

T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL HALKALAR ÜZERİNDE TANIMLI DEVİRLİ DNA KODLAR
HAKKINDA

ALEV YOKUVA

YÜKSEK LİSANS TEZİ

HESAPLAMALI BİLİMLER ANABİLİM DALI

TEZ DANIŞMANI: DOÇ. DR. YASEMİN ÇENGELLENMİŞ

EDİRNE-2019

Alev YOKUVA'nın hazırladığı “ Bazı Özel Halkalar Üzerinde Tanımlı Devirli DNA Kodlar Hakkında” başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Hesaplamalı Bilimler Anabilim Dalında bir Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri (Ünvan, Ad, Soyad):

İmza

Doç. Dr. Yasemin ÇENGELLENMİŞ



Doç. Dr. Seçil ÇEKEN (GEZEN)



Dr. Öğr. Üyesi Abdullah DERTLİ



Tez Savunma Tarihi: 10 / 09 / 2019

Bu tezin Yüksek Lisans Tezi olarak gerekli şartları sağladığımı onaylarım.

İmza

Doç. Dr. Yasemin ÇENGELLENMİŞ
Tez Danışmanı



Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı



Prof. Dr. Murat YURTCAN
Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ
HESAPLAMALI BİLİMLER ANABİLİM DALI YÜKSEK LİSANS PROGRAMI
DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uyarak hazırladığım bu çalışmada, tüm veriler bilimsel çerçevede hazırlanan makalelerden edinilmiş, kullanılan verilerde değişiklik yapılmamış, akademik ve etik açıdan kurallara uygun yazılmış, 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.

10 / 09 / 2019

Alev YOKUVA

İmza



Yüksek Lisans Tezi

BAZI ÖZEL HALKALAR ÜZERİNDE TANIMLI DEVİRLİ DNA KODLAR HAKKINDA

T.Ü. Fen Bilimleri Enstitüsü

Hesaplamalı Bilimler A.B.D.

ÖZET

Bu tezde, 16 elemanlı $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$, $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$, $\mathbb{Z}_4[w]/\langle w^2 + 2 \rangle$ sonlu zincir halkaları ve $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$; $u^2 = 0, v^2 = v, uv = vu, \mathbb{Z}_4 + u\mathbb{Z}_4$; $u^2 = 0, \mathbb{F}_4 + v\mathbb{F}_4$; $v^2 = v$ sonlu zincir olmayan halkaları üzerinde tanımlı devirli (cyclic) DNA kodların yapılarını inceleyen makaleler incelenmiştir. Bu makalelerde, 16 elemanlı bazı sonlu halkalar üzerinde tanımlı devirli kodların DNA özelliklerine sahip olması için gerek ve yeterli koşullar verilmiştir. Ters sıralı (reversible) ve ters sıralı tamamlayan (reversible complement) DNA kodlarını elde etmek için bazı makalelerde verilen yeni bir yaklaşım yöntemi incelenmiştir.

Yıl : 2019

Sayfa Sayısı : 88

Anahtar Kelimeler : Devirli Kodlar, Devirli DNA Kodlar, DNA Dönüşüm

Master of Science Thesis

ON THE CYCLIC DNA CODES OVER SOME SPECIAL RINGS

Trakya University Institute of Natural Sciences

Department of Computational Sciences

ABSTRACT

In this thesis, the papers which are about the structures of cyclic DNA codes over the finite chain rings $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$, $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$, $\mathbb{Z}_4[w]/\langle w^2 + 2 \rangle$ and the finite non chain rings $\mathbb{F}_4 + v\mathbb{F}_4$ where $v^2 = v$, $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ where $u^2 = 0, v^2 = v, uv = vu$, $\mathbb{Z}_4 + u\mathbb{Z}_4$ where $u^2 = 0$ with 16 elements are investigated. In these papers, necessary and sufficient conditions for cyclic codes over the some finite rings with 16 elements to have DNA properties have been explored. In order to obtain reversible DNA and reversible complements DNA codes, a novel approach which are given in some papers are investigated.

Year : 2019

Number of Pages : 88

Keywords : Cyclic Codes, Cyclic DNA Codes, DNA Map



Sevgili dedem İrfan Yokuva'ya...

ÖNSÖZ

Yüksek Lisans Tez danışmanlığı üstlenerek akademik hayata adım atmamı sağlayan, çalışmalarımı yürütürken yardımlarını, desteğini ve ilgisini esirgemeyen danışmanım, akademik alanda hayatıma yaptığı katkıları saymakla bitmeyecek sevgili hocam Sayın Doç. Dr. Yasemin ÇENGELLENMİŞ'e sonsuz teşekkürler ederim.

Tez çalışmam boyunca yaptığım tüm akademik araştırmalarda destek olan, değerli akademik katkılarda bulunan, fikir, öneri ve yol gösteren, yılmadan benim yanımda duran sevgili Dr. G. Gözde GÜZEL'e çok teşekkür ederim.

Bugüne kadarki eğitim hayatım boyunca maddi ve manevi desteğini esirgemediğim yanımda olan babam Cavit YOKUVA'ya, annem Ayşe YOKUVA'ya kardeşim Alp YOKUVA'ya ve sevgili tüm aileme çok teşekkür ederim.

Ayrıca, tez çalışmam boyunca beni motive etmiş ve manevi olarak destek sağlamış olan Cemre GÖKÇE'ye ve diğer adını sayamadığım tüm arkadaşlarıma çok teşekkür ederim.

Alev YOKUVA

İÇİNDEKİLER

ÖZET.....	iv
ABSTRACT	v
ÖNSÖZ.....	vii
İÇİNDEKİLER	viii
SEMBOLLER ve KISALTMALAR DİZİNİ	xi
ŞEKİLLER DİZİNİ	xii
ÇİZELGELER DİZİNİ	xiii
BÖLÜM 1 GİRİŞ	1
1.1. Tez Organizasyonu.....	5
BÖLÜM 2 TEMEL KAVRAMLAR	6
2.1. Cebir ile İlgili Alt Yapı	6
2.2. Kodlama Teorisi ile İlgili Alt Yapı	15
BÖLÜM 3 BAZI ÖZEL HALKALAR ÜZERİNDE TANIMLI DEVİRLİ DNA KODLAR.....	22
3.1. Giriş.....	22
3.2. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar ve Tek Uzunluklu Devirli DNA Kodların DNA Görüntüleri	23
3.2.1. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Kümesinin Cebirsel Yapısı	23
3.2.2. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkası Üzerinde Tanımlı Devirli Kodlar.....	24
3.2.3. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar	25

3.3. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkası Üzerinde Tanımlı Tek Uzunluklu Devirli DNA Kodlar ve Devirli DNA Kodlarının DNA Görüntüleri	29
3.3.1. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Kümesinin Cebirsel Yapısı	29
3.3.2. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkası Üzerinde Tanımlı Devirli Kodlar	29
3.3.3. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar	30
3.4. $w^2 = 2$ Olmak Üzere $\mathbb{Z}_4 + w \mathbb{Z}_4$ Sonlu Halkası Üzerinde Devirli DNA Kodlar	35
3.4.1. $\mathbb{Z}_4 + w \mathbb{Z}_4$ Kümesinin Cebirsel Yapısı	35
3.4.2. $\mathbb{Z}_4 + w \mathbb{Z}_4$ Halkası Üzerinde Tanımlı Devirli Kodlar	36
3.4.3. $\mathbb{Z}_4 + w \mathbb{Z}_4$ Sonlu Halkası Üzerinde Devirli DNA Kodlar	36
3.5. $\mathbb{F}_4[u]/(v^2 - v)$ Halkası Üzerinde Tanımlı Devirli Dna Kodlar ve Devirli DNA Kodlarının DNA Görüntüleri	40
3.5.1. $\mathbb{F}_4[v]/(v^2 - v)$ Kümesinin Cebirsel Yapısı	40
3.5.2. $\mathbb{F}_4[v]/(v^2 - v)$ Halkası Üzerinde Tanımlı Devirli Kodlar	42
3.5.3. $\mathbb{F}_4[v]/(v^2 - v)$ Halkası Üzerinde Tanımlı DNA Kodlar	42
3.5.4. $\mathbb{F}_4[v]/(v^2 - v)$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar	43
3.6. $u^2=0, v^2=v, uv=vu$ Olmak Üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Sonlu Halkası Üzerinde Devirli Kod İnşası Ve Devirli DNA Kodların DNA Görüntüleri	47
3.6.1. $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Kümesinin Cebirsel Yapısı	47
3.6.2. $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Sonlu Halkası Üzerinde Tanımlı Devirli Kodlar	50
3.6.3. Ters Sıralı Kodlar	51
3.6.4. Ters Sıralı Tamamlayan Kodlar	52
3.6.5. $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Halkası Üzerinde Tanımlı DNA Kodlar	53
3.7. $u^2=0$ Olmak Üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı Devirli DNA Kodlar	56
3.7.1. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Kümesinin Cebirsel Yapısı	56

3.7.2. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı Devirli Kodlar	57
3.7.3. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı DNA Kodlar.....	57
3.7.4. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı Ters Sıralı Kodlar	58
3.7.5. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Halkası Üzerinde Tanımlı Ters Sıralı Tamamlayan Kodlar	62
BÖLÜM 4.....	70
SONUÇLAR VE TARTIŞMA	70
KAYNAKLAR	71
ÖZGEÇMİŞ.....	75

SEMBOLLER VE KISALTMALAR DİZİNİ

$\mathbb{F}_q$	Finite Field with q elements	q elemanlı sonlu cisim
$\mathbb{F}_q^n$	n dimensional $\mathbb{F}_q$ -vector space	n boyutlu $\mathbb{F}_q$ -vektör uzayı
$d(x, y)$	The Hamming distance between x and y	x ile y arasındaki Hamming uzaklık
$d(C)$	Minimum Hamming distance of the code C	C kodunun minimum Hamming uzaklığı
$wt(x)$	The weight of the element x	x elemanının ağırlığı
$wt(C)$	The minimum weight of the code C	C kodunun minimum ağırlığı
(n, M, d)	The representation of a code with length n , M elements and minimum distance d	n uzunluklu, M elemanlı ve d minimum uzaklıklı kodun temsili
$[n, k, d]$	The representation of a linear code with length n , dimension k and minimum distance d	n uzunluklu, k boyutlu ve d minimum uzaklıklı lineer kodun temsili
$F_q[x]$	The polynomial ring in one variable x over $\mathbb{F}_q$	Katsayıları $\mathbb{F}_q$ 'da olan x değişkenli polinom halkası
$F_q[x]/\langle f \rangle$	The quotient ring	Bölüm halkası
σ	The cyclic shift	Devirli öteleme

ŞEKİLLER DİZİNİ

Şekil 1.1 Temel İletişim Sistemi.....	1
---------------------------------------	---



ÇİZELGELER DİZİNİ

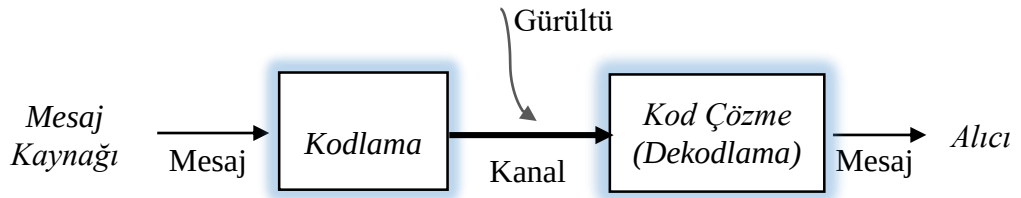
Çizelge 3.1 $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri	25
Çizelge 3.2 $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri	30
Çizelge 3.3 $\mathbb{Z}_4 + w \mathbb{Z}_4$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri.....	36
Çizelge 3.4 $\mathbb{F}_4[v]/\langle v^2 - v \rangle$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri...	44
Çizelge 3.5 $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri	53
Çizelge 3.6 $\mathbb{Z}_4 + u\mathbb{Z}_4$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri	58

BÖLÜM 1

GİRİŞ

'96 yılının Aralık ayında NASA'nın yaptığı Mars yüzeyini araştırma projesi kapsamında uzaya gönderdiği Parthfinder isimli bir robotun dünyaya gönderdiği fotoğraf ve çok sayıda veri, tüm dünyada büyük bir heyecana neden olmuştur. Yalnızca düşük kapasiteli bir lambayı yakabilecek güce sahip radyo frekans vericisi olan bu robotlardan, milyonlarca kilometre öteden doğru, bozulmamış, güvenilir bilgi alabilmenin mümkün olma sebebi disiplinler arası çalışılan Kodlama Teorisi'dir.

Kodlama teorisinin başlangıcı C. Shannon'ın bilgi teorisi ile ilgili yayımlanmış olduğu 'A Mathematical Theory of Communication' adlı makalesi kabul edilir. Bu makalede Shannon, gürültülü bir kanalda iletilmesi istenen mesajın, alıcıya doğru bir şekilde iletilmesinin kodlama ve kod çözme teknikleri sayesinde güvenilir iletişim sağlanabileceğini ifade etmiştir (Shannon, 1949; Shannon, 1948). Bir iletişim sisteminde mesajın kaynağından alıcıya kadar oluşan aşamalarından birisi kodlama, iletilen mesajda meydana gelebilecek hatalardan mesajı korur. Dekodlama ise, gönderilen mesajdaki hataların tespiti ve düzeltilmesi için yapılır.



Şekil 1.1 Temel İletişim Sistemi

Şekil 1.1, temel iletişim sisteminde ki mesajın, *mesaj kaynağından alıcıya* gidene kadar izlediği yol ifade edilmektedir. Bu iletişim sisteminde, *gönderilen mesaj* ortama aktarılır, mesajı bozarak hatalara sebep olabilecek, gürültü (noisy) adı verilen etmene karşı kodlanır. Kodlanan mesaj, hatalı bir biçimde dekodlama (kod çözme) aşamasına geldiğinde, mesajın kodlanma biçimiyle uyumlu bir dekodlama yöntemi belirlenip alıcıya ulaştırılması amaçlanır. *Şekil 1.1*'deki iletişim sisteminde, kodlama aşamasına giren mesaj ile kod çözme aşamasında çözülen *kod sözcüğü* aynı olmayabilir. Bu durumda, mesajın tekrar gönderilmesi istenir ve dekodlama aşamasında tekrar yollanan mesajda oluşan hataların düzeltilmesi beklenir.

Kodlama teorisinde, mesajın iletilmesi için alfabe ismi verilen sonlu kümeler kullanılır. Yapılan ilk araştırmalar, $\mathbb{F}_2$ sonlu cismi üzerindedir. $\mathbb{F}_2$ sonlu cismi üzerinde çalışılan kodlar (binary kodlar), sonrasında $\mathbb{F}_q$ sonlu cismi (q bir asal sayının kuvveti olmak üzere) üzerinde genelleştirilmiştir.

Kodlama teorisi çalışmaları, ilk olarak 1972 yılında Blake tarafından sonlu halkalar üzerine taşınmıştır (Blake, 1972; Blake, 1975). Hammons ve diğerleri 1994 yılında iyi parametrelili ancak lineer olmayan kodların ailelerinin, sonlu $\mathbb{Z}_4$ halkası üzerinde tanımlı lineer olan kodların Gray dönüşüm altındaki görüntüsü olarak elde edebilmiş ve böylece çalışmalar halkalar üzerine yoğunlaşmıştır. Bu yöntem, zengin cebirsel yapıya sahip halkalardan yararlanmayı ve lineer olmayan kodlarla çalışmanın zorluklarını ortadan kaldırmıştır. Böylece kodlama teorisi sonlu cisimler üzerinden sonlu halkalara taşınmıştır.

Sonlu cisimler üzerinde tanımlı lineer kodlar bir alt vektör uzaya, sonlu halkalar üzerinde tanımlı lineer kodlar ise bir alt modüle karşılık gelmektedirler. Lineer olan kodların kodlama ve dekodlama yöntemleri lineer olmayanlara göre daha kolaydır. Hamming kodlar, devirli kodlar, BCH kodlar bu lineer kodların önemli sınıflarından birkaçıdır.

Lineer kodların bir sınıfı olan devirli kodlar, Prange tarafından 1957 yılında ilk kez tanımlanmıştır. Prange, sonlu $\mathbb{F}_q$ cismi üzerinde n uzunluğunda sahip bir devirli kodu katsayıları $\mathbb{F}_q$ cisminde olan, $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ bölüm halkasının ideallerine karşılık getirmiştir (Prange, 1958; Prange, 1957). Prange'dan ilham alınarak devirli kodları içeren çeşitli makaleler yapılmıştır (Abualrub, Siap, 2008; Abualrub, Siap, 2007; Calderbank,

Sloane, 1995; Özen, Uzekmek, Aydın, 2016; Pless, Qian, 1996; Pless, Sole, Qian, 1997; Qian, Zang, Zhu, 2005; Yıldız, Aydın, 2014).

Kodlama ve bilgi teorisinin ilerlemesi ile 1994 yılında Bilgi ve İletişim Teknolojisinde iki yeni yön ortaya çıkmıştır: Kuantum hesaplama ve DNA hesaplama. İlk DNA hesaplama fikri Tom Head tarafından 1987 yılında ortaya atılmıştır ancak ilk başarılı deneysel çalışmayı yapan kişi L. Adleman'dır. Herhangi bir bilgi işlem veya iletişimin kalbi kodlama teorisidir. L. Adleman DNA hesaplamalarını doğuran Hamilton yolu probleminin bir örneğini çözmek için DNA iplikçiklerini kullanarak bir deney yapmıştır. Adleman'ın başarılı deneyinden sonra DNA hesaplama alanı sadece matematiksel özelliklerin tanımlanması ile DNA nano-yapıları inşa etmek, DNA dizilerinde hata düzeltme özelliklerini incelemek ve DNA tabanlı veri depolama sistemi gibi farklı yönlerle doğru gelişmiştir (Dixita, Bansari, Gupta, 2016).

DNA dizilerindeki matematiksel özellikler, birçok araştırmacıya biyoloji ve kodlama teorisini kullanarak disiplinler arası keşif için ilham vermiştir. DNA iplikçiklerini kullanarak hesaplama yapmak için, belirli özelliklere sahip belirli bir DNA dizi kümesi gerekir. Bu tür bir DNA dizi kümesi, biyomoleküler hesaplamada önemli bir rol oynayan çeşitli kısıtlamaları yerine getirir (Dixita vd., 2016).

DNA kodları, DNA bilişimi, yüzey bazlı DNA bilişimi, DNA Mikroarray teknolojisi, kimyasal kütüphaneler için moleküler barkodlar, DNA nano-yapıları, DNA origamisi, veri şifreleme, veri depolama, sinyal işleme ve DNA nano-araçları ve devreleri gibi çeşitli teknolojilerde kullanılır. Son zamanlarda filogenetik çalışmalarda DNA kodlarının potansiyeli rapor edilmiştir. Ayrıca gen düzenleyici ağları, protein kodlama genlerini ve genlerin yapısını devirli kodlarla incelemeye katkıda bulunmuştur. DNA kodlarından üretilen moleküler barkodlar ürünlerin doğrulanması için biyo-belirteç olarak kullanılır. Ayrıca DNA kodları, hedefli ilaç dağıtım sistemleri gibi potansiyel uygulamalarda kullanılan DNA nano-yapılarının oluşturulmasında kullanılır. Bu yüzden, DNA kodları için prosedürleri verimli bir şekilde kodlayarak elde edilebilecek nano-yapılar için yüksek kararlılığa ve sağlamlığa sahip spesifik özelliklere sahip DNA kodları gerekir (Dixita vd., 2016).

Son birkaç yılda, DNA tabanlı veri depolama sistemleri birçok araştırmacının dikkatini çekmiştir. Veri depolamak için kullanılan DNA kodlarının yoğun veri depolama kapasitesi ve daha iyi hata düzeltme kapasitesi için uygun özelliklere sahip olması gerekir.

Herhangi bir uygulamada DNA kodlarını kullanabilmek adına, DNA kodları için belirtilen temel kısıtlamaları kullanmak kaçınılmazdır. DNA kod tasarımı dayanıklılık için kısıtlama sınırını takip etmeli, ancak özel uygulama için DNA kodlarını tasarlamada, daha işlevsel ve pratik hale getirmek için de DNA kodlarına kısıtlamalar eklemek gerektirmektedir. Bu kısıtlamalar aşağıdaki şekildedir (Dixita vd., 2016):

- *Hamming kısıtlaması*: Herhangi iki $x, y \in C$ elemanı için, $x \neq y$ olmak üzere, $H(x, y) \geq d$.
- *Ters sıralı kısıtlaması*: Herhangi iki $x, y \in C$ elemanı için, x^R x elemanın sıralı terslenebilen elemanı olmak üzere, $H(x^R, y) \geq d$.
- *Ters sıralı tamlayan kısıtlaması*: Herhangi iki $x, y \in C$ elemanı için, x^{RC} x elemanın sıralı terslenebilen elemanı olmak üzere, $H(x^{RC}, y) \geq d$.
- *Sabit GC içeriği kısıtlaması*: Herhangi iki $x \in C$ kod sözcüğü için, aynı sayıdaki G ve C 'lerin sayısıdır.

Hamming kısıtlaması, ters sıralı kısıtlaması ve ters sıralı tamlayan kısıtlamaları farklı iplikçikler arasındaki istenmeyen hibritleşmeyi önlemek içindir. Sabit GC içeriği kısıtlaması tüm kod sözcüklerini sağlayan sabit GC içeriği benzer termodinamik karakteristiğe sahiptir (Dixita vd., 2016).

DNA, dört temel baz olan A (Adenin), T (Timin), G (Guanin), C (Sitozin)'den oluşan çift sarmallı bir yapıdır. DNA yoğun baz birikimi ve kendi kendini çoğaltma ve tamamlama yönünden zengin bir hesaplama kaynağıdır. Dört temel baz olan $A - T - G - C$ arasında $A - T$ ve $G - C$ tamamlanması vardır. DNA molekülünün bu elverişli yapısı sonlu cisimler ve sonlu halkalar üzerinde kodlama teorisine katkıda bulunmuştur. Bu çalışmalar öncelikle 4 elemanlı cisim olan $GF(4)$ üzerinde başlamıştır (Gaborit, King, 2005; Abualrub, Ghayeb, Zeng, 2006). Daha sonra bu çalışmalar 4 elemanlı sonlu halkalar üzerine taşınmıştır (Liang, Wang, 2015; Siap, Abualrub, Ghayeb, 2008; Siap, Abualrub, Ghayeb, 2009; Guenda, Gulliver, 2013). Farklı eleman sayılarına sahip sonlu halkalar üzerinde çalışmalar günümüze kadar devam etmiştir (Bayram, Öztaş, Şiap, 2015; Bennenni, Guenda, Mesnager, 2015; Gaborit, King, 2005; Guenda, Gulliver, Sole, 2013; Ma, Cao, Gao, 2015; Pattanayak, Sing, 2015; Pattanayak, Sing, Kumar, 2015; Pattanayak, Sing, 2016; Yıldız, Şiap, 2012; Zhu, Chen, 2015).

1.1. Tez Organizasyonu

Tezin geri kalan kısmı; Bölüm 2, tezde kullanılacak olan temel bilgiler ve kodlama teorisi ile ilgili temel teorem ve sonuçları içeren alt bölümden oluşmaktadır.

Bölüm 3’de, $\mathbb{Z}_4[u]/\langle u^2 - a \rangle$; $a = 2, a = 0$, $\mathbb{F}_4[v]/\langle v^2 - a \rangle$; $a = v, a = 1$, $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ ve $\mathbb{F}_2[u, v]/\langle u^2, v^2 - v, uv - vu \rangle$ ile adlandırılan bazı sonlu halkaların üzerinde tanımlı devirli kodların yapısı, bu yapılar üzerindeki devirli DNA kodların inşası, ve devirli DNA kodların DNA görüntüleri ile ilgili teorem ve sonuçlara yer verilmiştir.

BÖLÜM 2

TEMEL KAVRAMLAR

2.1. Cebir ile İlgili Alt Yapı

Kodlama teorisi, matematiğin bir dalı olan cebir ile ilişkidir. Dolayısıyla tezin bu bölümünde, tezin kapsamı dâhilinde kalan konularla ilgili birçok cebir kitabından alınan bazı temel tanım, teorem ve sonuçlara yer verilecektir.

2.1.1. Grup, Halka ve Cisim

2.1.1.1. Tanım:

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

$$\Delta : X \times X \rightarrow X$$

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

fonksiyonuna, X üzerinde tanımlı bir “*ikili işlem*” denir. Bir küme üzerinde en az bir ikili işlem tanımlı kümeye “*cebirsal yapı*” denir (Karakaş, 2012).

