0 \text{ ise;}\\ (x_1-x_2)+(y_1-y_2)u\in R\setminus R\cdot u\\ \text{Ayrıca } w_{\text{hom}} \text{ tanım.}}}{=} p^k-1 \text{ olur.}\cdots(viii)$$

Diğer taraftan; $d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$

$$=d_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right),\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$

$$=w_H\left(\left(y_1,\alpha_1\cdot x_1+y_1,\alpha_2\cdot x_1+y_1,\ldots,\alpha_{p^k-1}\cdot x_1+y_1\right)-\left(y_2,\alpha_1\cdot x_2+y_2,\alpha_2\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_2+y_2\right)\right)$$

$$\underset{ix}{=}w_H\left(\underbrace{\left(y_1-y_2\right)}_{\neq 0},\underbrace{\alpha_1\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\alpha_2\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right),\ldots,\alpha_{p^k-1}\cdot\left(x_1-x_2\right)+\left(y_1-y_2\right)}_{\substack{\text{Öyle tek şekilde belirli bir } k\in\{1,2,\ldots,p^k\} \text{ için } \alpha_k\cdot(x_1-x_2)=-(y_1-y_2)\in\mathbb{F}_{p^k}^{*} \text{ olduğundan; } \alpha_k\cdot(x_1-x_2)+(y_1-y_2)=0\text{'dır.}\\ \text{O halde;} p^k-2 \text{ tane eleman sıfırdan farklı bir tane eleman sıfırdır.}}}\right)$$

$$\underset{w_H \text{ tanım.}}{=} p^k-1 \text{ olur.}\cdots(x)$$

$\mathbb{F}_{p^k}=\left\{\alpha_0=0,\alpha_1,\alpha_2,\ldots,\alpha_{p^k}\right\}$ Galois cisminin 0'dan farklı elemanların oluşturduğu; $\mathbb{F}_{p^k}^{\ *}=\left\{\alpha_1,\alpha_2,\ldots,\alpha_{p^k}\right\}$ kümesinin herhangi bir $a\in\mathbb{F}_{p^k}^{\ *}$ elemanı düşünülsün. $i,\ j\in\left\{1,2,\ldots,p^k\right\}$ olmak üzere $\alpha_i\neq\alpha_j$ ise $a\cdot\alpha_i\neq a\cdot\alpha_j$'dir.

Gerçekten de;

$\alpha_i\neq\alpha_j$ iken $a\cdot\alpha_i=a\cdot\alpha_j$ olduğu varsayılsın.

$\underset{\substack{a\in\mathbb{F}_{p^k}\\ \mathbb{F}_{p^k}\text{ bir cisim}\\ a^{-1}\in\mathbb{F}_{p^k}\text{'dir.}}}{\Rightarrow}\ a^{-1}\cdot\left(a\cdot\alpha_i\right)=a^{-1}\cdot\left(a\cdot\alpha_j\right)$

$\Rightarrow\left(a^{-1}\cdot a\right)\cdot\alpha_i=\left(a^{-1}\cdot a\right)\cdot\alpha_j$

$\Rightarrow 1_{\mathbb{F}_{p^k}}\cdot\alpha_i=1_{\mathbb{F}_{p^k}}\cdot\alpha_j$ $\cdots(ix)$

$\Rightarrow\alpha_i=\alpha_j$ Çelişki!

O halde $\alpha_i\neq\alpha_j$ ise $a\cdot\alpha_i\neq a\cdot\alpha_j$'dir.

Bu durumda; $\left(x_1-x_2\right)\in\mathbb{F}_{p^k}^{\ *}$ ve $\alpha_i\in\mathbb{F}_{p^k}^{\ *}\ \left(i=1,2,\ldots,p^k\right)$ elemanları için;

$\alpha_1\cdot\left(x_1-x_2\right)\neq\alpha_2\cdot\left(x_1-x_2\right)\neq\cdots\neq\alpha_{p^k}\cdot\left(x_1-x_2\right)$ ve $\mathbb{F}_{p^k}$ sıfır bölenli olmadığından; $\alpha_i\cdot\left(x_1-x_2\right)\in\mathbb{F}_{p^k}^{\ *}\ \left(i=1,2,\ldots,p^k\right)$'dir.

O halde; $\mathbb{F}_{p^k}^{\ *}=\left\{\alpha_1\cdot\left(x_1-x_2\right),\alpha_2\cdot\left(x_1-x_2\right),\ldots,\alpha_{p^k}\cdot\left(x_1-x_2\right)\right\}$'dir.

Öyle bir $k\in\left\{1,2,\ldots,p^k\right\}$ için $\alpha_k\cdot\left(x_1-x_2\right)=-\left(y_1-y_2\right)\in\mathbb{F}_{p^k}^{\ *}$'dir. Ayrıca bir elemanın tersi varsa bir tane olacağından böyle bir $\alpha_k\cdot\left(x_1-x_2\right)\in\mathbb{F}_{p^k}^{\ *}$ bir tanedir.

O halde *viii* ve *x* 'den; $d_{\text{hom}}\left(x_1+y_1u,x_2+y_2u\right)=d_H\left(\Phi\left(x_1+y_1u\right),\Phi\left(x_2+y_2u\right)\right)$ 'dir.

O halde Φ bir izometridir. □

4.1.1.Teorem'de $p=2$, $k=1$ alınsın: 4.1.4.Tanımdan; $\bar{0}\in\mathbb{Z}_2$ elemanı için 0 'ın $2-$sel gösterimi kendisi olacağından $\gamma_{0,0}=0$; $\bar{1}\in\mathbb{Z}_2$ elemanı için 1'in $2-$sel gösterimi kendisi olacağından $\gamma_{0,1}=1$ elde edilir. $GF\left(2\right)=\mathbb{F}_2=\left\{0,1\right\}$ cisminin primitif elemanı; 1'dir. 0 sayısına karşılık; $\alpha_0=\gamma_{0,0}=0\in\mathbb{F}_2$ ve 1 sayısına karşılık; $\alpha_1=\gamma_{0,1}=1\in\mathbb{F}_2$ elemanları yazılır. Bu durumda $R=\mathbb{F}_2+u\cdot\mathbb{F}_2\left(u^2=0\right)$ halkası üzerinde Gray dönüşümü;

$$\Phi:R\rightarrow\mathbb{F}_2^{\ 2}$$
$$x+yu\mapsto\Phi\left(x+yu\right)=\left(y,\alpha_1\cdot x+y\right)\underset{\alpha_1=1}{=}\left(y,x+y\right)$$

biçimindedir. Bu dönüşümde 3.2.Bölüm'de $R_0=\mathbb{F}_2+u\cdot\mathbb{F}_2\left(u^2=0\right)$ halkası üzerinde tanımlanan Gray dönüşümü ile aynıdır.

4.1.2.Örnek: $p=2$ ve $k=2$ için $R=\mathbb{F}_4+u\,\mathbb{F}_4\left(u^2=0\right)$ halkası üzerindeki Φ Gray dönüşümü şu şekilde elde edilir:

$\mathbb{Z}_4=\left\{\bar{0},\bar{1},\bar{2},\bar{3}\right\}$ elemanlarını temsilcilerin 4.1.4.Tanım'dan; $2-$sel gösterimleri;

$$0 = 0 + 0 \cdot 2 \Rightarrow \gamma_{0,0} = 0,\ \gamma_{1,0} = 0$$
$$1 = 1 + 0 \cdot 2 \Rightarrow \gamma_{0,1} = 1,\ \gamma_{1,1} = 0$$
$$2 = 0 + 1 \cdot 2 \Rightarrow \gamma_{0,2} = 0,\ \gamma_{1,2} = 1$$
$$3 = 1 + 1 \cdot 2 \Rightarrow \gamma_{0,3} = 1,\ \gamma_{1,3} = 1$$

biçiminde elde edilir. Diğer taraftan;

$GF(4) = \mathbb{F}_4 = \left\{0, 1, \rho, \overline{\rho}\right\}$ cisminin işlem tabloları şu biçimdedir:

+	0	1	ρ	$\overline{\rho}$
0	0	1	ρ	$\overline{\rho}$
1	1	0	$\overline{\rho}$	ρ
ρ	ρ	$\overline{\rho}$	0	1
$\overline{\rho}$	$\overline{\rho}$	ρ	1	0

·	0	1	ρ	$\overline{\rho}$
0	0	0	0	0
1	0	1	ρ	$\overline{\rho}$
ρ	0	ρ	$\overline{\rho}$	1
$\overline{\rho}$	0	$\overline{\rho}$	1	ρ

$\mathbb{F}_4$ Galois cisminin çarpım tablosu incelendiğinde ρ elemanının bir primitif eleman olduğu görülür.Herhangi bir $\overline{\varepsilon} \in \mathbb{Z}_4$ için ε sayısına karşılık gelen herhangi bir $\alpha_\varepsilon \in \mathbb{F}_{p^k}$ elemanları;

$\alpha_0 = 0 + 0 \cdot \rho = 0$

$\alpha_1 = 1 + 0 \cdot \rho = 1$

$\alpha_2 = 0 + 1 \cdot \rho = \rho$

$\alpha_3 = 1 + 1 \cdot \rho = 1 + \rho \underset{\substack{\mathbb{F}_4 \text{Cisminin} \\ \text{"+" Tablosu}}}{=} \overline{\rho}$ biçimindedir. Bu durumda; $R = \mathbb{F}_4 + u\,\mathbb{F}_4\left(u^2 = 0\right)$ halkası üzerindeki Φ Gray dönüşümü, $u^2 = 0$ olmak üzere

$$\Phi : \mathbb{F}_4 + u \cdot \mathbb{F}_4 \to {\mathbb{F}_4}^4$$
$$x + yu \mapsto \Phi(x + yu) = \left(y, \alpha_1 \cdot x + y, \alpha_2 \cdot x + y, \alpha_3 \cdot x + y\right)$$
$$= \left(y, x + y, \rho \cdot x + y, \overline{\rho} \cdot x + y\right)$$

biçimindedir. □

Φ Gray dönüşümünün R^n 'e genişletilmesi

$$\Phi:\left(R^n,d_{\text{hom}}\right)\to\left(\mathbb{F}_{p^k}{}^{p^k\cdot n},d_H\right)$$

$$r=\left(x_1+y_1u,x_2+y_2u,\ldots,x_n+y_nu\right)\mapsto\Phi(r)=\left(y_1,y_2,\ldots,y_n,\alpha_1\cdot x_1+y_1,\alpha_1\cdot x_2+y_2,\ldots,\alpha_1\cdot x_n+y_n,\right.$$
$$\alpha_2\cdot x_1+y_1,\alpha_2\cdot x_2+y_2,\ldots,\alpha_2\cdot x_n+y_n,\ldots,$$
$$\left.\alpha_{p^k-1}\cdot x_1+y_1,\alpha_{p^k-1}\cdot x_2+y_2,\ldots,\alpha_{p^k-1}\cdot x_n+y_n\right)$$

biçimindedir. (Amarra & Nemenzo, 2008)

4.1.2.Önerme: Φ, R^n'den $\mathbb{F}_{p^k}{}^{p^k\cdot n}$ vektör uzayına tanımlanmış Gray dönüşümü, v, R^n üzerindeki $(1-u)-$constacyclic kaydırma dönüşümü, $\sigma^{\otimes p^{k-1}}$, $\mathbb{F}_{p^k}{}^{p^k\cdot n}$ vektör uzayı üzerinde tanımlı indeksi p^{k-1} olan quasicyclic kaydırma dönüşümü olmak üzere $\Phi\circ v=\sigma^{\otimes p^{k-1}}\circ\Phi$ 'dir. (Amarra & Nemenzo, 2008)

$$\begin{array}{ccc} R^n & \overset{\Phi}{\to} & \mathbb{F}_{p^k}{}^{p^k\cdot n} \\ \upsilon\downarrow & \circlearrowright & \downarrow\sigma^{\otimes p^{k-1}} \\ R^n & \overset{\Phi}{\to} & \mathbb{F}_{p^k}{}^{p^k\cdot n} \end{array}$$

Kanıt: Herhangi bir $r=\left(x_0+u\,y_0,x_1+u\,y_1,\ldots,x_{n-1}+u\,y_{n-1}\right)\in R^n$ alınsın ve $\Phi(r)=\left(a_0,a_1,\ldots,a_{p^k\cdot n-1}\right)$ olsun. Bu durumda;

$$b_{\varepsilon\cdot n+j}=\begin{cases}a_{(\varepsilon+p-1)\cdot n+(n-1)}; j=0,\gamma_{0,\varepsilon}=0 \text{ ise}\\ a_{(\varepsilon-1)\cdot n+(n-1)}\quad ; j=0,\gamma_{0,\varepsilon}\neq 0 \text{ ise}\\ a_{\varepsilon\cdot n+-1}\qquad ; j\neq 0 \text{ ise}\end{cases}$$

olmak üzere; $\sigma^{\otimes p^k-1}\left(\Phi(r)\right)=\left(b_0,b_1,\ldots,b_{p^k\cdot n-1}\right)$'dir. Diğer taraftan; $v(r)=\left((1-u)x_{n-1}+u\,y_{n-1},x_0+u\,y_0,x_1+u\,y_1,\ldots,x_{n-2}+u\,y_{n-2}\right)$'dir. Bu durumda;

$$c_{\varepsilon\cdot n+j}=\begin{cases}\left(\sum_{i=0}^{k-1}\gamma_{i,\in}\cdot\alpha^{i}-1\right)\cdot x_{n-1}\oplus y_{n-1}; & j=0 \text{ ise}\\ \left(\sum_{i=0}^{k-1}\gamma_{i,\in}\cdot\alpha^{i}\right)\cdot x_{j-1}\oplus y_{j-1} & ; j\neq 0 \text{ ise}\end{cases}$$

$$=\begin{cases}\left(\sum_{i=0}^{k-1}\gamma_{i,\in}\cdot\alpha^{i}+p-1\right)\cdot x_{n-1}\oplus y_{n-1}; & j=0,\gamma_{0,\varepsilon}=0 \text{ ise}\\ \left(\sum_{i=0}^{k-1}\gamma_{i,\in}\cdot\alpha^{i}-1\right)\cdot x_{n-1}\oplus y_{n-1} & ; j=0,\gamma_{0,\varepsilon}\neq 0 \text{ ise}\\ \left(\sum_{i=0}^{k-1}\gamma_{i,\in}\cdot\alpha^{i}\right)\cdot x_{j-1}\oplus y_{j-1} & ; j\neq 0 \text{ ise}\end{cases}$$

olmak üzere; $\Phi\left(v\left(r\right)\right)=\left(c_0,c_1,\ldots,c_{p^k\cdot n-1}\right)$ elde edilir.

Her $i=0,1,\ldots,p^k\cdot n-1$ için; $b_i=c_i$ olacağından $\Phi\circ v=\sigma^{\otimes p^{k-1}}\circ\Phi$'dir. □

4.1.2.Önermede $p=2$, $k=1$ alındığından indexi $\left(p^k-1\right)$ olan quasi-cyclic dönüşümü σ^{p^k-1}, $R=\mathbb{F}_2+u\cdot\mathbb{F}_2\left(u^2=0\right)$ halkası üzerindeki σ cyclic kaydırma dönüşümüne eşittir. Dolayısıyla; 4.1.2.Önerme 3.2.6.Önerme'ye eşit olur.

4.1.1.Sonuç: R üzerinde n uzunluklu bir kod C olsun. C kodu $\left(1-u\right)-$ constacyclic kod ise $\Phi\left(C\right)$ kodu $\mathbb{F}_{p^k}$ üzerinde $p^k\cdot n$ uzunluğunda p^{k-1} indeksli bir quasicyclic koddur. Bu ifadenin tersi de doğrudur. (Amarra & Nemenzo, 2008)

Kanıt: $\Rightarrow$: $C\subseteq R^n$ kodu $\left(1-u\right)-$constacyclic kod

$\Rightarrow v\left(C\right)=C$

$\Rightarrow \Phi\left(v\left(C\right)\right)=\Phi\left(C\right)$

$\underset{\Phi(v(C))=\sigma^{\otimes p^{k-1}}(\Phi(C))}{\overset{\text{4.1.2.Önerme}}{\Rightarrow}}$ $\sigma^{\otimes p^{k-1}}\left(\Phi\left(C\right)\right)=\Phi\left(C\right)$

$\underset{\text{tanımı}}{\overset{\sigma^{\otimes p^{k-1}}}{\Rightarrow}}$ $\Phi\left(C\right)$, p^{k-1} indeksli bir quasicyclic koddur.

$\Leftarrow: \Phi(C) \subseteq \mathbb{F}_{p^k}{}^{p^k \cdot n}$ kodu p^{k-1} indeksli bir quasicyclic kod

$$\underset{\sigma^{\otimes p^{k-1}} \text{ tanım}}{\Rightarrow} \sigma^{\otimes p^{k-1}}\left(\Phi(C)\right) = \Phi(C)$$

$$\underset{\substack{\text{4.1.2.Önerme;} \\ \Phi(\nu(C))=\sigma^{\otimes p^{k-1}}(\Phi(C))}}{\Rightarrow} \Phi\left(\nu(C)\right) = \Phi(C)$$

$$\underset{\substack{\text{4.1.1.Teorem} \\ \Phi \text{ birebir}}}{\Rightarrow} \nu(C) = C$$

$\underset{\nu \text{ tanım}}{\Rightarrow} C \subseteq R^n$ kodu, $(1-u)-$constacyclic koddur. □

4.1.3.Önerme: n ve p aralarında asal, $n' \in \{0,1,\ldots,p-1\}$ ve $n \cdot n' \equiv 1 (\text{mod } p)$ olmak üzere $\beta = 1 + n'u$ ise

$$\mu : {R[x]}/{\langle x^n - 1 \rangle} \to {R[x]}/{\langle x^n - (1-u) \rangle}$$
$$\overline{r(x)} \mapsto \mu\left(\overline{r(x)}\right) = \overline{r(\beta \cdot x)}$$

biçiminde tanımlanan dönüşüm bir izomorfizmadır. (Amarra & Nemenzo, 2008)

Kanıt: Herhangi bir

$$\overline{r(x)} = \overline{r_0 + r_1 \cdot x + \cdots + r_{n-1} \cdot x^{n-1}}, \overline{q(x)} = \overline{q_0 + q_1 \cdot x + \cdots + q_{n-1} \cdot x^{n-1}} \in {R[x]}/{\langle x^n - 1 \rangle}$$

$$\Rightarrow \mu\left(\overline{r(x)} + \overline{q(x)}\right) = \mu\left(\overline{r(x) + q(x)}\right) = \mu\left(\overline{(r_0 + q_0) + (r_1 + q_1) \cdot x + \cdots + (r_{n-1} + q_{n-1}) \cdot x^{n-1}}\right)$$

$$= \overline{(r_0 + q_0) + (r_1 + q_1) \cdot (\beta \cdot x) + \cdots + (r_{n-1} + q_{n-1}) \cdot (\beta \cdot x)^{n-1}} \in {R[x]}/{\langle x^n - (1-u) \rangle}$$

$$= \overline{r_0 + q_0 + r_1 \cdot (\beta \cdot x) + q_1 \cdot (\beta \cdot x) + \cdots + r_{n-1}(\beta \cdot x)^{n-1} + q_{n-1}(\beta \cdot x)^{n-1}}$$

$$= \overline{r_0 + r_1 \cdot (\beta \cdot x) + \cdots + r_{n-1} \cdot (\beta \cdot x)^{n-1} + q_0 + q_1 \cdot (\beta \cdot x) + \cdots + q_{n-1} \cdot (\beta \cdot x)^{n-1}}$$

$$= \overline{r_0 + r_1 \cdot (\beta \cdot x) + \cdots + r_{n-1} \cdot (\beta \cdot x)^{n-1}} + \overline{q_0 + q_1 \cdot (\beta \cdot x) + \cdots + q_{n-1} \cdot (\beta \cdot x)^{n-1}}$$

$= \mu\left(\overline{r(x)}\right) + \mu\left(\overline{q(x)}\right)$'dir.

