T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DEĞİŞMELİ OLMAYAN AYKIRI POLİNOM HALKALARI ÜZERİNDE TANIMLI DNA KODLAR

FATMANUR GÜRSOY

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
DR. ÖĞR. ÜYESİ AYTEN ÖZKAN

İSTANBUL, 2019

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DEĞİŞMELİ OLMAYAN AYKIRI POLİNOM HALKALARI ÜZERİNDE TANIMLI DNA KODLAR

Fatmanur GÜRSOY tarafından hazırlanan tez çalışması 12.07.2019 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Dr. Öğr. Üyesi Ayten ÖZKAN

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Dr. Öğr. Üyesi Ayten ÖZKAN

Yıldız Teknik Üniversitesi _____

Prof. Dr. Mehmet ÖZEN

Sakarya Üniversitesi _____

Doç. Dr. Murat ALAN

Yıldız Teknik Üniversitesi _____

Doç. Dr. Fatih DEMİRKALE

Yıldız Teknik Üniversitesi _____

Dr. Öğr. Üyesi Elif Segah ÖZTAŞ

Karamanoğlu Mehmetbey Üniversitesi _____

Bu çalışma, TÜBİTAK BİDEB 2211-E Yurt İçi Doktora Burs Programı ile desteklenmiştir.

ÖNSÖZ

Tez çalışmalarım sırasında desteğini benden esirgemeyen kıymetli hocam Dr. Öğr. Üyesi Ayten Özkan'a ve tez çalışmalarımın başlangıcı aşamasında bana yol gösteren değerli hocam Prof. Dr. İrfan Şiap'a, tez izleme sürecim boyunca fikirleriyle katkıda bulunan sayın Prof. Dr. Mehmet Özen ve Doç. Dr. Murat Alan'a, tezimi titizlikle değerlendirip, önerileriyle katkıda bulunan sayın Doç. Dr. Fatih Demirkale ve Doç. Dr. Emre Kolotoğlu'na en içten teşekkürlerimi sunarım.

Araştırmalarım sırasında bana fikirleri ve çözüm önerileriyle destek olan Dr. Öğr. Üyesi Elif Segah Öztaş'a ve maddi manevi destekçim olan tüm arkadaşlarıma da teşekkür ediyorum.

Hayatım boyunca her konuda maddi ve manevi desteklerini esirgemeyen kıymetli anneme, babama ve moral kaynağım olan kardeşlerim Halil, Beyza ve Ahmet Fazıl'a sonsuz teşekkürler.

Son olarak tez süresince maddi destek sağlayan TÜBİTAK-Bilim İnsanı Destekleme Daire Başkanlığı'na teşekkür ederim.

Temmuz, 2019

Fatmanur GÜRSOY

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

$der(f(x))$	$f(x)$ polinomunun derecesi
$f^t(x)$	$f(x)$ polinomunun ters sıralısı
$f^R(x)$	$f(x)$ polinomunun aykırı (skew) ters sıralısı
$wt(c)$	c kodsözünün Hamming ağırlığı
$d(C)$	C kodunun minimum Hamming uzaklığı
$m \mid n$	m böler n
$ord(\alpha)$	α elemanının mertebesi
F_q	q elemanlı cisim
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Z}_m$	Tam sayıların $\bmod m$'ye göre kalan sınıflarının kümesi
$Z(R)$	R halkasının merkezi
$C^{\perp}$	C kodunun duali
$\lvert\langle\theta\rangle\rvert$	θ otomorfizmasının mertebesi
$F_q[x]$	Katsayıları F_q cisminin elemanı olan polinom halkası
$F_q[x;\theta]$	Katsayıları F_q cisminin elemanı olan θ otomorfizması ile belirli aykırı (skew) polinom halkası
$C = \langle g(x) \rangle$	$g(x)$ polinomu tarafından üretilen aykırı (skew) devirli kod
$(n, \mathrm{M}, d)_q$	q elemanlı bir küme üzerinde tanımlı uzunluğu n, eleman sayısı M ve minimum Hamming uzaklığı d olan kodun parametreleri
$[n, k, d]_q$	F_q üzerinde tanımlı uzunluğu n, boyutu k ve minimum Hamming uzaklığı d olan lineer kodun parametreleri
A	Adenin
G	Guanin
T	Timin
C	Sitozin
u^r	u dizisinin ters sıralısı
u^c	u dizisinin tamlayanı
u^{rc}	u dizisinin ters sıralı tamlayanı