2.1.1.2. Tanım:

$G \neq \emptyset$ bir küme ve Δ , G kümesi üzerinde tanımlı bir ikili işlem olsun.

- (i) Her $a, b, c \in G$ için $a \Delta (b \Delta c) = (a \Delta b) \Delta c$,
- (ii) En az bir $e \in G$ vardır öyleki her $a \in G$ için $a \Delta e = e \Delta a = a$ ’dır.
- (iii) Her $a \in G$ için $a \Delta a^{-1} = a^{-1} \Delta a = e$ olacak şekilde en az bir $a^{-1} \in G$ vardır.

Koşulları sağlanıyorsa (G, Δ) cebirsal yapısına “*grup*” denir.

Ek olarak,

- (iv) Her $a, b \in G$ için $a \Delta b = b \Delta a$

koşulu sağlanıyor ise G grubuna “*değişmeli grup*” (veya *Abel grubu*) olarak adlandırılır (Karakaş, 2012).

2.1.1.3. Tanım:

Boştan farklı bir K kümesi ve bir $f: K \rightarrow K$ fonksiyonu verilsin. Eğer f fonksiyonu birebir ve örten ise, f fonksiyonuna K kümesi üzerinde bir “*permütasyon*” denir. Özel olarak, $K_n = \{1, 2, \dots, n\}$ kümesi üzerindeki tüm permütasyonların grubu S_n ile gösterilir ve S_n kümesine “ n –inci *simetrik grup*” denir. S_n ’deki herhangi bir α permütasyonu, $\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}$ biçiminde de gösterilir (Karakaş, 2012).

2.1.1.4. Tanım:

$R \neq \emptyset$ bir küme ve “+” ve “.”, R üzerinde tanımlı iki ikili işlem olsun.

- (i) $(R, +)$ değişmeli bir gruptur,
- (ii) Her $a, b, c \in R$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- (iii) Her $a, b, c \in R$ için $(a + b) \cdot c = a \cdot c + b \cdot c$ ve $a \cdot (b + c) = a \cdot b + a \cdot c$

koşulları sağlanıyor ise $(R, +, \cdot)$ cebirsel yapısına “*halka*” denir.

Ek olarak,

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

koşulu sağlanıyor ise R halkasına “*değişmeli halka*” denir.

R halkası,

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

koşulunu sağlayan bir 1_R elemanını içeriyorsa, R halkasına “*birimli halka*” denir (Hungerford, 1973).

2.1.1.5. Tanım:

R birimli bir halka olmak üzere $a \in R$ nin tersi varsa a ’ya R nin bir birimsel elemanı denir.

2.1.1.6. Tanım:

$a \in R$ sıfırdan farklı bir eleman olsun. Eğer R halkasında, $a \cdot b = 0_R$ ($b \cdot a = 0_R$) sağlayan sıfırdan farklı bir $b \in R$ elemanı varsa a elemanına R halkasının “*sol (sağ)*”

bölen”i denir. R halkasının hem sağ hem de sol bölen elemanına “*sıfır bölen*” denir (Hungerford, 1973).

2.1.1.7. Tanım:

$1_R \neq 0_R$ olacak şekilde R halkası birimli ve değişmeli bir halka olsun. R halkasının sıfır böleni yoksa R halkasına bir “*tamlık bölgesi*” denir. $1_D \neq 0_D$ birim elemanı olan D halkasının sıfırdan farklı her elemanı tersinir (birimsel) ise D halkasına “*bölme halkası (division ring)*” denir. Her “*cisim*” değişmeli bir bölme halkasıdır (Hungerford, 1973).

2.1.1.8. Tanım:

R ve S iki halka olmak üzere her $a, b \in R$ için $f(a + b) = f(a) + f(b)$ ve $f(ab) = f(a)f(b)$ koşullarını sağlayan $f: R \rightarrow S$ fonksiyonuna “*halka homomorfizması*” denir (Hungerford, 1973).

2.1.1.9. Tanım:

$f: R \rightarrow S$ halka homomorfizması;

- (i) $1 \mapsto 1$ ise f bir “*monomorfizma*”,
- (ii) Örten ise f bir “*epimorfizma*”,
- (iii) $1 \mapsto 1$ ve örten ise f bir “*izomorfizma*” olarak adlandırılır (Bu durumda, R ve S halkaları birbirine *izomorftur* denir ve $R \cong S$ ile gösterilir).

R bir halka olmak üzere, $f: R \rightarrow R$ bir izomorfizma ise f ’ye R ’nin “*otomorfizması*” denir (Hungerford, 1973).

2.1.1.10. Tanım:

0_D , D halkasının etkisiz elemanı olmak üzere, $f: R \rightarrow D$ bir halka homomorfizması ise

$$\text{Çek } f = \{a \in R: f(a) = 0_D\}$$

kümesine f ’nin “*çekirdeği*” denir (Çallıalp, 2013).

2.1.1.11. Tanım:

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

2.1.1.12. Tanım:

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

$$(i) \quad a - b \in I \text{ ve}$$

$$(ii) \quad ra \in I \text{ (} ar \in I \text{)}$$

olmasıdır (Hungerford, 1973).

2.1.1.13. Tanım:

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

X kümesinin elemanlarına (X) idealinin “üreteçleri” denir. X bir sonlu küme iken (X) idealine “sonlu üretilmiştir” denir. $X = \{x\}$ tek elemanlı bir küme ise “esas ideal” denir. Bütün idealleri esas ideal olan halkaya “esas ideal halkası” denir. Esas ideal halkası, tamlık bölgesi ise bu halkaya “esas ideal bölgesi” denir (Hungerford, 1973).

2.1.1.14. Teorem:

R ve S iki halka olmak üzere, $f: R \rightarrow S$ bir halka homomorfizması olsun. Çek f kümesi R halkasının bir idealidir. Aksine, I , R halkasının ideali ise $\varphi: R \rightarrow R/I$, $\varphi(r) = r + I = \bar{r}$ dönüşümü I çekirdek kümesi ile bir epimorfizmadır. Bu dönüşüme “doğal epimorfizma” (ya da *projeksiyon dönüşümü*) denir. (Hungerford, 1973).

2.1.1.15. Teorem:

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

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

koşulu sağlanıyorsa P idealine “asal ideal”dir denir. (Hungerford, 1973).

2.1.1.16. Teorem:

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

2.1.1.17. Tanım:

S , R halkasının bir ideali olsun. Eęer $S \neq R$ ve her $S \subset D \subset R$ kořulunu saęlayan D ideali için $D = S$ ya da $D = R$ oluyorsa S 'ye R halkasının bir “maksimal ideali” denir (Hungerford, 1973).

2.1.1.18. Teorem:

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

- (i) S maksimal ideal ve R deęiřmeli ise R/S bölüm halkası bir cisimdir.
- (ii) R/S bölüm halkası bir cisim ise S maksimal idealdir (Hungerford, 1973).

2.1.1.19. Teorem:

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

2.1.1.20. Tanım:

Tek maksimal ideale sahip birimli ve deęiřmeli halkaya “yerel (local) halka” denir. Birden fazla sonlu sayıda maksimal ideali olan birimli deęiřmeli halkaya ise “yarı yerel (semilocal) halka” denir (Jitman, Udomkavanich, Ling, 2012).

2.1.1.21. Tanım:

R bir halka ve $0 \neq a \in R$ olmak üzere $m \cdot a = 0$ eřitlięini saęlayan en küçük m pozitif tam sayısına R 'nin karakteristięi denir ve $kar(R)$ ile gösterilir.

2.1.1.22. Tanım:

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

2.1.1.23. Önerme:

R sonlu zincir halkası ise R ’nin bütün idealleri esas idealdir ve R halkası tek maksimal ideale sahiptir. γ , R halkasının maksimal idealinin üretici olmak üzere R halkasının tüm idealleri

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

biçiminde zincir formundadır. Burada k , R halkasının “nilpotentlik derecesi”dir (Jitman, vd., 2012).

2.1.1.24. Tanım:

$(R, +, \cdot)$ birimli ve değişmeli bir halka olsun. $R - \{0\} = R^*$ olmak üzere $(R^*, \cdot)$ bir grup ise R ’ye “cisim” denir (Jitman, vd., 2012).

2.1.1.25. Tanım:

Sonlu elemanlı cisme sonlu cisim denir (Hungerford, 1973).

2.1.1.26. Teorem:

$q \in \mathbb{Z}$ ve $1 < q$ olmak üzere q elemanlı bir cismin var olması için gerekli ve yeterli koşul q sayısının bir asalın kuvveti şeklinde yazılmasıdır (Hungerford, 1973).

2.1.1.27. Tanım:

p bir asal sayı $n \in \mathbb{N}$ olmak üzere $q = p^n$ elemanlı cisme Galois cismi denir. $\mathbb{GF}(q)$ veya $\mathbb{F}_q$ ile gösterilir (Hungerford, 1973).

2.1.1.28. Teorem:

$\mathbb{F}$ sonlu bir cisim olmak üzere $\mathbb{F}$ cisminin karakteristiği asal bir sayıdır (Hungerford, 1973).

2.1.1.29. Tanım:

F sonlu bir cisim olmak üzere $F^* = \langle \alpha \rangle$ eşitliğini gerçekleyen α elemanına cismin “*primitif (ilkel) eleman*”, primitif (ilkel) elemanı kök kabul eden polinoma “*primitif (ilkel) polinom*” adı verilir.

2.1.1.30. Teorem:

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

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

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

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

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

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

Bu $R[x]$ halkasına “*polinom halkası*” denir ve halkanın elemanlarına “*polinom*” denir (Hungerford, 1973).

2.1.1.31. Teorem:

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

(i) 1_R elemanı dizinin $(n+1)$ -inci bileşeni olmak üzere $x^n = (0, 0, \dots, 0, 1_R, 0, \dots)$,

(ii) r elemanı dizinin $(n+1)$ -inci bileşeni olmak üzere her $n \geq 0$ için, $rx^n = x^n r = (0, \dots, 0, r, 0, \dots)$ olmak üzere

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

2.1.1.32. Tanım:

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

olan polinoma “monik polinom” denir. $x = (0, 1_R, 0, 0, \dots)$ elemanına “bilinmeyen (indeterminate)” denir (Hungerford, 1973).

2.1.1.33. Tanım:

Katsayıları F cismi üzerinde alınan sabitten farklı bir $f(x)$ polinomu için $der(g(x)), der(h(x)) \leq der(f(x))$ ve $f(x) = g(x)h(x)$ olmak üzere $g(x), h(x) \in F[x]$ polinomları var ise bu durumda $f(x)$ ‘e indirgenebilir polinom, aksi halde indirgenemez polinom denir (Ling ve Xing 2004).

2.1.1.34. Tanım:

$p(x) \in \mathbb{F}_q[x]$ polinomu $der(p(x)) = d$ olan asal bir polinom olmak üzere $\mathbb{F}_q[x]/\langle p(x) \rangle$ bölüm halkası bir cisimdir ve $\mathbb{F}_q[x]/\langle p(x) \rangle = \{r(x) + \langle p(x) \rangle \mid d_{err} < d, r(x) \in \mathbb{F}_q[x]\}$ şeklindedir (Karakaş, 2012).

2.1.2. Modül ve Vektör Uzayı

2.1.2.1. Tanım:

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

$$\cdot : R \times K \rightarrow K$$

$$(r, k) \mapsto r \cdot k$$

biçiminde tanımlı fonksiyon, her $r, s \in R$ ve her $k, b \in K$ için,

$$(i) \quad r \cdot (k + b) = r \cdot k + r \cdot b$$

$$(ii) \quad (r + s) \cdot k = r \cdot k + s \cdot k$$

$$(iii) \quad r(s \cdot k) = (rs) \cdot k$$

koşullarını sağlıyorsa K ’ya bir “(sol) R – modül” denir.

Eğer $1_R \in R$ ve

$$(iv) \quad \text{Her } k \text{ için } 1_R \cdot k = k \text{ koşulu sağlanıyor ise}$$

K ’ya “birimsel R – modül (unitary R – modül)” denir. Eğer R bir cisim ise birimli

R – modüle bir “(sol) vektör uzayı” denir (Hungerford, 1973).

Bu tanım,

$$\cdot : K \times R \rightarrow K$$

$$(k, r) \mapsto a \cdot k$$

tanımlı fonksiyon ile (sağ) R – modül de benzer şekilde ifade edilebilir.

2.1.2.2. Tanım:

A ve B , R halkası üzerinde iki modül olsun. Her $a, c \in A$ ve her $r \in R$ için $f(a + c) = f(a) + f(c)$ ve $f(ra) = rf(a)$ koşullarını sağlayan $f: A \rightarrow B$ fonksiyonuna bir “ R -modül homomorfizması” denir (Hungerford, 1973).

2.1.2.3. Tanım:

R bir halka, N kümesi bir R -modül ve M kümesi N ’nin boş kümeden farklı bir alt kümesi olsun. M kümesi, N ’nin toplamsal alt grubu ve her $r \in R$, $m \in M$ için $rm \in M$ oluyorsa, M ’ye N ’nin bir “alt modülü” denir. Bir kesir halkası üzerindeki bir vektör uzayın alt modülüne “alt uzay” denir (Hungerford, 1973).

2.1.2.4. Tanım:

A bir R -modül ve B kümesi A ’nin bir alt kümesi ve $n \in \mathbb{N}$ olsun.

- (i) B kümesi A ’yi üretir. Yani her $x \in A$ için, $a_1, a_2, \dots, a_n \in R$, $n \in \mathbb{N}$ olmak üzere $x = a_1x_1 + a_2x_2 + \dots + a_nx_n$ olacak şekilde $x_1, x_2, \dots, x_n \in B$ vardır.
- (ii) B kümesi doğrusal bağımsızdır. Yani $a_1, a_2, \dots, a_n \in R$ ve $x_1, x_2, \dots, x_n \in B$ için $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$ iken $a_1 = a_2 = \dots = a_n = 0$.

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

2.1.2.5. Tanım:

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

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

koşulunu sağlayan $c_1, c_2, \dots, c_n \in F$ skalerleri varsa θ vektörüne $\alpha_1, \alpha_2, \dots, \alpha_n \in V$ vektörlerinin “doğrusal birleşimi” denir (Hoffman, vd., 1971).

2.1.2.6. Tanım:

V , F cismi üzerinde bir vektör uzayı ve $K \subseteq V$ alt kümesi olsun. K kümesi V üzerindeki vektör toplamı ve skalerle çarpma işlemlerine göre bir vektör uzayı ise K kümesine “ V ’nin bir alt uzayı” denir (Hoffman, vd., 1971).

2.1.2.7. Teorem:

V, F cismi üzerinde bir vektör uzayı ve $K \subseteq V$ alt kümesi olsun. K kümesinin V 'nin bir alt uzayı olması için gerekli ve yeterli koşul her $\alpha, \beta \in K$ ve her $c \in F$ için $c\alpha + \beta \in K$ olmasıdır (Hoffman, vd., 1971).

2.1.2.8. Tanım:

V bir vektör uzayı ve $T \subseteq V$ alt kümesi olsun. V vektör uzayının T 'yi kapsayan tüm alt uzaylarının arakesiti W 'ye " *T tarafından gerilen alt uzay*" denir. $T = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ sonlu kümesi için W 'ya " *$\alpha_1, \alpha_2, \dots, \alpha_n$ elemanları ile gerilen alt uzay*" denir (Hoffman, vd., 1971).

2.1.2.9. Teorem:

Herhangi bir vektör uzayının boş kümeden farklı T kümesi ile gerilen alt uzayı, T 'deki vektörlerin tüm doğrusal kombinasyonlarının kümesidir (Hoffman, vd., 1971).

2.1.2.10. Tanım:

V, F cismi üzerinde bir vektör uzayı ve $T \subseteq V$ alt kümesi olsun. Eğer,

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

koşulunu sağlayan $\alpha_1, \alpha_2, \dots, \alpha_n \in T$ vektörleri ve hepsi 0 olmayan $c_1, c_2, \dots, c_n \in F$ skalerleri varsa, T kümesine "*doğrusal bağımlıdır*" aksi halde, "*doğrusal bağımsızdır*" denir. Buna denk tanım şu şekildedir: T kümesinin vektörlerinin doğrusal bağımsız olması için gerekli ve yeterli koşul her $\alpha_1, \alpha_2, \dots, \alpha_n \in T$ için $c_1\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n = 0$ eşitliğini sağlayan tüm i 'ler için $c_i = 0$ olmasıdır (Hoffman, vd., 1971).

2.1.2.11. Tanım:

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

2.2. Kodlama Teorisi ile İlgili Alt Yapı

Kodlama teorisi, mesajın kodlanmasından başlar ve alıcıya ulaşana kadar (hatta varsa hataların tespiti ve düzeltilmesine kadar süren) bütün aşamaları kapsamaktadır. Bu bölümde, kodlama teorisi ile ilgili genel tanım ve teoremlere yer verilecektir.

2.2.1. Lineer Kodlar

$\mathbb{F}_q^n$ kümesi, $\mathbb{F}_q$ sonlu cismi üzerindeki sıralı n 'lilerin kümesi olsun. Bu küme $\mathbb{F}_q$ -vektör uzayıdır. $\mathbb{F}_q^n$ kümesinin M elemanlı bir C alt kümesine, $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı (n, M) kodu denir. $(a_1, a_2, \dots, a_n) \in \mathbb{F}_q^n$ vektörü $a_1 a_2 \dots a_n$ formunda da gösterilebilir ve C kümesindeki vektörlere “kod sözcükleri” denir. C kümesi $\mathbb{F}_q^n$ vektör uzayının k boyutlu olan bir alt uzayı ise, C kümesine $\mathbb{F}_q$ sonlu cismi üzerinde $[n, k]$ “lineer kodu” denir. C lineer kodunun q^k tane kod sözcüğü vardır. Satırları C alt uzayının bir tabanının bileşenleri ile oluşturulan ile yazılan bir $k \times n$ 'lik G matrisine, C $[n, k]$ lineer kodunun “üreteç matrisi” denir. Bir G üreteç matrisinin her doğrusal bağımsız k sütununun kümesi için onunla bağlantılı koordinatlarının kümesi C 'nin “bilgi kümesini” oluşturur. $r = n - k$ olmak üzere, r 'ye C 'nin “kalani (redundancy)” denir. I_k matrisi $k \times k$ 'lık birim matris olmak üzere, kodun $[I_k | A]$ formundaki üreteç matrisine “standart form” denir. $C = \{x \in \mathbb{F}_q^n \mid Hx^T = 0\}$ ile tanımlı $(n - k) \times k$ 'lık H matrisine, C $[n, k]$ lineer kodu için “kontrol matrisi (parity-check matrisi)” denir. Bir lineer kod üreteç matris veya kontrol matris ile ifade edilir (Huffman, Cary, Pless, 2003).

2.2.1.1. Teorem:

Eğer $G = [I_k | A]$ matrisi bir C $[n, k]$ lineer kodunun standart formdaki üreteç matrisi ise, $H = [-A^T | I_k]$ matrisi C kodunun bir kontrol matrisidir (Huffman, vd., 2003).

2.2.1.2. Teorem:

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

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

kümesinin bir R – alt modülü ise C 'ye R halkası üzerinde tanımlı “lineer kod” adı verilir. R^n kümesinin herhangi bir elemanına “sözcük”, C kodunun herhangi bir elemanına “kod sözcüğü” denir (Huffman, vd., 2003).

2.2.2. Ağırlık ve Uzaklıklar

Bir kodun minimum uzaklık parametresi en önemli öğelerinden biridir. Kodun minimum uzaklığı, kodun hatayı tespit etme ve düzeltme kapasitesi hakkında bilgi verir.

2.2.2.1. Tanım:

Her $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$ için

$$d: \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{N} \cup \{0\},$$

$$(x, y) \mapsto d(x, y) = |\{i \mid x_i \neq y_i\}|$$

dönüşümüne “*Hamming uzaklığı*” denir (Ling, vd., 2004).

2.2.2.2. Önerme:

Hamming uzaklığı;

- (i) Her $x, y \in \mathbb{F}_q^n$ için $0 \leq d(x, y) \leq n$,
- (ii) Her $x, y \in \mathbb{F}_q^n$ için $d(x, y) = 0$ olması için gerekli ve yeterli koşul $x = y$ olmasıdır.
- (iii) Her $x, y \in \mathbb{F}_q^n$ için $d(x, y) = d(y, x)$
- (iv) Her $x, y, z \in \mathbb{F}_q^n$ için $d(x, z) \leq d(x, y) + d(y, z)$ (üçgen eşitsizliği)

özelliklerini sağlayan bir metriktir (Ling, vd., 2004).

2.2.2.3. Tanım:

C bir kod olmak üzere,

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

sayısına C kodunun minimum uzaklığı denir (Ling, vd., 2004).

2.2.2.4. Tanım:

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

2.2.2.5. Teorem:

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

2.2.2.6. Tanım:

$x, \mathbb{F}_q^n$ vektör uzayının herhangi bir elemanı olmak üzere x elemanının sıfırdan farklı bileşenlerinin sayısına x elemanının Hamming ağırlığı denir ve $wt(x)$ ile gösterilir (Ling, vd., 2004).

2.2.2.7. Lemma:

Herhangi bir $x, y \in \mathbb{F}_q^n$ için $d(x, y) = wt(x - y)$ 'dir (Ling, vd., 2004).

2.2.2.8. Tanım:

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

2.2.2.9. Teorem:

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

2.2.3. Devirli Kodlar

2.2.3.1. Tanım:

$C, \mathbb{F}_q^n$ vektör uzayının bir alt kümesi olsun. Her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ için $\sigma(c) = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$ olmak üzere C kümesine "*devirli küme*" denir. C , bir lineer kod ve devirli bir küme ise bu koda "*devirli kod*" denir (Hill, 1986).

2.2.3.2. Teorem:

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

2.2.3.3. Teorem:

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

$a = (a_0, a_1, \dots, a_{n-1}) \mapsto \pi(a) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle = \overline{a(x)}$ ile tanımlı π vektör uzayı izomorfizması olmak üzere, $C, \mathbb{F}_q^n$ üzerinde tanımlı n uzunluğunda bir devirli kod olması için gerekli ve yeterli koşul $I = \pi(C)$ nin $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ halkasının bir ideali olmasıdır (Ling, vd., 2004).

NOT: π dönüşümü yardımıyla, C kodunun herhangi bir $a = (a_0, a_1, \dots, a_{n-1})$ elemanına $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ bölüm halkasının bir $\pi(a) = \overline{a(x)} = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle$ denklik sınıfı karşılık getirilir. Fakat kolay ve sade gösterim için $a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle$ denklik sınıfı yerine $a(x) = a_0 + a_1x + \dots +$

$a_{n-1}x^{n-1}$ polinomu kullanılacaktır. Bu durumda, bir devirli kodun elemanlarını onlara karşılık gelen polinom gösterimleri ile yazmak mümkündür.

2.2.3.4. Not:

R sonlu bir halka olmak üzere

$$\pi: R^n \rightarrow R[x]/\langle x^n - 1 \rangle$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1} + \langle x^n - 1 \rangle = \overline{c(x)}$$

π , R -modül izomorfizması tanımlanarak R halkası üzerinde tanımlı n uzunluğundaki devirli kodlar ile $R[x]/\langle x^n - 1 \rangle$ halkasının $\pi(C)$ idealleri arasında benzer bir ilişki kurulmuştur.

2.2.3.5. Teorem:

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

- (i) $g(x)$ polinomu I idealinin bir üreticidir ve bu monik polinom tektir.
- (ii) $g(x)$ polinomu $x^n - 1$ polinomunu böler (Ling, vd., 2004).

2.2.3.6. Tanım:

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

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

biçimindedir (Ling, vd., 2004).

2.2.3.7. Teorem:

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

2.2.3.8. Lemma:

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

2.2.3.9. Teorem:

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

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

biçimindedir (Hill, 1986).

2.2.4. Devirli DNA Kodlar İçin Alt Yapı

2.2.4.1. Tanım:

T sonlu halka, her $s = (s_0, s_1, \dots, s_{n-1}) \in T^n$ için, $(s_{n-1}, s_{n-2}, \dots, s_1, s_0) \in T^n$ vektörüne s 'in ters sıralısı (reverse) denir ve s^R biçiminde gösterilir. C kodu T üzerinde bir lineer kod olmak üzere, eğer her $s \in C$ için $s^R \in C$ oluyorsa, C koduna ters sıralı kod denir.

s sözcüğüne karşılık gelen polinom temsili $s(x) = s_0 + s_1x + \dots + s_{n-1}x^{n-1}$ olmak üzere $s(x)$ elemanının ters sıralısı $s(x)^R = s_{n-1} + s_{n-2}x + \dots + s_0x^{n-1}$ şeklinde gösterilirse ters sıralı kod, her $s(x) \in \pi(C)$ için $s(x)^R \in \pi(C)$ olması şeklinde de tanımlanır (Yıldız B., vd., 2012).