Herhangi bir

$$\overline{r(x)} = \overline{r_0 + r_1 \cdot x + \cdots + r_{n-1} \cdot x^{n-1}}, \overline{q(x)} = \overline{q_0 + q_1 \cdot x + \cdots + q_{n-1} \cdot x^{n-1}} \in {R[x]}/{\langle x^n - 1 \rangle}$$

$$\Rightarrow \mu\left(\overline{r(x)}\cdot\overline{q(x)}\right)=\mu\left(\overline{r(x)\cdot q(x)}\right)$$

$$=\mu\left(\overline{(r_0\cdot q_0)+(r_0\cdot q_1+r_1\cdot q_0)\cdot x+(r_0\cdot q_2+r_1\cdot q_1+r_2\cdot q_0)\cdot x^2\cdots+(r_{n-1}\cdot q_{n-1})\cdot x^{2\cdot n-2}}\right)$$

$$=\overline{(a_0\cdot b_0)+(a_0\cdot b_1+a_1\cdot b_0)\cdot(\beta\cdot x)+(a_0\cdot b_2+a_1\cdot b_1+a_2\cdot b_0)\cdot(\beta\cdot x)^2\cdots+(a_{n-1}\cdot b_{n-1})\cdot(\beta\cdot x)^{2\cdot n-2}}\in R[x]\Big/\langle x^n-(1-u)\rangle\cdots(i)$$

Diğer taraftan;

$$\mu\left(\overline{r(x)}\right)\cdot\mu\left(\overline{q(x)}\right)=\overline{r_0+r_1\cdot(\beta\cdot x)+r_2\cdot(\beta\cdot x)^2\cdots+r_{n-1}\cdot(\beta\cdot x)^{n-1}}\cdot\overline{q_0+q_1\cdot(\beta\cdot x)+q_2\cdot(\beta\cdot x)^2\cdots+q_{n-1}\cdot(\beta\cdot x)^{n-1}}$$

$$=\overline{(r_0\cdot q_0)+(r_0\cdot q_1+r_1\cdot q_0)\cdot(\beta\cdot x)+(r_0\cdot q_2+r_1\cdot q_1+r_2\cdot q_0)\cdot(\beta\cdot x)^2\cdots+(r_{n-1}\cdot q_{n-1})\cdot(\beta\cdot x)^{2\cdot n-2}}\in R[x]\Big/\langle x^n-(1-u)\rangle\cdots(ii)$$

O halde i ve ii'den; $\mu\left(\overline{r(x)}\cdot\overline{q(x)}\right)=\mu\left(\overline{r(x)}\right)\cdot\mu\left(\overline{q(x)}\right)$'dir.

Her $\overline{r(x)}=\overline{r_0+r_1\cdot x+\cdots+r_{n-1}\cdot x^{n-1}},\overline{q(x)}=\overline{q_0+q_1\cdot x+\cdots+q_{n-1}\cdot x^{n-1}}\in R[x]\Big/\langle x^n-1\rangle$

için; $\mu\left(\overline{r(x)}\right)=\mu\left(\overline{q(x)}\right)$

$$\Rightarrow\overline{r_0+r_1\cdot(\beta\cdot x)+r_2\cdot(\beta\cdot x)^2\cdots+r_{n-1}\cdot(\beta\cdot x)^{n-1}}=\overline{q_0+q_1\cdot\beta\cdot x+q_2\cdot(\beta\cdot x)^2\cdots+q_{n-1}\cdot(\beta\cdot x)^{n-1}}$$

$$\Rightarrow\left(q_0+q_1\cdot(\beta\cdot x)+q_2\cdot(\beta\cdot x)^2\cdots+q_{n-1}\cdot(\beta\cdot x)^{n-1}\right)-\left(r_0+r_1\cdot(\beta\cdot x)+r_2\cdot(\beta\cdot x)^2\cdots+r_{n-1}\cdot(\beta\cdot x)^{n-1}\right)\in\langle x^n-(1-u)\rangle$$

Bu durumda

$$(q_0-r_0)+(q_1-r_1)\cdot(\beta\cdot x)+(q_2-r_2)\cdot(\beta\cdot x)^2\cdots+(q_{n-1}-r_{n-1})\cdot(\beta\cdot x)^{n-1}=f(x)\cdot\left(x^n-(1-u)\right)$$

olacak biçimde bir $f(x)\in R[x]$ vardır.

$$\Rightarrow r_0=q_0,r_1=q_1,\ldots,r_{n-1}=q_{n-1}\Rightarrow\overline{r_0+r_1\cdot x+\cdots+r_{n-1}\cdot x^{n-1}}=\overline{q_0+q_1\cdot x+\cdots+q_{n-1}\cdot x^{n-1}}$$

$$\Rightarrow\overline{r(x)}=\overline{q(x)}$$

O halde μ birebirdir.

Herhangi bir $\overline{r(x)}=\overline{r_0+r_1\cdot x+\cdots+r_{n-1}\cdot x^{n-1}}\in R[x]\Big/\langle x^n-(1+u)\rangle$ için

$$\mu\left(\overline{q(x)}\right)=\overline{r_0+r_1\cdot(1-n'\cdot u)\cdot(1+n'\cdot u)\cdot x+r_2\cdot(1-n'\cdot u)^2\cdot(1+n'\cdot u)^2\cdot x^2+\cdots+r_{n-1}\cdot(1-n'\cdot u)^{n-1}\cdot(1+n'\cdot u)^{n-1}\cdot x^{n-1}}$$

$$\underset{iii\text{'den}}{=}\overline{r_0+r_1\cdot x+\cdots+r_{n-1}\cdot x^{n-1}}\in R[x]\Big/\langle x^n-(1+u)\rangle$$ olacak biçimde en az bir tane

$$q(x)=\overline{r_0+r_1\cdot(1-n'\cdot u)\cdot x+r_2\cdot(1-n'\cdot u)^2\cdot x^2+\cdots+r_{n-1}\cdot(1-n'\cdot u)^{n-1}\cdot x^{n-1}}\in R[x]\Big/\langle x^n-1\rangle$$

vardır

$$\left((1-n'\cdot u)\cdot(1+n'\cdot u)=1-(n')^2\cdot u^2\underset{u^2=0}{=}1\right)\cdots(iii)$$

O halde μ örtendir.

O halde μ bir izomorfizmadır. □

4.1.3.Önerme'de $p=2, k=1$ alındığında; n ile 2 aralarında asal olacağından n tek sayı olmalıdır. $n'\in\{0,1\}$ ve $n\cdot n'\equiv 1(\mathrm{mod}\,2)$ sağlayan $n'=1$ olduğundan; $\beta=1+n'\cdot u=1+u$ 'dir. Ayrıca $1-u\underset{\substack{\mathbb{F}_2\text{'de;}\\ -1=1}}{=}1+u$ olduğundan;

$$\mu: R[x]\Big/\langle x^n-1\rangle\to R[x]\Big/\langle x^n-(1+u)\rangle$$
$$\overline{r(x)}\mapsto\mu\left(\overline{r(x)}\right)=\overline{r\left((1+u)\cdot x\right)}$$

dönüşümü elde edilir ki; bu dönüşüm 3.2.5.Önerme'de elde edilen μ dönüşümü ile aynıdır.

4.1.2.Sonuç: I kümesi $R[x]\Big/\langle x^n-1\rangle$ halkasının bir ideali ise $\mu(I)$ kümesi $R[x]\Big/\langle x^n-(1-u)\rangle$ halkasının bir idealidir. Bu ifadenin tersi de doğrudur. (Amarra & Nemenzo, 2008)

4.1.4.Önerme: n ve p aralarında asal ve β 4.1.3.Önerme'deki gibi olmak üzere;

$$\bar{\mu}: R^n\to R^n$$
$$r=(r_0,r_1,r_2\ldots,r_{n-1})\mapsto\bar{\mu}(r)=(r_0,\beta\cdot r_1,\beta^2\cdot r_2\ldots,\beta^{n-1}\cdot r_{n-1})$$

dönüşümü tanımlansın. Bir C kümesi R halkası üzerinde n uzunluklu bir lineer cyclic kod ise $\bar{\mu}(C)$ kümesi R üzerinde n uzunluklu bir $(1-u)-$constacyclic koddur. Bu ifadenin tersi de doğrudur. (Amarra & Nemenzo, 2008) □

4.1.4.Önerme'de $p=2$, $k=1$ alındığında 3.2.6.Teorem elde edilir.

4.1.6.Tanım: n ve p aralarında asal ve $n' \in \{0,1,\ldots,p-1\}$ olmak üzere $n \cdot n' \equiv 1 \pmod{p}$ olsun.

Her $c = \left(c_0, c_1, \ldots, c_{p^k \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p^k \cdot n}$ elemanı için;

$c^{(0)} = \left(c_0, c_1, \ldots, c_{p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$c^{(1)} = \left(c_{p \cdot n}, c_{p \cdot n+1}, \ldots, c_{2 \cdot p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$c^{(2)} = \left(c_{2 \cdot p \cdot n}, c_{2 \cdot p \cdot n+1}, \ldots, c_{3 \cdot p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$\vdots$

$c^{(t)} = \left(c_{t \cdot p \cdot n}, c_{t \cdot p \cdot n+1}, \ldots, c_{(t+1) \cdot p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$;

$\vdots$

$c^{\left(p^{k-1}-1\right)} = \left(c_{\left(p^{k-1}-1\right) \cdot p \cdot n}, c_{\left(p^{k-1}-1\right) \cdot p \cdot n+1}, \ldots, c_{p^{k-1} \cdot p \cdot n-1}\right) \in \mathbb{F}_{p^k}{}^{p \cdot n}$ olmak üzere;

$c = \left(c_0, c_1, \ldots, c_{p^k \cdot n-1}\right) = \left(c^{(0)} \middle| c^{(1)} \middle| \cdots \middle| c^{\left(p^{k-1}-1\right)}\right)$ biçiminde yazılsın.

$0 \le \gamma \le p-1, 0 \le j \le n-1$ olmak üzere $\{0,1,\ldots,p \cdot n-1\}$ kümesinin herhangi bir elemanı $\gamma \cdot n + j$ olarak yazılsın. Ayrıca; $0 \le y \le p-1$ olmak üzere $\gamma + j \cdot n' \equiv y \pmod{p}$ olsun. τ permütasyonu

$$\tau : \{0,1,\ldots,p \cdot n-1\} \to \{0,1,\ldots,p \cdot n-1\}$$
$$\gamma \cdot n + j \mapsto \tau\left(\gamma \cdot n + j\right) = y \cdot n + j$$

şeklinde verilmek üzere

$$\pi : \mathbb{F}_{p^k}{}^{p \cdot n} \to \mathbb{F}_{p^k}{}^{p \cdot n}$$
$$a = \left(a_0, a_1, \ldots, a_{p \cdot n-1}\right) \mapsto \pi\left(a\right) = \left(a_{\tau(0)}, a_{\tau(1)}, \ldots, a_{\tau(p \cdot n-1)}\right)$$

biçiminde bir π dönüşümü tanımlansın.

$$\pi^{\otimes p^{k-1}} : \mathbb{F}_{p^k}{}^{p^k \cdot n} \to \mathbb{F}_{p^k}{}^{p^k \cdot n}$$

$$c = \left(c_0, c_1, \ldots, c_{p^k \cdot n-1}\right) = \left(c^{(0)} \middle| c^{(1)} \middle| \cdots \middle| c^{\left(p^{k-1}-1\right)}\right) \mapsto \pi^{\otimes p^{k-1}}(c) = \left(\pi\left(c^{(0)}\right) \middle| \pi\left(c^{(1)}\right) \middle| \cdots \middle| \pi\left(c^{\left(p^{k-1}-1\right)}\right)\right)$$

biçiminde ki $\pi^{\otimes p^{k-1}}$ dönüşümüne Nechaev permütasyonu denir. (Amarra & Nemenzo, 2008) □

4.1.6.Tanımda $p=2, k=1$ alınsın. n ve 2 aralarında asal olması gerektiğinden n tek doğal sayı olmalıdır. $n' \in \{0,1\}$ olmak üzere $n \cdot n' \equiv 1 \pmod 2$ olduğundan $n'=1$ 'dir. $0 \le \gamma \le 1, 0 \le j \le n-1$ olmak üzere;

$0 \le i \le \dfrac{n-1}{2}$ için; $2 \cdot i \in \{0,1,\ldots,2 \cdot n-1\}$ elemanı $\gamma \cdot n + j$ biçiminde yazılmak istenirse $\gamma = 0$ ve $j = 2 \cdot i \left(0 \le 2 \cdot i \le n-1\right)$ olmalıdır. Ayrıca;

$\gamma + j \cdot n' = 0 + 2 \cdot i \equiv y \pmod 2 \Rightarrow y = 0$ 'dır. Bu durumda; τ dönüşümü tanımından;

$0 \le i \le \dfrac{n-1}{2}$ için; $\tau(2 \cdot i) \underset{\tau(\gamma \cdot n + j) = y \cdot n + j}{=} 2 \cdot i$ 'dir.$\cdots (i)$

$\dfrac{n+1}{2} \le i \le n-1$ için; $2 \cdot i \in \{0,1,\ldots,2 \cdot n-1\}$ elemanı $\gamma \cdot n + j$ biçiminde yazılmak istenirse $\gamma = 1$ ve $j = 2 \cdot i - n \left(n+1 \le 2 \cdot i \le 2 \cdot n-2\right)$ olmalıdır. Ayrıca;

$\gamma + j \cdot n' = 1 + 2 \cdot i - n \equiv y \pmod 2 \Rightarrow y = 0$ 'dır. Bu durumda; τ dönüşümü tanımından;

$\dfrac{n+1}{2} \le i \le n-1$ için; $\tau(2 \cdot i) \underset{\tau(\gamma \cdot n + j) = y \cdot n + j}{=} 2 \cdot i - n$ 'dir.$\cdots (ii)$

$0 \le i \le \dfrac{n-3}{2}$ için; $2 \cdot i + 1 \in \{0,1,\ldots,2 \cdot n-1\}$ elemanı $\gamma \cdot n + j$ biçiminde yazılmak istenirse; $\gamma = 0$ ve $j = 2 \cdot i + 1 \left(1 \le 2 \cdot i + 1 \le n-2\right)$ olmalıdır.Ayrıca;

$\gamma + j \cdot n' = 0 + 2 \cdot i + 1 \equiv y \pmod 2 \Rightarrow y = 1$ 'dir.Bu durumda; τ dönüşümü tanımından;

$0 \le i \le \dfrac{n-3}{2}$ için; $\tau(2 \cdot i + 1) \underset{\tau(\gamma \cdot n + j) = y \cdot n + j}{=} n + 2 \cdot i + 1$ 'dir.$\cdots (iii)$

$\dfrac{n-1}{2} \le i \le n-1$ için; $2 \cdot i + 1 \in \{0,1,\ldots,2 \cdot n-1\}$ elemanı $\gamma \cdot n + j$ biçiminde yazılmak istenirse; $\gamma = 1$ ve $j = 2 \cdot i + 1 - n \left(n \le 2 \cdot i + 1 \le 2 \cdot n-1\right)$ olmalıdır.Ayrıca;

$\gamma + j \cdot n' = 1 + 2 \cdot i + 1 - n \equiv y \pmod 2 \Rightarrow y = 1$'dir.Bu durumda; τ dönüşümünün tanımından; $\frac{n-1}{2} \le i \le n-1$ için; $\tau(2 \cdot i + 1) \underset{\tau(\gamma \cdot n + j) = y \cdot n + j}{=} 1 \cdot n + 2 \cdot i + 1 - n = 2i + 1$ 'dir. $\cdots (iv)$

i, ii, iii ve iv'den; $\{0,1,2,\ldots,2 \cdot n - 1\}$ kümesi üzerindeki τ permütasyonu

$$\tau = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & \cdots & n-3 & n-2 & n-1 & n & n+1 & n+2 & n+3 & \cdots & 2 \cdot n-4 & 2 \cdot n-3 & 2 \cdot n-2 & 2 \cdot n-1 \\ 0 & n+1 & 2 & n+3 & 4 & \cdots & n-3 & 2 \cdot n-2 & n-1 & n & 1 & n+2 & 3 & \cdots & n-4 & 2 \cdot n-3 & n-2 & 2 \cdot n-1 \end{pmatrix}$$

biçimindedir. $p = 2, k = 1$ için π permütasyonu

$$\pi : \mathbb{F}_2^{\,2n} \to \mathbb{F}_2^{\,2 \cdot n}$$
$$a = (a_0, a_1, \ldots, a_{2 \cdot n-1}) \mapsto \pi(a) = \left(a_{\tau(0)}, a_{\tau(1)}, \ldots, a_{\tau(2 \cdot n-1)}\right)$$ biçimindedir. Ayrıca;

$\pi^{\otimes p^{k-1}}$ Nechaev permütasyonu $p = 2, k = 1$ için $\pi^{\otimes p^{k-1}} = \pi^{\otimes 2^{1-1}} = \pi^{\otimes 1}$ biçiminde gösterilir ve π permütasyonuna eşittir. $\pi^{\otimes 1}$ Nechaev permütasyonu $p = 2, k = 1$ için 3.2.6.Tanımda verilen Nechaev permütasyonu ile aynıdır.

4.1.5.Önerme: $\Phi \circ \bar{\mu} = \pi^{\otimes p^{k-1}} \circ \Phi$ 'dir. (Amarra & Nemenzo, 2008)

$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_{p^k}^{\,p^k \cdot n} \\ \bar{\mu} \downarrow & \circlearrowright & \downarrow \pi^{\otimes p^{k-1}} \\ R^n & \xrightarrow{\Phi} & \mathbb{F}_{p^k}^{\,p^k \cdot n} \end{array} \quad \square$$

4.1.5.Önerme'de $p = 2, k = 1$ alındığında 3.2.7.Önerme'nin elde edileceği açıktır.

4.1.3.Sonuç: C, R üzerinde n uzunluklu bir lineer cyclic kod ise $\Phi(C)$, $\mathbb{F}_{p^k}$ üzerinde $p^k \cdot n$ uzunluklu p^{k-1} indeksli bir quasi-cyclic koda denktir. (Amarra & Nemenzo, 2008)

Kanıt: $\Rightarrow$: R halkası üzerinde n uzunluklu bir lineer cyclic kod C $\underset{\text{4.1.4.Önerme}}{\Rightarrow}$ $\bar{\mu}(C)$ R üzerinde n uzunluklu bir lineer $(1-u)-$constacyclic koddur. $\underset{\text{4.1.1.Sonuç}}{\Rightarrow}$ $\Phi(\bar{\mu}(C))$ $\mathbb{F}_{p^k}$ üzerinde $p^k \cdot n$ uzunluklu p^{k-1} indeksli bir koddur.

$\overset{\Phi(\bar{\mu}(C))=\pi^{\otimes p^{k-1}}(\Phi(C))}{\overset{\text{4.1.5.Önerme:}}{\Rightarrow}}$ $\pi^{\otimes p^{k-1}}\left(\Phi(C)\right)$ $\mathbb{F}_{p^k}$ üzerinde $p^k \cdot n$ uzunluklu p^{k-1} indeksli bir koddur.

$\overset{\text{Denk kod tanımı.}}{\overset{\pi^{\otimes p^{k-1}} \text{ bir permütasyon.}}{\Rightarrow}}$ $\Phi(C)$ $\mathbb{F}_{p^k}$ üzerinde $p^k \cdot n$ uzunluklu p^{k-1} indeksli bir koda denktir.