KISALTMA LİSTESİ

DNA	Deoksiribo Nükleik Asit
TST	Ters Sıra Tamlayan
WCC	Watson Crick Complement

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖZET

DEĞİŞMELİ OLMAYAN AYKIRI POLİNOM HALKALARI ÜZERİNDE TANIMLI DNA KODLAR

Fatmanur GÜRSOY

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Dr. Öğr. Üyesi Ayten ÖZKAN

Adleman 1994 yılında yaptığı çalışmasında Hamilton yolu olarak bilinen kombinatöryel problemi DNA dizileri yardımıyla deney tüpünde çözmüştür. Adleman'ın çalışması ile birlikte DNA dizileri hesaplama işlemlerinde kullanılmaya başlanmıştır.

Bu tezde değişmeli olmayan aykırı (skew) polinom halkaları ve aykırı devirli (skew cyclic) kodların cebirsel özelliklerinden yararlanılarak ters sıralı DNA kodlar ve ters sıralı tamlayan DNA kodların elde edilmesi amaçlanmıştır.

Üçüncü bölümde $F_{4^{2s}}$ cismi üzerinde tanımlı bir aykırı devirli kodun DNA karşılığının ters sıralı DNA kod olması için gerek ve yeter şartlar belirlenmiştir. Ayrıca, C aykırı devirli kodunun DNA karşılığı bir ters sıralı DNA kod ise $C^{\perp}$ kodunun DNA karşılığının da ters sıralı DNA kod olduğu gösterilmiştir.

Dördüncü bölümde $F_{16}+uF_{16}+vF_{16}+uvF_{16}$ halkasının yapısal özellikleri belirlenmiş ve bu halka üzerinde tanımlı aykırı devirli kodlardan ters sıralı DNA kodlar elde edebilmek için uygun θ otomorfizması ve DNA 8-baz eşlemesi belirlenmiştir.

Beşinci bölümde $R_{k,s}=F_{4^{2k}}[u_1,\ldots,u_s]\Big/\left\langle u_1^{\,2}-u_1,\ldots,u_s^{\,2}-u_s\right\rangle$ halkasının üzerinde bir θ otomorfizması tanımlanmıştır. Bu otomorfizma sayesinde $R_{k,s}$ halkasının Çin Kalan Teoremi'ne göre ayrışımı belirlenmiştir. Uygun DNA eşlemesinin de belirlenmesi

sayesinde $R_{k,s}$ üzerinde tanımlı aykırı devirli kodlardan ters sıralı DNA kodlar elde edilmiştir.

Ayrıca çift uzunluğa sahip ters sıralı DNA kodlardan ters sıralı tamlayan DNA kodların kolaylıkla elde edilebileceğine dair bir teorem verilmiştir. Böylece her üç bölümde de elde edilen ters sıralı DNA kodlar çift uzunluğa sahip olduğu için aynı zamanda ters sıralı tamlayan DNA kodlara karşılık gelmektedir.

Anahtar Kelimeler: DNA kodlar, ters sıralı kodlar, lineer kodlar, aykırı devirli kodlar, aykırı polinom halkaları

ABSTRACT

DNA CODES OVER NON-COMMUTATIVE SKEW POLYNOMIAL RINGS

Fatmanur GÜRSOY

Department of Mathematics

Ph.D. Thesis

Adviser: Asst. Prof. Dr. Ayten ÖZKAN

DNA computing has started with the study of Adleman, in 1994. He solved the Hamiltonian path problem, which is a famous combinatorial problem, in a test tube by using DNA sequences.

In this thesis, it is aimed to obtain reversible DNA codes and reversible complement DNA codes by using the algebraic properties of skew polynomial rings and skew cyclic codes.

In Section 3, we give necessary and sufficient conditions for the corresponding DNA code of a skew cyclic code over the field $F_{4^{2s}}$ to be a reversible DNA code. Moreover, we show that if C is a skew cyclic code that corresponds to a reversible DNA code then its dual code $C^{\perp}$ also corresponds to a reversible DNA code.