2.2.4.2. Tanım:

T sonlu halka, her $s = (s_0, s_1, \dots, s_{n-1}) \in T^n$ için $\bar{s}_i, s_i \in T, i = 0, 1, \dots, n-1$ elemanının tamamlayıcı olmak üzere $(\bar{s}_0, \bar{s}_1, \dots, \bar{s}_{n-1}) \in T^n$ vektörüne s 'in tamamlayıcı denir ve s^C biçiminde gösterilir. C kodu T üzerinde bir lineer kod olmak üzere, eğer her $s \in C$ için $s^C \in C$ oluyorsa, C kodu tamamlayan koddur denir. s sözcüğüne karşılık gelen polinom temsili $s(x) = s_0 + s_1x + \dots + s_{n-1}x^{n-1}$ olmak üzere $s(x)$ elemanının tamamlayıcı $s^C(x) = \bar{s}_0 + \bar{s}_1x + \dots + \bar{s}_{n-1}x^{n-1}$ şeklinde gösterilirse C tamamlayan kod tanımı her $s(x) \in \pi(C)$ için $s(x)^C \in \pi(C)$ olması şeklinde de tanımlanır (Yıldız B., vd., 2012).

2.2.4.3. Tanım:

T sonlu halka, her $s = (s_0, s_1, \dots, s_{n-1}) \in T^n$ için, $(\overline{s_{n-1}}, \overline{s_{n-2}}, \dots, \overline{s_0}) \in T^n$ vektörüne s 'in ters sıralı tamamlayıcı denir ve s^{RC} biçiminde gösterilir. C kodu T üzerinde tanımlı bir lineer kod olmak üzere, eğer her $s \in C$ için $s^{RC} \in C$ oluyorsa, C koduna ters sıralı tamamlayıcı kod denir. s sözüğüne karşılık gelen polinom temsili $s(x) = s_0 + s_1x + \dots + s_{n-1}x^{n-1}$ olmak üzere $s(x)$ elemanının ters sıralı tamamlayıcı $s^{RC}(x) = \overline{s_{n-1}} + \overline{s_{n-2}}x + \dots + \overline{s_0}x^{n-1}$ şeklinde gösterilirse C , ters sıralı tamamlayıcı kod her $s(x) \in \pi(C)$ için $s(x)^{RC} \in \pi(C)$ olması şeklinde de tanımlanır (Yıldız B., vd., 2012).

2.2.4.4. Tanım:

$a_s \neq 0$ olmak üzere, $f(x) = a_0 + a_1x + \dots + a_sx^s$ olsun. $f^*(x) = x^s f(\frac{1}{x})$ polinomuna $f(x)$ polinomunun “*kendine ters sıralı (reciprocal) polinomu*” denir (Yıldız B., vd., 2012).

2.2.4.5. Tanım:

R bir halka olsun. $f^*(x)$, $f(x) = a_0 + a_1x + \dots + a_rx^r \in R[x]$ polinomunun reciprocal polinomu ve m terslenebilir bir eleman olmak üzere $f^*(x) = mf(x)$ oluyorsa, $f(x)$ polinomuna “*kendine ters sıralısına eş (self-reciprocal) polinom*” denir (Yıldız, vd., 2012).

2.2.4.6. Tanım:

C, T halkası üzerinde tanımlı n uzunluğunda bir devirli kod olsun. Her $s \in C$ için $s^{RC} \in C$ ise bu durumda C 'ye devirli DNA kod denir (Yıldız, vd., 2012).

BÖLÜM 3

BAZI ÖZEL HALKALAR ÜZERİNDE TANIMLI DEVİRLİ DNA KODLAR

3.1. Giriş

Öncelikle $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ ve $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ sonlu zincir halkaları üzerinde tek uzunluklu devirli kodların yapıları sırasıyla B. Yıldız, vd. ve F. Ma, vd. tarafından belirlenerek bir devirli kodun ters sıralı tamamlayan olması için gerekli ve yeterli koşullar verilmiştir. Ayrıca bir dönüşüm yardımıyla devirli DNA kodların DNA görüntüleri belirlenmiştir. Bir diğer zincir halkası $\mathbb{Z}_4[w]/\langle w^2 + 2 \rangle$ üzerinde tanımlı devirli kodların yapısı A. Dertli ve Y. Çengellenmiş tarafından belirlenerek devirli bir kodun ters sıralı tamamlayan olması için gerekli ve yeterli koşul verilmiştir.

Sonlu zincir olmayan $\mathbb{F}_4 + v\mathbb{F}_4$; $v^2 = v$ halkası üzerinde A. Bayram, E.S. Öztaş ve İ. Şiap devirli kodların cebirsel yapısını vererek devirli bir kodun ters sıralı olması için gerekli ve yeterli koşulu belirlemişlerdir. Ayrıca ters sıralama problemine bir çözüm olarak bir dönüşüm yardımıyla ters sıralı DNA ve ters sıralı tamamlayan DNA kodları elde etmişlerdir. 2015 yılında Zhu ve Chen sonlu zincir olmayan $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$; $u^2 = 0, v^2 = v, uv = vu$ halkası üzerinde tanımlı keyfi uzunluklu devirli kodların yapısını vererek bir devirli kodun ters sıralı ve ters sıralı tamamlayan olması için gerekli ve yeterli koşulları ifade etmişlerdir. Ters sıralı ve ters sıralı tamamlayan DNA kodları elde etmişlerdir. 2015 yılında Pattanayak tarafından yapılan çalışmada sonlu zincir olmayan $\mathbb{Z}_4 + u\mathbb{Z}_4$; $u^2 = 0$ halkası üzerinde tanımlı tek uzunluklu devirli kodların cebirsel yapısını belirleyerek bu devirli kodların ters sıralı ve ters sıralı tamamlayan olması için gerekli ve yeterli koşulları belirlemişlerdir.

3.2. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar ve Tek Uzunluklu Devirli DNA Kodların DNA Görüntüleri

2012 yılında B.Yıldız ve İ.Şiap $R = \mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ halkası üzerinde tanımlı tek uzunluğundaki devirli kodun ters sıralı tamamlayan olması için gerekli ve yeterli olma koşulunu vermiştir. Ardından R halkası üzerinde tanımlı tek uzunluğuna sahip devirli ters sıralı tamamlayan kodların (devirli DNA kodların) bir dönüşüm yardımıyla DNA görüntülerini belirlemiştir.

3.2.1. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Kümesinin Cebirsel Yapısı

$\mathbb{F}_2[u]/\langle u^4 - 1 \rangle = \{a + bu + cu^2 + du^3 + \langle u^4 - 1 \rangle : a, b, c, d \in \mathbb{F}_2\}$ bölüm halkası için, $u^4 = 1$ koşulları göz önüne alındığında,
 $a + bu + cu^2 + du^3 + \langle 0 \rangle = \{a + bu + cu^2 + du^3 + 0m : a, b, c, d \in \mathbb{F}_2, m \in \mathbb{F}_2[u]\} = \{a + bu + cu^2 + du^3\}$ olacağından,

$\mathbb{F}_2[u]/\langle u^4 - 1 \rangle = \{\{a + bu + cu^2 + du^3\} : a, b, c, d \in \mathbb{F}_2\}$ bulunur ve $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 = \{a + bu + cu^2 + du^3 + \langle u^4 - 1 \rangle : a, b, c, d \in \mathbb{F}_2\}$ kümesi de bir halkadır.

3.2.1.1. Teorem:

$$f: \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 \rightarrow \mathbb{F}_2[u]/\langle u^4 - 1 \rangle$$

$$a + bu + cu^2 + du^3 \mapsto f(a + bu + cu^2 + du^3) = \{a + bu + cu^2 + du^3\}$$

dönüşümü bir izomorfizmadır.

3.2.1.2. Sonuç:

$$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 \cong \mathbb{F}_2[u]/\langle u^4 - 1 \rangle \text{ dir.}$$

Üstelik $R = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2, u^4 = 1$ olmak üzere,

her $(a + bu + cu^2 + du^3), (a' + b'u + c'u^2 + d'u^3) \in R$ elemanları için;

$$\begin{aligned} (a + bu + cu^2 + du^3) + (a' + b'u + c'u^2 + d'u^3) &= (a + a') + \dots + (d + d')u^3 \\ (a + bu + cu^2 + du^3) \cdot (a' + b'u + c'u^2 + d'u^3) &= (aa' + bd' + cc' + db') + u(ab' + ba' + cd' + dc') \\ &\quad + u^2(ac' + bb' + ca' + dd') + u^3(ad' + bc' + cb' + da') \end{aligned}$$

şeklinde tanımlanan $+$ ve $\cdot$ işlemlerine göre 16 elemanlı, karakteristiği 2 olan değişmeli bir sonlu zincir halkasıdır.

R halkasının idealleri;

$\{0\} = (1+u)^4R \subset (1+u)^3R \subset (1+u)^2R \subset (1+u)R \subset R$ şeklindedir ve tek maksimal ideali $\langle u+1 \rangle$ olduğundan, $R/\langle u+1 \rangle \cong \mathbb{F}_2$ 'dir.

R halkasının birimsellerinin oluşturduğu;

$\mathcal{U}(R) = \{1, u, u^2, u^3, 1+u+u^2, 1+u^2+u^3, 1+u+u^3, u+u^2+u^3\} = \langle u, 1+u+u^3 \rangle$ kümesi çarpma işlemine göre bir gruptur.

R halkası üzerinde tanımlı n uzunluğuna sahip bir C kodu R^n 'nin bir alt kümesidir. R halkası üzerinde tanımlı n uzunluğuna sahip bir C lineer kodu R^n 'nin bir alt modülüdür. R halkasının idealleri yapısının özelliği sayesinde R üzerinde tanımlı n uzunluğa sahip her C lineer kodunun üreteç matrisi A_i, B_j, C_k ve D_1 bileşenleri R halkasından alınan matrisler olmak üzere

$$G = \begin{bmatrix} I_{k_1} & A_1 & A_2 & A_3 & A_4 \\ 0 & (1+u)I_{k_2} & (1+u)B_1 & (1+u)B_2 & (1+u)B_3 \\ 0 & 0 & (1+u)^2I_{k_3} & (1+u)^2C_1 & (1+u)^2C_2 \\ 0 & 0 & 0 & 0 & (1+u)^3D_1 \end{bmatrix}$$

şeklinde bir matrise denktir. Böyle bir üreteç matrise sahip lineer koda (k_1, k_2, k_3, k_4) tipinde bir kod adı verilir ve C lineer kodunun eleman sayısı $|C| = 2^{4k_1+3k_2+2k_3+k_4}$ 'dir (Yıldız vd., 2012).

3.2.2. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkası Üzerinde Tanımlı Devirli Kodlar

3.2.2.1. Teorem:

n tek olsun. $0 \leq i \leq 4$ olmak üzere $F_i(x) \in \mathbb{F}_2[x]$ polinomları $x^n - 1 = F_0(x) \dots F_4(x)$ i sağlayan basit, ikişerli aralarında asal ve indirgenemez polinomlar olsun. C, R halkası üzerinde tanımlı n uzunluğunda bir devirli kod ise bu durumda $i = 0, 1, \dots, 4$, $\widehat{F_i(x)} = (x^n - 1)/F_i(x)$ olmak üzere $\pi(C) = \langle \widehat{F_1(x)}, (1+u)\widehat{F_2(x)}, (1+u)^2\widehat{F_3(x)}, (1+u)^3\widehat{F_4(x)} \rangle$ şeklindedir (Yıldız vd., 2012).

3.2.2.2. Sonuç:

C, R halkası üzerinde tanımlı n uzunluğunda devirli bir kod olsun. Bu durumda $f_3(x)|f_2(x)|f_1(x)|f_0(x)|(x^n - 1)$ olmak üzere $f_0(x), f_1(x), f_2(x), f_3(x) \in \mathbb{F}_2[x]$

polinomları vardır ve $\pi(C) = \langle f_0(x), (1+u)f_1(x), (1+u)^2f_2(x), (1+u)^3f_3(x) \rangle$ ‘tir (Yıldız vd., 2012).

3.2.2.3. Sonuç:

C , R halkası üzerinde tanımlı tek uzunluğunda devirli bir kod olsun. Bu durumda $C = \langle g(x) \rangle$ olacak şekilde $g(x) \in R[x]/\langle x^n - 1 \rangle$ elemanı vardır (Yıldız vd., 2012).

3.2.3. $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar

$R = \mathbb{F}_2[u]/\langle u^4 - 1 \rangle = \{a + bu + cu^2 + du^3 \mid a, b, c, d \in \mathbb{F}_2\}$ olmak üzere Çizelge 3.1’de $\phi: R \rightarrow \{A, T, G, C\}^2$ birebir eşleşmesi ile $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ halkasının elemanları ile DNA çiftleri arasındaki ilişki verilmiştir (Yıldız vd., 2012).

Çizelge 3.1 $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

$0 \rightarrow AA$	$1 + u \rightarrow AT$	$1 \rightarrow GT$	$u \rightarrow AG$
$1 + u + u^2 + u^3 \rightarrow TT$	$u^2 + u^3 \rightarrow TA$	$1 + u^2 \rightarrow GG$	$u + u^2 \rightarrow GC$
$u + u^3 \rightarrow CC$	$1 + u^3 \rightarrow CG$	$1 + u + u^2 \rightarrow CT$	$1 + u^2 + u^3 \rightarrow TC$
$u^2 \rightarrow TG$	$1 + u + u^3 \rightarrow AC$	$u^3 \rightarrow GA$	$u + u^2 + u^3 \rightarrow CA$

NOT: Her bir DNA çiftine karşılık gelen R halkasının elemanının u^2 ile çarpımı DNA çiftinin ters sıralısına karşılık gelir.

3.2.3.1. Lemma:

$\bar{a}$, $a \in R$ nin tamamlayanı olmak üzere $a + \bar{a} = u^3 + u^2 + u + 1$ ’dir (Yıldız vd., 2012).

3.2.3.2. Lemma:

$f(x)$ ve $g(x)$, $R[x]$ polinom halkasının iki polinomu olsun. $\text{der } f(x) \geq \text{der } g(x)$ ve $m = \text{der } f(x) - \text{der } g(x)$ olmak üzere,

- i) $[f(x) + g(x)]^* = f(x)^* g(x)^*$
- ii) $[f(x) + g(x)]^* = f(x)^* + x^m g(x)^*$ dir (Yıldız vd., 2012).

3.2.3.3. Teorem:

$\pi(C) = \langle f_0(x), (1+u)f_1(x), (1+u)^2f_2(x), (1+u)^3f_3(x) \rangle$ kodu R halkası üzerinde tanımlı, tek uzunluğunda devirli bir kod olsun. Her $f(x) \in \pi(C)$ için $f(x)^{RC} \in \pi(C)$ ise bu durumda tüm $f_i(x)$ 'ler self-reciprocal polinom ve $(1+u+u^2+u^3)((x^n-1)/(x-1)) \in \pi(C)$ ' dir (Yıldız vd., 2012).

Kanıt:

C lineer kod olduğu için $(0,0,0, \dots, 0) \in C$ 'dir. C ters sıralı tamamlayan kod olduğu için

$$0^{RC} = (\bar{0}, \bar{0}, \bar{0}, \dots, \bar{0}) \in C \text{ dir.}$$

R 'de 0 'ın tamamlayıcı $1+u+u^2+u^3$ olduğundan $(1+u+u^2+u^3, 1+u+u^2+u^3, \dots, 1+u+u^2+u^3) \in C$ 'dir.

$f_0(x) = g_0 + g_1x + \dots + g_rx^r$ olsun. $\mathbb{F}_2[x]$ polinom halkasında $f_0(x)|x^n-1 \in \mathbb{F}_2[x]$ olduğu için $g_0 = g_r = 1$ alınabilir. Dolayısıyla,

$$f_0(x) = 1 + g_1x + \dots + x^r \text{ dir ve bu polinoma karşılık gelen vektör } (1, g_1, g_2, \dots, g_{r-1}, 1, 0, 0, \dots, 0) \text{ 'dir. } 0 \in R \text{ nin tamamlayıcı } 1+u+u^2+u^3 \text{ olduğu için,}$$

$$f_0(x)^{RC} = (1+u+u^2+u^3)(1+x+\dots+x^{n-r-2}) + (u+u^2+u^3)x^{n-r-1} + \overline{g_{r-1}}x^{n-r} + \overline{g_1}x^{n-2} + (u+u^2+u^3)x^{n-1} \in \pi(C) \text{ elde edilir.}$$

C lineer kod olduğundan, $f_0(x)^{RC} + (1+u+u^2+u^3)((x^n-1)/(x-1)) \in \pi(C)$ 'dir. Diğer bir deyişle;

$$x^{n-r-1} + (\overline{g_{r-1}} + (1+u+u^2+u^3))x^{n-r} + \dots + (\overline{g_1} + (1+u+u^2+u^3))x^{n-2} + x^{n-1})$$

$$= x^{n-r-1} [1 + (\overline{g_{r-1}} + (1+u+u^2+u^3))x + \dots + (\overline{g_1} + (1+u+u^2+u^3))x^{r-1} + x^r] \in \pi(C) \text{ 'dir. Bu polinom } x^{r+1} \text{ ile çarpılırsa } [1 + (\overline{g_{r-1}} + (1+u+u^2+u^3))x + \dots + (\overline{g_1} + (1+u+u^2+u^3))x^{r-1} + x^r] \in \pi(C) \text{ elde edilir}$$

$a \in R$ olmak üzere $\bar{a} + u^3 + u^2 + u + 1 = a$ eşitliği kullanırsa;

$f_0(x)^* = 1 + g_{r-1}x + \dots + x^r \in \pi(C)$ elde edilir. Bu nedenle $f_i(x), k_i(x) \in \mathbb{F}_2[x]$ olmak üzere,

$f_0(x)^* = f_0(x)k_0(x) + (1+u)f_1(x)k_1(x) + (1+u)^2f_2(x)k_2(x) + (1+u)^3f_3(x)k_3(x)$ şeklinde yazılabilir. $f_0(x)^* \in \mathbb{F}_2[x]$ olduğu için $k_1 = k_2 = k_3 = 0$ 'dır. $f_0(x)^* = f_0(x) \cdot k_0(x)$ 'tir. Her iki polinomun baş katsayısı ve sabit terimi 1 olduğu için $der(f_0(x)) = der(f_0(x)^*)$ 'dir. Dolayısıyla $f_0(x) = f_0(x)^*$ ' dir. Yani $f_0(x)$ self reciprocal polinomdur.

$(1+u)f_1(x) = (1+u)(1+a_1x + \dots + a_{t-1}x^{r-1} + x^t)$ olsun. Bu durumda, $(1+u)f_1(x)^{RC} = (1+u+u^2+u^3)[1+x+\dots+x^{n-t-2}] + \overline{(1+u)}x^{n-t-1} + \overline{(1+u)}a_{t-1}x^{n-t} + \dots + \overline{(1+u)}x^{n-1} \in \pi(C)$ dir.

C lineer kod olduğundan;

$(1+u)f_1(x)^{RC} + (1+u+u^2+u^3)((x^n-1)/(x-1)) \in \pi(C)$ dir. Dolayısıyla, $(1+u)x^{n-t-1} + (\overline{(1+u)}a_{t-1} + 1+u+u^2+u^3)x^{n-t} + \dots + \overline{(1+u)}x^{n-1} \in \pi(C)$ ' dir.

x^{n-t-1} parantezine alınırsa,

$x^{n-t-1}[(1+u) + (\overline{(1+u)}a_{t-1} + 1+u+u^2+u^3)x + \dots + (1+u)x^t] \in \pi(C)$ dir.

$a = 0$ ise $\overline{(1+u)}a + 1+u+u^2+u^3 = 0$, $a = 1$ ise $\overline{(1+u)}a + 1+u+u^2+u^3 = 1+u$ 'dur.

Dolayısıyla, her $a \in \mathbb{F}_2$ için $\overline{(1+u)}a + 1+u+u^2+u^3 = (1+u)a$ 'dır. Bu nedenle $(1+u)f_1(x)^* \in \pi(C)$ olduğu elde edilir. Yukarıdaki işlemler yapılırsa $f_1(x)^* = f_1(x)$ olduğu görülür. Benzer işlemler f_2 ve f_3 için de yapılarak self reciprocal polinom oldukları görülür.

3.2.3.4. Teorem:

$\mathbb{F}_2[x]$ polinom halkasında $f_3(x)|f_2(x)|f_1(x)|f_0(x)|(x^n-1)$ olmak üzere $\pi(C) = \langle f_0(x), (1+u)f_1(x), (1+u)^2f_2(x), (1+u)^3f_3(x) \rangle$ kodu R halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun. Eğer $(1+u+u^2+u^3)((x^n-1)/(x-1)) \in \pi(C)$ ve tüm $f_i(x)$ 'ler self-reciprocal polinom ise her $f(x) \in \pi(C)$ için $f(x)^{RC} \in \pi(C)$ ' dir (Yıldız vd., 2012).

Kanıt:

$f_0(x) = 1 + g_1x + \dots + x^r$ olsun. $c(x) \in \pi(C)$ alınırsa $k_i(x) \in \mathbb{F}_2[x]$ olmak üzere,

$c(x) = f_0(x)k_0(x) + (1+u)f_1(x)k_1(x) + (1+u)^2f_2(x)k_2(x) + (1+u)^3f_3(x)k_3(x)$ şeklinde yazılır. Tüm $f_i(x)$ 'lerin self-recipocal polinom olduğu kullanılırsa,

$$\begin{aligned} c(x)^* &= [f_0(x)k_0(x) + (1+u)f_1(x)k_1(x) + (1+u)^2f_2(x)k_2(x) + (1+u)^3f_3(x)k_3(x)]^* \\ &= (f_0(x)k_0(x))^* + (1+u)f_1(x)x^{m_1}(k_1(x))^* + (1+u)^2f_2(x)x^{m_2}(k_2(x))^* + \\ &(1+u)^3f_3(x)x^{m_3}(k_3(x))^* \text{ olacak şekilde } m_1, m_2, m_3 \in \mathbb{Z} \text{ vardır. Bu nedenle, her} \\ c(x) &\in \pi(C) \text{ için } c(x)^* \in \pi(C)' \text{ dir.} \end{aligned}$$

Dolayısıyla; $(1+u+u^2+u^3)((x^n-1)/(x-1)) \in \pi(C)$ olduğu için $(1+u+u^2+u^3) + (1+u+u^2+u^3)x + \dots + (1+u+u^2+u^3)x^{n-1} \in \pi(C)'$ dir. (1)

$$\begin{aligned} c(x) &= c_0 + c_1x + \dots + c_tx^t \in \pi(C) \text{ olsun. } C \text{ kodu devirli kod olduğu için,} \\ x^{n-t-1}c(x) &= c_0x^{n-t-1} + c_1x^{n-t} + \dots + c_tx^{n-1} \in \pi(C)' \text{ dir.} \end{aligned} \quad (2)$$

(1) ve (2) eşitliğinden;

$$[(1+u+u^2+u^3) + (1+u+u^2+u^3)x + \dots + (1+u+u^2+u^3)x^{n-t-2} + (c_0 + 1+u+u^2+u^3)x^{n-t-1} + \dots + (c_t + 1+u+u^2+u^3)x^{n-1}] \in \pi(C) \text{ elde edilir.}$$

$$\begin{aligned} a \in R \text{ için } a + (1+u+u^2+u^3) &= \bar{a} \text{ eşitliği kullanılarak,} \\ (1+u+u^2+u^3) + (1+u+u^2+u^3)x + \dots + (1+u+u^2+u^3)x^{n-t-2} + \\ \bar{c}_0x^{n-t-1} + \bar{c}_1x^{n-t} + \dots + \bar{c}_{t-1}x^{n-2} + \bar{c}_tx^{n-1} &\text{ elde edilir.} \end{aligned}$$

Bu da $(c(x)^*)^{RC}$ polinomuna eşittir. Dolayısıyla; $((c(x)^*)^{RC})^* = c(x)^{RC} \in \pi(C)$ elde edilir.

3.2.3.5. Sonuç:

C , n uzunluğunda R halkası üzerinde tanımlı d Hamming uzaklıklı bir devirli DNA kod olsun. Bu durumda $\phi(C)$, $2n$ uzunluğunda $\{A, T, G, C\}$ alfabesi üzerinde tanımlı en az d Hamming uzaklıklı bir DNA koddur (Yıldız vd., 2012).