4.1.3.Örnek: $GF(4)=\mathbb{F}_4=\{0,1,\rho,1+\rho=\rho^2\}$ olmak üzere; $R=\mathbb{F}_{p^k}+u\,\mathbb{F}_{p^k}\left(u^2=0\right)$ halkasında $p=2$, $k=2$ alınmasıyla elde edilen $R=\mathbb{F}_4+u\,\mathbb{F}_4\left(u^2=0\right)$ halkası üzerinde x^3-1 polinomu $x^3-1=(x+1)\cdot(x+\rho)\cdot\left(x+\rho^2\right)$ biçiminde çarpanlara ayrılır. $p=2$, $k=2$ ve $n=3$ için; $n'\in\{0,1\}$ olmak üzere $3\cdot n'\equiv 1(\mathrm{mod}\,2)$ olduğu için $n'=1$ elde edilir. Bu durumda; 4.1.3.Önerme'de tanımlanan β; $\beta=1+n'\cdot u=1+1\cdot u=1+u$ biçiminde, μ dönüşümü ise;

$$\mu: {R[x]}\Big/{\langle x^n-1\rangle} \to {R[x]}\Big/{\langle x^n-(1-u)\rangle}$$
$$\overline{r(x)} \mapsto \mu\left(\overline{r(x)}\right)=\overline{r(\beta\cdot x)}=\overline{r\left((1+u)\cdot x\right)}$$

biçimindedir.

$\overline{x^3-1}\in {R[x]}\Big/{\langle x^n-1\rangle}$ elemanı için;

$$\mu\left(\overline{x^3-1}\right)=\mu\left(\overline{(x+1)\cdot(x+\rho)\cdot\left(x+\rho^2\right)}\right)$$

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

$$=\overline{\left(x+(u+1)\right)}\cdot\overline{\left(x+(\rho\cdot u+\rho)\right)}\cdot\overline{\left(x+\left(\rho^2\cdot u+\rho^2\right)\right)}\in {R[x]}\Big/{\langle x^n-(1-u)\rangle}$$ 'dir.

$x+(u+1), x+(\rho\cdot u+\rho), x+\left(\rho^2\cdot u+\rho^2\right)\in R[x]$ polinomları sırasıyla; $f_1(x)$, $f_2(x)$ ve $f_3(x)$ ile gösterilirse; üreteç polinomu $f_1(x)\cdot f_2(x)$ olan, $R=\mathbb{F}_4+u\,\mathbb{F}_4\left(u^2=0\right)$

üzerinde 3 uzunluklu C kodu için $\Phi(C)$, $\mathbb{F}_4$ üzerinde 12 uzunluklu minimum uzaklığı 9 olan bir koddur. (Amarra & Nemenzo, 2008) □

4.2. $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ $(u^2=0)$ Halkası Üzerindeki p^s Uzunluklu Constacyclic Kodlar

Bu bölümde p herhangi bir asal sayı, s bir doğal sayı olmak üzere; $R=\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}(u^2=0)$ halkası üzerindeki p^s uzunluklu constacyclic kodlar çalışılmıştır. $\alpha\neq 0, \beta\in\mathbb{F}_{p^k}=GF(p^k)$ olmak üzere; $R=\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}(u^2=0)$ halkasının tersinir elemanları; $\alpha+u\beta$ biçimindedir ve $p^k\cdot\left(p^k-1\right)$ tanedir. (Dinh, 2010)

Bu bölüm boyunca aksi belirtilmedikçe R halkası denildiğinde $R=\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}(u^2=0)$ halkası düşünülecektir.

Bu bölümde ilk olarak R üzerinde n uzunluklu bir $\lambda-$constacyclic kodun dualinin bir $\lambda^{-1}-$constacyclic kod olduğu gösterilmiştir. Ayrıca R üzerinde n uzunluklu bir C kodu için $Tor(C)$ ve $Res(C)$ kodlar tanımlanmış ve C kodunun eleman sayısıyla $Tor(C)$ ve $Res(C)$ kodların eleman sayıları arasındaki ilişki verilmiştir. Daha sonra $\mathbb{F}_{p^k}$ sonlu cismi üzerindeki p^s uzunluklu $\lambda-$constacyclic kodlar için yapılan çalışmalar R halkası üzerinde $\alpha+u\beta-$constacyclic kodlara taşınmıştır. 4.1. Bölümde R halkası üzerinde keyfi n uzunluklu bir cyclic koda karşılık bir $(1-u)-$constacyclic kod getirilmiştir. Bu bölümde son olarak; γ; $\mathbb{F}_{p^k}=GF(p^k)$ cisminin sıfırdan farklı bir elemanı olmak üzere; R halkası üzerinde p^s uzunluklu bir cyclic koda karşılık bir $\gamma-$constacyclic kodu karşılık getiren bir izomorfizma tanımlanmıştır.

4.2.1.Önerme: R bir sonlu zincir halkası ise aşağıdaki koşullar denktir:

(i) R bir yerel halka ve R halkasının maksimal ideali bir esas idealdir.

(ii) R bir yerel, esas ideal halkasıdır.

(iii) $N(r)$; $r \in R$ elemanının nilpotentlik derecesi ve $0 \le i \le N(r)$ olmak üzere; R halkasının $\langle r^i \rangle$ idealleri bir zincir oluşturur. (Dinh, 2010)

R halkası maximal ideali $\langle u \rangle = u \cdot \mathbb{F}_{p^k}$ olan bir yerel halkadır. 4.2.1.Önerme'den bir zincir halkası olduğu görülür. (Dinh, 2010)

4.2.2.Önerme: p bir asal sayı ve R, p^α uzunluğunda bir zincir halkası olsun. R halkası üzerinde n uzunluğunda bir C lineer kodunun eleman sayısı $k \in \{0,1,\ldots,\alpha \cdot n\}$ olmak üzere p^k tanedir. Ayrıca; $k+l = \alpha \cdot n$ olmak üzere; $C^\perp$ kodunun eleman sayısı p^l'dir. (Dinh, 2010)

4.2.3.Önerme: Bir $\lambda-$constacyclic kodun duali bir $\lambda^{-1}-$constacyclic koddur. (Dinh, 2010)

Kanıt: C, R halkası üzerinde tanımlı n uzunluğunda bir $\lambda-$constacyclic kod olsun. Herhangi iki $x = (x_0, x_1, \ldots, x_{n-1}) \in C^\perp$ ve $y = (y_0, y_1, \ldots, y_{n-1}) \in C$ için;

$$\tau_\lambda(y) = (\lambda \cdot y_{n-1}, y_0, y_1, \ldots, y_{n-2})$$

$$\tau_\lambda{}^2(y) = \tau_\lambda(\tau_\lambda(y)) = (\lambda \cdot y_{n-2} \lambda \cdot y_{n-1}, y_0, y_1, \ldots, y_{n-3})$$

$$\tau_\lambda{}^2(y) = \tau_\lambda(\tau_\lambda(\tau_\lambda(y))) = (\lambda \cdot y_{n-3}, \lambda \cdot y_{n-2} \lambda \cdot y_{n-1}, y_0, y_1, \ldots, y_{n-4})$$

$$\vdots$$

$$\tau_\lambda{}^{n-1}(y) = (\lambda \cdot y_1, \lambda \cdot y_2, \lambda \cdot y_3, \ldots, \lambda \cdot y_{n-1}, y_0) \text{'dir.} \cdots (i)$$

Ayrıca; C kodu $\lambda-$constacyclic kod olduğundan her $c \in C$ için $\tau_\lambda(c) \in C$'dir. Bu durumda; $\tau_\lambda{}^{n-1}(y) \in C$'dir.

λ tersinir eleman olduğundan $\lambda^{-1} \in R$'dir. Bu durumda;

$$\tau_{\lambda^{-1}}(x) = \tau_{\lambda^{-1}}(x_0, x_1, \ldots, x_{n-1}) = (\lambda^{-1} \cdot x_{n-1}, x_0, x_1, \ldots, x_{n-2})$$

$$\Rightarrow \lambda \cdot \tau_{\lambda^{-1}}(x) \cdot y = \lambda \cdot (\lambda^{-1} \cdot x_{n-1}, x_0, x_1, \ldots, x_{n-2}) \cdot (y_0, y_1, \ldots, y_{n-1})$$

$$= \underbrace{\left(\lambda \cdot \lambda^{-1} \cdot x_{n-1}, \lambda \cdot x_0, \lambda \cdot x_1, \ldots, \lambda \cdot x_{n-2} \right)}_{=1_R} \cdot \left(y_0, y_1, \ldots, y_{n-1} \right)$$

$$= x_{n-1} \cdot y_0 + \lambda \cdot x_0 \cdot y_1 + \lambda \cdot x_1 \cdot y_2 + \cdots + \lambda \cdot x_{n-2} \cdot y_{n-1} \ldots (i)$$

$$x \cdot \tau_\lambda^{n-1}(y) \underset{i\text{'den}}{=} \left(x_0, x_1, \ldots, x_{n-1} \right) \cdot \left(\lambda \cdot y_1, \lambda \cdot y_2, \lambda \cdot y_3, \ldots, \lambda \cdot y_{n-1}, y_0 \right)$$

$$= x_0 \cdot \lambda \cdot y_1 + x_1 \cdot \lambda \cdot y_2 + \cdots + x_{n-2} \cdot \lambda \cdot y_{n-1} + x_{n-1} \cdot y_0$$

$$\underset{\substack{+ \text{ ve } \cdot \text{'nın} \\ \text{değişme} \\ \text{özelliği}}}{=} x_{n-1} \cdot y_0 + \lambda \cdot x_0 \cdot y_1 + \lambda \cdot x_1 \cdot y_2 + \cdots + \lambda \cdot x_{n-2} \cdot y_{n-1} \ldots (ii)$$

O halde i ve ii 'den; $\lambda \cdot \tau_{\lambda^{-1}}(x) \cdot y = x \cdot \tau_\lambda^{n-1}(y)$ olur.$\cdots (ii)$

Bu durumda;

$$\Rightarrow \lambda \cdot \tau_{\lambda^{-1}}(x) \cdot y = 0$$

$$\underset{\substack{\lambda \text{ tersinir} \\ \text{eleman} \\ \text{olduğundan} \\ \lambda \neq 0 \\ \text{ve } R\text{; sıfır} \\ \text{bölensiz} \\ \text{halka}}}{\Rightarrow} \tau_{\lambda^{-1}}(x) \cdot \underset{\in C}{y} = 0$$

$$\underset{C^\perp \text{ tanımı}}{\Rightarrow} \tau_{\lambda^{-1}}(x) \in C^\perp$$

O halde $C^\perp$, $\lambda^{-1}-$constacyclic koddur.

4.2.1.Tanım: C, $R = \mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\left(u^2 = 0\right)$ halkası üzerinde n uzunluğunda bir kod olsun. $Tor(C) = \left\{ b \in \mathbb{F}_{p^k}{}^n \middle| ub \in C \right\}$, $Res(C) = \left\{ a \in \mathbb{F}_{p^k}{}^n \middle| \exists b \in \mathbb{F}_{p^k}{}^n \text{ için } a + ub \in C \right\}$ biçiminde tanımlanan kümelere sırasıyla C kodunun **torsiyon ve rezidü kodları** denir. (Dinh, 2010)

4.2.4.Önerme: C, R üzerinde n uzunluklu, torsiyon kodu $Tor(C)$, rezidü kodu $Res(C)$ olan bir constacyclic kod olsun. Bu durumda, $|C| = |Tor(C)| \cdot |Res(C)|$'dir. (Dinh, 2010)

Kanıt: C, $R = \mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\left(u^2 = 0\right)$ halkası üzerinde n uzunluğunda bir kod olmak üzere;

$$f : C \to Res(C)$$
$$a + u\,b \mapsto f(a + u\,b) = a$$

biçiminde bir f dönüşümü tanımlansın.

f dönüşümünün tanımı kullanılarak toplama ve çarpma işlemlerini koruduğu kolaylıkla gösterilir.

Herhangi bir $a \in Res(C)$

$\underset{\substack{Res(C)\\ \text{tanımı}}}{\Rightarrow} a + u\,b \in C$ olacak şekilde en az bir $b \in \mathbb{F}_{p^k}{}^n$ vardır.

$\Rightarrow f(a + u \cdot b) = a$ olur.

O halde f örtendir.

O halde f örten bir homomorfizmadır.

f için $Çek\ f = Tor(C)$'dir. Ayrıca f dönüşümü örten olduğundan; $f(C) = Res(C)$ 'dir.

$$C \underset{\substack{\text{örten}\\ \text{homomorfizma}}}{\overset{f}{\to}} Res(C)$$
$$\varphi \downarrow \quad \nearrow \overline{f}$$
$$\underbrace{C/Çek\varphi}_{=C/Tor(C)}$$

Yukarıda diyagramı verilen 1. İzomorfizma teoreminden; $C/Tor(C) \cong Res(C)$ dir. C, $Tor(C)$ ve $Res(C)$ kümeleri sonlu küme olduklarından; $\left|\frac{C}{Tor(C)}\right| = |Res(C)|$ dir. Bu durumda; $|C| = |Tor(C)| \cdot |Res(C)|$ elde edilir.

4.2.1.Lemma: $\mathbb{F}$ q elemanlı sonlu bir cisim olsun. Bu durumda; $\mathbb{F}$ cisminin herhangi bir β elemanı için; $\beta^q = \beta$ 'dır. (Ling, Xing, 2004, s.26)

Kanıt: $\beta = 0 \Rightarrow \beta^q = \beta$ olacağı açıktır.

$\beta \neq 0$ olsun.

$\mathbb{F}$ cisminin 0 'dan farklı tüm elemanlarının kümesi; $\mathbb{F}^* = \{\beta_1, \beta_2, \ldots, \beta_{q-1}\}$

$\Rightarrow \mathbb{F}^* = \{\beta \cdot \beta_1, \beta \cdot \beta_2, \ldots, \beta \cdot \beta_{q-1}\}$ 'dir.

(Cisimde 0 bölen olmadığından; sıfırdan farklı β elemanı ile, sıfır olmayan herhangi bir elemanın çarpımı sıfırdan farklı olur. Dolayısıyla bu çarpımların sonuçlarının kümesi $\mathbb{F}^*$ kümesidir.)

$$\Rightarrow \beta_1 \cdot \beta_2 \cdot \beta_3 \cdot \ldots \cdot \beta_{q-1} = (\beta \cdot \beta_1) \cdot (\beta \cdot \beta_2) \cdot (\beta \cdot \beta_3) \ldots \cdot (\beta \cdot \beta_{q-1}) \underset{\substack{\text{'nın} \\ \text{birleşme ve} \\ \text{değişme} \\ \text{özelliği}}}{=} \beta^{q-1} \cdot (\beta_1 \cdot \beta_2 \cdot \beta_3 \cdot \ldots \cdot \beta_{q-1})$$

$\Rightarrow \beta^{q-1} = 1 \Rightarrow \beta^q = \beta$ 'dir. □

$\mathbb{F}_{p^k}$ üzerinde $\lambda-$constacyclic kodların varlığı için λ, $\mathbb{F}_{p^k}$ cisminin bir tersinir elemanı olmalıdır. λ tersinir olduğundan; $\mathbb{F}_{p^k}$ cisminde sıfırdan farklı λ^{-1} elemanı vardır.. 4.2.1.Lemmadan; $\left(\lambda^{-1}\right)^{p^k} = \lambda^{-1} \Rightarrow \lambda^{-p^k} = \lambda^{-1}$ 'dir.

4.2.5.Önerme: Bölme algoritmasını kullanılarak s doğal sayısı k doğal sayısına bölünürse; $s = \lambda_q \cdot k + \lambda_r$, $0 \leq \lambda_r \leq k-1$ olacak şekilde λ_q, λ_r pozitif tam sayıları vardır. $\lambda_0 = -\lambda^{-p^{(\lambda_q+1)k-s}}$ biçiminde tanımlanan λ_0 elemanının p^s. kuvveti; λ elemanının $\cdot$ işlemine göre ters elemanının $+$ işlemine göre ters elemanıdır. (Dinh, 2010)

Kanıt:

$\lambda_0 = -\lambda^{-p^{\lambda_q \cdot k + k - s}} \underset{s=\lambda_q \cdot k + \lambda_r}{=} -\lambda^{-p^{\lambda_q \cdot k + k - \lambda_q \cdot k - \lambda_r}} = -\lambda^{-p^{k-\lambda_r}}$ 'dir. Bu durumda;

$$\lambda_0{}^{p^s} = \left(-\lambda^{-p^{k-\lambda_r}}\right)^{p^s} = -\lambda^{-p^{k-\lambda_r+s}} \underset{s=\lambda_q \cdot k + \lambda_r}{=} -\lambda^{-p^{k-\lambda_r+\lambda_q \cdot k+\lambda_r}}$$

$$= -\lambda^{-\left(p^k\right)^{1+\lambda_q}} = -\lambda^{-\overbrace{p^k \cdot p^k \cdot p^k \ldots . p^k}^{(1+\lambda_q)\text{ tane}}}$$

$$\underset{\substack{(1+\lambda_q)\text{ defa}\\ p^k\text{. kuvvet}\\ \text{alınacak}}}{=} -\left(\left(\left(\left(\lambda^{-p^k}\right)^{p^k}\right)^{p^k}\right)^{\iddots}\right)^{p^k} \underset{\lambda^{-p^k}=\lambda^{-1}}{=} -\left(\left(\left(\left(\lambda^{-1}\right)^{p^k}\right)^{p^k}\right)^{\iddots}\right)^{p^k} = -\lambda^{-p^k} = -\lambda^{-1}\text{'dir.}\square$$

Bu bölüm boyunca $\mathbb{F}_{p^k}$ cisminin λ_0 elemanı; 4.2.5.Önerme'de tanımladığı gibi olacaktır.

4.2.6.Önerme: λ_0 4.2.5.Önermedeki gibi olmak üzere;

$$\mu : \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}+1 \right\rangle \to \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}-\lambda \right\rangle$$
$$\overline{f(x)} \mapsto \mu\left(\overline{f(x)}\right) = \overline{f(\lambda_0 \cdot x)}$$

biçiminde tanımlanan μ dönüşümü bir izomorfizmadır. (Dinh, 2010)

Kanıt: Herhangi iki $\overline{f(x)}, \overline{g(x)} \in \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}+1 \right\rangle$ için

$\overline{f(x)} = \overline{g(x)}$

$\Leftrightarrow f(x) \equiv g(x)\left(\mathrm{mod}\left(x^{p^s}+1\right)\right)$

$\Leftrightarrow x^{p^s}+1 \mid f(x)-g(x)$

$\Leftrightarrow f(x)-g(x) = h(x)\cdot\left(x^{p^s}+1\right)$ olacak biçimde öyle bir $h(x) \in \mathbb{F}_{p^k}[x]$ vardır.

$\Leftrightarrow f(\lambda_0 \cdot x)-g(\lambda_0 \cdot x) = h(\lambda_0 \cdot x)\cdot\left((\lambda_0 \cdot x)^{p^s}+1\right)$

$\underset{\substack{\lambda_0{}^{p^s}=-\lambda^{-1}\\ 1_{\mathbb{F}_{p^k}}=\lambda\cdot\lambda^{-1}}}{\Leftrightarrow} f(\lambda_0 \cdot x)-g(\lambda_0 \cdot x) = h(\lambda_0 \cdot x)\cdot\left(-\lambda^{-1}\cdot x^{p^s}+\lambda\cdot\lambda^{-1}\right)$

$\Leftrightarrow f(\lambda_0 \cdot x)-g(\lambda_0 \cdot x) = \underbrace{-\lambda^{-1}\cdot h(\lambda_0 \cdot x)}_{\in\mathbb{F}_{p^k}[x]}\cdot\left(x^{p^s}-\lambda\right)$

$\Leftrightarrow x^{p^s}-\lambda \mid f(\lambda_0 \cdot x)-g(\lambda_0 \cdot x)$

$\Leftrightarrow f(\lambda_0 \cdot x) \equiv g(\lambda_0 \cdot x)\left(\mathrm{mod}\left(x^{p^s}-\lambda\right)\right)$

$\Leftrightarrow \overline{f(\lambda_0 \cdot x)} = \overline{g(\lambda_0 \cdot x)}$

$\Leftrightarrow \mu\left(\overline{f(x)}\right) = \mu\left(\overline{g(x)}\right)$

O halde μ iyi tanımlı ve birebirdir.