In Section 4, we determine the structural properties of the ring $F_{16}+uF_{16}+vF_{16}+uvF_{16}$. Afterward, to obtain reversible DNA codes from the skew cyclic codes over this ring, we determine the proper automorphism θ and the proper correspondence between DNA 8-bases and the elements of this ring.

In Section 5, we use Chinese Remainder Theorem to decompose the ring $R_{k,s}=F_{4^{2k}}[u_1,\ldots,u_s]\Big/\left\langle u_1^{\,2}-u_1,\ldots,u_s^{\,2}-u_s\right\rangle$. We achieve this by defining an

automorphism over $R_{k,s}$. Furthermore, we obtain reversible DNA codes via skew cyclic codes over $R_{k,s}$ by establishing the proper DNA correspondence.

In addition, we give a theorem that states if a reversible DNA code has even length, then that code can easily be converted into a reversible complement DNA code. Therefore, since the obtained reversible DNA codes are of even lengths in the aforementioned sections, they also correspond to reversible complement DNA codes.

Keywords: DNA codes, reversible codes, linear codes, skew cyclic codes, skew polynomial rings

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

DNA hesaplamalarında öncü kabul edilen çalışması ile Adleman, Hamilton yolu olarak bilinen problemi sentetik DNA dizileri ile test tüpünde, 1994'te çözmüştür. Bu problemin çözümünde DNA'nın WCC (Watson Crick Complement) özelliğinden yararlanmıştır [1]. Adleman'ın çalışmasının önemli bir özelliği de DNA molekülleri yardımıyla yapılan hesaplamanın standart bilgisayarlara göre daha kısa sürede gerçekleşebileceğini göstermesidir. Bu nedenle DNA hesaplamaları farklı alanlardaki birçok araştırmacının dikkatini çekmiştir. Örneğin, [2] ve [3] çalışmalarında bazı NP-tam problemlerin çözümü DNA dizileri yardımıyla yapılmıştır. [4] ve [5] numaralı çalışmalarda şifreleme alanında önemli bir sistem olan ve kırılması zor olan DES (Data Encryption Standart) olarak bilinen veri şifreleme standardı DNA molekülleri yardımı ile kırılmıştır. [6] ve [7] çalışmalarında DNA moleküllerinin veri depolama ortamı olarak kullanılabileceğini göstermiştir. Ayrıca DNA kodlarından üretilen moleküler barkodlar ürünlerin doğrulanması için biyobelirteç olarak kullanılır [8].

DNA'nın hibridizasyon özelliği DNA hesaplamalarının temelini oluşturur ki bu aynı zamanda hataların kaynağıdır. Dolayısıyla, DNA hesaplamalarının başarıya ulaşması oluşabilecek hatalı hibridizasyonların kontrol edilmesine bağlıdır. Doğal olarak hata düzelten kodlar teorisi DNA hesaplamalarında oluşabilecek bu tip problemlerin çözümünde önem arz etmektedir. Böylelikle kodlama teorisi ile DNA hesaplamalarının bir araya gelmesinden DNA kodlar ortaya çıkmıştır [9].

DNA kodlarda, hatalı hibridizasyonların minimuma indirgenmesi amacıyla yaygın olarak; ters sıra (reverse) kısıtı, ters sıra tamlayan (reverse-complement) kısıtı, Hamming uzaklığı kısıtı ve GC-miktar (GC-content) kısıtı kullanılır [10], [11]. Bu kısıtların bir veya birkaçını sağlayan kodları inşa etmek için stokastik araştırma [12], genetik ve evrimsel algoritmalar [13], [14], sözlüksel (lexicographic) inşa [15] gibi yöntemler uygulanmıştır. [11] çalışmasında ise F_4 cismi ve $\mathbb{Z}_4$ halkası üzerindeki lineer kodlardan TST (ters sıra tamlayan) kısıtı ve GC-miktar kısıtını sağlayan DNA kodlar elde edilmiştir. Kısıtları sağlayan DNA kodların eleman sayısı için alt ve üst sınırlar hesaplanmıştır [15], [16]. Belirli bir Hamming uzaklığı için TST ve GC-miktar kısıtlarını sağlayan DNA kodların maksimum eleman sayısı için sınırlar verilmiştir [15].