3.2.3.6. Sonuç:

$g(x)|(x^n-1)$ olmak üzere, $C = \langle (1+u^2)g(x) \rangle$ kodu, n uzunluğunda R halkası üzerinde tanımlı minimum uzaklığı d olan bir devirli DNA kod ise $\phi(C)$, $2n$ uzunluğunda $\{AA, TT, GG, CC\}$ alfabesi üzerinde tanımlı en az d Hamming uzaklıklı bir lineer DNA koddur (Yıldız vd., 2012).

3.2.3.7. Sonuç:

$g(x)|(x^n - 1)$ olmak üzere, $C = \langle (1 + u^2)g(x) \rangle$ kodu, $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ halkası üzerinde tanımlı d minimum uzaklıklı, M eleman sayılı, n uzunluğunda bir devirli DNA kod ise minimum uzaklığı d , eleman sayısı M , uzunluğu n olacak şekilde bir DNA lineer kodu vardır (Yıldız vd., 2012).

3.3. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkası Üzerinde Tanımlı Tek Uzunluklu Devirli DNA Kodlar ve Devirli DNA Kodlarının DNA Görüntüleri

2015 yılında F.Ma, Y.Cao ve J. Gao; $R = \mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ sonlu halkası üzerinde tanımlı bir tek uzunluklu devirli kodun ters sıralı tamamlayan özelliğine sahip olması için gerek ve yeter koşulu vermiştir. Ardından devirli DNA kodların özel bir dönüşüm altındaki görüntüsünü bazı kısıtlamalara sahip DNA kodları olarak belirlemiştir.

3.3.1. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Kümesinin Cebirsel Yapısı

$\alpha, x^2 + x + 1$ primitif polinomunun bir kökü olmak üzere $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, 4 elemanlı sonlu bir cisim ve $u^2 = 1$ olmak üzere

$$R = \mathbb{F}_4[u]/\langle u^2 + 1 \rangle \cong \mathbb{F}_4 + u\mathbb{F}_4 = \{a + bu | a, b \in \mathbb{F}_4\} \text{ dir.}$$

R kümesi, her $a + bu, c + du \in R$ için

$$(a + bu) + (c + du) = (a + c) + (b + d)u$$

$$(a + bu).(c + du) = (ac + bd) + u(ad + bc)$$

şeklinde tanımlı $+$ ve $.$ işlemlerine göre 16 elemanlı, karakteristiği 2 olan değişmeli bir sonlu zincir halkasıdır. $\{1, 1 + u\}$ kümesi R 'nin $\mathbb{F}_4$ üzerinde bir tabanı olduğu olugu için, R halkasının her bir elemanı $a, b \in \mathbb{F}_4$ olmak üzere $a + b(1 + u)$ şeklinde tek türlü yazılabilir (Ma vd., 2015).

3.3.2. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkası Üzerinde Tanımlı Devirli Kodlar

3.3.2.1. Lemma:

C, R halkası üzerinde n uzunluğuna sahip bir devirli kod olsun.

(1) n tek ise, $a(x)|g(x)|(x^n - 1)$ ve $g(x)$ ve $a(x) \in \mathbb{F}_4[x]$ olmak üzere

$$C = \langle g(x), (1 + u)a(x) \rangle \text{ dir.}$$

(2) n çift ise;

- (a) $g(x) = a(x)$ ise $g(x) + (1 + u)p(x)|(x^n - 1)$ ve $g(x)|(x^n - 1)$, $g(x)$ ve $a(x) \in \mathbb{F}_4[x]$ olmak üzere; $C = \langle g(x) + (1 + u)p(x) \rangle$ 'dir.
- (b) $\text{der}(g(x)) > \text{der}(a(x)) > \text{der}(p(x))$, $a(x)|g(x)|x^n - 1$ ve $g(x)a(x), p(x) \in \mathbb{F}_4[x]$ olmak üzere $C = \langle g(x) + (1 + u)p(x), (1 + u)a(x) \rangle$ 'dir (Ma vd., 2015).

3.3.3. $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar

$R = \mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ olmak üzere Çizelge 3.2'de $\phi: R \rightarrow \{A, T, G, C\}^2$ birebir eşleşmesi ile $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ halkasının elemanlarına karşılık gelen DNA çiftleri verilmiştir (Ma vd., 2015).

Çizelge 3.2 $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

$AA \rightarrow 0$	$TT \rightarrow \alpha + 1 + (\alpha + 1)u$	$GT \rightarrow 1$	$CA \rightarrow \alpha + (\alpha + 1)u$
$AG \rightarrow \alpha$	$TC \rightarrow 1 + (\alpha + 1)u$	$AT \rightarrow \alpha + 1$	$TA \rightarrow (\alpha + 1)u$
$TG \rightarrow u$	$AC \rightarrow \alpha + 1 + \alpha u$	$GA \rightarrow \alpha u$	$CT \rightarrow 1 + \alpha + u$
$GC \rightarrow 1 + \alpha u$	$CG \rightarrow \alpha + u$	$CC \rightarrow 1 + u$	$GG \rightarrow \alpha + \alpha u$

Bu ϕ dönüşümüne göre $\bar{0} = \alpha + 1 + (\alpha + 1)u$, $\bar{1} = \alpha + (\alpha + 1)u$, $\bar{\alpha} = 1 + (\alpha + 1)u$, $\overline{\alpha + 1} = (\alpha + 1)u$, $\bar{u} = \alpha + 1 + \alpha u$, $\overline{\alpha u} = 1 + \alpha + u$, $\overline{1 + \alpha u} = \alpha + u$, $\overline{1 + u} = \alpha + \alpha u$ 'dir.

NOT: Her bir DNA çiftine karşılık gelen R halkasının elemanının u ile çarpımı, bu DNA çiftinin ters sıralı tamamlayanına karşılık gelir.

3.3.3.1. Lemma:

$\bar{a}$, herhangi bir $a \in R$ elemanının tamamlayıcı olmak üzere $a + \bar{a} = \alpha + 1 + (\alpha + 1)u$ dir (Ma vd., 2015).

3.3.3.2. Lemma:

$a \in \{0,1,\alpha,\alpha+1\}$ olmak üzere $\alpha+1+(\alpha+1)u+\overline{\alpha+1+(\alpha+1)u}=(\alpha+1+(\alpha+1)u)a$ 'dir (Ma vd., 2015).

Kanıt:

$a = 0$ ise;

$$\begin{aligned} & \alpha+1+(\alpha+1)u+\overline{\alpha+1+(\alpha+1)u} \\ &= \alpha+1+(\alpha+1)u+\bar{0} \\ &= \alpha+1+(\alpha+1)u+\alpha+1+(\alpha+1)u=0 \\ &= (\alpha+1+(\alpha+1)u)a \text{ elde edilir.} \end{aligned}$$

$a = 1$ ise;

$$\begin{aligned} & \alpha+1+(\alpha+1)u+\overline{(\alpha+1+(\alpha+1)u)a} \\ &= \alpha+1+(\alpha+1)u+\overline{\alpha+1+(\alpha+1)u} \\ &= \alpha+1+(\alpha+1)u=0 \\ &= (\alpha+1+(\alpha+1)u)a \text{ elde edilir.} \end{aligned}$$

Benzer şekilde $a = \alpha$ ve $\alpha+1$ durumları da gösterilebilir.

3.3.3.3. Lemma:

$f(x), g(x) \in R[x]$ herhangi iki polinom olsun. $\text{der}(f(x)) - \text{der}(g(x)) = m$ ise

- i) $[f(x) + g(x)]^* = f(x)^* g(x)^*$
- ii) $[f(x) + g(x)]^* = f(x)^* + x^m g(x)^*$ 'dir (Ma vd., 2015).

3.3.3.4. Teorem:

$\pi(C) = \langle g(x), (1+u)a(x) \rangle$, R halkası üzerinde tanımlı, n uzunluğunda bir devirli kod olsun. Her $f(x) \in \pi(C)$ için $f(x)^{RC} \in \pi(C)$ ise bu durumda $(1+u)((x^n-1)/(x-1)) \in \pi(C)$ ve $g(x)^* = cg(x)$, $a(x)^* = d.a(x)$ olacak şekilde $c, d \in \mathbb{F}_4 \setminus \{0\}$ sabit sayıları vardır (Ma vd., 2015).

Kanıt:

$a(x)$ ve $g(x)$, $\mathbb{F}_4[x]$ te $a(x)|g(x)|(x^n-1)$ sağlayan iki polinom olsun. $\pi(C) = \langle g(x), (1+u)a(x) \rangle$ n uzunluğunda devirli bir C lineer kod olduğu için $(0,0,0, \dots, 0) \in$

C' dir. Dolayısıyla C ters sıralı tamamlayan kod olduğu için $(0,0,0, \dots, 0) \in C$ iken $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C'$ dir. Dolayısıyla

$$\begin{aligned} & (\alpha + 1 + (\alpha + 1)u, \alpha + 1 + (\alpha + 1)u, \dots, \alpha + 1 + (\alpha + 1)u) \\ &= (\alpha + 1)(1 + u)(1, 1, \dots, 1) \in C \\ &\Leftrightarrow (\alpha + 1)(1 + u)(1 + x + x^2 + \dots + x^{n-1}) \\ &= (\alpha + 1)(1 + u)((x^n - 1)/(x - 1)) \in \pi(C) \end{aligned}$$

Dolayısıyla, $0 \neq \alpha + 1 \in \mathbb{F}_4$ olduğu için $(1 + u)((x^n - 1)/(x - 1)) \in \pi(C)$ dir.

$$g(x)^{RC} = \alpha + 1 + (\alpha + 1)u + (\alpha + 1 + (\alpha + 1)u)x + \dots + (\alpha + 1 + (\alpha + 1)u)x^{n-r-2} + \bar{g}_r x^{n-r-1} \dots + \bar{g}_1 x^{n-2} + \bar{g}_0 x^{n-1} \in \pi(C) \text{ 'dir.}$$

C lineer kod olduğundan;

$$\begin{aligned} & g(x)^{RC} + (\alpha + 1)(1 + u)((x^n - 1)/(x - 1)) \in \pi(C) \text{ olur. Dolayısıyla,} \\ & x^{n-r-1}(\bar{g}_r + \alpha + 1 + (\alpha + 1)u) + (\bar{g}_{r-1} + \alpha + 1 + (\alpha + 1)u)x + \dots + (\bar{g}_0 + \alpha + 1 + (\alpha + 1)u)x^r \in \pi(C) \text{ 'dir.} \end{aligned}$$

$$\begin{aligned} & \text{Her } a \in R \text{ için } a = \bar{a} + \alpha + 1 + (\alpha + 1)u \text{ olduğu kullanılırsa,} \\ & x^{n-r-1}(g_r + g_{r-1}x + \dots + g_0x^r) = x^{n-r-1}g(x)^* \in \pi(C) \text{ elde edilir.} \end{aligned}$$

Dolayısıyla; $l(x), k(x) \in \mathbb{F}_4[x]$ olmak üzere $g(x)^* = g(x)l(x) + (1 + u)a(x)k(x)$ şeklindedir. Her $i = 0, 1, \dots, r$ için $g_i \in \{0, 1, \alpha, \alpha + 1\}$ olduğu için, $k(x) = 0$ elde edilir. $\text{der}(g(x)^*) = \text{der}(g(x))$ olduğu için $l(x) \in \mathbb{F}_4 \setminus \{0\}$ 'dır. Bu nedenle $g(x)^* = cg(x)$ olacak şekilde bir $c \in \mathbb{F}_4 \setminus \{0\}$ sabit sayısı vardır. Dolayısıyla $g(x)$ self-reciprocal polinomdur.

$$(\alpha + 1)(1 + u)a(x) = (\alpha + 1)(1 + u)a_0 + (\alpha + 1)(1 + u)a_1(x) + \dots + (\alpha + 1)(1 + u)a_{t-1}x^{t-1} + \alpha + 1)(1 + u)a_tx^t \text{ olsun.}$$

Bu durumda,

$$\begin{aligned} & ((\alpha + 1)(1 + u)a(x))^{RC} = (\alpha + 1)(1 + u) + (\alpha + 1)(1 + u)x + \dots + \\ & \overline{(\alpha + 1)(1 + u)a_tx^{n-t-1}} + \overline{(\alpha + 1)(1 + u)a_{t-1}x^{n-t}} + \dots + \overline{(\alpha + 1)(1 + u)a_1x^{n-2}} + \\ & \overline{(\alpha + 1)(1 + u)a_0x^{n-1}} \in \pi(C) \text{ 'dir.} \end{aligned}$$

$$(\alpha + 1)(1 + u)((x^n - 1)/(x - 1)) \in \pi(C) \text{ olur ve } C \text{ lineer kod olduğu için,}$$

$$((\alpha + 1)(1 + u)a(x))^{RC} + (\alpha + 1)(1 + u)((x^n - 1)/(x - 1)) \in \pi(C) \text{ 'dir.}$$

Dolayısıyla;

$$x^{n-t-1} \left[\left(\overline{(\alpha+1)(1+u)a_1} + (\alpha+1)(1+u) \right) + \left(\overline{(\alpha+1)(1+u)a_{t-1}} + (\alpha+1)(1+u) \right) x + \cdots + \left(\overline{(\alpha+1)(1+u)a_1} + (\alpha+1)(1+u) \right) x^{t-1} + \left(\overline{(\alpha+1)(1+u)a_0} + (\alpha+1)(1+u) \right) x^t \right] \in \pi(C) \text{ 'dir.}$$

$\alpha + 1 + (\alpha + 1)u + \overline{(\alpha + 1 + (\alpha + 1)u)a} = (\alpha + 1 + (\alpha + 1)u)a$ eşitliğini kullanarak

$$\begin{aligned} & x^{n-t-1} \left((\alpha + 1)(1 + u)a_t + (\alpha + 1)(1 + u)a_{t-1}x + \cdots + (\alpha + 1)(1 + u)a_tx^{t-1} + \right. \\ & \left. (\alpha + 1)(1 + u)a_0x^t \right) \\ & = x^{n-t-1}(\alpha + 1)(1 + u)a(x)^* \in \pi(C) \text{ elde edilir.} \end{aligned}$$

$0 \neq \alpha + 1 \in \mathbb{F}_4$ olduğu için $(1 + u)a(x)^* \in \pi(C)$ 'dir. Dolayısıyla $(1 + u)a(x)^* = g(x)h(x) + (1 + u)a(x)s(x)$ 'dir. Buradan $h(x) = 0$ ve $a(x)^* = a(x)s(x)$ elde edilir.

Dolayısıyla $\text{der}(a(x)^*) = \text{der}(a(x))$ olduğundan $s(x) \in \mathbb{F}_4 \setminus \{0\}$ elde edilir. Yani $a(x)^* = da(x)$ olacak şekilde bir $d \in \mathbb{F}_4 \setminus \{0\}$ sabit sayısı vardır.

3.3.3.5. Teorem:

$C = \langle g(x), (1 + u)a(x) \rangle$, R halkası üzerinde tanımlı n uzunluğunda bir devirli kod olsun. $(1 + u)((x^n - 1)/(x - 1)) \in \pi(C)$ ve $g(x)^* = cg(x)$, $a(x)^* = da(x)$ olacak şekilde $c, d \in \mathbb{F}_4 \setminus \{0\}$ sabit sayıları var ise her $f(x) \in \pi(C)$ için $f(x)^{RC} \in \pi(C)$ dir (Ma vd., 2015).

Kanıt:

$\pi(C) = \langle g(x), (1+u)a(x) \rangle$, $g^*(x) = cg(x)$ ve $a^*(x) = da(x)$ olsun. $g(x) = g_0 + g_1x + \dots + g_{r-1}x^{r-1} + g_rx^r$ ve $c(x) \in \pi(C)$ olsun.

Bu durumda,

$c(x) = g(x)l(x) + (1+u)a(x)k(x)$ olacak şekilde $l(x), k(x) \in R[x]$ polinomları vardır. Dolayısıyla, $g(x)^* = cg(x)$ ve $a(x)^* = d.a(x)$ olduğu için,

$$\begin{aligned} c(x)^* &= (g(x)l(x) + (1+u)a(x)k(x))^* \\ &= (g(x)l(x))^* + x^m((1+u)a(x)k(x))^* \\ &= g(x)^*l(x)^* + (1+u)a(x)^*(x^mk(x)^*) \\ &= cg(x)l(x)^* + d(1+u)a(x)(x^mk(x)^*) \text{ elde edilir.} \end{aligned}$$

Dolayısıyla, $c(x)^* \in \pi(C)$ olur. $0 \neq \alpha + 1 \in \mathbb{F}_4$ olduğu için $(\alpha + 1)(1 + u)((x^n - 1)/(x - 1)) \in \pi(C)$ ' dir.

Bu nedenle, $(\alpha + 1)(1 + u)((x^n - 1)/(x - 1)) = (\alpha + 1)(1 + u) + (\alpha + 1)(1 + u)x + \dots + (\alpha + 1)(1 + u)x^{n-1} \in \pi(C)$ elde edilir.

$c(x) = c_0 + c_1x + \dots + c_tx^t \in \pi(C)$ olsun. C bir devirli kod olduğu için $x^{n-t-1}c(x) = c_0x^{n-t-1} + c_1x^{n-t} + \dots + c_tx^{n-1} \in \pi(C)$ ' dir. İki denklem toplanırsa, $(\alpha + 1)(1 + u)(x^n - 1/x - 1) + x^{n-t-1}c(x) = (\alpha + 1)(1 + u) + (\alpha + 1)(1 + u)x + \dots + (\alpha + 1)(1 + u)x^{n-t-2} + (c_0 + (\alpha + 1)(1 + u))x^{n-t-1} + (c_1 + (\alpha + 1)(1 + u))x^{n-t} + \dots + (c_t + (\alpha + 1)(1 + u))x^{n-1} \in \pi(C)$ elde edilir.

$a \in R$ için $\alpha + 1 + (\alpha + 1)u + a = \bar{a}$ eşitliği kullanılarak, $(\alpha + 1)(1 + u) + (\alpha + 1)(1 + u)x + \dots + (\alpha + 1)(1 + u)x^{n-t-2} + \bar{c}_0x^{n-t-1} + \bar{c}_1x^{n-t} + \dots + \bar{c}_tx^{n-1} \in \pi(C)$

elde edilir.

Bu da $(c(x)^*)^{RC}$ polinomuna eşittir. Dolayısıyla; $((c(x)^*)^{RC})^* = (x^{n-t-1}c(x))^{RC}$, dir.

3.3.3.6. Sonuç:

C , n uzunluğunda R halkası üzerinde tanımlı d Hamming uzaklıklı bir devirli DNA kod olsun. Bu durumda $\phi(C)$, $2n$ uzunluğunda $\{A, T, G, C\}$ alfabesi üzerinde tanımlı en az d Hamming uzaklıklı bir DNA koddur (Ma vd., 2015).

3.4. $w^2 = 2$ Olmak Üzere $\mathbb{Z}_4 + w \mathbb{Z}_4$ Sonlu Halkası Üzerinde Devirli DNA Kodlar

A. Dertli ve Y. Çengellenmiş $w^2 = 2$ olmak üzere $\mathbb{Z}_4 + w \mathbb{Z}_4$ halkası üzerinde n uzunluğundaki devirli kodların cebirsel yapısını verdikten sonra bu kodların ters sıralı ve ters sıralı tamamlayan olması için gerekli ve yeterli koşulu vermişlerdir.

3.4.1. $\mathbb{Z}_4 + w \mathbb{Z}_4$ Kümesinin Cebirsel Yapısı

$R = \mathbb{Z}_4[w]/\langle w^2 - 2 \rangle \cong \mathbb{Z}_4 + w \mathbb{Z}_4 = \{a + wb | a, b \in \mathbb{Z}_4\}$, $w^2 = 2$ kümesi değişmeli, karakteristiği 4 olan, 16 elemanlı bir esas ideal halkasıdır. R aynı zamanda sonlu zincir halkasıdır.

Halkanın birimselleri kümesi,

$$\{1, 3, 1 + w, 3 + w, 1 + 2w, 1 + 3w, 3 + 3w, 3 + 2w\}$$

Halkanın birimsel olmayan elemanları kümesi;

$$\{0, 2, w, 2w, 3w, 2 + w, 2 + 2w, 2 + 3w\} \text{ dir.}$$

Halkanın idealleri;

- $\langle 0 \rangle = \{0\}$
- $\langle 1 \rangle = \langle 3 \rangle = \langle 1 + 3w \rangle = \dots = R$
- $\langle w \rangle = \{0, 2, w, 2w, 3w, 2 + w, 2 + 2w, 2 + 3w\} = \langle 3w \rangle = \langle 2 + w \rangle = \langle 2 + 3w \rangle$
- $\langle 2w \rangle = \{0, w\}$
- $\langle 2 \rangle = \langle 2 + 2w \rangle = \{0, 2, 2w, 2 + 2w\}$

$$\langle 0 \rangle \subset \langle 2w \rangle \subset \langle 2 \rangle \subset \langle w \rangle \subset R$$

şeklindedir. Gray dönüşümü,

$$\phi: R \rightarrow \mathbb{Z}_4^2$$

$$a + wb \mapsto \phi(a + wb) = (a, b)$$

şeklinde tanımlanır. Gray dönüşümü $i = 1, 2, \dots, n$ için $\alpha_i = a_i + b_i w \in R$ olmak üzere aşağıdaki şekilde R^n ' e genişletilir.

$$\phi: R^n \rightarrow \mathbb{Z}_4^{2n}$$

$$(\alpha_1, \alpha_2, \dots, \alpha_n) \mapsto (a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n)$$

Ayrıca ϕ , bir $\mathbb{Z}_4$ – modül izomorfizmasıdır (Dertli A., Cengellenmiş Y., 2016).

3.4.2. $\mathbb{Z}_4 + w \mathbb{Z}_4$ Halkası Üzerinde Tanımlı Devirli Kodlar

3.4.2.1. Teorem:

C, R halkası üzerinde tanımlı n uzunluğunda bir devirli kod olsun. $a(x)|g(x)|(x^n - 1)$ olmak üzere $C = \langle g(x), wa(x) \rangle$ olacak şekilde $g(x), a(x)$ polinomları vardır ve n tek uzunluğunda olduğunda $R[x]/\langle x^n - 1 \rangle$ halkası esas ideal halkası olduğu için $C = \langle s(x) \rangle$ olacak şekilde bir $s(x) \in R[x]/\langle x^n - 1 \rangle$ vardır (Dertli A., vd., 2016).

3.4.3. $\mathbb{Z}_4 + w \mathbb{Z}_4$ Sonlu Halkası Üzerinde Devirli DNA Kodlar

DNA alfabesi $\{A, T, G, C\}$ olmak üzere $0 \rightarrow A, 1 \rightarrow C, 2 \rightarrow G, 3 \rightarrow T$ dönüşümü ve gray dönüşümü yardımı ile ve $R \rightarrow \{A, T, G, C\}^2$ birebir eşleşmesi Çizelge 3.3'te verilmiştir (Dertli A., vd., 2016).

Çizelge 3.3 $\mathbb{Z}_4 + w \mathbb{Z}_4$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

Elemanlar	Gray Görüntüler	DNA çiftleri
0	(0,0)	AA
1	(1,0)	CA
2	(2,0)	GA
3	(3,0)	TA
w	(0,1)	AC
$2w$	(0,2)	AG
$3w$	(0,3)	AT
w	(1,1)	CC
$1 + 2w$	(1,2)	CG
$1 + 3w$	(1,3)	CT
$2 + w$	(2,1)	GC

$2 + 2w$	$(2,2)$	GG
$2 + 3w$	$(2,3)$	GT
$3 + w$	$(3,1)$	TC
$3 + 2w$	$(3,2)$	TG
$3 + 3w$	$(3,3)$	TT

3.4.3.1. Lemma:

Her $f(x), g(x) \in R[x]$ için $der f(x) - der g(x) = m$ olmak üzere

i) $(f(x)g(x))^* = f(x)^*g(x)^*$

ii) $(f(x) + g(x))^* = f(x)^* + x^m g(x)^*$ dir (Dertli A., vd., 2016)..

3.4.3.2. Lemma:

$\bar{a}$, herhangi $a \in R$ elemanının tamamlayanı olmak üzere $a + \bar{a} = 3 + 3w$ dir (Dertli A., vd., 2016).

3.4.3.3. Lemma:

$a \in \{0,1,2,3\}$ olmak üzere $(3 + 3w) - \bar{w}a = wa$ dir (Dertli A., vd., 2016).

3.4.3.4. Teorem:

$C = \langle g(x), wa(x) \rangle, R$ halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun. Her $f(x) \in \pi(C)$ için $f(x)^{RC} \in \pi(C)$ ise, bu durumda $(1 + w)(1 + x + x^2 + \dots + x^{n-1}) \in \pi(C)$ ve $g(x)^* = eg(x)$ ve $a(x)^* = d.a(x)$ olacak şekilde $e, d \in \mathbb{Z}_4^*$ elemanları vardır (Dertli A., vd., 2016).