Herhangi bir $\overline{f(x)} \in {\mathbb{F}_{p^k}[x]}\Big/{\left\langle x^{p^s} - \lambda \right\rangle}$

$\Rightarrow f(x) \in \mathbb{F}_{p^k}[x] \underset{\substack{\lambda_0 \in \mathbb{F}_{p^k} \\ \lambda_0^{-1} \in \mathbb{F}_{p^k}}}{\Rightarrow} f\left(\lambda_0^{-1} \cdot x\right) \in \mathbb{F}_{p^k}[x]$'dir.

Öyle bir $\overline{f\left(\lambda_0^{-1} \cdot x\right)} \in {\mathbb{F}_{p^k}[x]}\Big/{\left\langle x^{p^s} + 1 \right\rangle}$ elemanı için;

$\mu\left(\overline{f\left(\lambda_0^{-1} \cdot x\right)}\right) = f\left(\lambda_0 \cdot \left(\lambda_0^{-1} \cdot x\right)\right) = \overline{f(x)} \in {\mathbb{F}_{p^k}[x]}\Big/{\left\langle x^{p^s} - \lambda \right\rangle}$'dir.

O halde μ örtendir.

μ fonksiyonunun tanımlanışından toplama ve çarpma işlemlerini koruduğunu göstermek kolaydır.

O halde μ bir izomorfizmadır.

4.2.1.Sonuç: $\pi(C)$ kümesinin ${\mathbb{F}_{p^k}[x]}\Big/{\left\langle x^{p^s} + 1 \right\rangle}$ halkasının bir ideali olması için gerekli ve yeterli koşul $\mu\left(\pi(C)\right)$ kümesinin ${\mathbb{F}_{p^k}[x]}\Big/{\left\langle x^{p^s} - \lambda \right\rangle}$ halkasının bir ideali olmasıdır. □

4.2.1.Sonuçta verilen idealler ile $\mathbb{F}_{p^k}$ üzerinde p^s uzunluklu kodlar arasındaki ilişki düşünüldüğünde; $\mathbb{F}_{p^k}$ üzerinde p^s uzunluklu negacyclic kodlarla $\lambda-$constacyclic kodlar arasında izomorfik ilişki kurulmuş olur.

4.2.7.Önerme: ${\mathbb{F}_{p^k}[x]}\Big/{\left\langle x^{p^s} - \lambda \right\rangle}$ halkasının $\left\langle \overline{\lambda_0 \cdot x + 1} \right\rangle$ elemanı; nilpotentlik derecesi p^s olan bir nilpotent elemandır. (Dinh, 2010)

Kanıt: Her $\overline{\lambda_0 \cdot x+1} \in \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}-\lambda \right\rangle$ için;

$$\left(\overline{\lambda_0 \cdot x+1}\right)^{p^s} = \overline{\left(\lambda_0 \cdot x+1\right)^{p^s}} \underset{\substack{\text{Binom}\\ \text{Açılımı}}}{=} \overline{\left(\lambda_0 \cdot x\right)^{p^s}} + \bar{1} + \overline{\sum_{i=1}^{p^s-1} \binom{p^s}{i} \cdot \left(\lambda_0 \cdot x\right)^i} \underset{i\text{'den}}{=} \overline{\lambda_0^{p^s} \cdot x^{p^s}} + \bar{1}$$

$$\underset{\substack{\text{4.2.5.Önerme,}\\ x^{p^s} \equiv \lambda \left(\bmod\left(x^{p^s}-\lambda\right)\right)}}{=} \overline{-\lambda^{-1} \cdot \lambda} + \bar{1} = \bar{0} \in \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}-\lambda \right\rangle \text{'dir.}$$

$$\left(\begin{array}{l} 1 \le i \le p^s - 1 \text{ için; } p \left| \binom{p^s}{i} \right. \text{ ve Char } \mathbb{F}_{p^k} = p \text{ olduğundan;} \\ \overline{\sum_{i=1}^{p^s-1} \binom{p^s}{i} \cdot \left(\lambda_0 \cdot x\right)} = \bar{0} \in \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}-\lambda \right\rangle \text{'dir.} \end{array} \right) \cdots (i)$$

O halde $\overline{\lambda_0 \cdot x+1}$ nilpotentlik derecesi p^s olan nilpotent bir elemandır.

4.2.2.Sonuç: $\mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}-\lambda \right\rangle$ halkası maximal ideali $\overline{\lambda_0 \cdot x+1}$ olan bir zincir halkasıdır. $\mathbb{F}_{p^k}$ üzerindeki p^s uzunluklu $\lambda-$constacyclic kodlarına karşılık gelen idealler; $0 \le i \le p^s$ olmak üzere; $\left\langle \overline{\left(\lambda_0 \cdot x+1\right)^i} \right\rangle \subseteq \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}-\lambda \right\rangle$ idealleridir. Bu ideallerin oluşturduğu zincir;

$$\left\langle \bar{0} \right\rangle = \left\langle \overline{\left(\lambda_0 \cdot x+1\right)^{p^s}} \right\rangle \underset{\neq}{\subset} \left\langle \overline{\left(\lambda_0 \cdot x+1\right)^{p^s-1}} \right\rangle \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \left\langle \overline{\lambda_0 \cdot x+1} \right\rangle \underset{\neq}{\subset} \left\langle \bar{1} \right\rangle = \mathbb{F}_{p^k}[x] \Big/ \left\langle x^{p^s}-\lambda \right\rangle$$

biçimindedir. (Dinh, 2010) □

$\alpha + u\beta$, $R = \mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ $(u^2 = 0)$ halkasının tersinir elemanı olmak üzere; R üzerinde p^s uzunluklu $\alpha + u\beta-$constacyclic kodlarla $R[x] \Big/ \left\langle x^{p^s} - (\alpha + u\beta) \right\rangle$ bölüm

halkasının idealleri arasında birebir eşleme vardır. Bu bölümde $R[x] \Big/ \left\langle x^{p^s} - (\alpha + u\beta) \right\rangle$ bölüm halkası kısaca $R_{\alpha,\beta}$ biçiminde gösterilecektir.

Bu bölüm devamında; $\mathbb{F}_{p^k}$ cismi üzerinde p^s uzunluklu $\lambda-$constacyclic kodlar için yapılan çalışmalar, R halkası üzerinde p^s uzunluklu $(\alpha+u\beta)-$constacyclic kodlar için yapılacaktır.

4.2.8.Önerme: Bölme algoritmasını kullanılarak s doğal sayısı k doğal sayısına bölünürse; $s=\alpha_q\cdot k+\alpha_r$, $0\le\alpha_r\le k-1$ olacak şekilde α_q,α_r pozitif tam sayıları vardır. $\alpha_0=-\alpha^{-p^{(\lambda_q+1)k-s}}$ biçiminde tanımlanan α_0 elemanının p^s. kuvveti; α elemanının " $\cdot$ " işlemine göre ters elemanıdır. (Dinh, 2010)

Kanıt: $\alpha_0=\alpha^{-p^{\alpha_q\cdot k+k-s}} \underset{s=\alpha_q\cdot k+\alpha_r}{=} \alpha^{-p^{\alpha_q\cdot k+k-\alpha_q\cdot k-\alpha_r}}=\alpha^{-p^{k-\alpha_r}}$'dir. Bu durumda;

$$\alpha_0{}^{p^s}=\left(\alpha^{-p^{k-\alpha_r}}\right)^{p^s}=\alpha^{-p^{k-\alpha_r+s}} \underset{s=\alpha_q\cdot k+\alpha_r}{=} \alpha^{-p^{k-\alpha_r+\alpha_q\cdot k+\alpha_r}}$$

$$=-\alpha^{-\left(p^k\right)^{1+\alpha_q}}=\alpha^{-\overbrace{p^k\cdot p^k\cdot p^k\cdot\cdots\cdot p^k}^{(1+\alpha_q)\text{ tane}}}$$

$$\underset{\substack{(1+\lambda_q)\text{ defa}\\ p^k\text{. kuvvet}\\ \text{alınacak}}}{=}\left(\left(\left(\left(\alpha^{-p^k}\right)^{p^k}\right)^{p^k}\right)^{\cdot^{\cdot}}\right)^{p^k} \underset{\substack{\text{4.2.1.Lemma'dan;}\\ \alpha^{-p^k}=\alpha^{-1}}}{=}\left(\left(\left(\left(\alpha^{-1}\right)^{p^k}\right)^{p^k}\right)^{\cdot^{\cdot}}\right)^{p^k}=\alpha^{-p^m}=\alpha^{-1}\text{'dir.}\square$$

Bu bölüm boyunca $\mathbb{F}_{p^k}$ cisminin α_0 elemanı; 4.2.8.Önerme'de tanımladığı gibi olacaktır.

4.2.9.Önerme: $\overline{\alpha_0\cdot x-1}$, $R_{\alpha,\beta}$ halkasının nilpotentlik derecesi $2\cdot p^s$ olan nilpotent elemanıdır. Ayrıca; $\left\langle\left(\overline{\alpha_0\cdot x-1}\right)^{p^s}\right\rangle=\left\langle\bar{u}\right\rangle$'dur. (Dinh, 2010)

Kanıt: $\overline{\alpha_0\cdot x-1}\in R_{\alpha,\beta}$ için;

$$\left(\overline{\alpha_0\cdot x-1}\right)^{p^s}=\overline{\left(\alpha_0\cdot x-1\right)^{p^s}} \underset{\substack{\text{Binom}\\ \text{Açılımı}}}{=} \overline{\left(\alpha_0\cdot x\right)^{p^s}}-\bar{1}+\overline{\sum_{i=1}^{p^s-1}\binom{p^s}{i}\cdot\left(\alpha_0\cdot x\right)^i\cdot(-1)^{p^s-i}}$$

$$=\overline{\left(\alpha_0\cdot x\right)^{p^s}-1}=\overline{{\alpha_0}^{p^s}\cdot x^{p^s}-1}\underset{\substack{4.2.8.\\ \text{Önerme}}}{=}\overline{\alpha^{-1}\cdot x^{p^s}-1}$$

$$\underset{x^{p^s}\equiv(\alpha+u\cdot\beta)\left(\bmod\left(x^{p^s}-(\alpha+u\cdot\beta)\right)\right)}{=}\overline{\alpha^{-1}\cdot(\alpha+u\,\beta)-1}=\overline{\alpha^{-1}\cdot\alpha+u\left(\alpha^{-1}\cdot\beta\right)-1}$$

$=\overline{1+u\left(\alpha^{-1}\cdot\beta\right)-1}=\overline{u\left(\alpha^{-1}\cdot\beta\right)}\cdots(i)$'dir. Bu durumda;

$$\left(\overline{\alpha_0\cdot x-1}\right)^{2\cdot p^s}=\left(\left(\overline{\alpha_0\cdot x-1}\right)^{p^s}\right)^2=\left(\overline{u\left(\alpha^{-1}\cdot\beta\right)}\right)^2=\overline{\left(u\left(\alpha^{-1}\cdot\beta\right)\right)^2}=\overline{u^2\left(\alpha^{-1}\cdot\beta\right)^2}\underset{u^2=0}{=}\bar{0}\in R_{\alpha,\beta}$$ 'dir.

$$\left(\overline{\alpha_0\cdot x-1}\right)^{p^s}=\overline{\left(\alpha_0\cdot x-1\right)^{p^s}}\underset{\substack{\text{Binom}\\ \text{Açılımı}}}{=}\overline{\left(\alpha_0\cdot x\right)^{p^s}}-\bar{1}+\overline{\sum_{i=1}^{p^s-1}\binom{p^s}{i}\cdot\left(\alpha_0\cdot x\right)^i\cdot(-1)^{p^s-i}}$$

$$=\overline{\left(\alpha_0\cdot x\right)^{p^s}-1}=\overline{{\alpha_0}^{p^s}\cdot x^{p^s}-1}\underset{\substack{4.2.8.\\ \text{Önerme}}}{=}\overline{\alpha^{-1}\cdot x^{p^s}-1}$$

$$\underset{x^{p^s}\equiv(\alpha+u\,\beta)\left(\bmod\left(x^{p^s}-(\alpha+u\cdot\beta)\right)\right)}{=}\overline{\alpha^{-1}\cdot(\alpha+u\,\beta)-1}=\overline{\alpha^{-1}\cdot\alpha+u\left(\alpha^{-1}\cdot\beta\right)-1}=$$

$$\overline{1+u\left(\alpha^{-1}\cdot\beta\right)-1}=\overline{u\left(\alpha^{-1}\cdot\beta\right)}$$

$$\Rightarrow\left(\overline{\alpha_0\cdot x-1}\right)^{2\cdot p^s}=\left(\left(\overline{\alpha_0\cdot x-1}\right)^{p^s}\right)^2=\left(\overline{u\left(\alpha^{-1}\cdot\beta\right)}\right)^2=\overline{\left(u\left(\alpha^{-1}\cdot\beta\right)\right)^2}$$

$$\left\langle\left(\overline{\alpha_0\cdot x-1}\right)^{p^s}\right\rangle=\left\langle\overline{u\left(\alpha^{-1}\cdot\beta\right)}\right\rangle=\overline{u\left(\alpha^{-1}\cdot\beta\right)}\cdot R_{\alpha,\beta}=\bar{u}\underbrace{\overline{\left(\alpha^{-1}\cdot\beta\right)}\cdot R_{\alpha,\beta}}_{\substack{=R_{\alpha,\beta}\\ \left(\alpha^{-1}\cdot\beta\right)\in R}}=\bar{u}\,R_{\alpha,\beta}=\left\langle\bar{u}\right\rangle$$

4.2.10.Önerme: $R_{\alpha,\beta}$ bölüm halkası

$\left\langle\bar{0}\right\rangle=\left\langle\overline{\left(\alpha_0\cdot x-1\right)^{2\cdot p^s}}\right\rangle\underset{\neq}{\subset}\left\langle\overline{\left(\alpha_0\cdot x-1\right)^{2\cdot p^s-1}}\right\rangle\underset{\neq}{\subset}\cdots\underset{\neq}{\subset}\left\langle\overline{\alpha_0\cdot x-1}\right\rangle\underset{\neq}{\subset}\left\langle\bar{1}\right\rangle=R_{\alpha,\beta}$ idealleri ile bir zincir halkasıdır. (Amarra, Nemenzo,2008) □

$R=\mathbb{F}_{p^k}+u\cdot\mathbb{F}_{p^k}\left(u^2=0\right)$ halkası üzerindeki p^s uzunluklu $(\alpha+u\,\beta)-$ constacyclic kodların polinom temsilleri, $0\le i\le 2\cdot p^s$ olmak üzere $R_{\alpha,\beta}$ zincir halkasının $\left\langle\left(\alpha_0\,x-1\right)^i\right\rangle$ idealleridir. (Dinh, 2010)

4.2.2.Lemma: $\mathbb{F}$, p^m elemanlı sonlu bir cisim ise $Char\left(\mathbb{F}\right)=p$'dir. (Crandall, Pomerance, 2005, s.93)

Kanıt: $i \in \mathbb{Z}^+$ için $\gamma_i = \underbrace{1+1+\cdots+1}_{i \text{ tane}}$ biçiminde tanımlansın. Her $i \in \mathbb{Z}^+$ için $\gamma_i \in \mathbb{F}_{p^m}$'dir. $\mathbb{F}_{p^m}$ sonlu olduğundan öyle bir $i < j$ için $\gamma_i = \gamma_j$'dir.

$$\Rightarrow \underbrace{1+1+\cdots+1}_{i \text{ tane}} = \underbrace{1+1+\cdots+1}_{i \text{ tane}} + \underbrace{1+1+\cdots 1}_{j-i \text{ tane}}$$

$\Rightarrow$ En az bir $j-i \in \mathbb{Z}^+$ için $\gamma_{j-i} = 0$

$\Rightarrow Char\left(\mathbb{F}_{p^m}\right) \neq 0$'dır.

$Char\left(\mathbb{F}_{p^m}\right) = c \in \mathbb{Z}^+$ olsun. c asal olmasın.

$\Rightarrow$ $c = a \cdot b$ olacak biçimde öyle bir $a, b \in \mathbb{Z}^+$ vardır.

$$\underset{Char\left(\mathbb{F}_{p^m}\right)=c}{\Rightarrow} \underbrace{1+1+\cdots+1}_{c \text{ tane}} = 0$$

$$\underset{c=a\cdot b}{\Rightarrow} \underbrace{\left(\underbrace{1+1+\cdots 1}_{a \text{ tane}}\right) \cdot \left(\underbrace{1+1+\cdots 1}_{a \text{ tane}}\right) \cdot \cdots \cdot \left(\underbrace{1+1+\cdots 1}_{a \text{ tane}}\right)}_{b \text{ tane}} = 0$$

$$\underset{\substack{\cdot \text{ işleminin} \\ + \text{ üzerine} \\ \text{dağılma} \\ \textit{özelliği}}}{\Rightarrow} \left(\underbrace{1+1+\cdots 1}_{a \text{ tane}}\right) \cdot \left(\underbrace{1+1+\cdots 1}_{b \text{ tane}}\right) = 0$$

$\Rightarrow Char\left(\mathbb{F}_{p^m}\right) = a$ ya da $Char\left(\mathbb{F}_{p^m}\right) = b$ dir. Çelişki! ($Char\left(\mathbb{F}_{p^m}\right) = c$ idi.)

Bu durumda $Char\left(\mathbb{F}_{p^m}\right) = p$'dir.

4.2.3.Lemma: $\mathbb{F}$ karakteristiği p olan sonlu bir cisim ise $\mathbb{F}$ cisminin herhangi iki a, b elemanı ve sıfırdan büyük bir i tamsayısı için $\left(a+b\right)^{p^i} = a^{p^i} + b^{p^i}$ ve $\left(a-b\right)^{p^i} = a^{p^i} - b^{p^i}$'dir. (Crandall, Pomerance, 2005, s.93)

Kanıt: $\left(a+b\right)^{p^i} = a^{p^i} + b^{p^i}$ eşitliği i üzerinden tümevarımla kanıtlanmak istenirse;

$i = 1$ için $\left(a+b\right)^{p} = a^{p} + b^{p} + \sum_{i=1}^{p-1} \binom{p}{i} \cdot a^i \cdot b^{p-i} \underset{\substack{i \text{ ve} \\ \text{Char}(\mathbb{F})=p}}{=} a^p + b^p$'dir.

$$\left(\begin{array}{l} 1\le i\le p-1 \text{ için } \binom{p}{i}=\dfrac{(p-i+1)\cdot\ldots\cdot(p-1)\cdot p}{i!} \text{ eşitliğinde paydada yer alan tam sayılar} \\ p\text{'den daha küçük ve } p \text{ asal sayı olduğundan paydada yer alan sayılarla } p \text{ arasında bölünme} \\ \text{olmaz. Diğer taraftan kombinasyon hesabın sonucu bir doğalsayı olması gerektiğinden} \\ (i!)\big|(p-i+1)\cdot\ldots\cdot(p-1)\text{'dir.} \\ \Rightarrow \text{ Öyle bir } k\in\mathbb{N}^+ \text{ için } (p-i+1)\cdot\ldots\cdot(p-1)=k\cdot(i!) \\ \Rightarrow \text{Öyle bir } k\in\mathbb{N}^+ \text{ için } \binom{p}{i}=k\cdot p\text{'dir.} \end{array}\right)\cdots(i)$$

$i=t$ için önerme doğru olsun. Yani; $(a+b)^{p^t}=a^{p^t}+b^{p^t}$ olsun.