Abualrub vd., F_4 cismi üzerinde tanımlı devirli kodları DNA kodlar ile ilişkilendirmiştir [17]. Şiap vd. ise $F_2[u]/\langle u^2-1\rangle$ halkasını kullanarak ters sıralı devirli DNA kodlar elde etmişlerdir [18]. Yıldız vd. tarafından yapılan [19] numaralı çalışmada ise DNA kod eldesi için 16 elemanlı $F_2[u]/\langle u^4-1\rangle$ halkası ile DNA baz çiftleri (DNA 2-bazları) eşleştirilmiştir. [20] nolu çalışmada F_4+vF_4 halkası üzerinde tanımlı lineer kodlardan ters sıralı DNA kodlar elde edilmiştir. Öztaş vd. [21] nolu çalışmada F_{16} cisminin elemanları ile DNA baz çiftleri eşleştirmiş daha sonra [22] numaralı çalışmada daha genel olarak $F_{4^{2s}}$ cisminin elemanları ile $2s$-bazlar eşleştirmiştir. Her iki çalışmada özel polinomlar tanımlanmış ve bu polinomlar yardımıyla elde edilen özel üreteç kümelerinden ters sıralı DNA kodlar ve ters sıralı tamlayan DNA kodlar elde edilmiştir.

Canlılara ait DNA parçalarında kendi kendini onarma (self-repairing) gibi özelliklerin olması yaşayan DNA'larda gizli hata düzelten kod yapısı olup olmadığı sorusunu gündeme getirmiştir. [23] çalışmasında TRAV7 geninin $\mathbb{Z}_4$ üzerindeki bir BCH koda tekabül ettiği gösterilmiştir.

DNA'nın protein sentezlemek veya çoğalmak gibi fonksiyonları gerçekleştirmesi için ilgili genin olduğu kısımdaki zincir açılır ve sentezleme işlemi yapıldıktan sonra da zincir kapanır. Zincirin açılması işlemi bağlanma bölgesi (binding site) denilen bölgeye bir proteinin bağlanması ile mümkün olmaktadır. Bağlanma bölgesi bilindiği takdirde gerekli protein ile DNA'nın ilgili kısmındaki zinciri açılıp, işlevini tam gerçekleştiremeyip

hastalıklara neden olan gen çalıştırılarak tedavi için gereken proteinlerin üretilmesi, fonksiyonlarının belirlenmesi gibi işlemlerde kullanılabileceği öngörülmektedir.

[24] nolu çalışmada Arabidopsis genomunun bağlanma bölgelerini tespit edebilmek için DNA dizilimi 8 uzunluğundaki DNA baz parçalarına kayan pencere (sliding window) yöntemi ile ayrılmış ve her bir parça için görülme sıklığı hesaplanarak tablolar oluşturulmuştur. Bu sık görülen DNA 8-bazlarından biri veya birkaçının bağlanma bölgesi olabileceği öngörülmektedir. Oluşturulan tablolarda DNA 8-baz parçalarının büyük çoğunluğunun hem kendilerinin hem de ters sıra tamlayanlarının yoğun bir şekilde ilk 25 sıraya yerleştiği gözlemlenmiştir. Dolayısıyla, bağlanma bölgesi olma ihtimali yüksek olan kısımların bir ters sıralı tamlayan DNA kod veya alt kümesi olduğu düşünülmektedir. Bu da ters sıralı tamlayan DNA kodları önemli kılmaktadır.

Hammons vd. tarafından yapılan [25] nolu çalışmada $\mathbb{Z}_4$ halkası üzerinde tanımlı lineer kod ailelerinin özel bir dönüşüm altındaki görüntülerinden Kerdock, Preparata gibi iyi hata düzeltme kabiliyetine sahip, lineer olmayan ikili (binary) kodlar elde edilmiştir. Bu çalışma ile birlikte çeşitli halkalar üzerinde kod aileleri tanımlanması önem kazanmıştır.