Kanıt:

$a(x)$ ve $g(x), \mathbb{Z}_4[x]$ te $a(x)|g(x)|x^n - 1$ sağlayan iki polinom olmak üzere $C = \langle g(x), wa(x) \rangle$ ters sıralı tamamlayan kod olsun.

$(0,0, \dots, 0) \in C$ olduğu için $(0,0, \dots, 0)^{RC} = (\bar{0}, \bar{0}, \dots, \bar{0}) = 3(1 + w)(1,1, \dots, 1) \in C$ dir.

Bu kod sözcüğüne karşılık gelen polinom temsili $(3 + 3w) \frac{x^n - 1}{x - 1}$ dir.

$3 \in \mathbb{Z}_4^*$ olduğu için $(1+w)(1+x+\dots+x^{n-1}) \in \pi(C)$ dir.

$g(x) = g_0 + g_1x + \dots + g_sx^s$ olsun.

$g(x)^{RC} = (3+3w) + (3+3w)x + \dots + (3+3w)x^{n-s-2} + \overline{g_s}x^{n-s-1} + \dots + \overline{g_1}x^{n-2} + \overline{g_0}x^{n-1} \in \pi(C)$ dir.

C lineer kod olduğu için,

$3(1+w)(1+x+\dots+x^{n-1}) - g(x)^{RC} \in \pi(C)$ dir.

Dolayısıyla,

$((3+3w) - \overline{g_s})x^{n-s-1} + ((3+3w) - \overline{g_{s-1}})x^{n-s-2} + \dots + ((3+3w) - \overline{g_0})x^{n-1} \in \pi(C)$ dir.

Her $a \in R$ için

$(3+3w) - \overline{a} = a$ olduğu için

$x^{n-s-1}(g_s + g_{s-1}x + \dots + g_0x^s) = x^{n-s-1}g(x)^* \in \pi(C)$ dir.

$g(x)^* \in \pi(C)$ olduğu için

$g(x)^* = g(x).u(x) + wa(x)v(x)$ olacak şekilde $u(x), v(x) \in \mathbb{Z}_4[x]$ vardır.

$i = 0, 1, \dots, s$ olmak üzere $g_i \in \mathbb{Z}_4$ olduğu için $v(x) = 0$ elde edilir.

$derg(x)^* = derg(x)$ olduğu için $u(x) \in \mathbb{Z}_4^*$ dir. Bu nedenle $g(x)^* = eg(x)$ olacak şekilde bir $e \in \mathbb{Z}_4^*$ vardır. Dolayısıyla $g(x)$ bir reciprocal polinomdur.

$a(x) = a_0 + a_1x + \dots + a_tx^t$ olsun.

$wa(x) = wa_0 + wa_1x + \dots + wa_tx^t$ olsun. Bu durumda,

$(wa(x))^{RC} = (3+3w) + (3+3w)x + \dots + \overline{wa_t}x^{n-t-1} + \dots + \overline{wa_1}x^{n-2} + \overline{wa_0}x^{n-1} \in \pi(C)$ dir.

$(3+3w)\frac{x^{n-1}}{x-1} \in \pi(C)$ ve C lineer bir kod olduğu için,

$-(wa(x))^{RC} + (3+3w)\frac{x^{n-1}}{x-1} \in \pi(C)$ dir.

Dolayısıyla,

$x^{n-t-1}[(-(wa_t) + (3+3w) + (-(wa_{t-1}) + (3+3w))x + \dots + (-(wa_1) + (3+3w))x^t]$ dir.

$x^{n-t-1}(wa_t + wa_{t-1}x + \dots + wa_0x^t) = x^{n-t-1}wa^*(x) \in \pi(C)$ elde edilir.

$wa(x)^* \in \pi(C)$ olduğu için,

$wa(x)^* = g(x)h(x) + wa(x)s(x)$ olacak şekilde $h(x)$ ve $s(x) \in \mathbb{Z}_4[x]$ polinomları vardır. Buradan $h(x) = 0$ ve $a(x)^* = a(x).s(x)$ elde edilir.

$dera(x)^* = dera(x)$ olduğu için $s(x) \in \mathbb{Z}_4^*$ dir. Dolayısıyla $a(x)$ bir self reciprocal polinomdur.

3.4.3.5. Teorem:

$C = \langle g(x), wa(x) \rangle, R$ halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun. $(1+w)(1+x+x^2+\dots+x^{n-1}) \in \pi(C)$ ve $g(x)^* = eg(x)$ ve $a(x)^* = d.a(x)$ olacak şekilde $e, d \in \mathbb{Z}_4^*$ var ise her $c(x) \in \pi(C)$ için $c(x)^{RC} \in \pi(C)$ dir (Dertli A., vd., 2016).

Kanıt:

$C = \langle g(x), wa(x) \rangle$ olduğu için her $c(x) \in \pi(C)$ için $c(x) = g(x)m(x) + wa(x)n(x)$ olacak şekilde $m(x), n(x) \in R[x]/\langle x^n - 1 \rangle$ vardır.

$$\begin{aligned} c(x)^* &= (g(x)m(x) + wa(x)n(x))^* \\ &= (g(x)m(x))^* + x^s(wa(x)n(x)) \\ &= g(x)^*m(x)^* + wa(x)^*(x^s n(x)^*) \end{aligned}$$

$e, d \in \mathbb{Z}_4^*$ olmak üzere $g(x)^* = eg(x), a(x)^* = da(x)$ olduğu için,

$$c(x)^* = eg(x)m(x)^* + dwa(x)(x^s n(x)^*) \in \pi(C) \text{ dir.}$$

$$c(x) = c_0 + c_1x + \dots + c_tx^t \in \pi(C) \text{ olsun.}$$

C devirli kod olduğu için $x^{n-t-1}c(x) = c_0x^{n-t-1} + c_1x^{n-t} + \dots + c_tx^{n-1} \in \pi(C)$ elde edilir.

$(1+w) + (1+w)x + \dots + (1+w)x^{n-1} \in \pi(C)$ ve C lineer kod olduğu için

$$\begin{aligned} -(1+w)\frac{x^n-1}{x-1} - x^{n-t-1}c(x) &= -(1+w) - (1+w)x + \dots + (-c_0 - (1+w) \\ &+ w)x^{n-t-1} + \dots + (-c_t - (1+w))x^{n-1} \in \pi(C) \text{ dir.} \end{aligned}$$

$a \in R$ olmak üzere $\bar{a} + (1+w) = -a$ olduğu kullanılırsa

$-(1+w) - (1+w)x + \dots + \bar{c}_0x^{n-t-1} + \dots + \bar{c}_tx^{n-1} \in \pi(C)$ elde edilir. Dolayısıyla $(c(x)^*)^{RC} \in \pi(C)$ dir.

$((c(x)^*)^{RC})^* = \bar{c}_t + \bar{c}_{t-1}x + \dots + (3+3w)x^{n-1}$ polinomu $(\bar{c}_t, \bar{c}_{t-1}, \dots, \bar{c}_0, \bar{0}, \dots, \bar{0})$ vektörüne karşılık gelir.

$(c(x)^*)^{RC} = (x^{n-t-1}c(x))^{RC}$ olduğu için $c(x)^{RC} \in \pi(C)$ dir.

3.5. $\mathbb{F}_4[v]/(v^2 - v)$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar ve Devirli DNA Kodlarının DNA Görüntüleri

2015 yılında A. Bayram ,E. S. Öztaş ve İ. Şiap sonlu zincir olmayan $\mathbb{F}_4[v]/(v^2 - v)$ halkası üzerinde tanımlı devirli kodların yapısını çalışmıştır. Ters sıralı ve ters sıralı tamamlayan DNA kod kavramlarını inşa etmişlerdir.

3.5.1. $\mathbb{F}_4[v]/(v^2 - v)$ Kümesinin Cebirsel Yapısı

$w, x^2 + x + 1$ primitif (ilkel) polinomunun bir kökü olmak üzere,

$\mathbb{F}_4 = \{0, 1, w, w^2 = w + 1\}$ dört elemanlı sonlu cisim olsun.

$R = \mathbb{F}_4[v]/(v^2 - v) \cong \mathbb{F}_4 + v\mathbb{F}_4 = \{a + vb \mid a, b \in \mathbb{F}_4\}$ kümesi,

Her $a + vb, c + vd \in R$ için

$$(a + vb) + (c + vd) = a + c + (b + d)v$$

$$(a + vb) \cdot (c + vd) = ac + v(ad + bc + db)$$

şeklinde tanımlı $+$ ve $\cdot$ işlemlerine göre 16 elemanlı karakteristiği 2 olan değişmeli bir halkadır. R halkasının her elemanı $a, b \in \mathbb{F}_4$ olmak üzere $c = a + vb$ şeklinde tek türlü yazılır.

$\phi: R \rightarrow \mathbb{F}_4 \times \mathbb{F}_4$ şeklinde tanımlanan Gray dönüşüm bir halka izomorfizması olduğu için R sonlu yarı lokal bir Frobenious halkasıdır.

R halkasının idealleri;

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

R halkasının $\langle v \rangle$ ve $\langle v + 1 \rangle$ şeklinde iki maksimal ideali olduğu için Çin Kalan Teoremi ile;

$$R \cong \mathbb{F}_4[v]/\langle v - 1 \rangle \oplus \mathbb{F}_4[v]/\langle v \rangle \cong \mathbb{F}_4 \oplus \mathbb{F}_4 \cong \langle v \rangle \oplus \langle 1 + v \rangle \text{ dir.}$$

Dolayısıyla, R halkasının her bir elemanı $a, b \in \mathbb{F}_4$ olmak üzere $a + vb = (a + b)v + a(v + 1)$ biçiminde de tek şekilde yazılır.

R halkasının birimsellerinin oluşturduğu

$\mathcal{U}(R) = \{1, w, w + 1, v + w, 1 + v + w, 1 + vw, 1 + v + vw, 1 + w + vw, v + w + vw\}$ kümesi çarpma işlemine göre bir grup oluşturur.

S herhangi sonlu bir halka, $a \in S$ olsun. a elemanının Hamming ağırlığı $a \in S \setminus \{0\}$ ise $wt(a) = 1$ aksi halde $wt(a) = 0$ 'dır. $a = (a_1, a_2, \dots, a_n) \in S^n$ elemanının Hamming ağırlığı $wt(a) = \sum_{i=1}^n wt(a_i)$ şeklindedir. $a, b \in S$ elemanları arasındaki Hamming uzaklık $d(a - b) = wt(a - b)$ şeklinde tanımlanır. d Hamming uzaklığı S^n üzerinde bir metriktir.

Gray dönüşüm,

$$\begin{aligned}\phi: R &\rightarrow \mathbb{F}_4^2 \\ a + vb &\rightarrow (a + b, a)\end{aligned}$$

şeklindedir.

R halkasının herhangi bir elemanının Lee ağırlığı, görüntüsünün Hamming ağırlığına eşittir ve $c \in R$ için $w_L(c) = wt(\phi(c))$ şeklinde gösterilir.

A ve B iki lineer kod olsun.

$$\begin{aligned}A \otimes B &= \{(a, b) \mid a \in A, b \in B\} \\ A \oplus B &= \{a + b \mid a \in A, b \in B\}\end{aligned}$$

olarak tanımlanır.

R halkası üzerinde tanımlı sıfırdan farklı bir C kodunun üreteç matrisi tüm $1 \leq i, j \leq 4$ için A_i, B_j bileşenleri $\mathbb{F}_4$ cisminde alınan matrisler olmak üzere,

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

matrisine denktir.

C, R üzerinde tanımlı bir lineer kod olsun.

$$C_1 = \{x + y \in F_4^n \mid (x + y)v + x(v + 1) \in C; \exists x, y \in F_4^n\}$$

$$C_2 = \{x \in F_4^n \mid (x + y)v + x(v + 1) \in C; \exists y \in F_4^n\}$$

olmak üzere C_1 ve C_2 $\mathbb{F}_4$ cismi üzerinde tanımlı lineer kodlardır.

$C = vC_1 \oplus (1 + v)C_2$ şeklinde yazılır ve C kodunun eleman sayısı $|C| = 16^{k_1} 4^{k_2} 4^{k_3}$ dır (Bayram vd., 2015).

3.5.1.1. Lemma:

$C = vC_1 \oplus (1 + v)C_2$, R halkası üzerinde tanımlı n uzunluğunda bir lineer kod ve $i = 1, 2$ için $C_i, [n, k_i, d(C_i)]$ parametrelı $\mathbb{F}_4$ cismi üzerinde tanımlı lineer kodlar olsun. Bu durumda $\phi(C), \mathbb{F}_4$ cismi üzerinde tanımlı $[2n, k_1 + k_2, \min\{d(C_1), d(C_2)\}]$ parametrelı bir koddur (Bayram vd., 2015).

3.5.2. $\mathbb{F}_4[v]/(v^2 - v)$ Halkası Üzerinde Tanımlı Devirli Kodlar

3.5.2.1. Sonuç:

$C = vC_1 \oplus (1 + v)C_2$, R halkası üzerinde tanımlı n uzunluğuna sahip bir lineer kod olsun. Bu durumda C 'nin devirli bir kod olabilmesi için gerekli ve yeterli koşul C_1 ve C_2 'nin $\mathbb{F}_4$ cismi üzerinde tanımlı devirli kodlar olmasıdır (Bayram vd., 2015).

3.5.2.2. Sonuç:

C, R halkası üzerinde tanımlı n uzunluğuna sahip bir devirli kod olsun. Bu durumda $g_1(x)$ ve $g_2(x)$ sırasıyla $\pi(C_1)$ ve $\pi(C_2)$ kodlarının üretic polinomları olmak üzere $\pi(C) = \langle vg_1(x) + (1 + v)g_2(x) \rangle$ ve $|C| = 4^{2n - \deg(g_1(x)) - \deg(g_2(x))}$ 'tir (Bayram vd., 2015).

3.5.2.3. Sonuç:

C, R halkası üzerinde tanımlı n uzunluğuna sahip bir devirli kod ise $\pi(C) = \langle vg_1(x) + (1 + v)g_2(x) \rangle$ kodu $g_1(x)$ ve $g_2(x)$ polinomlarıyla teklikle üretilir (Bayram vd., 2015).

3.5.3. $\mathbb{F}_4[v]/(v^2 - v)$ Halkası Üzerinde Tanımlı DNA Kodlar

3.5.3.1. Teorem:

$\mathbb{F}_q$ sonlu cismi üzerinde tanımlı $C = \langle g(x) \rangle$ şeklindeki bir kodun ters sıralı olması için gerek ve yeter koşul $g(x)$ 'in self reciprocal polinom olmasıdır (Massey, 1964).

3.5.3.2. Teorem:

$\pi(C) = \langle g(x) \rangle = \langle vg_1(x) + (1 + v)g_2(x) \rangle$, R halkası üzerinde tanımlı ters sıralı devirli kod olması için gerekli ve yeterli koşul $g_1(x), g_2(x) \in \mathbb{F}_4[x]$ self reciprocal

polinomlar olması ve $i = 1, 2$ için $g_i(x)|(x^n - 1)$ özelliğini sağlamasıdır (Bayram vd., 2015).

Kanıt:

$\text{der}(g_1(x)) = t$ ve $\text{der}(g_2(x)) = m$ olmak üzere $t \leq m$ olsun.

$t = m$ ise $g(x) = (v)g_1(x) + (1 + v)g_2(x)$ polinomu R halkası üzerinde ters sıralı kodu üreten bir self reciprocal polinomdur.

Genelleme yapmaksızın $t < m$ olsun. $g_1(x) = a_0 + a_1x + \dots + a_1x^{t-1} + a_0x^t$, $g_2(x) = b_0 + b_1x + \dots + b_1x^{m-1} + b_0x^m$ olmak üzere,

$$\pi(C) = \langle g(x) = (v)g_1(x) + (1 + v)g_2(x) \rangle \text{ olsun.}$$

Bu yüzden $\pi(C) = \langle g(x) \rangle$ olduğu için $g(x) \in \pi(C)$ 'dir.

Diğer bir yandan, $vx^{n-t-1}g_1(x) + (v + 1)x^{n-m-1}g_2(x)$, $g(x)$ polinomunun ters sıralı polinomu olmak üzere $vx^{n-t-1}g_1(x) + (v + 1)x^{n-m-1}g_2(x) \in \pi(C)$ 'dir. Dolayısıyla,

$x^i g(x) \in \pi(C)$ ise $x^i g(x) \in \pi(C)$ 'in ters sıralısı $vx^{n-t-i-1}g_1(x) + (v + 1)x^{n-m-i-1}g_2(x)$ olmak üzere $vx^{n-t-i-1}g_1(x) + (v + 1)x^{n-m-i-1}g_2(x) \in \pi(C)$ 'dir. C lineer kod olduğu için ve $x^i g(x)$ 'nin bütün lineer kombinasyonları $\pi(C)$ kümesindedir.

Dolayısıyla, $\pi(C) = \langle (v)g_1(x) + (1 + v)g_2(x) \rangle$ R halkası üzerinde tanımlı n uzunluğunda ters sıralı koddur.

Tersine, $\pi(C) = \langle g(x) = (v)g_1(x) + (1 + v)g_2(x) \rangle$, R üzerinde tanımlı n uzunluğunda ters sıralı kod olsun. Bu durumda her bir kod sözcüğünün Gray görüntüsü kullanılarak C_1 ve C_2 ters sıralı olur. O zaman, $C_1 = \langle g_1(x) \rangle$, $C_2 = \langle g_2(x) \rangle$ $\mathbb{F}_4$ üzerinde ters sıralı kod olduğu için $g_1(x), g_2(x)$ self reciprocal polinomlar olduğu görülür.

3.5.4. $\mathbb{F}_4[v]/(v^2 - v)$ Halkası Üzerinde Tanımlı Devirli DNA Kodlar

2015 yılında Ayşegül Bayram, Elif Segah Öztaş ve İrfan Şiap tarafından $\mathbb{F}_4[v]/(v^2 - v)$ halkası üzerinde tanımlı DNA kodlar elde edilmiş ve ters sıralama problemini çözmek için yeni bir yaklaşım verilmiştir (Bayram vd., 2015).

$S_{D_4} = \{A, T, G, C\}$ DNA alfabesi olmak üzere,

T. Abualrub, A. Ghayeb ve X.N. Zeng tarafından S_{D_4} kümesi ile $\mathbb{F}_4$ cismi elemanları arasında $A \rightarrow 0, T \rightarrow 1, C \rightarrow w, G \rightarrow w + 1 = w^2$ götüren bir dönüşüm

tanımlamıştır. Bu dönüşüm ve Gray dönüşüm yardımıyla A. Bayram, E. S. Öztaş ve İ. Şiap, $S_{D_{16}} = \{AA, AT, AG, AC, TT, TA, TG, GG, GA, GC, GT, CC, CA, CG, CT\}$ kümesinin elemanları ile R halkasının elemanları arasında bir dönüşümü Çizelge 3.4'deki gibi göstermişlerdir (Bayram vd., 2015).

$$\xi: R \rightarrow S_{D_4}^2 = \{A, T, G, C\}^2$$

Çizelge 3.4 $\mathbb{F}_4[v]/(v^2 - v)$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

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

3.5.4.1. Örnek:

$(c_0, c_1, c_2, c_3) = (1, v, w, w + v)$ ise bu eleman $(\xi(1), \xi(v), \xi(w), \xi(v + w)) = TTTACCGC$ ile eşleşir.

NOT: S_{D_4} kümesindeki Watson-Crick tamamlayıcı ; $\bar{A} = T, \bar{T} = A, \bar{G} = C, \bar{C} = G$ ile verildiği için bu $S_{D_{16}}$ kümesinin elemanlarına $\overline{AA} = TT, \dots, \overline{TA} = AT$ şeklinde genişletilmiştir (Bayram vd., 2015).

3.5.4.2. Not:

$\xi: R \rightarrow S_{D_4}^2$ dönüşümü R^n e aşağıdaki şekilde genişletilir.

$$\Theta: R^n \rightarrow S_{D_4}^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto (\xi(c_0)\xi(c_1) \dots \xi(c_{n-1}))$$

şeklindedir. C, R halkası üzerinde tanımlı n uzunluğunda bir kod ve $c_i \in R$ olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in C$ ise $\Theta(C)$ kümesi

$\Theta(C) = \{(\xi(c_0)\xi(c_1) \dots \xi(c_{n-1})) | \forall (c_0, c_1, \dots, c_{n-1}) \in C\}$ şeklindedir (Bayram vd., 2015).

3.5.4.3. Önerme:

$$\psi: R \rightarrow R$$

$$a + bv \mapsto a + (1 + v)b$$

şeklinde tanımlı dönüşüm aşıkâr olmayan bir otomorfizmadır (Bayram vd., 2015).

3.5.4.4. Tanım:

$der(g_1(x)) = t_1, der(g_2(x)) = t_2$ ve $i = 1, 2$ için $g_1(x), g_2(x) | x^n - 1$ sağlayan $g_1(x), g_2(x) \in F_4[x]$ polinomları verilsin.

$l = \min\{n - t_1, m - t_2\}$ ve $g(x) = vg_1(x) + (v + 1)g_2(x) \in R[x]$ olsun.

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

olmak üzere $E(g) = \{E_0(x), E_1(x), \dots, E_{l-1}(x)\}$ şeklinde tanımlanan $E(g)$ kümesine ψ kümesi denir. $E(g), C = \langle g(x) \rangle_\psi$ ile gösterilen R halkası üzerinde tanımlı bir C lineer kodunu üretir (Bayram vd., 2015).

3.5.4.5. Uyarı:

$\langle E(g) \rangle$ ile $E(g)$ ile üretilen R -altmodülü $\langle g(x) \rangle$ ile $g(x)$ ile üretilen ideal gösterilecektir (Bayram vd., 2015).

3.5.4.6. Uyarı:

$g(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1} + a_tx^t \in R[x]$ olmak üzere $E(g)$ ile üretilen R -alt modül ve ψ , R halkası üzerinde tanımlı aşıkarak olmayan otomorfizma olmak üzere,

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

matrisinin satırları ile üretilmiştir (Bayram vd., 2015).

3.5.4.7. Teorem:

$g_1(x)$ ve $g_2(x)$ sırasıyla $\text{der}(g_1(x)) = t_1$, $\text{der}(g_2(x)) = t_2$ ve $\mathbb{F}_4[x]$ 'te $i = 1, 2$ için $g_i(x)|x^n - 1$ sağlayan iki self-reciprocal polinom ve l , $2 \leq l$ koşulunu sağlayan bir çift tamsayı olsun.

- 1) $\text{der}(g_1(x)) = \text{der}(g_2(x))$ veya $g_1(x)$, $g_2(x)$ polinomlarından biri sıfıra eşit ise bu durumda $g(x) = vg_1(x) + (v+1)g_2(x)$ ve sırasıyla $|\langle E(g) \rangle| = 16^l$ ve $|\langle E(g) \rangle| = 4^l$ dir.
- 2) $\text{der}(g_1(x)) \neq \text{der}(g_2(x))$ ve $2 \leq s = |t_1 - t_2|$ çift sayı ise bu durumda $\text{der}(g_2(x)) < \text{der}(g_1(x))$ için $g(x) = vg_1(x) + (v+1)x^{\frac{s}{2}}g_2(x)$ veya $\text{der}(g_1(x)) < \text{der}(g_2(x))$ için $g(x) = vx^{\frac{s}{2}}g_1(x) + (v+1)g_2(x)$ şeklindedir ve $|\langle E(g) \rangle| = 16^l$ dir.

Her iki durumda da $\pi(C) = \langle E(g) \rangle$, R halkası üzerinde tanımlı bir lineer kod ve $\Theta(C)$ bir ters sıralı DNA koddur (Bayram vd., 2015).

3.5.4.8. Sonuç:

$g_1(x)$ ve $g_2(x)$, $x^n - 1$ polinomunu bölen $\mathbb{F}_4[x]$ 'te iki reciprocal polinom ve $\pi(C) = \langle E(g) \rangle$, R halkası üzerinde tanımlı bir lineer kod olsun. $r(x) = 1 + x + x^2 + \dots + x^{n-1}$, $\pi(C)$ kümesinin bir elemanı ise $\Theta(C)$ de bir ters sıralı tamamlayan DNA koddur (Bayram vd., 2015).

3.5.4.9. Sonuç:

$g_1(x)$ ve $g_2(x)$, $x^n - 1$ polinomunu bölen $\mathbb{F}_4[x]$ 'te iki reciprocal polinom ve $\pi(C) = \langle E(g) \rangle$, R halkası üzerinde tanımlı bir lineer kod ve $\Theta(C)$ de bir ters sıralı tamamlayan DNA kod olsun. $r(x) = 1 + x + x^2 + \dots + x^{n-1}$ polinomu $E(g)$ üreteç kümesine eklenirse $\Theta(C)$ bir ters sıralı tamamlayan DNA koddur (Bayram vd., 2015).