$i=t+1$ için;

$$(a+b)^{p^{t+1}}=\left((a+b)^p\right)^{p^t}\underset{\substack{i=1 \text{ için}\\ \text{önerme}\\ \text{doğru.}}}{=}\left(a^p+b^p\right)^{p^t}\underset{\substack{i=t \text{ için}\\ \text{önerme}\\ \text{doğru.}}}{=}\left(a^p\right)^{p^t}+\left(b^p\right)^{p^t}=a^{p^{t+1}}+b^{p^{t+1}}\text{'dir.}$$

O halde her $i\in\mathbb{Z}^+$ için; $(a+b)^{p^i}=a^{p^i}+b^{p^i}$'dir.$\cdots(ii)$

Diğer taraftan; her $i\in\mathbb{Z}^+$ için $a^{p^i}=\left((a-b)+b\right)^{p^i}\underset{\text{ii'}den}{=}(a-b)^{p^i}+b^{p^i}$

$\Rightarrow(a-b)^{p^i}=a^{p^i}-b^{p^i}$ olur.□

4.2.11.Önerme: $\alpha+u\beta$, $R=\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ $(u^2=0)$ halkasının tersinir bir elemanı olmak üzere $(\alpha+u\beta)^{-1}=\alpha^{-1}+u\beta\cdot\alpha^{-2}$'dir. (Dinh, 2010)

Kanıt: $(\alpha+u\beta)^{p^k}\underset{\text{4.2.3.Lemma}}{=}\alpha^{p^k}+(u\beta)^{p^k}\underset{\text{4.2.1.Lemma}}{=}\alpha+u^{p^k}\beta^{p^k}\underset{\substack{p^k\ge 2\\ ve\\ u^2=0}}{=}\alpha$'dir.$\cdots(i)$

$\alpha\cdot\alpha^{-1}=1$

$\underset{\text{i'dan}}{\Rightarrow}(\alpha+u\beta)^{p^k}\cdot\alpha^{-1}=1$

$\Rightarrow(\alpha+u\beta)^{-1}\cdot\left((\alpha+u\beta)^{p^k}\cdot\alpha^{-1}\right)=(\alpha+u\beta)^{-1}\cdot 1$

$\Rightarrow(\alpha+u\beta)^{-1}=(\alpha+u\beta)^{p^k-1}\cdot\alpha^{-1}$

$$\left(\begin{array}{l}(\alpha+u\beta)^{p^{k-1}}=\alpha^{p^{k-1}}+\binom{p^k-1}{1}\cdot\alpha^{p^{k-2}}\cdot(u\beta)+\underbrace{\binom{p^k-1}{2}\cdot\alpha^{p^{k-3}}\cdot(u\beta)^2+\cdots+\binom{p^k-1}{p^m-2}\cdot\alpha^{1}\cdot(u\beta)^{p^m-2}}_{=0\ (u^2=0\ \text{olduğundan.})}\\ =\alpha^{p^{k-1}}+(p^k-1)\cdot\alpha^{p^{k-2}}\cdot(u\beta)=\alpha^{p^k}\cdot\alpha^{-1}+\left(p^k\cdot\alpha^{p^k}\cdot\alpha^{-2}-\alpha^{p^k}\cdot\alpha^{-2}\right)\cdot(u\beta)\underset{\substack{3.2.1.Lemma\\ Char\left(\mathbb{F}_{p^k}\right)=p}}{=}\alpha\cdot\alpha^{-1}-\alpha\cdot\alpha^{-2}\cdot(u\beta)\cdots(ii)\\ =1-u\beta\cdot\alpha^{-1}\text{'dir.}\end{array}\right)$$

$\underset{**\text{'dan.}}{=}\left(1-u\beta\cdot\alpha^{-1}\right)\cdot\alpha^{-1}=\alpha^{-1}-u\beta\cdot\alpha^{-2}$ 'dir. □

4.2.3.Önerme ve 4.2.11.Önermeden aşağıdaki 4.2.3.Sonuç verilir.

4.2.3.Sonuç: R üzerinde p^s uzunluklu bir $(\alpha+u\beta)-$constacyclic kodun dual kodu bir $\left(\alpha^{-1}-u\beta\cdot\alpha^{-2}\right)-$constacyclic koddur. (Dinh, 2010) □

R halkası üzerinde p^s uzunluklu bir $\left(\alpha^{-1}-u\beta\cdot\alpha^{-2}\right)-$constacyclic kod $\left\langle\overline{u},\overline{x-1}\right\rangle$ zincir halkasının bir idealidir. (Dinh, 2010)

R halkası üzerinde tanımlı p^s uzunluklu bir cyclic kodun polinom temsili $R_1=R[x]\Big/\left\langle x^{p^s}-1\right\rangle$ bölüm halkasının bir idealidir. (Dinh, 2010)

4.2.12.Önerme: $\overline{x-1}$, R_1 halkasının nilpotentlik derecesi p^s olan bir nilpotent elemanıdır. (Dinh, 2010)

Kanıt: $\left(\overline{x-1}\right)^{p^s}=\overline{(x-1)^{p^s}}\underset{4.2.3.Lemma}{=}\overline{x^{p^s}-1^{p^s}}\underset{x^{p^s}\equiv 1\left(\bmod\left(x^{p^s}-1\right)\right)}{=}\overline{1^{p^s}-1^{p^s}}=\overline{0}$ 'dır.

O halde $\overline{x-1}$ bir nilpotent elemandır.

Herhangi bir $k<p^s, k\in\mathbb{Z}^+$ için

$\left(\overline{x-1}\right)^k=\overline{(x-1)^k}\underset{4.2.3.Lemma}{=}\overline{x^k-1^{p^s}}\underset{x^{p^s}\not\equiv 1\left(\bmod\left(x^{p^s}-1\right)\right)}{\neq}\overline{0}$ 'dır.

O halde $\overline{x-1}$ elemanının nilpotentlik derecesi p^s 'dir.

4.2.13.Önerme: R_1 halkası maximal ideali $\langle \bar{u}, \overline{x-1} \rangle$ olan bir yerel halkadır fakat bir zincir halkası değildir. (Dinh, 2010)

4.2.14.Önerme: $\mathbb{F}_{p^k}$ cisminde sıfırdan farklı herhangi bir γ elemanı için $\mathbb{F}_{p^k}$ cisminde ${\gamma_0}^{p^s} = \gamma^{-1}$ olacak şekilde en az bir γ_0 elemanı vardır. (Dinh, 2010)

Kanıt: Bölme algoritması kullanılarak s, m'ye bölündüğünde $s = \gamma_q \cdot k + \gamma_r$ olacak biçimde γ_q, γ_r pozitif tam sayıları vardır.

$\gamma_0 = \gamma^{-p^{(\gamma_q+1)\cdot k - s}} = \gamma^{-p^{k-\gamma_r}}$ olsun.

$${\gamma_0}^{p^s} = \left(\gamma^{-p^{k-\gamma_r}}\right)^{p^s} = \gamma^{-p^{k-\gamma_r+s}} \underset{s=\gamma_q\cdot k+\gamma_r}{=} \gamma^{-p^{k+\gamma_q\cdot k}} = \gamma^{-p^k\cdot p^{k\cdot\gamma_q}} = \left(\gamma^{-p^k}\right)^{p^{k\cdot\gamma_q}} = \left(\gamma^{-p^k}\right)^{\left(p^k\right)^{\gamma_q}}$$

$$= \left(\gamma^{-p^k}\right)^{\underbrace{p^k\cdot p^k\cdot\ldots\cdot p^k}_{\gamma_q \text{ tane}}} \underset{\text{4.2.1.}Lemma}{=} \left(\gamma^{-1}\right)^{\underbrace{p^k\cdot p^k\cdot\ldots\cdot p^k}_{\gamma_q \text{ tane}}} = \left(\left(\left(\left(\gamma^{-1}\right)^{p^k}\right)^{p^k}\right)^{\cdot^{\cdot^{\cdot}}}\right)^{p^k} \underset{\text{4.2.1.}Lemma}{=} \gamma^{-1} \text{ olur.}$$

4.2.15.Önerme: γ ve γ_0, 4.2.14.Önermede tanımlandığı gibi olmak üzere;

$$\psi : \frac{R[x]}{\langle x^{p^s}-1\rangle} \to \frac{R[x]}{\langle x^{p^s}-\gamma\rangle}$$
$$\overline{f(x)} \mapsto \psi\left(\overline{f(x)}\right) = \overline{f(\gamma_0 \cdot x)}$$

biçiminde tanımlanan ψ dönüşümü bir izomorfizmadır. (Dinh, 2010)

Kanıt: Herhangi iki $\overline{f(x)}, \overline{g(x)} \in \frac{R[x]}{\langle x^{p^s}-1\rangle}$ için

$\overline{f(x)} = \overline{g(x)} \Leftrightarrow \overline{f(x)} \equiv \overline{g(x)} \left(\mathrm{mod}\left(x^{p^s}-1\right)\right)$

$\Leftrightarrow \left(x^{p^s}-1\right) \left| \overline{f(x)} - \overline{g(x)} \right.$

$\Leftrightarrow \overline{f(x)} - \overline{g(x)} = \left(x^{p^s}-1\right)\cdot h(x)$ olacak biçimde en az bir $h(x) \in R[x]$ vardır.

$\Leftrightarrow \overline{f(\gamma_0 \cdot x)} - \overline{g(\gamma_0 \cdot x)} = \left((\gamma_0 \cdot x)^{p^s}-1\right)\cdot h(\gamma_0 \cdot x)$ olacak biçimde en az bir $h(\gamma_0 \cdot x) \in R[x]$ vardır.

$\Leftrightarrow \overline{f(\gamma_0 \cdot x)} - \overline{g(\gamma_0 \cdot x)} = \left({\gamma_0}^{p^s} \cdot x^{p^s} - 1\right) \cdot h(\gamma_0 \cdot x)$ olacak biçimde en az bir $h(\gamma_0 \cdot x) \in R[x]$ vardır.

$\underset{\substack{\text{4.2.14.Önerme,} \\ 1=\gamma \cdot \gamma^{-1}}}{\Leftrightarrow} \overline{f(\gamma_0 \cdot x)} - \overline{g(\gamma_0 \cdot x)} = \left(\gamma^{-1} \cdot x^{p^s} - \gamma^{-1} \cdot \gamma\right) \cdot h(\gamma_0 \cdot x)$ olacak biçimde en az bir $h(\gamma_0 \cdot x) \in R[x]$ vardır.

$\Leftrightarrow \overline{f(\gamma_0 \cdot x)} - \overline{g(\gamma_0 \cdot x)} = \left(x^{p^s} - \gamma\right) \cdot \gamma^{-1} \cdot h(\gamma_0 \cdot x)$ olacak biçimde en az bir $h(\gamma_0 \cdot x) \in R[x]$ vardır.

$\Leftrightarrow \overline{f(\gamma_0 \cdot x)} - \overline{g(\gamma_0 \cdot x)} = \left(x^{p^s} - \gamma\right) \cdot k(x)$ olacak biçimde en az bir $k(x) \in R[x]$ vardır.

$\underset{\substack{k(x)=\gamma^{-1} \cdot h(\gamma_0 \cdot x) \text{ olacak} \\ \text{biçimde öyle bir} \\ k(x) \in R[x] \text{ vardır.}}}{\Leftrightarrow} \left(x^{p^s} - \gamma\right) \left| \left(\overline{f(\gamma_0 \cdot x)} - \overline{g(\gamma_0 \cdot x)}\right)\right.$

$\Leftrightarrow \overline{f(\gamma_0 \cdot x)} \equiv \overline{g(\gamma_0 \cdot x)} \left(\mathrm{mod}\left(x^{p^s} - \gamma\right)\right)$

$\Leftrightarrow \overline{f(\gamma_0 \cdot x)} = \overline{g(\gamma_0 \cdot x)}$

O halde ψ iyi tanımlı ve birebirdir.

Herhangi bir $\overline{f(x)} \in R[x] \Big/ \left\langle x^{p^s} - \gamma \right\rangle$ için

$\psi\left(\overline{f\left(\gamma_0^{-1} \cdot x\right)}\right) = \overline{f\left(\gamma_0 \cdot \left(\gamma_0^{-1} \cdot x\right)\right)} = \overline{f(x)} \in R[x] \Big/ \left\langle x^{p^s} - \gamma \right\rangle$ olacak biçimde en az bir

$\overline{f\left(\gamma_0^{-1} \cdot x\right)} \in R[x] \Big/ \left\langle x^{p^s} - 1 \right\rangle$ vardır.

O halde ψ örtendir.

ψ dönüşümünün tanımlanışından toplama ve çarpma işlemlerini koruduğunu göstermek kolaydır.

O halde ψ bir izomorfizmadır.□

4.2.4.Sonuç: C, R halkası üzerinde tanımlı p^s uzunluklu bir cyclic kod ise $\psi(C)$'nin R üzerinde p^s uzunluklu $\gamma-$constacyclic koddur. Bu ifadenin tersi de doğrudur. (Dinh, 2010) □

BÖLÜM 5

$\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ HALKASI ÜZERİNDEKİ CYCLIC VE $(1-u^2)-$ CONSTACYCLIC KODLAR

Bu bölümde $p=2$, $u^3=0$ olması durumunda ve $p=3$, $u^3=0$ ya da $u^3=1$ durumunda $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ halkası üzerindeki cyclic, $(1-u^2)-$constacyclic veya quasi-cyclic kodlar incelenmiştir. $u^3=0$ olması durumunda $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerinde yapılan çalışmalar $u^3=0$ durumunda $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ halkası üzerine genelleştirilmiştir.

5.1. $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2\,(u^3=0)$ Halkası Üzerindeki $(1-u^2)-$ Constacyclic Kodlar

Bu bölümde $R=\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2\,(u^3=0)$ halkasından $\mathbb{F}_2$ cismi üzerine bir Gray dönüşümü tanımlandı ve 3.2. veya 4.1. Bölümde tanımlanan σ, υ, μ, $\overline{\mu}$, σ^{p^k-1} dönüşümlerine benzer biçimde bu dönüşümler R halkası veya $\mathbb{F}_2^4$ vektör uzayı üzerinde tanımlanmıştır. 3.2. ve 4.1. Bölümdeki Nechaev permütasyonu kullanılanarak $\pi^{\otimes 2}$ permütasyonu tanımlanmıştır. 3.2. ve 4.1. Bölümdeki sonuçlar bu dönüşümler kullanılarak R halkası üzerine genelleştirilmiştir.

5.1. Bölüm boyunca $u^3 = 0$ durumunda $\mathbb{F}_2 + u\,\mathbb{F}_2 + u^2\,\mathbb{F}_2$ halkası R ile gösterilecektir. R halkası maksimal ideali $u \cdot R$ ve rezidü cismi $\mathbb{F}_2$ cismine izomorf olan sonlu bir zincir halkasıdır. (Çengellenmiş, 2009b)

σ ve υ dönüşümleri sırasıyla R^n üzerinde tanımlanan cyclic kaydırma ve $\left(1-u^2\right)-$constacyclic kaydırma dönüşümleri olsun. Bu durumda R üzerinde n uzunluğunda bir C kodu için $\upsilon(C) = C$ oluyorsa C koduna R üzerinde n uzunluğunda bir $\left(1-u^2\right)-$constacyclic kod denir. (Çengellenmiş, 2009b)

$\mathbb{F}_2^{\,4}$ vektör uzayı üzerindeki 2 indeksli quasi-cyclic kod dönüşümü

$$\sigma^{\otimes 2} : \mathbb{F}_2^{\,4\cdot n} \to \mathbb{F}_2^{\,4\cdot n}$$
$$a = \left(a_0, a_1, \ldots, a_{2\cdot n-2}, a_{2\cdot n-1}, a_{2\cdot n}, a_{2\cdot n+1}, \ldots, a_{4\cdot n-2}, a_{4\cdot n-1}\right) \mapsto \sigma^{\otimes 2}(a) = \left(a_{2\cdot n-1}, a_0, a_1, \ldots, a_{2\cdot n-2}, a_{4\cdot n-1}, a_{2\cdot n}, a_{2\cdot n+1}, \ldots, a_{4\cdot n-2}\right)$$

biçiminde tanımlanır. (Çengellenmiş, 2009b)

R halkası üzerindeki homogeneous ağırlık fonksiyonu aşağıdaki biçimde tanımlanır:

5.1.1.Tanım:

$$w_{\text{hom}} : R \to \{0,2,4\} \subset \mathbb{Z}$$
$$r \mapsto w_{\text{hom}}(r) = \begin{cases} 2; & r \in R \setminus R \cdot u^2 \text{ ise} \\ 4; & r \in R \cdot u^2 \setminus \{0\} \text{ ise} \\ 0; & \text{diğer durumlarda} \end{cases} = \begin{cases} 2; & r \in \left\{1, u, 1+u, 1+u^2, u+u^2, 1+u+u^2\right\} \text{ ise} \\ 4; & r = u^2 \text{ ise} \\ 0; & r = 0 \text{ ise} \end{cases}$$

biçiminde tanımlanan w_{hom} fonksiyonuna homogenous ağırlık fonksiyonu herhangi bir $r \in R$ için $w_{\text{hom}}(r)$ değerine r elemanının homogenous ağırlığı denir. (Greferath & Schmidt, 1999) □

R^n'nin herhangi bir $c = \left(c_0, c_1, \ldots, c_{n-1}\right)$ elemanının ağırlığı $w_{\text{hom}}(c) = \sum_{i=0}^{n-1} w_{\text{hom}}(c_i)$ biçimindedir. Ayrıca R^n'nin herhangi iki x, y elemanı arasındaki homogeneous uzaklığı $d_{\text{hom}}(x,y) = w_{\text{hom}}(x-y)$ olarak tanımlanır. (Çengellenmiş, 2009b) □

Önceki bölümlerde tanımlandığı gibi bu bölüm boyunca da w_H Hamming ağırlık fonksiyonunu, d_H ise Hamming uzaklığını gösterecektir.

5.1.1.Önerme: R halkası üzerinde homogeneous, $\mathbb{F}_2{}^4$ vektör uzayı üzerinde Hamming uzaklığı verilsin. Bu durumda;

$$\Phi : R \to \mathbb{F}_2{}^4$$
$$x = \left(a + u\,b + u^2\,c\right) \mapsto \Phi\left(x\right) = \left(c, c+a, c+b, c+b+a\right)$$

biçiminde tanımlanan Φ dönüşümü bir izometridir. (Çengellenmiş, 2009b)

Kanıt: Herhangi iki $x = a_1 + u\,b_1 + u^2\,c_1, y = a_2 + u\,b_2 + u^2\,c_2 \in R$ için $d_{\text{hom}}\left(x,y\right) = d_H\left(\Phi\left(x\right), \Phi\left(y\right)\right)$ olduğu sekiz adımda gösterilecektir.

I) $a_1 \neq a_2, b_1 = b_2, c_1 = c_2$

$$d_{\text{hom}}\left(x,y\right) = w_{\text{hom}}\left(x-y\right) = w_{\text{hom}}\left(\left(a_1-a_2\right) + u\left(b_1-b_2\right) + u^2\left(c_1-c_2\right)\right)$$

$$\underset{\substack{a_1\neq a_2\\ b_1=b_2\\ c_1=c_2}}{=} w_{\text{hom}}\left(a_1-a_2\right) \underset{\substack{w_{\text{hom}}\\ \text{tanımı}}}{=} 2 \text{ olur.}$$

$$d_H\left(\Phi\left(x\right), \Phi\left(y\right)\right) = w_H\left(\Phi\left(x\right) - \Phi\left(y\right)\right)$$

$$= w_H\left(c_1-c_2, \left(c_1-c_2\right)+\left(a_1-a_2\right), \left(c_1-c_2\right)+\left(b_1-b_2\right), \left(c_1-c_2\right)+\left(b_1-b_2\right)+\left(a_1-a_2\right)\right)$$

$$\underset{\substack{a_1\neq a_2\\ b_1=b_2\\ c_1=c_2}}{=} w_H\left(0, a_1-a_2, 0, a_1-a_2\right) = 2$$

O halde $a_1 \neq a_2, b_1 = b_2, c_1 = c_2$ için; $d_{\text{hom}}\left(x,y\right) = d_H\left(\Phi\left(x\right), \Phi\left(y\right)\right)$'dir.