D. Boucher vd. [26] nolu çalışmada değişmeli olmayan halkalar kullanarak devirli kodların genellemesini yapmış bu yeni kod ailesini aykırı devirli (skew cyclic) kodlar olarak adlandırmıştır. Böylece devirli kodlar alanına yeni bir boyut kazandırmıştır. Bu çalışmada F_q, q elemanlı bir cisim ve θ bu cisim üzerinde bir otomorfizma olmak üzere $F_q[x;\theta]$ aykırı (skew) polinom halkaları kullanılmıştır. $F_q[x;\theta]$ halkasının en önemli özelliği çarpanlara ayrılışın tek türlü olmamasıdır. Bu özellik sayesinde devirli kodlara kıyasla daha fazla sayıda üreteç polinomu ve böylece aynı n uzunluğuna ve k boyutuna sahip daha fazla sayıda kod elde etmek mümkündür. Dolayısıyla aykırı devirli kodlar optimal kod eldesi açısından avantajlıdır. Boucher vd. bilinenden daha iyi parametrelere sahip kodlar elde etmişlerdir [26].

Fakat, [26] nolu çalışmada aykırı devirli kodların uzunluğu n, θ otomorfizmasının mertebesi m olmak üzere, $m|n$ olarak kısıtlanmıştır. Daha sonra Şiap vd. tarafından yapılan [27] nolu çalışmada uzunluk üzerindeki bu kısıtlama kaldırılmıştır. Aynı çalışmada aykırı devirli kodlar ile devirli ve parçalı (quasi) devirli kodlar arasındaki ilişki

incelenmiştir. [28] nolu çalışmada ise aykırı polinom halkaları kullanılarak aykırı parçalı devirli kodların inşası üzerine çalışılmış ve bilinenden daha iyi parametrelere sahip kod örnekleri elde edilmiştir.

[29] nolu çalışmada aykırı devirli kodların dualleri üzerinde durulmuş ve bir aykırı devirli kodun dualinin de aykırı devirli kod olduğu gösterilmiştir. Ayrıca, aykırı devirli kodlar farklı halkalar üzerinde tanımlanmıştır [30], [31], [32].

1.2 Tezin Amacı

Değişmeli olmayan aykırı polinom halkaları ve aykırı devirli kodların cebirsel yapısından yararlanılarak ters sıralı DNA kodlar ve ters sıralı tamlayan DNA kodların elde edilmesi amaçlanmıştır.

1.3 Orijinal katkı

Literatürde ilk olarak DNA kodlar değişmeli olmayan halkalar yardımıyla çalışılmış, DNA kodlar ile aykırı devirli kodlar ilişkilendirilmiştir. Aykırı devirli kodların zengin cebirsel yapısından yararlanılarak DNA kodlar için ters sıralılık problemi farklı cebirsel yapılar üzerinde ele alınmış ve elde edilen sonuçlar uluslararası yayın olarak literatüre kazandırılmıştır.

BÖLÜM 2

TEMEL KAVRAMLAR

Bu bölümde hata düzelten kodlar ile ilgili temel bilgiler, aykırı devirli kodlar ve DNA kodların tanımı ile bazı özellikleri verilecektir. Ayrıca Bölüm 4'te ve Bölüm 5'te kullanılacak olan sonlu zincir halkası tanımı ile halkalar için Çin Kalan Teoremi'nin bir sonucu ve ispatı verilecektir.

2.1 Halkalar ile İlgili Bazı Kavramlar

Bu başlık altında halkalar ile ilgili bu tezde kullanılacak bazı kavramlar verilecektir. İlgili tanım ve teoremler [33] nolu kaynak esas alınarak düzenlenmiştir.

Tanım 2.1 (Halka) R boştan farklı bir küme ve "+" ile "." ikili işlemler olmak üzere, aşağıdaki üç özelliği sağlayan $(R,+,.)$ cebirsel yapısına bir halka denir.

i. $(R,+)$ bir değişmeli gruptur.

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

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

Ayrıca, her $a,b \in R$ için $ab = ba$ sağlanıyorsa R halkasına bir değişmeli halka denir. Her $a \in R$ için $1_R a = a1_R = a$ olacak şekilde $1_R \in R$ mevcutsa R halkasına birimli halka denir.

Tanım 2.2 (Halkanın karakteristiği) R bir halka olsun. Her $a \in R$ için $na = 0$ eşitliğini sağlayan en küçük pozitif n tamsayısına halkanın karakteristiği denir. Eğer böyle bir pozitif n tamsayısı yoksa halkanın karakteristiği sıfırdır denir.