3.5.4.10. Teorem:

$g_1(x)$, $x^n - 1$ 'i bölen $\mathbb{F}_4[x]$ 'te bir self reciprocal polinom ve $g(x) = vg_1(x) + (v+1)g_2(x) \in R[x]$ olsun. Bu durumda $\pi(C) = \langle g(x) \rangle$ (veya $C = \langle g(x) \rangle_\psi$) R üzerinde ters sıralı DNA koddur ve $\Theta(C)$ ters sıralı DNA koddur. Eğer, $x - 1 \nmid g(x)$ oluyor ise $\Theta(C)$ ters sıralı tamamlayan DNA koddur (Bayram vd., 2015).

3.6. $u^2 = 0, v^2 = v, uv = vu$ Olmak Üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Sonlu Halkası Üzerinde Devirli Kod İnşası Ve Devirli DNA Kodların DNA Görüntüleri

Zhu ve X. Chen tarafından $u^2 = 0, v^2 = v, uv - vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ halkası üzerinde tanımlı devirli kodların ters sıralı ve ters sıralı tamamlayan olması için gerekli ve yeterli koşullar ve DNA kodlar elde edilmiştir.

3.6.1. $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Kümesinin Cebirsel Yapısı

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

$a + bu + cv + duv + \langle 0 \rangle = \{a + bu + cv + duv + 0t : a, b, c, d \in \mathbb{F}_2, t \in \mathbb{F}_2[u, v]\} = \{a + bu + cv + duv\}$ olacağından,

$\mathbb{F}_2[u, v] / \langle u^2, v^2 - v, uv - vu \rangle = \{\{a + bu + cv + duv\} : a, b, c, d \in \mathbb{F}_2\}$ elde edilir ve $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 = \{a + bu + cv + duv + \langle u^2, v^2 - v, uv - vu \rangle : a, b, c, d \in \mathbb{F}_2\}$ kümesi de bir halkadır.

3.6.1.1. Teorem:

$$f: \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 \rightarrow \mathbb{F}_2[u, v] / \langle a + bu + cv + duv \rangle$$

$$a + bu + cv + duv \mapsto f(a + bu + cv + duv) = \{a + bu + cv + duv\}$$

dönüşümü bir izomorfizmadır.

Kanıt:

Herhangi $a_1 + b_1u + c_1v + d_1uv, a_2 + b_2u + c_2v + d_2uv \in \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ için,

$$a_1 + b_1u + c_1v + d_1uv = a_2 + b_2u + c_2v + d_2uv \Leftrightarrow a_1 = a_2, b_1 = b_2, c_1 = c_2, d_1 = d_2$$

$$\Leftrightarrow \{a_1 + b_1u + c_1v + d_1uv\} = \{a_2 + b_2u + c_2v + d_2uv\}$$

$$\Leftrightarrow f(a_1 + b_1u + c_1v + d_1uv) = f(a_2 + b_2u + c_2v + d_2uv)$$

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

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

Herhangi $a_1 + b_1u + c_1v + d_1uv, a_2 + b_2u + c_2v + d_2uv \in \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ için,

$$\begin{aligned} & f(a_1 + b_1u + c_1v + d_1uv + a_2 + b_2u + c_2v + d_2uv) \\ &= f((a_1 + a_2) + (b_1 + b_2)u + (c_1 + c_2)v + (d_1 + d_2)uv) \\ &= \{(a_1 + a_2) + (b_1 + b_2)u + (c_1 + c_2)v + (d_1 + d_2)uv\} \\ &= \{a_1 + b_1u + c_1v + d_1uv\} + \{a_2 + b_2u + c_2v + d_2uv\} \\ &= f(a_1 + b_1u + c_1v + d_1uv) + f(a_2 + b_2u + c_2v + d_2uv) \end{aligned}$$

$$\begin{aligned} & f((a_1 + b_1u + c_1v + d_1uv) \cdot (a_2 + b_2u + c_2v + d_2uv)) \\ &= f(a_1a_2 + (a_1b_2 + b_1a_2)u + (a_1c_2 + b_1b_2 + c_1a_2)v \\ &+ (a_1d_2 + d_1d_2 + d_1a_2)uv) \\ &= \{a_1a_2 + (a_1b_2 + b_1a_2)u + (a_1c_2 + b_1b_2 + c_1a_2)v + (a_1d_2 + d_1d_2 \\ &+ d_1a_2)uv\} \end{aligned}$$

$$\begin{aligned} & f(a_1 + b_1u + c_1v + d_1uv) \cdot f(a_2 + b_2u + c_2v + d_2uv) \\ &= \{a_1 + b_1u + c_1v + d_1uv\} \cdot \{a_2 + b_2u + c_2v + d_2uv\} \\ &= \{a_1a_2 + (a_1b_2 + b_1a_2)u + (a_1c_2 + b_1b_2 + c_1a_2)v + (a_1d_2 + d_1d_2 \\ &+ d_1a_2)uv\} \end{aligned}$$

bulunur ve bu durumda,

$$f((a_1 + b_1u + c_1v + d_1uv).(a_2 + b_2u + c_2v + d_2uv)) \\ = f(a_1 + b_1u + c_1v + d_1uv).f(a_2 + b_2u + c_2v + d_2uv)$$

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

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

biçiminde yazılır.

Üstelik $\mathbb{F}_2$ iki elemanlı cisim olmak üzere,

$$\mathbb{F}_2[u, v]/\langle u^2, v^2 - v, uv - vu \rangle \cong \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 = \{a + bu + cv + duv \mid a, b, c, d \in \mathbb{F}_2\} \text{ kümesi}$$

Her $a + bu + cv + duv, a' + b'u + c'v + d'uv \in R$ için

$$(a + bu + cv + duv) + (a' + b'u + c'v + d'uv) = (a + a') + \dots + (d + d')uv$$

$$(a + bu + cv + duv).(a' + b'u + c'v + d'uv) = aa' + \dots + (ad' + dd' + da')uv$$

şeklinde tanımlanan $+$ ve $\cdot$ işlemlerine göre 16 elemanlı karakteristiği 2 olan değişmeli bir semilocal halkadır. Maksimal idealleri I_{u+v}, I_{1+u+v} 'dir (Zhu vd., 2015).

$I_v = \{av \mid a \in R\}$ ve $I_{1+v} = \{(v+1)b \mid b \in R\}$ olmak üzere R 'nin parçalanışı $R = I_v \oplus I_{1+v}$ şeklindedir. $R_1 = \mathbb{F}_2 + u\mathbb{F}_2, u^2 = 0$ sonlu zincir halkası olmak üzere $I_v \cong R_1, I_{1+v} \cong R_1$ olduğu kolayca görülür Bu nedenle herhangi bir $c \in R, a, b \in R$ olmak üzere $c = a + bv$ şeklinde teklikle yazılır (Zhu vd., 2015).

$R_1 = \mathbb{F}_2[u]/\langle u^2 \rangle$ olmak üzere

$$R = \mathbb{F}_2[u, v]/\langle u^2, v^2 - v, uv - vu \rangle = R_1[v]/\langle v^2 - v \rangle \\ \cong \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2, u^2 = 0, v^2 = v, uv = vu \\ = (\mathbb{F}_2 + u\mathbb{F}_2) + v(\mathbb{F}_2 + u\mathbb{F}_2), u^2 = 0, v^2 = v, uv = vu \\ = R_1 + vR_1, v^2 = v$$

şeklinde yazılır (Zhu vd., 2015).

Gray dönüşümü

$$\phi: R \rightarrow R_1^2$$

$$a + bv \mapsto \phi(a + bv) = (a, a + b)$$

şeklindedir.

C, R halkası üzerinde tanımlı bir lineer kod olsun.

$$C_1 = \{x + y \in R_1^n : (x + y)v + x(v + 1) \in C; \exists x, y \in R_1^n\}$$

$$C_2 = \{x \in R_1^n : (x + y)v + x(v + 1) \in C; \exists y \in R_1^n\}$$

olmak üzere C_1 ve C_2 , R_1 halkası üzerinde tanımlı iki lineer koddur ve $C = vC_1 \oplus (1 + v)C_2$ şeklinde yazılır (Zhu vd., 2015).

3.6.2. $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Sonlu Halkası Üzerinde Tanımlı Devirli Kodlar

Zhu ve X. Chen, Taher Abualrub ve İ. Şiap tarafından sınıflandırılan R_1 halkası üzerinde tanımlı devirli kodlar kullanılarak R halkası üzerinde devirli kodların yapısını aşağıdaki şekilde ifade etmiştir.

3.6.2.1. Teorem:

C , R_1 halkası üzerinde tanımlı n uzunluğunda bir devirli kod olsun. (Yani $\pi(C) \subset R_1[x]/\langle x^n - 1 \rangle = R_{1,n}$ 'in ideali)

(i) Eğer n tek ise $R_{1,n}$ esas ideal halkasıdır. $g(x), a(x), a(x)|g(x)|x^n - 1$ olacak şekilde $F_2[x]$ 'te iki polinom olmak üzere $\pi(C) = \langle g(x), ua(x) \rangle = \langle g(x) + ua(x) \rangle$ şeklindedir.

(ii) Eğer n tek değil ise bu durumda

a) $g(x), (x^n - 1)$ 'i bölen $\mathbb{F}_2[x]$ 'te bir polinom ve $g(x) + up(x), (x^n - 1)$ 'i bölen $R[x]$ 'te bir polinom ve $g(x)|p(x)\widehat{g(x)}$ olmak üzere $\pi(C) = \langle g(x) + ua(x) \rangle$ şeklindedir. Veya

b) $g(x), a(x), p(x), a(x)|g(x)|x^n - 1, a(x)|p(x)\widehat{g(x)}$ ve $derp(x) \leq dera(x)$ olacak şekilde $\mathbb{F}_2[x]$ 'te üç polinom ise $\pi(C) = \langle g(x) + up(x), ua(x) \rangle$ şeklindedir (Abualrub vd., 2007).

3.6.2.2. Not:

$\widehat{f(x)}$ polinomu $(x^n - 1)/f(x)$ polinomunu göstermektedir (Zhu vd., 2015).

3.6.2.3. Lemma:

i. C, R halkası üzerinde tanımlı $C = vC_1 \oplus (1 + v)C_2$ şeklinde bir lineer kod olsun. Bu durumda C 'nin devirli olması için gerekli ve yeterli koşul C_1 ve C_2 'nin R_1 halkası üzerinde iki devirli kod olmasıdır.

ii. C, R halkası üzerinde tanımlı $C = vC_1 \oplus (1 + v)C_2$ şeklinde bir lineer kod ise $f_1(x)$ ve $f_2(x)$ sırasıyla C_1 ve C_2 kodlarının üreteç polinomları ise $\pi(C) = \langle vf_1(x), (1 + v)f_2(x) \rangle$ şeklindedir (Zhu vd., 2015).

3.6.3. Ters Sıralı Kodlar

Zhu ve X. Chen, Guenda, K. Aaron, Gulliver T., Liang J. ve Wang L. nin R_1 halkası üzerinde tanımlı bir devirli kodun ters sıralı olması için belirledikleri gerekli ve yeterli koşulu kullanarak bir kodun R halkası üzerinde tanımlı ters sıralı ve ters sıralı tamamlayan kod olması için gerekli ve yeterli koşulları aşağıdaki şekilde vermiştir.

3.6.3.1. Lemma:

$\pi(C) = \langle g(x), up(x) \rangle = \langle g(x) + up(x) \rangle$, R_1 halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun. Bu durumda C kodunun ters sıralı olması için gerek ve yeter koşul $g(x)$ ve $a(x)$ polinomlarının self reciprocal olmalıdır (Guenda vd., 2013).

3.6.3.2. Lemma:

$\pi(C) = \langle g(x) + up(x) \rangle$, R_1 halkası üzerinde tanımlı çift uzunluğunda bir devirli kod olsun. Bu durumda C 'nin ters sıralı kod olması için gerek ve yeter koşul

- i) $g(x)$ polinomu self reciprocaldir
- ii) $i = \text{der}g(x) - \text{der}p(x)$ olmak üzere,
 - a) $x^i p(x)^* = p(x)$ veya
 - b) $g(x) = x^i p(x)^* + p(x)$ olmasıdır (Liang vd., 2015).

3.6.3.3. Lemma:

$g(x), a(x), p(x)$, $a(x)|g(x)|x^n - 1$, $a(x)|p(x)\widehat{g(x)}$ ve $\text{der}p(x) \leq \text{der}a(x)$ olacak şekilde $\mathbb{F}_2[x]$ 'te üç polinom ise $\pi(C) = \langle g(x) + up(x), ua(x) \rangle$ R_1 halkası üzerinde tanımlı çift uzunluğunda bir devirli kod olsun. Bu durumda C 'nin ters sıralı olması için gerek ve yeter koşul

- i. $g(x)$ ve $a(x)$ self reciprocal polinomlar,
- ii. $i = \text{der}g(x) - \text{der}p(x)$ olmak üzere $a(x)|x^i p(x)^* + p(x)$ olmasıdır (Liang vd., 2015).

3.6.3.4. Teorem:

$C = vC_1 \oplus (1 + v)C_2$, R halkası üzerinde tanımlı keyfi uzunluklu bir devirli kod olsun.

C kodunun ters sıralı olması için gerek ve yeterli koşul C_1 ve C_2 devirli kodlarının R_1 halkası üzerinde tanımlı ters sıralı kodlar olmasıdır (Zhu vd., 2015).

Kanıt:

C_1 ve C_2 ters sıralı iki kod olsun. Herhangi bir $\mathbf{b} \in C$ için $\mathbf{b}_1 \in C_1, \mathbf{b}_2 \in C_2$ olmak üzere $\mathbf{b} = v\mathbf{b}_1 + (1 + v)\mathbf{b}_2$ olduğu ve C_1 ve C_2 'nin ters sıralı olduğu kullanılırsa $\mathbf{b}^R = v\mathbf{b}_1^R + (1 + v)\mathbf{b}_2^R \in C$ elde edilir. Dolayısıyla C ters sıralı bir kod olur.

Tersine, C ters sıralı bir kod ise $\mathbf{b}_1 \in C_1, \mathbf{b}_2 \in C_2$ olmak üzere herhangi bir $\mathbf{b} = v\mathbf{b}_1 + (1 + v)\mathbf{b}_2 \in C$ için $\mathbf{b}^R = v\mathbf{b}_1^R + (1 + v)\mathbf{b}_2^R \in C$ elde edilir.

$e_1 \in C_1, e_2 \in C_2$ olmak üzere $\mathbf{b}^R = v\mathbf{b}_1^R + (1 + v)\mathbf{b}_2^R = v\mathbf{e}_1 + (1 + v)\mathbf{e}_2$ olsun. Bu durumda $v(\mathbf{b}_1^R - \mathbf{e}_1) + (1 + v)(\mathbf{b}_2^R - \mathbf{e}_2) = 0$ 'dır. Dolayısıyla, $\mathbf{b}_1^R = \mathbf{e}_1 \in C_1$ ve $\mathbf{b}_2^R = \mathbf{e}_2 \in C_2$ elde edilir.

Böylece C_1 ve C_2 iki ters sıralı koddur.

3.6.4. Ters Sıralı Tamamlayan Kodlar

Bu bölümde Zhu ve Chen tarafından R halkası üzerinde tanımlı keyfi uzunluklu devirli bir C kodunun ters sıralı tamamlayan olması için gerekli ve yeterli koşullar verilecektir.

3.6.4.1. Lemma:

$\bar{c}, c \in R$ elemanının tamamlayıcı olmak üzere $c + \bar{c} = u$ dir (Zhu vd., 2015).

3.6.4.2. Lemma:

Her $a, b \in R$ ise $\overline{a + b} = \bar{a} + \bar{b} + u$ dir (Zhu vd., 2015).

3.6.4.3. Lemma:

Her $c \in \mathbb{F}_2$ ise $u + \bar{u}c = uc$ dir (Zhu vd., 2015).

3.6.4.4. Teorem:

$C = vC_1 \oplus (1 + v)C_2$, R halkası üzerinde tanımlı keyfi uzunluklu bir devirli kod olsun. C 'nin ters sıralı tamamlayan olması için gerekli ve yeterli koşul C_1 ve C_2 R_1 halkası üzerinde tanımlı iki devirli kod olmak üzere C ters sıralı bir kod ve $(\bar{0}, \bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olmasıdır (Zhu vd., 2015).

Kanıt:

C_1 ve C_2 , R_1 üzerinde tanımlı iki devirli kod olmak üzere $C = vC_1 \oplus (1 + v)C_2$ olsun. Her $c = (c_0, \dots, c_{n-1}) \in C$ için C ters sıralı tamamlayan bir kod olduğundan $c^{RC} = (\bar{c}_{n-1}, \bar{c}_{n-2}, \dots, \bar{c}_0) \in C$ 'dir. C lineer bir kod olduğu için $(0, 0, \dots, 0) \in C$ 'dir. C nin ters sıralı tamamlayan kod olduğu kullanılırsa $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ elde edilir. Dolayısıyla $c^R = (c_{n-1}, c_{n-2}, \dots, c_0) = (\bar{c}_{n-1}, \bar{c}_{n-2}, \dots, \bar{c}_0) + (\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ dir.

Diğer yandan,

C ters sıralı kod ise her $c = (c_0, \dots, c_{n-1}) \in C$ için $c^R = (c_{n-1}, c_{n-2}, \dots, c_0) \in C$ dir.

$(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olduğundan $c^{RC} = (\bar{c}_{n-1}, \bar{c}_{n-2}, \dots, \bar{c}_0) = (c_{n-1}, c_{n-2}, \dots, c_0) + (\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ elde edilir. Dolayısıyla C ters sıralı tamamlayan koddur.

3.6.5. $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Halkası Üzerinde Tanımlı DNA Kodlar

$S_{D_4} = \{A, T, G, C\}$ DNA alfabesi olmak üzere S_{D_4} ile R_1 halkasının elemanları arasında tanımlı $0 \rightarrow A, 1 \rightarrow G, u \rightarrow T, 1 + u \rightarrow C$ tanımlı dönüşümü kullanılarak Zhu ve X. Chen Çizelge 3.5' de gösterildiği şekilde,

$S_{D_{16}} = \{AA, AT, AG, AC, TT, TA, TG, GG, GA, GC, GT, CC, CA, CG, CT\}$ kümesi ile R sonlu halkasının elemanları arasındaki birebir eşleşmeyi vermişlerdir (Zhu vd., 2015).

Çizelge 3.5 $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

R halkasının Elemanları	Gray Görüntüleri	Dna çiftleri
0	(0,0)	AA
v	(0,1)	AG

uv	$(0, u)$	AT
$v + uv$	$(0, 1 + u)$	AC
1	$(1, 1)$	GG
$1 + v$	$(1, 0)$	GA
$1 + uv$	$(1, 1 + u)$	GC
$1 + v + uv$	$(1, u)$	GT
u	(u, u)	TT
$u + v$	$(u, 1 + u)$	TC
$u + uv$	$(u, 0)$	TA
$u + v + uv$	$(u, 1)$	TG
$1 + u$	$(1 + u, 1 + u)$	CC
$1 + u + v$	$(1 + u, u)$	CT
$1 + u + uv$	$(1 + u, 1)$	CG
$1 + u + v + uv$	$(1 + u, 0)$	CA

S_{D_4} kümesindeki Watson-Crick tamamlayanları; $\bar{A} = T, \bar{T} = A, \bar{G} = C, \bar{C} = G$ ile verildiği için bu $S_{D_{16}}$ kümesinin elemanlarına $\overline{AA} = TT, \dots, \overline{TA} = (AT)$ şeklinde genişletilir (Zhu vd., 2015).

3.6.5.1. Not:

C, R halkası üzerinde tanımlı keyfi uzunluğunda bir kod ve $c_i \in R$ olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in C$ olsun. Çizelge 3.5' i kullanarak Θ

$$\Theta: C \longrightarrow S_{D_4}^{2n}$$

$$(a_0 + b_0v, a_1 + b_1v, \dots, a_{n-1} + b_{n-1}v) \longrightarrow (a_0, a_1, \dots, a_{n-1}, a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1})$$

şeklinde tanımlanır (Zhu vd., 2015).

3.6.5.2. Örnek:

$(c_0, c_1, c_2, c_3) = (1, v, u, u + v)$ elemanı $\Theta(1, v, u, u + v) = GATTGGTC$ ile eşleşir (Zhu vd., 2015).

3.6.5.3. Teorem:

$a, b \in R_1$ olmak üzere,

$$\sigma: \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 \longrightarrow \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2,$$

$$a + bv \mapsto a + (1 + v)b$$

şeklinde tanımlanan dönüşüm aşıkarak olmayan bir otomorfizmadır (Zhu vd., 2015).

3.6.5.4. Tanım:

$f_1(x)$ ve $f_2(x)$, $x^n - 1$ polinomunu bölen, dereceleri sırasıyla t_1 ve t_2 olan $R[x]$ te iki polinom olsun. $m = \min\{n - t_1, n - t_2\}$ ve $f(x) = vf_1(x) + (1 + v)f_2(x) \in R[x]$ olsun. $t_2 \geq t_1$ iken $h(x) = vx^{t_2-t_1}f_1(x) + (1 + v)f_2(x)$, aksi takdirde $h(x) = vf_1(x) + (1 + v)x^{t_2-t_1}f_2(x)$, $0 \leq i \leq m - 1$ için $E_i(x) = x^i f(x)$, $F_i(x) = x^i \sigma(h(x))$ olsun. Bu durumda $L(f) = \{E_0(x), E_1(x), \dots, E_{m-1}(x), F_0(x), F_1(x), \dots, F_{m-1}(x)\}$ olarak tanımlanan kümeye σ kümesi denir. $L(f)$ R halkası üzerinde C lineer kodunu üretir ve $C = \langle f \rangle_\sigma$ ile gösterilir (Zhu vd., 2015).

3.6.5.5. Uyarı:

$\langle L(f) \rangle$ (yada) $\langle f \rangle_\sigma$ ile $L(f)$ kümesi ile üretilen R -alt modül, $(f(x))$ ile $f(x)$ ile üretilen ideali gösterilecektir (Zhu vd., 2015).

3.6.5.6. Not:

$g(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1} + a_t x^t \in R[x]$, $\sigma(h(x)) = b_0 + b_1x + \dots + b_s x^s$ olmak üzere $L(f)$ ile üretilen R -alt modül,

$$L(f) = \begin{pmatrix} E_0(x) \\ F_0(x) \\ E_1(x) \\ F_1(x) \\ \dots \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_t & 0 & \dots & \dots & \dots & 0 \\ b_0 & b_1 & b_2 & \dots & \dots & b_s & 0 & \dots & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_t & \dots & \dots & \dots & \dots & 0 \\ 0 & b_0 & b_1 & \dots & \dots & \dots & \dots & b_s & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

matrisinin satırları ile üretilmiştir (Zhu vd., 2015).

3.6.5.7. Teorem:

$f_1(x)$ ve $f_2(x)$, $x^n - 1$ polinomunu bölen, sırasıyla t_1 ve t_2 dereceli $R_1[x]$ te iki self reciprocal polinom olsun. $f_1(x) = f_2(x)$ ise $f(x) = vf_1(x) + (1 + v)f_2(x)$ ve

$|\langle L(f) \rangle| = 16^m$ dir. Ayrıca $C = \langle L(f) \rangle$, R halkası üzerinde tanımlı bir lineer koddur ve $\Theta(C)$ ters sıralı DNA koddur (Zhu vd., 2015).

3.6.5.8. Sonuç:

C_1 ve C_2 iki kod olmak üzere $C = vC_1 \oplus (1 + v)C_2$ keyfi uzunluklu R halkası üzerinde tanımlı bir devirli kod ve $C = \langle L(f) \rangle$ olsun. Eğer $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ ise bu durumda $\Theta(C)$ ters sıralı tamamlayan DNA koddur (Zhu vd., 2015).

3.6.5.9. Sonuç:

C_1 ve C_2 ters sıralı kodlar olmak üzere $C = vC_1 \oplus (1 + v)C_2$ keyfi uzunluklu R halkası üzerinde tanımlı bir devirli kod, $C = \langle L(f) \rangle$ ve $\Theta(C)$ ters sıralı DNA kod olsun. $(\bar{0}, \bar{0}, \dots, \bar{0})$ elemanları $L(f)$ üreteç kümesine eklenirse bu durumda $\Theta(C)$ ters sıralı tamamlayan DNA koddur (Zhu vd., 2015).