II) $a_1 \neq a_2, b_1 \neq b_2, c_1 = c_2$

$$d_{\text{hom}}\left(x,y\right) = w_{\text{hom}}\left(x-y\right) = w_{\text{hom}}\left(\left(a_1-a_2\right) + u\left(b_1-b_2\right) + u^2\left(c_1-c_2\right)\right)$$

$$\underset{\substack{a_1\neq a_2\\ b_1\neq b_2\\ c_1=c_2}}{=} w_{\text{hom}}\left(\left(a_1-a_2\right) + u\left(b_1-b_2\right)\right) \underset{\substack{w_{\text{hom}}\\ \text{tanımı}}}{=} 2 \text{ olur.}$$

$$d_H\left(\Phi\left(x\right), \Phi\left(y\right)\right) = w_H\left(\Phi\left(x\right) - \Phi\left(y\right)\right)$$

$$= w_H\left(c_1-c_2, \left(c_1-c_2\right)+\left(a_1-a_2\right), \left(c_1-c_2\right)+\left(b_1-b_2\right), \left(c_1-c_2\right)+\left(b_1-b_2\right)+\left(a_1-a_2\right)\right)$$

$$\underset{\substack{a_1\neq a_2\\ b_1\neq b_2\\ c_1=c_2}}{=} w_H\left(0, a_1-a_2, b_1-b_2, \left(b_1-b_2\right)+\left(a_1-a_2\right)\right) \underset{\substack{b_1-b_2=1\in\mathbb{F}_2\\ a_1-a_2=1\in\mathbb{F}_2}}{=} w_H\left(0, a_1-a_2, b_1-b_2, 0\right) = 2$$

O halde $a_1 \neq a_2, b_1 \neq b_2, c_1 = c_2$ için; $d_{\text{hom}}(x,y) = d_H\left(\Phi(x), \Phi(y)\right)$'dir.

III) $a_1 \neq a_2, b_1 = b_2, c_1 \neq c_2$

$$d_{\text{hom}}(x,y) = w_{\text{hom}}(x-y) = w_{\text{hom}}\left((a_1-a_2)+u(b_1-b_2)+u^2(c_1-c_2)\right)$$

$$\underset{\substack{a_1\neq a_2\\ b_1=b_2\\ c_1\neq c_2}}{=} w_{\text{hom}}\left((a_1-a_2)+u^2(c_1-c_2)\right) \underset{\substack{w_{\text{hom}}\\ \text{tanımı}}}{=} 2 \text{ olur.}$$

$$d_H\left(\Phi(x), \Phi(y)\right) = w_H\left(\Phi(x)-\Phi(y)\right)$$

$$= w_H\left(c_1-c_2, (c_1-c_2)+(a_1-a_2), (c_1-c_2)+(b_1-b_2), (c_1-c_2)+(b_1-b_2)+(a_1-a_2)\right)$$

$$\underset{\substack{a_1\neq a_2\\ b_1=b_2\\ c_1\neq c_2}}{=} w_H\left(c_1-c_2, (c_1-c_2)+(a_1-a_2), c_1-c_2, (c_1-c_2)+(a_1-a_2)\right)$$

$$\underset{\substack{c_1-c_2=1\in\mathbb{F}_2\\ a_1-a_2=1\in\mathbb{F}_2}}{=} w_H(c_1-c_2, 0, c_1-c_2, 0) = 2$$

O halde $a_1 \neq a_2, b_1 = b_2, c_1 \neq c_2$ için; $d_{\text{hom}}(x,y) = d_H\left(\Phi(x), \Phi(y)\right)$'dir.

IV) $a_1 \neq a_2, b_1 \neq b_2, c_1 \neq c_2$

$$d_{\text{hom}}(x,y) = w_{\text{hom}}(x-y) = w_{\text{hom}}\left((a_1-a_2)+u(b_1-b_2)+u^2(c_1-c_2)\right) \underset{\substack{a_1\neq a_2\\ b_1\neq b_2\\ c_1\neq c_2\\ w_{\text{hom}}\text{ tanımı}}}{=} 2$$

$$d_H\left(\Phi(x), \Phi(y)\right) = w_H\left(\Phi(x)-\Phi(y)\right)$$

$$= w_H\left(c_1-c_2, (c_1-c_2)+(a_1-a_2), (c_1-c_2)+(b_1-b_2), (c_1-c_2)+(b_1-b_2)+(a_1-a_2)\right)$$

$$\underset{\substack{a_1\neq a_2\\ b_1\neq b_2\\ c_1\neq c_2\\ (c_1-c_2)+(a_1-a_2)=0\in\mathbb{F}_2\\ (c_1-c_2)+(b_1-b_2)=0\in\mathbb{F}_2}}{=} w_H(c_1-c_2, 0, 0, a_1-a_2) = 2$$

O halde $a_1 \neq a_2, b_1 \neq b_2, c_1 \neq c_2$ için; $d_{\text{hom}}(x,y) = d_H\left(\Phi(x), \Phi(y)\right)$'dir.

V) $a_1 = a_2, b_1 = b_2, c_1 = c_2$

$$d_{\text{hom}}(x,y) = w_{\text{hom}}(x-y) = w_{\text{hom}}\left((a_1-a_2)+u(b_1-b_2)+u^2(c_1-c_2)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1=b_2\\ c_1=c_2}}{=} w_{\text{hom}}(0) \underset{\substack{w_{\text{hom}}\\ \text{tanımı}}}{=} 0 \text{ olur.}$$

$$d_H\left(\Phi(x), \Phi(y)\right) = w_H\left(\Phi(x)-\Phi(y)\right)$$

$$= w_H\left(c_1-c_2, (c_1-c_2)+(a_1-a_2), (c_1-c_2)+(b_1-b_2), (c_1-c_2)+(b_1-b_2)+(a_1-a_2)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1=b_2\\ c_1=c_2}}{=} w_H\left(0,0,0,0\right)=0$$

O halde $a_1=a_2, b_1=b_2, c_1=c_2$ için; $d_{\text{hom}}\left(x,y\right)=d_H\left(\Phi\left(x\right),\Phi\left(y\right)\right)$'dir.

VI) $a_1=a_2, b_1=b_2, c_1\neq c_2$

$$d_{\text{hom}}\left(x,y\right)=w_{\text{hom}}\left(x-y\right)=w_{\text{hom}}\left(\left(a_1-a_2\right)+u\left(b_1-b_2\right)+u^2\left(c_1-c_2\right)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1=b_2\\ c_1\neq c_2}}{=} w_{\text{hom}}\left(u^2\cdot\left(c_1-c_2\right)\right) \underset{\substack{w_{\text{hom}}\\ \text{tanımı}}}{=} 4 \text{ olur.}$$

$$d_H\left(\Phi\left(x\right),\Phi\left(y\right)\right)=w_H\left(\Phi\left(x\right)-\Phi\left(y\right)\right)$$

$$=w_H\left(c_1-c_2,\left(c_1-c_2\right)+\left(a_1-a_2\right),\left(c_1-c_2\right)+\left(b_1-b_2\right),\left(c_1-c_2\right)+\left(b_1-b_2\right)+\left(a_1-a_2\right)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1=b_2\\ c_1\neq c_2}}{=} w_H\left(c_1-c_2,c_1-c_2,c_1-c_2,c_1-c_2\right)=4$$

O halde $a_1=a_2, b_1=b_2, c_1\neq c_2$ için; $d_{\text{hom}}\left(x,y\right)=d_H\left(\Phi\left(x\right),\Phi\left(y\right)\right)$'dir.

VII) $a_1=a_2, b_1\neq b_2, c_1=c_2$

$$d_{\text{hom}}\left(x,y\right)=w_{\text{hom}}\left(x-y\right)=w_{\text{hom}}\left(\left(a_1-a_2\right)+u\left(b_1-b_2\right)+u^2\left(c_1-c_2\right)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1\neq b_2\\ c_1=c_2}}{=} w_{\text{hom}}\left(u\cdot\left(b_1-b_2\right)\right) \underset{\substack{w_{\text{hom}}\\ \text{tanımı}}}{=} 2 \text{ olur.}$$

$$d_H\left(\Phi\left(x\right),\Phi\left(y\right)\right)=w_H\left(\Phi\left(x\right)-\Phi\left(y\right)\right)$$

$$=w_H\left(c_1-c_2,\left(c_1-c_2\right)+\left(a_1-a_2\right),\left(c_1-c_2\right)+\left(b_1-b_2\right),\left(c_1-c_2\right)+\left(b_1-b_2\right)+\left(a_1-a_2\right)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1\neq b_2\\ c_1=c_2}}{=} w_H\left(0,0,b_1-b_2,b_1-b_2\right)=2$$

O halde $a_1=a_2, b_1\neq b_2, c_1=c_2$ için; $d_{\text{hom}}\left(x,y\right)=d_H\left(\Phi\left(x\right),\Phi\left(y\right)\right)$'dir.

VIII) $a_1=a_2, b_1\neq b_2, c_1\neq c_2$

$$d_{\text{hom}}\left(x,y\right)=w_{\text{hom}}\left(x-y\right)=w_{\text{hom}}\left(\left(a_1-a_2\right)+u\left(b_1-b_2\right)+u^2\left(c_1-c_2\right)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1\neq b_2\\ c_1\neq c_2}}{=} w_{\text{hom}}\left(u\left(b_1-b_2\right)+u^2\left(c_1-c_2\right)\right) \underset{\substack{w_{\text{hom}}\\ \text{tanımı}}}{=} 2 \text{ olur.}$$

$$d_H\left(\Phi\left(x\right),\Phi\left(y\right)\right)=w_H\left(\Phi\left(x\right)-\Phi\left(y\right)\right)$$

$$= w_H\left(c_1-c_2,(c_1-c_2)+(a_1-a_2),(c_1-c_2)+(b_1-b_2),(c_1-c_2)+(b_1-b_2)+(a_1-a_2)\right)$$

$$\underset{\substack{a_1=a_2\\ b_1\neq b_2\\ c_1\neq c_2}}{=} w_H\left(c_1-c_2,c_1-c_2,(c_1-c_2)+(b_1-b_2),(c_1-c_2)+(b_1-b_2)\right)$$

$$= w_H\left(c_1-c_2,c_1-c_2,0,0\right)$$

$$= 2$$

O halde $a_1=a_2, b_1\neq b_2, c_1\neq c_2$ için; $d_{\text{hom}}(x,y)=d_H\left(\Phi(x),\Phi(y)\right)$'dir.

O halde Φ bir izometridir. □

5.1.1.Not: Φ dönüşümü R^n üzerine

$$\Phi: R^n \to \mathbb{F}_2^{4\cdot n}$$

$$r=\left(a_0+ub_0+u^2c_0, a_1+ub_1+u^2c_1,\ldots,a_{n-1}+ub_{n-1}+u^2c_{n-1}\right)\mapsto \Phi(r)=\left(c_0,c_1,\ldots,c_{n-1},c_0+a_0,c_1+a_1,\ldots,c_{n-1}+a_{n-1},\right.$$
$$c_0+b_0,c_1+b_1,\ldots,c_{n-1}+b_{n-1},$$
$$\left.c_0+b_0+a_0,c_1+b_1+a_1,\ldots,c_{n-1}+b_{n-1}+a_{n-1}\right)$$

biçiminde genelleştirilir. (Çengellenmiş, 2009b)

4.1.2.Önerme'ye benzer olarak aşağıdaki 5.1.2.Önerme verilir.

5.1.2.Önerme: $\Phi\circ\upsilon=\sigma^{\otimes 2}\circ\Phi$ (Çengellenmiş, 2009b)

Kanıt: Φ,υ ve $\sigma^{\otimes 2}$ dönüşümleri ve

$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_2^{4\cdot n} \\ \upsilon\downarrow & \circlearrowright & \downarrow\sigma^{\otimes 2} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_2^{4\cdot n} \end{array}$$

diyagramı düşünülerek 4.1.2.Önerme'nin kanıtına benzer biçimde ispatlanır.

5.1.1.Sonuç: C, R halkası üzerinde tanımlı n uzunluğunda bir kod olsun. Eğer C $\left(1-u^2\right)-$constacyclic kod ise $\Phi(C)$ kodu $\mathbb{F}_2$ üzerinde $4\cdot n$ uzunluğunda 2 indeksli bir quasi-cyclic koddur. Bu ifadenin tersi de doğrudur.

Kanıt: $\Rightarrow$: C, R halkası üzerinde tanımlı n uzunluğunda bir $\left(1-u^2\right)-$ constacyclic kod

$$\underset{\substack{5.1.2.\\ \text{Önerme}}}{\Rightarrow} \sigma^{\otimes 2}\left(\Phi(C)\right)=\Phi\left(\upsilon(C)\right)$$

$\underset{\nu \text{ tanımı}}{\Rightarrow} \sigma^{\otimes 2}\left(\Phi(C)\right)=\Phi(C)$

$\underset{\sigma^{\otimes 2} \text{ tanımı}}{\Rightarrow} \Phi(C)$ $\mathbb{F}_2$ cismi üzerinde tanımlı $4\cdot n$ uzunluğunda 2 indeksli bir quasi-cyclic koddur.

$\Leftarrow: \Phi(C)$ $\mathbb{F}_2$ cismi üzerinde tanımlı $4\cdot n$ uzunluğunda 2 indeksli bir quasi-cyclic kod

$\underset{\substack{5.1.2.\\ \text{Önerme}}}{\Rightarrow} \Phi\left(\upsilon(C)\right)=\sigma^{\otimes 2}\left(\Phi(C)\right)$

$\underset{\substack{\text{Varsayım ve}\\ \sigma^{\otimes 2} \text{ tanımı}}}{\Rightarrow} \Phi\left(\upsilon(C)\right)=\Phi(C)$

$\underset{\Phi \text{ birebir}}{\Rightarrow} \upsilon(C)=C$

$\underset{\nu \text{ tanımı}}{\Rightarrow} C$ R üzerinde n uzunluğunda bir $\left(1-u^2\right)-$constacyclic koddur.□

n tek ise $\left(1-u^2\right)^n=1-u^2$, n çift ise $\left(1-u^2\right)^n=1$'dir. (Çengellenmiş, 2009b)

5.1.2.Not: 4.1.3. ve 3.2.5. Önermelerde verildiğine benzer biçimde μ dönüşümü

$$\mu: R[x]\Big/\left\langle x^n-1\right\rangle \to R[x]\Big/\left\langle x^n-\left(1-u^2\right)\right\rangle$$
$$\overline{c(x)} \mapsto \mu\left(\overline{c(x)}\right)=\overline{c\left(\left(1-u^2\right)\cdot x\right)}$$

biçiminde tanımlanır. n sayısının tek olması durumunda μ bir izomorfizmadır. □ (Çengellenmiş, 2009b)

3.2.6.Teorem ve 4.1.4.Önermeye benzer biçimde aşağıdaki 5.1.3.Önerme verilir:

5.1.3.Önerme:

$$\bar{\mu}: R^n \to R^n$$
$$r=\left(r_0, r_1, r_2 \ldots, r_{n-1}\right) \mapsto \bar{\mu}(r)=\left(r_0,\left(1-u^2\right)\cdot r_1,\left(1-u^2\right)^2\cdot r_2 \ldots,\left(1-u^2\right)^{n-1}\cdot r_{n-1}\right)$$

permütasyonu verilsin. Bir C kümesi R üzerinde n uzunluklu bir lineer cyclic kod ise $\bar{\mu}(C)$ kümesi R üzerinde n uzunluklu bir $(1-u^2)-$constacyclic koddur. Bu ifadenin tersi de doğrudur. (Çengellenmiş, 2009b) □

5.1.4.Önerme: n tek bir doğal sayı, π 3.2.6.Tanım'da tanımlanan Nechaev Permütasyonu ve

$$\pi^{\otimes 2}:\mathbb{F}_2^{4\cdot n}\to\mathbb{F}_2^{4\cdot n}$$

$$c=(c_0,c_1,\ldots,c_{2\cdot n-1},c_{2\cdot n},c_{2\cdot n+1},\ldots,c_{4\cdot n-1})\mapsto\pi^{\otimes 2}(c)=\left(\pi(c_0,c_1,\ldots,c_{2\cdot n-1})\middle|\pi(c_{2\cdot n},c_{2\cdot n+1},\ldots,c_{4\cdot n-1})\right)$$

olmak üzere $\Phi\circ\bar{\mu}=\pi^{\otimes 2}\circ\Phi$ eşitliği sağlanır. (Çengellenmiş, 2009b)

Kanıt:

$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_2^{4\cdot n} \\ \bar{\mu}\downarrow & \circlearrowright & \downarrow\pi^{\otimes 2} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_2^{4\cdot n} \end{array}$$

Herhangi bir $r=(a_0+ub_0+u^2c_0,a_1+ub_1+u^2c_1,\ldots,a_{n-1}+ub_{n-1}+u^2c_{n-1})\in R^n$ için

$$\bar{\mu}(r)=(a_0+ub_0+u^2c_0,(1-u^2)(a_1+ub_1+u^2c_1),(1-u^2)^2(a_2+ub_2+u^2c_2),\ldots,$$
$$(1-u^2)^{n-2}(a_{n-2}+ub_{n-2}+u^2c_{n-2}),(1-u^2)^{n-1}(a_{n-1}+ub_{n-1}+u^2c_{n-1}))$$

$$=(a_0+ub_0+u^2c_0,(1-u^2)(a_1+ub_1+u^2c_1),(a_1+ub_1+u^2c_1),\ldots,$$
$$(1-u^2)(a_{n-2}+ub_{n-2}+u^2c_{n-2}),(a_{n-1}+ub_{n-1}+u^2c_{n-1}))$$

$$=(a_0+ub_0+u^2c_0,a_1+ub_1+u^2(c_1-a_1),a_2+ub_2+u^2c_2,\ldots,$$
$$a_{n-2}+ub_{n-2}+u^2(c_{n-2}-a_{n-2}),a_{n-1}+ub_{n-1}+u^2c_{n-1})$$

$$\Rightarrow\Phi(\bar{\mu}(r))=(c_0,c_1-a_1,c_2,c_3-a_3,\ldots,c_{n-2}-a_{n-2},c_{n-1},$$
$$c_0+a_0,c_1-a_1+a_1,c_2+a_2,c_3-a_3+a_3,\ldots,c_{n-2}-a_{n-2}+a_{n-2},c_{n-1}+a_{n-1},$$
$$c_0+b_0,c_1-a_1+b_1,c_2+b_2,c_3-a_3+b_3,\ldots,c_{n-2}-a_{n-2}+b_{n-2},c_{n-1}+b_{n-1},$$
$$c_0+b_0+a_0,c_1-a_1+b_1+a_1,c_2+b_2+a_2,c_3-a_3+b_3+a_3,\ldots,c_{n-2}-a_{n-2}+b_{n-2}+a_{n-2},c_{n-1}+b_{n-1}+a_{n-1})$$

$$=(c_0,c_1+a_1,c_2,c_3+a_3,\ldots,c_{n-2}+a_{n-2},c_{n-1},$$
$$c_0+a_0,c_1,c_2+a_2,c_3,\ldots,c_{n-2},c_{n-1}+a_{n-1},$$
$$c_0+b_0,c_1-a_1+b_1,c_2+b_2,c_3-a_3+b_3,\ldots,c_{n-2}-a_{n-2}+b_{n-2},c_{n-1}+b_{n-1},$$
$$c_0+b_0+a_0,c_1+b_1,c_2+b_2+a_2,c_3+b_3,\ldots,c_{n-2}+b_{n-2},c_{n-1}+b_{n-1}+a_{n-1})\cdots(i)$$

Diğer taraftan;

$$\Phi(r)=(c_0,c_1,c_2,\ldots,c_{n-1},c_0+a_0,c_1+a_1,c_2+a_2,\ldots,c_{n-1}+a_{n-1},$$
$$c_0+b_0,c_1+b_1,c_2+b_2,\ldots,c_{n-1}+b_{n-1},c_0+b_0+a_0,c_1+b_1+a_1,c_2+b_2+a_2,\ldots,c_{n-1}+b_{n-1}+a_{n-1})$$

$$\Rightarrow \pi^{\otimes 2}(\Phi(r))=(\pi(c_0,c_1,c_2,\ldots,c_{n-1},c_0+a_0,c_1+a_1,c_2+a_2,\ldots,c_{n-1}+a_{n-1})|\pi(c_0+b_0,c_1+b_1,c_2+b_2,\ldots,$$
$$c_{n-1}+b_{n-1},c_0+b_0+a_0,c_1+b_1+a_1,c_2+b_2+a_2,\ldots,c_{n-1}+b_{n-1}+a_{n-1}))$$

$$=(c_0,c_1+a_1,c_2,c_3+a_3,\ldots,c_{n-2}+a_{n-2},c_{n-1},$$
$$c_0+a_0,c_1,c_2+a_2,c_3,\ldots,c_{n-2},c_{n-1}+a_{n-1},$$
$$c_0+b_0,c_1-a_1+b_1,c_2+b_2,c_3-a_3+b_3,\ldots,c_{n-2}-a_{n-2}+b_{n-2},c_{n-1}+b_{n-1},$$
$$c_0+b_0+a_0,c_1+b_1,c_2+b_2+a_2,c_3+b_3,\ldots,c_{n-2}+b_{n-2},c_{n-1}+b_{n-1}+a_{n-1})\cdots(ii)$$

O halde i ve ii'den $\Phi\circ\bar{\mu}=\pi^{\otimes 2}\circ\Phi$'dir.

5.1.2.Sonuç: n tek doğal sayı olmak üzere; C, R üzerinde n uzunluğunda bir lineer cyclic kod ise $\Phi(C)$ $\mathbb{F}_2$ cismi üzerinde tanımlı $4\cdot n$ uzunluğunda 2 indeksli bir quasi-cyclic koda denktir. (Çengellenmiş, 2009b)

Kanıt: n tek doğal sayı ve C, R halkası üzerinde tanımlı n uzunluğunda bir lineer cyclic kod

$\underset{\text{5.1.3.Önerme}}{\Rightarrow}$ $\bar{\mu}(C)$ bir $(1-u^2)-$constacyclic koddur.

$\underset{\text{5.1.1.Sonuç}}{\Rightarrow}$ $\Phi(\bar{\mu}(C))$ $\mathbb{F}_2$ cismi üzerinde tanımlı $4\cdot n$ uzunluğunda 2 indeksli bir quasi-cyclic koddur.

$\underset{\text{5.1.4.Önerme}}{\Rightarrow}$ $\pi^{\otimes 2}(\Phi(C))$ $\mathbb{F}_2$ cismi üzerinde tanımlı $4\cdot n$ uzunluğunda 2 indeksli bir quasi-cyclic koddur.

$\mathbb{F}_2$ cismi üzerinde tanımlı $4\cdot n$ uzunluğunda 2 indeksli bir quasi-cyclic koda denktir.

5.2. $\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$ ($u^3=0$ ya da $u^3=1$) Halkaları Üzerindeki Cyclic Kodlar

Bu bölümde $u^3=1$ koşuluyla halka olan $R=\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$ halkası üzerinden $\mathbb{F}_3{}^3$ vektör uzayı üzerine 5.1. Bölümde verilen Gray dönüşümünden farklı bir Gray dönüşümü tanımlanmıştır. Tanımlanan bu Gray dönüşümüyle R halkası üzerinde n uzunluklu bir cyclic kodun Gray dönüşümü altındaki görüntüsünün indexi 3 olan bir

quasi-cyclic kod olduğu gösterilmiştir. $u^3 = 0$ koşuluyla halka olan $S = \mathbb{F}_3 + u\,\mathbb{F}_3 + u^2\,\mathbb{F}_3$ halkasıyla R halkası arasında bir izomorfizma tanımlanmıştır. Ayrıca S halkası üzerinde n uzunluklu bir lineer koda permütasyon denk bir kod için üreteç matrisi verilmiştir. Daha sonra R ve S halkaları üzerindeki izomorfizma kullanılarak R halkası üzerinde n uzunluklu bir lineer koda permütasyon denk bir kod için üreteç matrisi verilmiştir.

R ve S halkaları karakteristiği 3 olan sonlu zincir halkalarıdır. Ayrıca R halkasının idealleri $\langle 0\rangle = \left\langle (u+2)^3 \right\rangle \subsetneq \left\langle (u+2)^2 \right\rangle \subsetneq \langle u+2\rangle \subsetneq \langle 1\rangle = R$ biçimindedir. $u+2$ R halkasının nilpotentlik derecesi 3 olan bir nilpotent elemanıdır. R halkasının bütün tersinir elemanlarının kümesi $R \setminus \langle u+2\rangle$ kümesidir. (Xiong, Yun, Xing & Xu, 2013)

5.2.1.Önerme:

$$f : R \to S$$
$$a+bu+cu^2 \mapsto f\left(a+bu+cu^2\right) = (a+b+c)+(b+2\cdot c)u+cu^2$$

biçiminde tanımlanan dönüşüm bir izomorfizmadır. (Xiong vd., 2013)

Kanıt: f fonksiyonunun tanımından toplama ve çarpma işlemlerini koruduğunu ve de birebir olduğunu göstermek kolaydır.

Herhangi bir $x+yu+zu^2 \in S$ için

$f\left((x+z-y)+(y-2\cdot z)u+zu^2\right) = (x+z-y+y-2\cdot z+z)+(y-2\cdot z+2\cdot z)u+zu^2$

$= x+yu+zu^2$ olacak biçimde en az bir $(x+z-y)+(y-2\cdot z)u+zu^2 \in R$ vardır.

O halde f örtendir.

O halde f bir izomorfizmadır.

5.2.2.Önerme: S halkası üzerinde tanımlı n uzunluğunda herhangi bir C lineer kodu, I_{k_1}, I_{k_2}, I_{k_3} sırasıyla k_1, k_2 ve k_3 mertebeli birim matrisler, $k = k_1 + k_2 + k_3$, A_{11}, A_{12}, A_{22} ve $i = 1,2,3$ için B_{i1}, B_{i2}, B_{i3} $\mathbb{F}_3$ cismi üzerinde matrisler ve $i = 1,2,3$ için $A_i = B_{i1} + u\cdot B_{i2} + u^2 \cdot B_{i3}$ olmak üzere üreteç matrisi

$$G=\begin{pmatrix} I_{k_1} & A_1 & A_2 & A_3 \\ 0 & u\cdot I_{k_2} & u\cdot A_{11} & u\cdot A_{12} \\ 0 & 0 & u^2\cdot I_{k_3} & u^2\cdot A_{22} \end{pmatrix}$$

biçiminde olan bir koda permütasyon denktir. (Xiong vd., 2013)

Kanıt: $G_1=\left(g_{ij}\right)_{k\times n}$ matrisi S halkası üzerinde tanımlı n uzunluklu C lineer kodunun bir üreteç matrisi olsun. G_1 matrisi içerisinde tersinir bir eleman varsa öncelikle o elemanın çarpmaya göre ters elemanıyla matris çarpılır ve 1 bulunur. Daha sonra satır ve sütunlar yer değiştirilerek 1, 1. Satırın 1. elemanı yapılır. 1. Sütunun 0 olmayan diğer elemanları için 1'in yer aldığı 1. satır 0 yapılmak istenen elemanın bulunduğu satırda yer alan ilk elemanın toplamaya göre ters elemanıyla çarpılır ve ilk elemanı 0 yapılmak istenilen satıra eklenir. Bu işlem ilk elemanı 0 olmayan tüm satırlar için tekrarlanır. Sonuç olarak G_1 matrisi birinci sütunu;

$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ olan bir matrise çevrilmiş olur. Bu matris G_2 ile gösterilsin. G_2 matrisinde tersinir eleman varsa G_1 matrisine uygulanan satır sütun işlemleri benzer biçimde G_2 matrisine uygulandığında ikinci sütunu;

$\begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ olan G_3 matrisi elde edilir. Benzer yöntem k_1 adım tekrarlandığında; I_{k_1} ; k_1 mertebeli birim matris, M_1, M_2; S halkası üzerinde matrisler olmak üzere; $G_{k_1+1}=\begin{pmatrix} I_{k_1} & M_1 \\ 0 & M_2 \end{pmatrix}$ matrisi elde edilir. Burada M_2 matrisinde tersinir eleman olmadığından $u\cdot S$ üzerinde bir matristir. S halkası üzerinde $M_2=u\cdot\tilde{M}_2$ olacak şekilde $\tilde{M}_2$ matrisi vardır. G_1 matrisine yapılan satır sütun işlemleri $\tilde{M}_2$ matrisi için G_{k_1+1} matrisine uygulandığında k_2 adım sonra; A_1, M_3; S, M_4; $u\cdot S$, M_5; $u^2\cdot S$ halkası üzerinde matrisler ve I_{k_2} ; k_2 mertebeli birim matris olmak üzere;

$G_{k_1+k_2+1} = \begin{pmatrix} I_{k_1} & A_1 & M_3 \\ 0 & u \cdot I_{k_2} & M_4 \\ 0 & 0 & M_5 \end{pmatrix}$ matrisi elde edilir. S halkası üzerinde $M_5 = u^2 \cdot \tilde{M}_5$ olacak şekilde $\tilde{M}_5$ matrisi vardır. G_1 matrisine yapılan satır sütun işlemleri $\tilde{M}_5$ matrisi için $G_{k_1+k_2+1}$ matrisine uygulandığında k_3 adım sonra; I_{k_1}, I_{k_2}, I_{k_3} sırasıyla k_1, k_2 ve k_3 mertebeli birim matrisler, A_{11}, A_{12}, A_{22} ve $i = 1,2,3$ için B_{i1}, B_{i2}, B_{i3}; $\mathbb{F}_3$ cismi üzerinde matrisler ve $i = 1,2,3$ için; $A_i = B_{i1} + u \cdot B_{i2} + u^2 \cdot B_{i3}$ olmak üzere

$G = \begin{pmatrix} I_{k_1} & A_1 & A_2 & A_3 \\ 0 & u \cdot I_{k_2} & u \cdot A_{11} & u \cdot A_{12} \\ 0 & 0 & u^2 \cdot I_{k_5} & u^2 \cdot A_{22} \end{pmatrix}_{k \times n}$ matrisi elde edilir. □

5.2.1. ve 5.2.2.Önermelerden 5.2.1.Sonuç verilir.

5.2.1.Sonuç: R halkası üzerinde tanımlı n uzunluğunda herhangi bir C lineer kodu, I_{k_1}, I_{k_2}, I_{k_3} sırasıyla k_1, k_2 ve k_3 mertebeli birim matrisler, $k = k_1 + k_2 + k_3$, A_{11}, A_{12}, A_{22} ve $i = 1,2,3$ için B_{i1}, B_{i2}, B_{i3} $\mathbb{F}_3$ cismi üzerinde matrisler ve $i = 1,2,3$ için $A_i = B_{i1} + u \cdot B_{i2} + u^2 \cdot B_{i3}$ olmak üzere üreteç matrisi

$G = \begin{pmatrix} I_{k_1} & A_1 & A_2 & A_3 \\ 0 & (u+2) \cdot I_{k_2} & (u+2) \cdot A_{11} & (u+2) \cdot A_{12} \\ 0 & 0 & (u+2)^2 \cdot I_{k_3} & (u+2)^2 \cdot A_{22} \end{pmatrix}$ olan bir koda permütasyon denktir.

(Xiong vd., 2013)

5.2.3.Önerme:

$$\Phi : R \to \mathbb{F}_3^3$$
$$a + ub + u^2 c \mapsto \Phi(a + ub + u^2 c) = (a + b + c, b + 2 \cdot c, c)$$

biçiminde tanımlanan Φ dönüşümü bir halka homomorfizmasıdır. (Xiong, 2013)

5.2.1.Tanım: w_H Hamming ağırlık fonksiyonu olmak üzere, R halkasının herhangi bir x elemanının Lee ağırlığı $w_L(x) = w_H(\Phi(x))$ biçiminde tanımlanır. □

5.2.1.Tanımda 3.2. Bölümde $u^2 = 0$ koşuluyla halka olan $R_0 = \mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde tanımlanan Φ Gray dönüşümü düşünüldüğünde 3.2.2.Tanım elde edilir. Gerçekten de;

$$w_H\left(\Phi(1)\right) \underset{\Phi(1)=(0,1)}{=} 1 \underset{\text{3.2.2.Tanım}}{=} w_L(1),$$

$$w_H\left(\Phi(0)\right) \underset{\Phi(0)=(0,0)}{=} 0 \underset{\text{3.2.2.Tanım}}{=} w_L(0),$$

$$w_H\left(\Phi(u)\right) \underset{\Phi(u)=(1,1)}{=} 2 \underset{\text{3.2.2.Tanım}}{=} w_L(u),$$

$$w_H\left(\Phi(1+u)\right) \underset{\Phi(1+u)=(1,0)}{=} 1 \underset{\text{3.2.2.Tanım}}{=} w_L(1+u)$$ 'dir.

5.2.4.Önerme: R halkası üzerinde Lee uzaklığı, $\mathbb{F}_3$ cismi üzerinde Hamming uzaklığı düşünüldüğünde 5.2.3.Önerme'de tanımlanan Φ dönüşümü bir izometridir. (Xiong vd., 2013)

Kanıt: Her $x, y \in R$ için;

$$d_L(x,y) = w_L(x-y) \underset{\text{5.2.1.Tanım}}{=} w_H\left(\Phi(x-y)\right)$$

$$\underset{\substack{\text{5.2.3.Önerme}\\ \Phi \text{ bir homomorfizma}}}{=} w_H\left(\Phi(x)-\Phi(y)\right) = d_H\left(\Phi(x),\Phi(y)\right)$$'dir.

O halde Φ bir izometridir. □

3.1.1.Tanım'da $\mathbb{F}_2$ cismi üzerinde tanımlanan indexi s olan quasi-cyclic kod dönüşümü $\sigma^{\otimes s}$ benzer biçimde $\mathbb{F}_3$ cismi üzerinde de tanımlanır. Bu bölümde $\mathbb{F}_3^{3\cdot n}$ üzerinde tanımlanan indexi 3 olan bir quasi-cyclic kod dönüşümü $\sigma^{\otimes 3}$ biçiminde gösterilecektir. Daha önceki bölümlerde olduğu gibi bu bölümde de σ dönüşümü cyclic kaydırma dönüşümü anlamındadır.

5.2.1.Teorem: C, R halkası üzerinde tanımlı n uzunluğunda bir cyclic kod ise $\Phi(C)$ $\mathbb{F}_3$ üzerinde $3\cdot n$ uzunluğunda 3 indexli bir quasi-cyclic koddur. (Xiong vd., 2013)

$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_3^{3\cdot n} \\ \sigma\downarrow & \circlearrowright & \downarrow\sigma^{\otimes 3} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_3^{3\cdot n} \end{array}$$

Kanıt: Herhangi bir

$x=\left(a_1+ub_1+u^2c_1,a_2+ub_2+u^2c_2,a_3+ub_3+u^2c_3,\ldots,a_n+ub_n+u^2c_n\right)\in C$ için

$\sigma(x)=\left(a_n+ub_n+u^2c_n,a_1+ub_1+u^2c_1,a_2+ub_2+u^2c_2,\ldots,a_{n-1}+ub_{n-1}+u^2c_{n-1}\right)_{\substack{\in C \\ C \text{ cyclic} \\ \text{kod}}}$

$\Rightarrow\Phi\left(\sigma(x)\right)=\left(a_n+b_n+c_n,a_1+b_1+c_1,\ldots,a_{n-1}+b_{n-1}+c_{n-1},b_n+2\cdot c_n,b_1+2\cdot c_1\right.$

$\left.\ldots,b_{n-1}+2\cdot c_{n-1},c_n,c_1,\ldots,c_{n-1}\right)\in\Phi(C)\cdots(i)$

Herhangi bir $y=\left(y_1,y_2,\ldots,y_{3\cdot n}\right)\in\Phi(C)$ için $\Phi(x)=y$ olacak biçimde en az bir

$x=\left(a_1+ub_1+u^2c_1,a_2+ub_2+u^2c_2,a_3+ub_3+u^2c_3,\ldots,a_n+ub_n+u^2c_n\right)\in C$ vardır.

$\Rightarrow\Phi(x)=\left(a_1+b_1+c_1,a_2+b_2+c_2,\ldots,a_n+b_n+c_n,b_1+2\cdot c_1,b_2+2\cdot c_2,\ldots,b_n+2\cdot c_n,c_1,c_2,\ldots,c_n\right)$

$\Rightarrow\sigma^{\otimes 3}\left(\Phi(x)\right)$

$=\sigma^{\otimes 3}\left(a_1+b_1+c_1,a_2+b_2+c_2,\ldots,a_n+b_n+c_n,b_1+2\cdot c_1,b_2+2\cdot c_2,\ldots,b_n+2\cdot c_n,c_1,c_2,\ldots,c_n\right)$

$=\left(\sigma\left(a_1+b_1+c_1,a_2+b_2+c_2,\ldots,a_n+b_n+c_n\right)\middle|\sigma\left(b_1+2\cdot c_1,b_2+2\cdot c_2,\ldots,b_n+2\cdot c_n\right)\middle|\sigma\left(c_1,c_2,\ldots,c_n\right)\right)$

$=\left(\left(a_n+b_n+c_n,a_1+b_1+c_1,\ldots,a_{n-1}+b_{n-1}+c_{n-1}\right)\middle|\left(b_n+2\cdot c_n,b_1+2\cdot c_1,\ldots,b_{n-1}+2\cdot c_{n-1}\right)\middle|\left(c_n,c_1,\ldots,c_{n-1}\right)\right)$

$=\left(a_n+b_n+c_n,a_1+b_1+c_1,\ldots,a_{n-1}+b_{n-1}+c_{n-1},b_n+2\cdot c_n,b_1+2\cdot c_1,\ldots,b_{n-1}+2\cdot c_{n-1},c_n,c_1,\ldots,c_{n-1}\right)\cdots(ii)$

O halde i ve ii'den $\sigma^{\otimes 3}(y)=\sigma^{\otimes 3}\left(\Phi(x)\right)=\Phi\left(\sigma(x)\right)\in\Phi(C)$'dir.

O halde $\Phi(C)$ $\mathbb{F}_3$ cismi üzerinde tanımlı $3\cdot n$ uzunluğunda 3 indexli bir quasi-cyclic koddur. □

5.3. $\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ $(u^2=0)$ Halkası Üzerindeki Cyclic Kodlar

Bu bölümde 5.1.Bölümde $u^3=0$ koşuluyla halka olan $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ halkası üzerinde yapılan çalışmalar $\mathbb{F}_p=GF(p)$ ve $u^3=0$ olmak üzere $R=\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkası üzerine genelleştirilmiştir.

Bu bölüm boyunca aksi belirtilmedikçe $u^3=0$ koşuluyla halka olan $\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkası R ile gösterilecektir. R maximal ideali $u\cdot R$ olan $\{0\}=R\cdot u^3\subset_{\neq} R\cdot u^2\subset_{\neq} R\cdot u\subset_{\neq} R$ idealleri ile 3 uzunluğunda bir sonlu zincir halkasıdır. (Çengellenmiş, 2009c)

5.2.Bölümde tanımlanan cyclic kaydırma dönüşümü; σ, $(1-u^2)-$constacyclic kaydırma dönüşümü υ aynı şekilde R^n üzerinde tanımlanır. 5.2.Bölümde $\mathbb{F}_2^{4\cdot n}$ üzerinde tanımlı 2 indexli quasi-cyclic dönüşümü; $\mathbb{F}_p^{p^2\cdot n}$ üzerinde 5.3.1.Tanımdaki gibi genelleştirilir.