3.6.5.10. Teorem:

C_1 , R_1 halkası üzerinde tanımlı ters sıralı kod ve $f(x) = vf_1(x) + (v + 1)f_2(x) \in R[x]$ olsun. Bu durumda $C = \langle f(x) \rangle$, R halkası üzerinde tanımlı ters sıralı devirli koddur ve $\Theta(C)$ ters sıralı DNA koddur. Eğer, $x - 1 \nmid f(x)$ ise bu durumda $\Theta(C)$ ters sıralı tamamlayan DNA koddur (Zhu vd., 2015).

3.7. $u^2 = 0$ Olmak Üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı Devirli DNA Kodlar

Pattanayak, Abualrub, Kumar Sing tarafından $\mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = 0$ halkası üzerinde tanımlı tek uzunluğundaki devirli kodların ters sıralı ve ters sıralı tamamlayan olması için gerekli ve yeterli koşullar verilmiştir.

3.7.1. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Kümesinin Cebirsel Yapısı

$R = \mathbb{Z}_4[u]/\langle u^2 \rangle \cong \mathbb{Z}_4 + u\mathbb{Z}_4 = \{a + ub : a, b \in \mathbb{Z}_4\}$ kümesi

Her $a + bu, c + du \in R$ için

$$(a + bu) + (c + du) = (a + c) + u(b + d)$$

$$(a + bu) \cdot (c + du) = ac + u(ad + bc)$$

şeklinde tanımlanan $+$ ve $\cdot$ işlemlerine göre, karakteristiği 4 olan, değişmeli, lokal bir halkadır. Tek maksimal ideali $\langle 2, u \rangle$ 'dur. Dolayısıyla R esas ideal halkası değildir. Aynı zamanda R sonlu zincir olmayan bir halkadır.

Halkanın idealleri;

- $I_u = u(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, u, 2u, 3u\}$
- $I_2 = 2(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, 2, 2u, 2 + 2u\}$
- $I_{2+u} = (2 + u)(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, 2 + u, 2u, 2 + 3u\}$
- $I_{2,u} = \{0, 2, u, 2u, 3u, 2 + u, 2 + 2u, 2 + 3u\}$ olmak üzere
- $I_0 = \{0\} \subseteq I_{2u} = 2u(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, 2u\} \subseteq I_u, I_2, I_{2+u} \subseteq I_{2,u} \subseteq I_1 = (\mathbb{Z}_4 + u\mathbb{Z}_4)$ şeklindedir.

3.7.2. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı Devirli Kodlar

3.7.2.1. Teorem:

C, R halkası üzerinde tanımlı tek uzunluklu bir devirli kod olsun. Bu durumda

- 1) $1 \leq i \leq 4$ için $f_i(x)$ ler $f_2(x)|f_1(x)|(x^n - 1)$ ve $f_4(x)|f_3(x)|(x^n - 1)$ sağlayan polinomlar olmak üzere $\pi(C) = \langle f_1(x) + 2f_2(x) + 2uf_4(x), uf_3(x) + 2uf_4(x) \rangle \subset R[x]/\langle x^n - 1 \rangle$ 'tir.
- 2) $f_2(x)|f_1(x)|(x^n - 1)$ olmak üzere $f_1(x) = f_4(x)$ ise bu durumda $\pi(C) = \langle f_1(x) + f_2(x) + 2uf_4(x) \rangle$ tir (Pattanayak vd., 2016).

3.7.3. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı DNA Kodlar

$0 \leq i \leq 1$ için $x_i \in \{A, T, G, C\} = S_{D_4}$ olmak üzere n uzunluğunda bir DNA kod sözcüğü $(x_0, x_1, \dots, x_{n-1})$ olarak tanımlanır. Bu makalede çalışılmış DNA kod alfabesi; $\{AA, TT, GG, CC, AT, TA, GC, CG, GT, TG, AC, CA, CT, TC, AG, GA\}$ 'dir. Çizelge 3.6' da $\theta: R \rightarrow \{A, T, G, C\}^2$ dönüşümü yardımıyla $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkasının elemanlarına karşılık gelen DNA çiftlerinin çizelgesi verilmiştir (Pattanayak vd., 2016).

Çizelge 3.6 $\mathbb{Z}_4 + u\mathbb{Z}_4$ Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

$AA \rightarrow 0$	$TT \rightarrow 1 + u$	$GG \rightarrow 1$	$CC \rightarrow u$
$AT \rightarrow 2$	$TA \rightarrow 3 + u$	$GC \rightarrow 3$	$CG \rightarrow 2 + u$
$GT \rightarrow 2u$	$CA \rightarrow 1 + 3u$	$AC \rightarrow 3u$	$TG \rightarrow 1 + 2u$
$CT \rightarrow 2 + 3u$	$GA \rightarrow 3 + 2u$	$AG \rightarrow 2 + 2u$	$TC \rightarrow 3 + 3u$

3.7.4. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Sonlu Halkası Üzerinde Tanımlı Ters Sıralı Kodlar

3.7.4.1. Lemma:

Her $f(x), g(x), h(x) \in R[x]$ için $\text{der}(f(x)) > \text{der}(g(x)) > \text{der}(h(x))$ olmak üzere,

$$1) [f(x)g(x)h(x)]^* = f(x)^*g(x)^*h(x)^* \text{ tir.}$$

$$2) [f(x) + g(x) + h(x)]^* = f(x)^* + x^{\text{der}f(x) - \text{der}g(x)}g(x)^* + x^{\text{der}f(x) - \text{der}h(x)}h(x)^* \text{ dir (Pattanayak vd., 2016).}$$

3.7.4.2. Lemma:

$C = \langle f(x) \rangle$, $\mathbb{Z}_4$ halkası üzerinde tanımlı bir devirli kod olsun. C kodunun ters sıralı olması için gerekli ve yeterli koşul $f(x)$ 'in self reciprocal polinom olmasıdır (Pattanayak vd., 2016).

3.7.4.3. Teorem:

$f_2(x)|f_1(x)|(x^n - 1)$ olmak üzere $\pi(C) = \langle f_1(x) + f_2(x) + 2uf_4(x) \rangle$ kodu R halkası üzerinde tanımlı tek uzunluğuna sahip devirli bir kod olsun. C 'nin ters sıralı olması için gerekli ve yeterli koşul

$$i) f_1(x), \text{ self reciprocal bir polinom}$$

$$ii) i = \text{der}f_1(x) - \text{der}f_2(x), j = \text{der}f_1(x) - \text{der}f_4(x) \text{ olmak üzere}$$

$$a) x^i f_2(x)^* = f_2(x) \text{ ve}$$

$$b) x^j f_4(x)^* = f_4(x) \quad \text{veya} \quad f_2(x)|(2x^j f_4(x)^* + 2f_4(x)) \quad \text{olmasıdır}$$

(Pattanayak vd., 2016).

Kanıt:

$\pi(C) = \langle f_1(x) + f_2(x) + 2uf_4(x) \rangle$ kodu R halkası üzerinde tanımlı ters sıralı bir kod olsun. $C, \mathbb{Z}_4$ üzerinde ters sıralı ise $f_1(x)$ self-reciprocal bir polinomdur. $i = \text{der}f_1(x) - \text{der}f_2(x), j = \text{der}f_1(x) - \text{der}f_4(x)$ olmak üzere

$$(f_1(x) + 2f_2(x) + 2uf_{14}(x))^* = f_1(x)^* + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \dots \quad (1)$$

$$= f_1(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \dots \quad (2)$$

$$= (f_1(x) + 2f_2(x) + 2uf_4(x))(a(x)) \text{ şeklindedir.}$$

(1) ve (2) eşitliğinin dereceleri karşılaştırıldığında $c \in R$ olmak üzere $a(x) = c$ elde edilir. Bu durumda

$$f_1(x) + 2x^i f_2(x)^* + 2ux^j f_{14}(x)^* = cf_1(x) + c2f_2(x) + c2uf_4(x) \dots \quad (3)$$

dir.

(3) eşitliğinin her iki tarafı $2u$ ile çarpılırsa, $2uf_1(x) = c.2uf_1(x)$ elde edilir. Bu durumda $c = 1, 1 + u, 1 + 2u$ veya $1 + 3u$ 'dur.

$c = 1$ ise (3) eşitliğinde yazıldığında;

$$2x^i f_2(x)^* + 2ux^j f_4(x)^* = 2f_2(x) + 2uf_4(x) \dots \quad (4)$$

elde edilir.

(4) eşitliğinin her iki tarafı u ile çarpılırsa, $u^2 = 0$ olduğunda $2ux^i f_2^*(x) = 2uf_2(x)$ elde edilir. Bu durumda $i = \text{der}f_1(x) - \text{der}f_2(x)$ olmak üzere $x^i f_2(x)^* = f_2(x)$ tir.

Tekrar (4) kullanılırsa, $j = \text{der}f_1(x) - \text{der}f_4(x)$ olmak üzere $x^j f_4(x)^* = f_4(x)$ elde edilir. $c = 1 + u$ ise (3) eşitliğinde yerine yazıldığında;

$$f_1(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^* = f_1(x) + uf_1(x) + 2f_2(x) + 2uf_2(x) + 2uf_4(x) \dots \quad (5)$$

elde edilir.

(5) eşitliğinin her iki tarafı u ile çarpılırsa, $x^i f_2(x)^* = f_2(x)$ bulunur.

(5) denklemini kullanarak $2ux^j f_4(x)^* + 2uf_4(x) = uf_1(x) + 2uf_2(x)$ elde edilir.

$f_2(x)|f_1(x)$ olduğu için $\langle 2x^j f_4(x)^* + 2f_4(x) \rangle \in \langle f_2(x) \rangle$ tir. Dolayısıyla, $f_2(x)|\langle 2x^j f_4(x)^* + 2f_4(x) \rangle$ tir.

$c = 1 + 2u$ için eşitliğinde yazıldığında;

$$f_1(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^* = f_1(x) + 2uf_1(x) + 2f_2(x) + 2uf_4(x) \dots \quad (6)$$

Benzer şekilde (6) eşitliğinin her iki tarafı u ile çarpılırsa;

$x^i f_2(x)^* = f_2(x)$ bulunur. (6) denklemi kullanılarak $2x^j f_4(x)^* + 2f_4(x) = 2f_1(x)$ bulunur.

Dolayısıyla $f_2(x)|f_1(x)$ olduğu için $f_2(x)|2x^j f_4(x)^* + 2f_4(x)$ dir.

$c = 1 + 3u$ için benzer sonuç alınacaktır.

Diğer yandan $c = 1, 1 + u, 1 + 2u$ ya da $1 + 3u$ ve $i = \text{der} f_1(x) - \text{der} f_2(x), j = \text{der} f_1(x) - \text{der} f_4(x)$ olmak üzere

$$(f_1(x) + 2f_2(x) + 2uf_4(x))^* = f_1(x)^* + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \dots (1)$$

$$= f_1(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \dots (2)$$

$$= (f_1(x) + 2f_2(x) + 2uf_4(x))c \in \pi(C) \quad \text{elde}$$

edilir.

Sonuç olarak, C ters sıralı bir koddur.

3.7.4.4. Teorem:

$f_2(x)|f_1(x)|x^n - 1$ ve $f_4(x)|f_3(x)|x^n - 1$ olmak üzere $\pi(C) = \langle f_1(x) + 2f_2(x) + 2uf_4(x), uf_3(x) + 2uf_4(x) \rangle$ kodu R halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun. C kodunun ters sıralı olması için gerekli ve yeterli koşul

i) $f_1(x)$ ve $f_3(x)$ self reciprocal polinomlar

ii) $i = \text{der} f_1(x) - \text{der} f_2(x), j = \text{der} f_1(x) - \text{der} f_4(x)$ olmak üzere

a) $x^i f_2(x)^* = f_2(x)$ ve

b) $f_4(x)|2x^j f_4(x)^* + 2f_4(x)$ veya $f_4(x)|(2x^j f_4(x)^* + 2f_4(x) + 2f_2(x))$

olmasıdır (Pattanayak vd., 2016).

Kanıt:

$C = \langle f_1(x) + 2f_2(x) + 2uf_4(x), uf_3(x) + 2uf_4(x) \rangle$ ters sıralı bir kod olsun.

Öyleyse; $\langle f_1(x) \rangle$ ve $\langle f_3(x) \rangle$, $\mathbb{Z}_4$ halkası üzerinde tanımlı ters sıralı kodlardır. $f_1(x)$ ve $f_3(x)$ self reciprocal polinomlardır.

C ters sıralı kod ve, $f_4(x)|f_3(x)$ olduğundan $i = \text{der} f_1(x) - \text{der} f_2(x), j = \text{der} f_1(x) - \text{der} f_4(x)$ olmak üzere

$$(f_1(x) + 2f_2(x) + 2uf_4(x))^* = f_1(x)^* + 2x^i f_2(x)^* + 2ux^j f_4(x)^*$$

$$= f_1(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \dots (7)$$

$$\begin{aligned}
&= (f_1(x) + 2f_2(x) + 2uf_4(x))a(x) + \\
&\quad u(f_3(x) + 2f_4(x))b_1(x) \\
&= (f_1(x) + 2f_2(x) + 2uf_4(x))a(x) + \\
&\quad uf_4(x)b(x) \quad \dots \quad (8)
\end{aligned}$$

elde edilir.

(7) ve (8) eşitliğindeki denklemlerin dereceleri kıyaslanırsa $c \in R$ olmak üzere $a(x) = c$ elde edilir. Bu durumda

$$\begin{aligned}
&f_1(x) + 2x^i f_2(x)^* + 2ux^j f_{14}(x)^* \\
&= c \cdot f_1(x) + c \cdot 2f_2(x) + c \cdot 2uf_{14}(x) + u(f_3(x) + 2f_4(x))b(x) \dots \quad (9)
\end{aligned}$$

tir.

(9) eşitliğinin her iki tarafı $2u$ ile çarpılırsa, $2uf_1(x) = c \cdot 2uf_1(x)$ elde edilir. Bu durumda $c = 1, 1 + u, 1 + 2u$ veya $1 + 3u$ dir.

$c = 1$ ise (9)' dan,

$$\begin{aligned}
&f_1(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \\
&= f_1(x) + 2f_2(x) + 2uf_4(x) + u(f_3(x) + 2f_4(x))b(x) \dots \quad (10)
\end{aligned}$$

bulunur.

(10) eşitliğinin her iki tarafı u ile çarpılırsa, $u^2 = 0$ olduğu için

$2ux^i f_2(x)^* = 2uf_2(x)$ elde edilir. Dolayısıyla $i = \text{der} f_1(x) - \text{der} f_2(x)$ olmak üzere $x^i f_2(x)^* = f_2(x)$ şeklindedir.

(10) eşitliğinden

$2ux^j f_4(x)^* + 2uf_4(x) = u(f_3(x) + 2f_4(x))b(x)$ elde edilir.

$f_4(x)|f_3(x)$ olduğu için $\langle 2x^j f_4(x)^* + 2f_4(x) \rangle \in \langle f_4(x) \rangle$ tir.

Dolayısıyla, $f_4(x)|\langle 2x^j f_4(x)^* + 2f_4(x) \rangle$ tir.

$c = 1 + u$ ise (9) eşitliğinden,

$$\begin{aligned}
&f_1(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \\
&= f_1(x) + uf_1(x) + 2f_2(x) + 2uf_2(x) + 2f_4(x) \\
&+ u(f_3(x) + 2f_4(x))b(x) \quad \dots \quad (11)
\end{aligned}$$

elde edilir.

(11) eşitliğinin her iki tarafı u ile çarpılırsa, $x^i f_2(x)^* = f_2(x)$ bulunur.

(11) eşitliğinden,

$2ux^j f_4(x)^* + 2uf_4(x) + 2uf_2(x) = uf_1(x) + u(f_3(x) + 2f_4(x))b(x)$ elde edilir.

$f_4(x)|f_3(x)|f_1(x)$ olduğu için $(2x^j f_4(x)^* + 2uf_4(x) + 2f_2(x)) \in \langle f_4(x) \rangle$ tir.

Dolayısıyla, $f_4(x)|(2x^j f_4(x)^* + 2f_4(x) + 2f_2(x))$ dir.

$c = 1 + 2u$ ve $c = 1 + 3u$ için de $c = 1$ ve $c = 1 + u$ dakine benzer şekilde aynı sonuçlar elde edilir.

Aksine, C 'nin ters sıralı bir kod olduğunu göstermek için $(f_1(x) + 2f_2(x) + 2uf_4(x))^*$ ve $u(f_3(x) + 2f_4(x))^*$ C elemanlarının kümesinde olduğunu göstermek yeterlidir.

$f_4(x)|f_3(x)$ ve $f_3(x)$ self reciprocal bir polinom ise $uf_4(x) \in C$ dir.

Aynı zamanda,

$$\begin{aligned} (f_1(x) + 2f_2(x) + 2uf_4(x))^* &= f_1(x)^* + 2x^i f_2(x)^* + 2ux^j f_4(x)^* \\ &= (f_1(x) + 2f_2(x) + 2uf_4(x)) + 2ux^j f_4(x)^* + 2uf_{14}(x) \\ &= (f_1(x) + 2f_2(x) + 2uf_4(x)) + uf_4(x)b(x) \in C \text{ dir.} \end{aligned}$$

Dolayısıyla C , ters sıralı bir koddur.

3.7.5. $\mathbb{Z}_4 + u\mathbb{Z}_4$ Halkası Üzerinde Tanımlı Ters Sıralı Tamamlayan Kodlar

R halkası üzerinde tanımlı tek uzunluğa sahip devirli kodun ters sıralı tamamlayan olması için gerekli ve yeterli şartlar verilecektir.

3.7.5.1. Lemma:

$\bar{a}$, herhangi $a \in R$ nin tamamlayıcı olmak üzere $a + \bar{a} = 1 + u$ dir (Pattanayak vd., 2016).

3.7.5.2. Lemma:

Her $a, b, c \in R$ için

- i) $\overline{a + b} = \bar{a} + \bar{b} + 3(1 + u);$
- ii) $\overline{a + b + c} = \bar{a} + \bar{b} + \bar{c} + 2(1 + u)$ dir (Pattanayak vd., 2016).

3.7.5.3. Lemma:

Her $a \in \mathbb{Z}_4$ için $\overline{2ua} + 3(1 + u) = 2au$ dir (Pattanayak vd., 2016).

3.7.5.4. Lemma:

Her $a \in R$ için

$$i) \overline{2a} + 3(1 + u) = 2a,$$

$$ii) \bar{a} + 3(1 + u) = 3a \text{ dir (Pattanayak vd., 2016).}$$

3.7.5.5. Teorem:

$f_2(x)|f_1(x)|x^n - 1$ olmak üzere $\pi(C) = \langle f_1(x) + 2f_2(x) + 2uf_{14}(x) \rangle$ kodu R halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun. C 'nin ters sıralı tamamlayan olması için gerekli ve yeterli koşul

$$a) f_1(x) \text{ self reciprocal bir polinom ve } 3(1 + u)((1 - x^n)/(1 - x)) \in \pi(C);$$

$$b) i) i = \text{der} f_1(x) - \text{der} f_2(x), j = \text{der} f_1(x) - \text{der} f_4(x) \text{ olmak üzere}$$

$$x^i f_2(x)^* = f_2(x) \text{ ve}$$

$$ii) x^j f_4(x)^* = f_4(x) \quad \text{veya} \quad f_2(x) | (2x^j f_4(x)^* + 2f_4(x)) \quad \text{olmasıdır}$$

(Pattanayak vd., 2016).

Kanıt:

$f_2(x)|f_1(x)|x^n - 1$ olmak üzere $\pi(C) = \langle f_1(x) + 2f_2(x) + 2uf_4(x) \rangle$ kodu R halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun.

$$(0, 0, \dots, 0) \in C \text{ olduğu için } (\bar{0}, \bar{0}, \dots, \bar{0}) \in C \text{ olur.}$$

$$3(\overline{0, 0, \dots, 0}) = 3(1 + u, 1 + u, \dots, 1 + u) \in C \leftrightarrow 3(1 + u) \frac{1 - x^n}{1 - x} \in \pi(C).$$

$$s > r > t \text{ olmak üzere } f_1(x) = 1 + g_1'x + \dots + g_{s-1}'x^{s-1} + x^s,$$

$$f_2(x) = 1 + g_1''x + \dots + g_{r-1}''x^{r-1} + x^r,$$

$$\text{ve } f_4(x) = 1 + g_1'''x + \dots + g_{t-1}'''x^{t-1} + x^t \text{ olsun.}$$

Bu durumda,

$$\begin{aligned} & f_1(x) + 2f_2(x) + 2f_4(x) \\ &= (1 + g_1'x + \dots + g_{s-1}'x^{s-1} + x^s) \\ &+ (2 + 2g_1''x + \dots + 2g_{r-1}''x^{r-1} + 2x^r) \\ &+ (2 + 2ug_1'''x + \dots + 2ug_{t-1}'''x^{t-1} + 2ux^t) \end{aligned}$$

$$=(3+2u)+(g_1'+2g_1''+2ug_1''')x+\dots(g_{t-1}'+2g_{t-1}''+2ug_{t-1}''')x^{t-1}+\dots+(g_t'+2g_t''+2u)x^t+(g_{t+1}'+2g_{t+1}'')x^{t+1}+\dots+(g_{r-1}'+2g_{r-1}'')x^{r-1}+(g_r'+2)x^r+g_{r+1}'x^{r+1}+\dots+g_{s-1}'x^{s-1}+x^s \text{ tir.}$$

Dolayısıyla,

$$\begin{aligned} & (f_1(x) + 2f_2(x) + 2uf_4(x))^{RC} \\ &= (1+u)(1+x+\dots+x^{n-s-2}) + ux^{n-s-1} + \overline{g_{s-1}'}x^{n-s} + \dots \\ &+ \overline{g_{r+1}'}x^{n-r-2} + \overline{(g_r'+2)}x^{n-r-1} + \overline{(g_{r-1}'+2g_{r-1}'')}x^{n-r} + \dots \\ &+ \overline{(g_{t+1}'+2g_{t+1}'')}x^{n-t-2} + \overline{(g_t'+2g_t''+2u)}x^{n-t-1} \\ &+ \overline{(g_{t-1}'+2g_{t-1}''+2ug_{t-1}''')}x^{n-t} + \dots + \overline{(g_1'+2g_1''+2ug_1''')}x^{n-2} \\ &+ (3+2u)x^{n-1} \\ &= (1+u)(1+x+\dots+x^{n-s-2}) + ux^{n-s-1} + \overline{g_{s-1}'}x^{n-s} + \dots + \\ &\overline{g_{r+1}'}x^{n-r-2} + \overline{g_r'}x^{n-r-1} + 2x^{n-r-1} + \overline{g_{r-1}'}x^{n-r} + 2g_{r-1}''x^{n-r} + \dots + \\ &\overline{g_{t+1}'}x^{n-t-2} + 2g_{t+1}''x^{n-t-2} + \overline{g_t'}x^{n-t-1} + 2g_t''x^{n-t-1} + 2ux^{n-t-1} + \overline{g_{t-1}'}x^{n-t} + \\ &2g_{t-1}''x^{n-t} + 2ug_{t-1}'''x^{n-t} + \dots + \overline{g_1'}x^{n-2} + 2g_1''x^{n-2} + 2ug_1'''x^{n-2} + (3+ \\ &2u)x^{n-1} \\ &= (1+u)(1+x+\dots+x^{n-s-2}) + ux^{n-s-1} + \overline{g_{s-1}'}x^{n-s} + \dots + \\ &\overline{g_{r+1}'}x^{n-r-2} + \overline{g_r'}x^{n-r-1} + \overline{g_{r-1}'}x^{n-r} + \overline{g_{t+1}'}x^{n-t-2} + \overline{g_t'}x^{n-t-1} + \overline{g_{t-1}'}x^{n-t} + \\ &\dots + \overline{g_1'}x^{n-2} + ux^{n-1} + 2x^{n-r-1} + 2g_{r-1}''x^{n-r} + \dots + 2g_{t+1}''x^{n-t-2} + \\ &2g_t''x^{n-t-1} + 2g_{t-1}''x^{n-t} + \dots + 2g_1''x^{n-2} + 2x^{n-1} + 2ux^{n-t-1} + 2ug_{t-1}'''x^{n-t} + \\ &\dots + 2ug_1'''x^{n-2} + 2ux^{n-1} \\ &= (1+u)(1+x+\dots+x^{n-s-2}) + ux^{n-s-1} + \overline{g_{s-1}'}x^{n-s} + \dots + \\ &\overline{g_1'}x^{n-2} + ux^{n-1} + 3.2x^{n-r-1} + 3.2g_{r-1}''x^{n-r} + \dots + 3.2g_1''x^{n-2} + \\ &3.2x^{n-1} + 3.2ux^{n-t-1} + 3.2ug_{t-1}'''x^{n-t} + \dots + 3.2ug_1'''x^{n-2} + 3.2ux^{n-1} \text{ tir.} \end{aligned}$$

C lineer kod olduğundan,

$$(f_1(x) + 2f_2(x) + 2f_{14}(x))^{RC} + 3(1+u)\frac{1-x^n}{1-x} \in \pi(C)$$

elde edilir.

Dolayısıyla,

$$\begin{aligned}
& (f_1(x) + 2f_2(x) + 2f_4(x))^{RC} + 3(1+u) \frac{1-x^n}{1-x} \\
&= 3x^{n-s-1} + (\overline{g_{s-1}'} + 3(1+u))x^{n-s} + \dots + (\overline{g_1'} + 3(1+u))x^{n-2} \\
&+ 3x^{n-1} + 3.2x^{n-r-1}(1 + g_{r-1}''x + \dots + g_1''x^{r-1} + x^r) \\
&+ 3.2ux^{n-t-1}(1 + g_{t-1}'''x + \dots + g_1'''x^{t-1} + x^t) \\
&= 3x^{n-s-1} + 3g_{s-1}'x^{n-s} + \dots + 3g_1'x^{n-2} + 3x^{n-1} \\
&\quad + 3.2x^{n-r-1}(1 + g_{r-1}''x + \dots + g_1''x^{r-1} + x^r) \\
&\quad + 3.2ux^{n-t-1}(1 + g_{t-1}'''x + \dots + g_1'''x^{t-1} + x^t) \\
&= 3x^{n-s-1}(1 + g_{s-1}'x + \dots + g_1'x^{s-1} + x^s) \\
&\quad + 3.2x^{n-r-1}(1 + g_{r-1}''x + \dots + g_1''x^{r-1} + x^r) \\
&\quad + 3.2ux^{n-t-1}(1 + g_{t-1}'''x + \dots + g_1'''x^{t-1} + x^t) \\
&= 3x^{n-s-1}f_1^*(x) + 3.2x^{n-r-1}f_2^*(x) + 3.2ux^{n-t-1}f_4^*(x). \\
&= 3x^{n-s-1}(f_1^*(x) + 2x^{s-r}f_2^*(x) + 2ux^{s-t}f_4^*(x)) \text{ elde edilir.}
\end{aligned}$$

Bu nedenle,

$$f_1(x)^* + 2x^{s-r}f_2(x)^* + 2ux^{s-t}f_4(x)^* \in \pi(C) \text{ dir.}$$

Dolayısıyla,

$$f_1(x)^* + 2x^{s-r}f_2(x)^* + 2ux^{s-t}f_4(x)^* = (f_1(x) + 2f_2(x) + 2f_4(x))a(x)$$

elde edilir. Bu durumda,

$$a(x) = 1, 1+u, 1+2u \text{ veya } 1+3u \text{ olabilir.}$$

$f_1(x) = f_1(x)^*$ yani $f_1(x)$ self reciprocal bir polinomdur. Aynı zamanda; $i = s-r, j = s-t$ olmak üzere $x^i f_2(x)^* = f_2(x)$ ve $x^j f_4(x)^* = f_4(x)$ veya $f_2(x)|(2x^j f_4(x)^* + 2f_4(x))$ tir.

Diğer taraftan, $c(x) \in \pi(C)$ ise, $c(x) = (f_1(x) + 2f_2(x) + 2f_4(x))a(x)$ 'dir.

$f_1(x)$ self reciprocal bir polinom ve $i = \text{der} f_1(x) - \text{der} f_2(x), j = \text{der} f_1(x) - \text{der} f_4(x)$ olmak üzere $x^i f_2(x)^* = f_2(x)$ ve $x^j f_4(x)^* = f_4(x)$ veya $f_2(x)|(2x^j f_4(x)^* + 2f_4(x))$ olduğu için

$$\begin{aligned}
c(x)^* &= (f_1(x) + 2f_2(x) + 2f_4(x))a(x)^* \\
&= (f_1(x)^* + 2x^i f_2(x)^* + 2ux^j f_4(x)^*)a(x)^* \\
&= (f_1(x) + 2f_2(x) + 2uf_4(x))c.a(x)^* \text{ elde edilir.}
\end{aligned}$$

Bu durumda $c = 1, 1+u, 1+2u$ veya $1+3u$ dir.

Dolayısıyla, $c(x)^* \in \pi(C)$ dir.

$$3(1+u) \frac{1-x^n}{1-x} \in \pi(C) \text{ olduğundan,}$$

$$3(1+u) \frac{1-x^n}{1-x} = 3(1+u) + 3(1+u)x + \dots + 3(1+u)x^{n-1} \in \pi(C) \text{ elde edilir.}$$

$c(x) = c_0 + c_1x + \dots + c_mx^m \in \pi(C)$ olsun. C n uzunluğunda bir devirli kod olduğundan,

$$x^{n-m-1}c(x) = c_0x^{n-m-1} + c_1x^{n-m} + \dots + c_mx^{n-1} \in \pi(C).$$

Bu yüzden,

$$\begin{aligned} & 3(1+u) + 3(1+u)x + \dots + 3(1+u)x^{n-m-2} + (c_0 + 3(1+u))x^{n-m-1} \\ & \quad + (c_1 + 3(1+u))x^{n-m} + \dots + (c_m + 3(1+u))x^{n-1} \\ & = 3(1+u) + 3(1+u)x + \dots + 3(1+u)x^{n-m-2} + 3\bar{c}_0x^{n-m-1} + 3\bar{c}_1x^{n-m} + \dots \\ & \quad + 3\bar{c}_mx^{n-1} \\ & = 3((1+u) + (1+u)x + \dots + (1+u)x^{n-m-2} + \bar{c}_0x^{n-m-1} + \bar{c}_1x^{n-m} + \dots \\ & \quad + \bar{c}_mx^{n-1}) \in \pi(C) \text{ elde edilir.} \end{aligned}$$

$c^*(x)^{RC} \in \pi(C)$ dir. Dolayısıyla, $(c^*(x)^{RC})^* = c(x)^{RC}$ elde edilir.

3.7.5.6. Teorem:

$f_2(x)|f_1(x)|x^n - 1$ ve $f_4(x)|f_3(x)|x^n - 1$ olmak üzere $\pi(C) = \langle f_1(x) + 2f_2(x) + 2uf_4(x), uf_3(x) + 2uf_4(x) \rangle$ kodu R halkası üzerinde tanımlı tek uzunluğunda bir devirli kod olsun. C kodunun ters sıralı tamamlayan kod olması için gerekli ve yeterli koşul

- a) $3(1+u)((1-x^n)/(1-x)) \in \pi(C)$ ve $f_1(x), f_3(x)$ polinomlarının self reciprocal;
- b) $i = \text{der}f_1(x) - \text{der}f_2(x), j = \text{der}f_1(x) - \text{der}f_4(x)$ olmak üzere
 - i. $x^i f_2(x)^* = f_2(x)$ ve
 - ii. $f_4(x) | (2x^j f_4(x)^* + 2f_4(x))$ veya $f_4(x) | (2x^j f_4(x)^* + 2f_4(x) + 2f_2(x))$ olmasıdır (Pattanayak vd., 2016).

Kanıt:

$f_2(x)|f_1(x)|x^n - 1$ ve $f_4(x)|f_3(x)|x^n - 1$ olmak üzere $\pi(C) = \langle f_1(x) + 2f_2(x) + 2uf_4(x), uf_3(x) + 2uf_4(x) \rangle$ olsun.

$(0,0, \dots, 0) \in C$ olduğu için $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olur. Dolayısıyla

$$3(\bar{0}, \bar{0}, \dots, \bar{0}) = 3(1+u, 1+u, \dots, 1+u) \in C \leftrightarrow 3(1+u) \left(\frac{1-x^n}{1-x} \right) \in \pi(C)$$

elde edilir. Bir önceki teoremin ispatında olduğu gibi $der f_1(x) = s, der f_2(x) = r, der f_4(x) = t$ olmak üzere

$$f_1(x)^* + 2x^{s-r} f_2(x)^* + 2ux^{s-t} f_4(x)^* \in \pi(C) \text{ elde edilir.}$$

$$\begin{aligned} f_1(x)^* + 2x^{s-r} f_2(x)^* + 2ux^{s-t} f_4(x)^* \\ = (f_1(x) + 2f_2(x) + 2uf_4(x))a(x) + u(f_3(x) + 2f_4(x))b(x) \dots \end{aligned} \quad (12)$$

elde edilir. Bu durumda

$$a(x) = 1, 1+u, 1+2u \text{ veya } 1+3u \text{ dir.}$$

$f_1(x) = f_1(x)^*$ yani $f_1(x)$ self reciprocal bir polinomdur. Aynı zamanda; $x^l f_2(x)^* = f_2(x)$ dir.

$$uf_3(x) = u + uh'x + \dots + uh_{k-1}'x^{k-1} + ux^k \text{ ve } k > l \text{ olmak üzere}$$

$$2uf_4(x) = 2u + 2uh_1''x + \dots + 2uh_{l-1}''x^{l-1} + 2ux^l \text{ olsun. Bu durumda}$$

$$\begin{aligned} uf_3(x) + 2uf_4(x) &= (u + 2u) + (uh' + 2uh_1'')x + \dots + (uh_{l-1}' + \\ &2uh_{l-1}'')x^{l-1} + (uh_l' + 2u)x^l + uh_{l+1}'x^{l+1} + \dots + h_{k-1}'x^{k-1} + ux^k. \end{aligned}$$

$$(uf_3(x) + 2uf_4(x))^{RC}$$

$$\begin{aligned} &= (1+u)(1+x+\dots+x^{n-k-2}) + x^{n-k-1} + \overline{uh_{k-1}'}x^{n-k} + \dots \\ &+ \overline{uh_{l+1}'}x^{n-l-2} + \overline{(uh_l' + 2u)}x^{n-l-1} + \overline{(uh_{l-1}' + 2uh_{l-1}'')}x^{n-l} + \dots \\ &+ \overline{(uh_1' + 2uh_1'')}x^{n-2} + (1+2u)x^{n-1} \end{aligned}$$

$$\begin{aligned} &= (1+u)(1+x+\dots+x^{n-k-2}) + x^{n-k-1} + \overline{uh_{k-1}'}x^{n-k} + \dots \\ &+ \overline{uh_{l+1}'}x^{n-l-2} + \overline{uh_l'}x^{n-l-1} + 2ux^{n-l-1} + \overline{uh_{l-1}'}x^{n-l} \\ &+ 2uh_{l-1}''x^{n-l} + \dots + \overline{uh_1'}x^{n-2} + 2uh_1''x^{n-2} + 2ux^{n-1} + x^{n-1} \end{aligned}$$

$$\begin{aligned} &= (1+u)(1+x+\dots+x^{n-k-2}) + x^{n-k-1} + \overline{uh_{k-1}'}x^{n-k} + \dots + \\ &\overline{uh_{l+1}'}x^{n-l-2} + \overline{uh_l'}x^{n-l-1} + \dots + \overline{uh_1'}x^{n-2} + x^{n-1} + 3.2ux^{n-l-1} + \\ &3.2uh_{l-1}''x^{n-l} + 3.2uh_1''x^{n-2} + 3.2ux^{n-1} \text{ tir.} \end{aligned}$$

$$C \text{ lineer kod olduğundan, } (uf_3(x) + 2uf_4(x))^{RC} + 3(1+u) \frac{1-x^n}{1-x} \in \pi(C) \text{ dir.}$$

Bu nedenle,

$$\begin{aligned}
& (uf_3(x) + 2uf_4(x))^{RC} + 3(1+u)((1-x^n)/(1-x)) \\
& = 3ux^{n-k-1} + (\overline{uh_{k-1}}' + 3(1+u))x^{n-k} + \dots \\
& + (\overline{uh_1}' + 3(1+u))x^{n-2} + 3ux^{n-1} \\
& + 3.2x^{n-l-1}(u + uh_{l-1}''x + \dots + uh_1''x^{l-1} + ux^l) \\
& = 3ux^{n-k-1} + 3uh_{k-1}'x^{n-k} + \dots + 3uh_1'x^{n-2} + 3ux^{n-1} \\
& + 3.x^{n-l-1}(2u + 2uh_{l-1}''x + \dots + 2uh_1''x^{l-1} + 2ux^l) \\
& = 3x^{n-k-1} + (u + uh_{k-1}'x + \dots + uh_1'x^{k-1} + ux^k) \\
& + 3.x^{n-l-1}(2u + 2uh_{l-1}''x + \dots + 2uh_1''x^{l-1} + 2ux^l) \\
& = 3x^{n-k-1}uf_3^*(x) + 3.2ux^{n-l-1}f_4^*(x) \\
& = 3x^{n-k-1}(uf_3^*(x) + x^{k-l}2uf_4^*(x)) \in \pi(C) \text{ elde edilir.}
\end{aligned}$$

Dolayısıyla, $f_3(x) = f_3(x)^*$ dir.

(12) eşitliğinden $j = \text{der}f_1(x) - \text{der}f_4(x)$ olmak üzere,

$$f_4(x)|2x^j f_4(x)^* + 2f_4(x) \text{ veya } f_4(x)|(2x^j f_4(x)^* + 2f_4(x) + 2f_2(x)) \text{ elde edilir.}$$

Tersine, $c(x) \in \pi(C)$ ise $c(x) = (f_1(x) + 2f_2(x) + 2uf_4(x))m(x) + (uf_3(x) + 2uf_4(x))n(x)$ tir. $f_1(x)$ ve $f_3(x)$ self reciprocal polinomlar olduğundan, $i = \text{der}f_1(x) - \text{der}f_2(x)$ olmak üzere $x^i f_2(x)^* = f_2(x)$ ve $j = \text{der}f_1(x) - \text{der}f_4(x)$ olmak üzere $f_4(x)|(2x^j f_4(x)^* + 2f_4(x))$ veya $f_4(x)|(2x^j f_4(x)^* + 2f_4(x) + 2f_2(x))$ tir. Bu durumda $f_4(x)|f_3(x)$ olduğu için

$$\begin{aligned}
c(x)^* & = ((f_1(x) + 2f_2(x) + 2uf_4(x))m(x))^* + ((uf_3(x) + 2uf_4(x))n(x))^* \\
& = (f_1^*(x) + 2x^i f_2(x)^* + 2ux^j f_4(x)^*)m^*(x) + (uf_3(x)^* + \\
& 2ux^k f_4(x)^*)n(x)^* \\
& = (f_1(x) + 2f_2(x) + 2uf_4(x))m(x)^* + (2ux^j f_4(x)^* + 2uf_4(x))m(x)^* \\
& + (uf_3(x) + 2ux^k f_4(x)^*)n(x)^* \\
& = (f_1(x) + 2f_2(x) + 2uf_4(x))m(x)^* + uf_4(x)q(x) \text{ elde edilir.}
\end{aligned}$$

Dolayısıyla $c = 1, 1+u, 1+2u$ veya $1+3u$ dir. Bu nedenle, $c(x)^* \in \pi(C)$ dir.

$$3(1+u)((1-x^n)/(1-x)) \in \pi(C) \text{ olduğundan,}$$

$$3(1+u)\frac{1-x^n}{1-x} = 3(1+u) + 3(1+u)x + \dots + 3(1+u)x^{n-1} \in \pi(C) \text{ dir.}$$

$c(x) = c_0 + c_1x + \dots + c_mx^m \in \pi(C)$ olsun. C n uzunluğunda devirli kod olduğundan,

$$x^{n-m-1}c(x) = c_0x^{n-m-1} + c_1x^{n-m} + \dots + c_mx^{n-1} \in \pi(C) \text{ dir.}$$

Dolayısıyla,

$$\begin{aligned} & 3(1+u) + 3(1+u)x + \dots + 3(1+u)x^{n-m-2} + (c_0 + 3(1+u))x^{n-m-1} \\ & \quad + (c_1 + 3(1+u))x^{n-m} + \dots + (c_m + 3(1+u))x^{n-1} \\ &= 3(1+u) + 3(1+u)x + \dots + 3(1+u)x^{n-m-2} + 3\bar{c}_0x^{n-m-1} + 3\bar{c}_1x^{n-m} + \dots \\ & \quad + 3\bar{c}_mx^{n-1} \\ &= 3((1+u) + (1+u)x + \dots + (1+u)x^{n-m-2} + \bar{c}_0x^{n-m-1} + \bar{c}_1x^{n-m} + \dots + \\ & \quad \bar{c}_mx^{n-1}) \in \pi(C) \text{ dir.} \end{aligned}$$

Buradan, $(c(x)^*)^{RC} \in \pi(C)$ olduğu görülür. Dolayısıyla, $((c(x)^*)^{RC})^* = c(x)^{RC} \in \pi(C)$ 'dir.

BÖLÜM 4

SONUÇLAR VE TARTIŞMA

Bazı 16 elemanlı sonlu halkaların cebirsel yapısı ve bu halkalar üzerinde tanımlanmış devirli DNA kodların inşası, devirli kodların üreteçleri, bu kodların DNA görüntüleri incelendiği çalışmalar derlenmiştir.

Bu çalışmada incelenen devirli DNA kodların yapılarına benzer yapıya sahip kodların yeni bazı sonlu 16 elemanlı halkalar üzerinde elde edilebileceği gözlemlenmiştir.

KAYNAKLAR

- Abualrub T., Ghrayeb A., Zeng X. (2006). Construction of cyclic codes over $GF(4)$ for DNA computing. *Journal of Franklin Institute*, 343, 448-457
- Abualrub, T. ve Siap, I. (2007). Cyclic Codes over The Rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, *Des. Codes Cryptogr.*, 42, 273-287.,
- Bayram A., Oztas E., Siap I. (2015). Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications, *Designs, Codes and Cryptography*, 80(2), 379-393.
- Bennenni N., Guenda K., Mesnager S. (2015). New DNA cyclic codes over rings, <https://arxiv.org/abs/1505.06263>.
- Blake, I. F. (1972). Codes over Certain Rings, *Information and Control*, 20, 396-404,
- Blake, I. F. (1975). Codes over Integer Residue Rings, *Information and Control*, 29, 295-300.
- Calderbank, A. R. ve Sloane, N. J. A. (1995). Modular and p-adic Cyclic Codes, *Designs, Codes and Cryptography*, 6, 21-35.
- Çallıalp, F. (2013). Örneklerle Soyut Cebir. İstanbul: Birsen yayınevi.
- Dertli A., Cengellenmis Y. (2017). On cyclic DNA codes over the rings $\mathbb{Z}_4 + w\mathbb{Z}_4$ and $\mathbb{Z}_4 + w\mathbb{Z}_4 + v\mathbb{Z}_4 + wv\mathbb{Z}_4$, *Biomath*, 6, 1-11.
- Dixita Limbachiya, Bansari Rao, Manish K. Gupta. (2016). The Art of DNA Strings: Sixteen Years of DNA Coding Theory, <https://arxiv.org/abs/1607.00266v1>.
- Dougherty, S. T. (2017). *Algebraic Coding Theory over Finite Commutative Rings*, PA, USA: Springer.

- Gaborit P., King O. D. (2005). Linear construction for DNA codes, *Theoretical Computer Science*, 334, 99-113.
- Guenda K., Gulliver T. A., Sole P. (2013). On cyclic DNA codes, *IEEE International Symposium on Information Theory*, 3(2),120-136.
- Guenda K., Gulliver T. A. (2013). Construction of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ for DNA computing, *Journal of Applicable Algebra in Engineering, Communication and Computing (AAECC)* , 24, 445-459.
- Hill, R. (1986). *First Course in Coding Theory*, Oxford: Clarendon Press.
- Hoffman, K. ve Kunze, R. (1971). *Linear Algebra Second Edition*, New Jersey: Prentice-Hall, Inc. , Englewood Cliffs.
- Huffman, W. C., Cary, W. ve Pless, V. (2003). *Fundamentals of Error-Correcting Codes*, Cambridge: Cambridge University Press.
- Hungerford, T. (1973). *Algebra*, New York: Springer-Verlag.
- Jitman, S., Udomkavanich, P. ve Ling, S. (2012). Skew Constacyclic Codes over Finite Chain Rings, *Advances Mathematics Communications*, 6, 29-63.
- Karakaş, H. İ. (2012). *Cebir Dersleri*, Ankara: Tüba yayınları.
- Ling, S. ve Xing, C. (2004). *Coding Theory a First Course*, New York: Cambridge University Press.
- Liang J., Wang L. (2016). On cyclic DNA codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *Journal of Applied Mathematics and Computing*, 51, 81-91. DOI: 10.1007/s12190-015-0892-8.
- Ma F., Yonglin C., Jian G. (2015). On cyclic DNA codes over $\mathbb{F}_4[u]/\langle u^2 + 1 \rangle$, *International Journal of Recent Research and Applied Studies (IJRRAS)*, 24(3),1-9.
- MacWilliams, F. ve Sloane, N.J.A. (1983). *The Theory of Error-Correcting Codes*, New York: North-Holland Publishing Company.

- Massey J. L. (1964). Reversible Codes, *Information and Control*, 7, 369-380.
- Özen, M., Uzekmek, F. Z., Aydin, N. ve Özzaim, N. T. (2016). Cyclic and Some Constacyclic Codes over the Ring $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$, *Finite Fields and Their Applications*, 38, 27-39.
- Pattanayak S., Singh A. K. (2015). On cyclic DNA codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, <https://arxiv.org/abs/1508.02015>.
- Pattanayak S., Singh A. K., Kumar P. (2015). DNA cyclic codes over the ring $\mathbb{F}_2[u, v]/\langle u^2 - 1, v^2 - v, uv - vu \rangle$, <https://arxiv.org/abs/1511.03937>.
- Pattanayak S., Singh A. K. (2016). Construction of Cyclic DNA codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$ based on deletion distance, <https://arxiv.org/abs/1603.04055>.
- Pless, V. S. ve Qian, Z. (1996). Cyclic Codes and Quadratic Residue Codes over $\mathbb{Z}_4$, *IEEE Transactions on Information Theory*, 42(5), 1594-1600.
- Pless, V. S., Solé, P. ve Qian, Z. (1997). Cyclic Self-Dual $\mathbb{Z}_4$ -codes, *Finite Fields Their Application*, 3, 48-69.
- Prange, E. (1957). *Cyclic Error-Correcting Codes in Two Symbols*, Cambridge: Air Force Cambridge Research Center.
- Prange, E. (1958). *Some Cyclic Error-Correcting Codes with Simple Decoding Algorithms*, Cambridge: Air Force Cambridge Research Center.
- Shannon, C. E. (1949). Communication Theory of Secrecy Systems, *Bell System Technical Journal*, cilt 28, 656-715.
- Siap I., Abualrub T., Ghayeb A. (2009). Cyclic DNA codes over the ring $\mathbb{F}_2[u]/\langle u^2 - 1 \rangle$ based on the deletion distance, *Journal of Franklin Institute*, 346, 731-740.
- Siap I., Abualrub T., Ghayeb A. (2008). Similarity cyclic DNA codes over rings, *IEEE*, 42(3), 273-287.

Qian, J., Zang, L. ve Zhu, S. (2005). Cyclic Codes over $\mathbb{F}_p + u\mathbb{F}_p + \dots + u^{k-1}\mathbb{F}_p$, *IEICE Transaction of Fundamentals*, 3, 795-797.

Taşcı, D. (2007). *Soyut Cebir*, Ankara: Alp Yayınevi.

Yıldız, B. ve Aydın, N. (2014). On Cyclic Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and Their $\mathbb{Z}_4$ – Images, *International Journal of Information and Coding Theory*, 4, 226-237.

Yıldız B., Siap I. (2012). Cyclic DNA codes over the ring $\mathbb{F}_2[u]/\langle u^4 - 1 \rangle$ and applications to DNA codes, *Computers and Mathematics Application*, 63, 1169-1176.

Zhu S., Chen X. (2015). Cyclic DNA codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, <https://arxiv.org/abs/1508.07113v1>.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Alev YOKUVA
Doğum Yeri ve Tarihi : EDİRNE / Merkez – 1991
e-mail : alvyokuva@gmail.com

Eğitim Bilgileri

Lise : Muzaffer Atasay Anadolu Lisesi, Uzunköprü, EDİRNE 2009
Lisans : Matematik Bölümü, Balıkesir Üniversitesi, Fen Fakültesi, Edirne 2015
Y. Lisans : Matematik, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne 2019

İş Deneyimleri

2015 - 2016 Fen Bilimleri Temel Lisesi, Edirne Matematik Öğretmeni
2016 - ... Bilim Özel Öğretim Kursu, Edirne Matematik Öğretmeni

Yabancı Diller

İngilizce