5.3.1.Tanım:
$$\sigma:\mathbb{F}_p^{p\cdot n}\to\mathbb{F}_p^{p\cdot n}$$
$$\left(a_1,a_2,\ldots,a_{p\cdot n}\right)\mapsto\sigma\left(a_1,a_2,\ldots,a_{p\cdot n}\right)=\left(a_{p\cdot n},a_1,\ldots,a_{p\cdot n-1}\right)$$

biçiminde σ cyclic kaydırma dönüşümü tanımlansın. Ayrıca $i=1,2,\ldots,s$ için;

$a^{(1)}=\left(a_1,a_2,\ldots,a_{p\cdot n}\right)\in\mathbb{F}_p^{p\cdot n}$

$a^{(2)}=\left(a_{p\cdot n+1},a_{p\cdot n+2},\ldots,a_{2\cdot p\cdot n}\right)\in\mathbb{F}_p^{p\cdot n}$

$a^{(3)}=\left(a_{2\cdot p\cdot n+1},a_{2\cdot p\cdot n+2},\ldots,a_{3\cdot p\cdot n}\right)\in\mathbb{F}_p^{p\cdot n}$

$\vdots$

$a^{(i)}=\left(a_{(i-1)\cdot p\cdot n+1},a_{(i-1)\cdot p\cdot n+2},\ldots,a_{i\cdot p\cdot n}\right)\in\mathbb{F}_p^{p\cdot n}$ olmak üzere;

her $a=\left(a_1,a_2,\ldots,a_{p^2\cdot n}\right)\in\mathbb{F}_p^{p^2\cdot n}$ elemanı $a=\left(a^{(1)}\middle|a^{(2)}\middle|\ldots\middle|a^{(p)}\right)\in\mathbb{F}_p^{p^2\cdot n}$ gösterimiyle yazılsın.

$$\sigma^{\otimes p}:\mathbb{F}_p^{p^2\cdot n}\to\mathbb{F}_p^{p^2\cdot n}$$
$$a=\left(a_1,a_2,\ldots,a_{p^2\cdot n}\right)\mapsto\sigma^{\otimes p}(a)=\sigma^{\otimes p}\left(a^{(1)}\middle|a^{(2)}\middle|\ldots\middle|a^{(p)}\right)=\left(\sigma\left(a^{(1)}\right)\middle|\sigma\left(a^{(2)}\right)\middle|\ldots\middle|\sigma\left(a^{(p)}\right)\right)$$

biçiminde tanımlanan $\sigma^{\otimes p}$ dönüşümüne bir quasi-cyclic dönüşümü denir. Ayrıca; bir $C\subseteq\mathbb{F}_p^{p^2\cdot n}$ kodu için eğer $\sigma^{\otimes p}(C)=C$ oluyorsa C koduna p indexli $p^2\cdot n$ uzunluklu bir quasi-cyclic kod denir. (Çengellenmiş, 2009c)

5.3.2.Tanım:

$$w_{\text{hom}} : R \to \{p^2, p^2 - p, 0\} \subset \mathbb{Z}$$

$$r \mapsto w_{\text{hom}}(r) = \begin{cases} p^2 - p; & r \in R \setminus R \cdot u^2 \text{ ise} \\ p^2; & r \in R \cdot u^2 \setminus \{0\} \text{ ise} \\ 0; & \text{diğer durumlarda} \end{cases}$$

biçiminde tanımlanan fonksiyona Homogeneous ağırlık fonksiyonu denir.□ (Greferath & Schmidt, 1999)

5.3.2.Tanımda $p = 2$ alındığında 5.1.1.Tanım elde edilir. R^n 'in bir elemanının Homogeneous ağırlığı ve iki elemanı arasındaki Homogeneous uzaklığı 5.1.Bölümdeki gibi tanımlanır.

5.3.1.Önerme: $c = \left(x_1 + y_1 u + z_1 u^2,\ x_2 + y_2 u + z_2 u^2, \ldots, x_n + y_n u + z_n u^2\right) \in R^n$

olsun,

$$\Phi : \left(R^n, d_{\text{hom}}\right) \to \left(\mathbb{F}_p{}^{p^2 \cdot n}, d_H\right)$$

$$\begin{aligned} c \mapsto \Phi(c) = (&z_1, z_2, \ldots, z_n, x_1 + z_1, x_2 + z_2, \ldots, x_n + z_n, 2 \cdot x_1 + z_1, 2 \cdot x_2 + z_2, \ldots, 2 \cdot x_n + z_n, \ldots, \\ &(p-1) \cdot x_1 + z_1, (p-1) \cdot x_2 + z_2, \ldots, (p-1) \cdot x_n + z_n, \\ &y_1 + z_1, y_2 + z_2, \ldots, y_n + z_n, x_1 + y_1 + z_1, x_2 + y_2 + z_2, \ldots, x_n + y_n + z_n, \ldots, \\ &(p-1) \cdot x_1 + y_1 + z_1, (p-1) \cdot x_2 + y_2 + z_2, \ldots, (p-1) \cdot x_n + y_n + z_n, \\ &2 \cdot y_1 + z_1, 2 \cdot y_2 + z_2, \ldots, 2 \cdot y_n + z_n, x_1 + 2 \cdot y_1 + z_1, x_2 + 2 \cdot y_2 + z_2, \ldots, x_n + 2 \cdot y_n + z_n, \ldots, \\ &(p-1) \cdot x_1 + 2 \cdot y_1 + z_1, (p-1) \cdot x_2 + 2 \cdot y_2 + z_2, \ldots, (p-1) \cdot x_n + 2 \cdot y_n + z_n, \\ &\vdots \\ &(p-1) \cdot y_1 + z_1, (p-1) \cdot y_2 + z_2, \ldots, (p-1) \cdot y_n + z_n, x_1 + (p-1) \cdot y_1 + z_1, x_2 + (p-1) \cdot y_2 + z_2, \ldots, \\ &x_n + (p-1) \cdot y_n + z_n, \ldots, (p-1) \cdot x_1 + 2 \cdot y_1 + z_1, (p-1) \cdot x_2 + (p-1) \cdot y_2 + z_2, \ldots, (p-1) \cdot x_n + (p-1) \cdot y_n + z_n) \end{aligned}$$

dönüşümü bir izometridir. (Çengellenmiş, 2009c)

5.3.2.Önerme: Φ Gray, υ $\left(1 - u^2\right)-$constacyclic kaydırma ve $\sigma^{\otimes p}$ p indexli quasi-cyclic kaydırma dönüşümü olmak üzere $\Phi \circ \upsilon = \sigma^{\otimes p} \circ \Phi$'dir. (Çengellenmiş, 2009c)

$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_p{}^{p^2 \cdot n} \\ \upsilon \downarrow & \circlearrowright & \downarrow \sigma^{\otimes p} \\ R^n & \xrightarrow{\Phi} & \mathbb{F}_p{}^{p^2 \cdot n} \end{array}$$

5.3.1.Teorem: C R halkası üzerinde tanımlı n uzunluğunda bir kod olsun. C bir $(1-u^2)-$constacyclic kod ise $\Phi(C)$ kodu $\mathbb{F}_p$ üzerinde $p^2 \cdot n$ uzunluklu p indexli bir quasi-cyclic koddur. Bu ifadenin tersi de doğrudur. (Çengellenmiş, 2009c)

Kanıt: $\Rightarrow$: C, R halkası üzerinde tanımlı n uzunluğunda $(1-u^2)-$ constacyclic kod $\underset{\upsilon \text{ tanımı}}{\Rightarrow} \upsilon(C)=C \Rightarrow \Phi(\upsilon(C))=\Phi(C) \underset{5.3.2.\text{Önerme}}{\Rightarrow} \Phi(C)=\sigma^{\otimes p}(\Phi(C))$

$\underset{\sigma^{\otimes p} \text{ tanımı}}{\Rightarrow} \Phi(C)$, $\mathbb{F}_p$ cismi üzerinde tanımlı $p^2 \cdot n$ uzunluklu p indexli bir quasi-cyclic koddur.

$\Leftarrow$: $\Phi(C)$, $\mathbb{F}_p$ cismi üzerinde tanımlı $p^2 \cdot n$ uzunluğunda p indexli bir quasi-cyclic kod

$\underset{\sigma^{\otimes p} \text{ tanımı}}{\Rightarrow} \sigma^{\otimes p}(\Phi(C))=\Phi(C) \underset{5.3.2.\text{Önerme}}{\Rightarrow} \Phi(\upsilon(C))=\Phi(C) \underset{\Phi \text{ birebirdir.}}{\Rightarrow} \upsilon(C)=C$

$\underset{\upsilon \text{ tanımı}}{\Rightarrow} C$, R halkası üzerinde tanımlı n uzunluğunda bir $(1-u^2)-$constacyclic koddur.

5.3.3.Önerme: $(n,p)=1$, $n' \in \{0,1,2,\ldots,p-1\}$ ve $n \cdot n' \equiv 1 (\text{mod } p)$ olmak üzere $\beta = 1+n' \cdot u^2$ olsun.

$$\mu : \frac{R[x]}{\langle x^n-1 \rangle} \to \frac{R[x]}{\langle x^n-(1-u^2) \rangle}$$
$$\overline{r(x)} \mapsto \mu(\overline{r(x)}) = \overline{r(\beta \cdot x)}$$

biçiminde tanımlanan μ dönüşümü bir halka izomorfizmasıdır. (Çengellenmiş, 2009c)

5.3.2.Teorem: β 5.3.3.Önerme'de tanımlandığı gibi olmak üzere;

$$\bar{\mu} : R^n \to R^n$$
$$r=(r_0,r_1,\ldots,r_{n-1}) \mapsto \bar{\mu}(r)=(r_0,\beta \cdot r_1,\beta^2 \cdot r_2,\ldots,\beta^{n-1} \cdot r_{n-1})$$

biçiminde $\bar{\mu}$ dönüşümü tanımlansın.

C kodunun R üzerinde n uzunluğunda bir cyclic kod olması için gerekli ve yeterli koşul $\bar{\mu}(C)$ kodunun R üzerinde n uzunluklu bir $(1-u^2)-$constacyclic kod olmasıdır. □ (Çengellenmiş, 2009c)

5.1.4.Önerme'de yer alan $\mathbb{F}_2^{4\cdot n}$ üzerinde tanımlanan $\pi^{\otimes 2}$ permütasyonunun $\mathbb{F}_p^{p^2\cdot n}$ vektör uzayı üzerindeki genellemesi;

Her $c=\left(c_0,c_1,\ldots c_{p\cdot n-1},c_{p\cdot n},c_{p\cdot n+1},\ldots,c_{2\cdot p\cdot n-1},\ldots,c_{(p-1)\cdot p\cdot n},c_{(p-1)\cdot p\cdot n+1},\ldots,c_{p^2\cdot n-1}\right)\in\mathbb{F}_p^{p^2\cdot n}$ için

$c^{(1)}=\left(c_0,c_1,\ldots c_{p\cdot n-1}\right)\in\mathbb{F}_p^{p\cdot n}$

$c^{(2)}=\left(c_{p\cdot n},c_{p\cdot n+1},\ldots,c_{2\cdot p\cdot n-1}\right)\in\mathbb{F}_p^{p\cdot n}$

$\vdots$

$c^{(p)}=\left(c_{(p-1)\cdot p\cdot n},c_{(p-1)\cdot p\cdot n+1},\ldots,c_{p^2\cdot n-1}\right)\in\mathbb{F}_p^{p\cdot n}$ ve π 4.1.6.Tanım'da $k=1$ alınmasıyla elde edilen $\mathbb{F}_p^{p\cdot n}$ üzerindeki Nechaev Permütasyonu olmak üzere;

$$\pi^{\otimes p}:\mathbb{F}_p^{p^2\cdot n}\to\mathbb{F}_p^{p^2\cdot n}$$
$$c\mapsto\pi^{\otimes p}(c)=\left(\pi\left(c^{(1)}\right)\middle|\pi\left(c^{(2)}\right)\middle|\ldots\middle|\pi\left(c^{(p)}\right)\right)$$

dönüşümüyle verilir. (Çengellenmiş, 2009c)

5.3.4.Önerme: $\Phi\circ\bar{\mu}=\pi^{\otimes p}\circ\Phi$'dir. (Çengellenmiş, 2009c)

5.3.3.Teorem: C R halkası üzerinde tanımlı n uzunluklu bir lineer cyclic kod ise $\Phi(C)$ kodu $\mathbb{F}_p$ üzerinde $p^2\cdot n$ uzunluğunda p indexli quasi-cyclic koda permütasyon denktir. (Çengellenmiş, 2009c)

$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_p^{p^2\cdot n} \\ \bar{\mu}\downarrow & \circlearrowright & \downarrow\pi^{\otimes p} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_p^{p^2\cdot n} \end{array}$$

Kanıt: C R halkası üzerinde tanımlı n uzunluklu bir lineer cyclic kod

$\underset{\text{5.3.2.Teorem}}{\Rightarrow}\bar{\mu}(C)$, R halkası üzerinde tanımlı n uzunluğunda $\left(1-u^2\right)-$constacyclic kod

$\underset{\text{5.3.1.Teorem}}{\Rightarrow}\Phi\left(\bar{\mu}(C)\right)$, $\mathbb{F}_p$ cismi üzerinde tanımlı $p^2\cdot n$ uzunluğunda p indexli quasi-cyclic kod

$\underset{\text{5.3.4.Önerme}}{\Rightarrow}\Phi\left(\bar{\mu}(C)\right)=\pi^{\otimes p}\left(\Phi(C)\right)\subseteq\mathbb{F}_p^{p^2\cdot n}$

$\underset{\text{permütasyon}}{\overset{\pi^{\otimes p}}{\Rightarrow}}$ $\Phi(C)$ $\mathbb{F}_p$ cismi üzerinde tanımlı $p^2 \cdot n$ uzunluğunda p indexli quasi-cyclic koda permütasyon denktir. □

BÖLÜM 6

SONUÇLAR VE TARTIŞMA

Φ Gray dönüşümü, σ cyclic kaydırma dönüşümü, ν constacyclic kaydırma dönüşümü, $\sigma^{\otimes p^{k-1}}$ indeksi p^{k-1} olan quasi-cyclic kaydırma dönüşümü, $\pi^{\otimes p}$ Bölüm 5'de π Nechaev Permütasyonu kullanılarak tanımlanan permütasyon olmak üzere

3.2.6.Önerme'de;
$$\begin{array}{ccc} R_0^{\,n} & \xrightarrow{\Phi} & \mathbb{F}_2^{\,2\cdot n} \\ \upsilon\downarrow & \circlearrowright & \downarrow\sigma \\ R_0^{\,n} & \xrightarrow{\Phi} & \mathbb{F}_2^{\,2\cdot n} \end{array}$$

4.1.2.Önerme'de;
$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_{p^k}^{\,p^k\cdot n} \\ \upsilon\downarrow & \circlearrowright & \downarrow\sigma^{\otimes p^{k-1}} \\ R^n & \xrightarrow{\Phi} & \mathbb{F}_{p^k}^{\,p^k\cdot n} \end{array}$$

5.1.2.Önerme'de;
$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_2^{\,4\cdot n} \\ \upsilon\downarrow & \circlearrowright & \downarrow\sigma^{\otimes 2} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_2^{\,4\cdot n} \end{array}$$

5.1.4.Önerme'de;
$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_2^{\,4\cdot n} \\ \bar{\mu}\downarrow & \circlearrowright & \downarrow\pi^{\otimes 2} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_2^{\,4\cdot n} \end{array}$$

5.2.1.Teorem'de;
$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_3^{\,3\cdot n} \\ \sigma\downarrow & \circlearrowright & \downarrow\sigma^{\otimes 3} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_3^{\,3\cdot n} \end{array}$$

5.3.2.Önerme'de;
$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_p^{\,p^2\cdot n} \\ \upsilon\downarrow & \circlearrowright & \downarrow\sigma^{\otimes p} \\ R^n & \xrightarrow{\Phi} & \mathbb{F}_p^{\,p^2\cdot n} \end{array}$$

5.3.3.Teorem'de;
$$\begin{array}{ccc} R^n & \xrightarrow{\Phi} & \mathbb{F}_p^{\,p^2\cdot n} \\ \bar{\mu}\downarrow & \circlearrowright & \downarrow\pi^{\otimes p} \\ R^n & \xrightarrow[\Phi]{} & \mathbb{F}_p^{\,p^2\cdot n} \end{array}$$

diyagramları elde edilmiştir. Bu diyagramlar incelendiğinde belirli halkalar üzerindeki bir $[n,k,d]-C$ kodundan yeni kod elde edilmesine rağmen n uzunluğunun arttığı görülmektedir. Kodun n uzunluğunun büyümesi iletimde zaman kaybına neden olacaktır. Bu yüzden n 'nin artması istenen bir özellik değildir. Bunun içinde bu diyagramlarda tanımlanan dönüşümler yerine uygun dönüşümler tanımlanarak en azından uzunluğu sabit kalan yeni kodların elde edilmesi amaçlanmalıdır. Bu çalışmanın ardından belirli halkalar üzerindeki var olan kodlardan yeni ve iyi kodlar elde edilmesi problemi üzerinde çalışılmalıdır.

KAYNAKLAR

Amarra, M. C. V. &Nemenzo, F.R. (2008). On $(1-u)-$cyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$. *Applied Mathematics Letters, 21,* 1129-1133.

Crandall, R. & Pomerance, C. (2005). *Prime Numbers a Computational Perspective Second Edition.* New York: Springer.

Çengellenmiş, Y. (2005). *Değerlendirme Teorisi Ve Kodlama Teorisi Üzerine*. (Yayımlanmış doktora tezi). Trakya Üniversitesi/Fen Bilimleri Enstitüsü, Ankara.

Çengellenmiş, Y. (2009a). The gray image of the cyclic codes over $\mathbb{F}_2[u]/\langle u^2-1\rangle$. *Journal of Discrete Mathematical Sciences & Cryptography, 2,* 175-178.

Çengellenmiş, Y. (2009b). On $(1-u^m)-$ Cyclic Codes over $F_2+uF_2+u^2F_2+\cdots+u^mF_2$. *Int. J. Contemp. Math. Sciences, 20,* 987-992.

Çengellenmiş, Y. (2009c). On $(1-u^2)-$ cyclic and cyclic codes over $F_p+uF_p+u^2F_p$. *Journal of Discrete Mathematical Sciences & Cryptography, 2,* 239-243.

Dinh, H. Q. (2010). Constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. *Journal of Algebra, 324,* 940-950.

Flaut, C. (2000). Cyclic codes over some special rings. *Bull. Korean Math. Soc., 5,* 1513-1521.

Greferath, M. &Schmidt, S.E. (1999). Gray Isometries for Finite Chain Rings and a Nonlinear Ternary $(36,3^{12},15)$ Code. *IEE Transactıons On Information Theory, 7,* 2522-2524.

Hill, R. (1986). *A First Course in CodingTheory.* Oxford: Oxford University Press.

Holdman, G.R. (2016). *Error-Correcting Codes Over Galois Rings.* (Yayımlanmış Yükseklisans Tezi) Whitman College, Washington.

Huffman, W. C. &Pless, V. (2003). *Fundamentals of Error Correcting Codes.* Cambridge: Cambridge UniversityPress.

Hungerford, T.W. (1974). *Algebra*. New York: Springer Verlag.

Kai, X., Zhu, S., Li, P. (2010). $(1+\lambda u)-$ Constacyclic codes over $\mathbb{F}_p[u]/\langle u^m \rangle$. *Journal of The Franklin Institute, 347,* 751-762.

Ling, S. &Xing, C. (2004). *Coding Theory A First Course.* Cambridge: Cambridge UniversityPress.

Qian, J., Zhang, L. &Zhu, S. (2006). $(1+u)$ constacyclic and cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$. *Applied Mathematics Letters, 19,* 820-823.

Roman, S. (1992). *Coding and Information Theory. New York:* Springer Verlag.

Xiong, Y., Yun, S., Xing, J. & Xu, X. (2013). The Gray images of linear codes over the ring $F_3+vF_3+v^2F_3$. Inter*national Journal of Computer Science Issues,* 400-405.

Zhu, S., Wang, Y. & Shi, M. (2010). Some Result on Cylic Codes Over $\mathbb{F}_2+v\mathbb{F}_2$. *IEE Transactıons On Information Theory,* 1680-1684.

ÖZGEÇMİŞ

1987 yılında Çorum'da doğdum. 2000 yılında Çorum Yahya Kemal Beyatlı İlköğretim Okulundan, 2003 yılında Çorum Eti Lisesinden mezun oldum. 2004 yılında girmiş olduğum Dokuz Eylül Üniversitesi İlköğretim Matematik Öğretmenliği Programından 2008 senesinde mezun oldum ve yine aynı sene Edirne'de Milli Eğitim Bakanlığına bağlı bir okula atandım. Hâlen Milli Eğitim Bakanlığında öğretmenlik görevime devam etmekteyim.