Tanım 2.3 R bir halka ve $e \in R$ olsun. Eğer $e^2 = e$ eşitliği sağlanıyorsa e elemanına idempotent eleman adı verilir.

Tanım 2.4 (Halkanın merkezi) R bir halka olsun.

$$Z(R) = \{a \mid ar = ra, \forall r \in R\} \tag{2.1}$$

kümesine halkanın merkezi denir.

Tanım 2.5 (Alt Halka) R bir halka ve S, R'nin boştan farklı bir alt kümesi olsun. Eğer S kümesi R'nin işlemlerine göre halka şartlarını sağlıyorsa S'ye R'nin bir alt halkasıdır denir.

Tanım 2.6 (İdeal) R bir halka ve I, R'nin bir alt halkası olsun.

i. Her $r \in R$ ve $a \in I$ için $ra \in I$ oluyorsa I bir sol idealdir.

ii. Her $r \in R$ ve $a \in I$ için $ar \in I$ oluyorsa I bir sağ idealdir.

iii. I hem sağ hem de sol ideal oluyorsa I'ya R'nin bir idealidir denir.

Teorem 2.7 R bir halka ve I, R'nin boştan farklı bir alt kümesi olsun. I kümesinin R'nin bir sağ ideali (sol ideali) olması için gerek ve yeter koşul;

i. Her $a, b \in I$ için $a - b \in I$ ve

ii. Her $a \in I, r \in R$ için $ar \in I$ $(ra \in I)$ olmasıdır.

Sonuç 2.8 $\{A_i \mid i \in \mathrm{I}\}$ kümesi R halkasının (sol) ideallerinin bir ailesi olsun. Bu durumda A_i (sol) ideallerinin kesişimi; $\bigcap_{i \in \mathrm{I}} A_i$ de R'nin bir (sol) idealidir.

Tanım 2.9 X, R halkasının bir alt kümesi ve R'nin X'i içeren tüm (sol) ideallerinin ailesi $\{A_i \mid i \in \mathrm{I}\}$ olsun. $\bigcap_{i \in \mathrm{I}} A_i$ kesişimine X kümesi tarafından üretilen (sol) ideal denir.

X kümesi tarafından üretilen ideal $\langle \mathrm{X} \rangle$ ile gösterilir. X kümesinin elemanlarına $\langle \mathrm{X} \rangle$ idealinin üreteçleri denir. Eğer $\mathrm{X} = \{x_1, \ldots, x_n\}$ ise $\langle \mathrm{X} \rangle$ ideali sonlu üretilmiştir denir ve $\langle x_1, \ldots, x_n \rangle$ olarak gösterilir. Tek bir x elemanı tarafından üretilen ideal, $\langle x \rangle$, temel ideal olarak adlandırılır.

Teorem 2.10 R birimli bir halka ve $a \in R$ olsun. a elemanı tarafından üretilen sol ideal $Ra = \{ra \,|\, r \in R\}$ ve sağ ideal $aR = \{ar \,|\, r \in R\}$ şeklindedir. Ayrıca $a \in Z(R)$ ise $aR = \langle a \rangle = Ra$ sağlanır.

Teorem 2.11 I , R halkasının bir ideali olsun. $R/I = \{a + I \,|\, a \in R\}$ kümesi toplama işleminin $(a+I)+(b+I) = (a+b)+I$ olarak, çarpma işleminin ise $(a+I)(b+I) = ab+I$ olarak tanımlanması halinde halka belirtir.

Tanım 2.12 R bir halka ve I onun bir ideali olsun. R/I halkasına bölüm halkası denir.

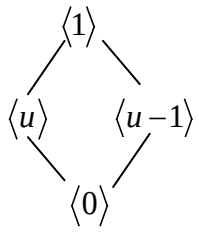
Tanım 2.13 R bir değişmeli halka olsun. Eğer R halkasının tüm ideallerinin kümesi tam sıralı ise R bir zincir halkasıdır denir.

Örnek 2.14 $\mathbb{Z}_8$ halkasının idealleri aşağıdaki gibi sıralanır.

$$\langle 0 \rangle \subseteq \langle 4 \rangle \subseteq \langle 2 \rangle \subseteq \langle 1 \rangle = \mathbb{Z}_8 \tag{2.2}$$

Dolayısıyla $\mathbb{Z}_8$ bir zincir halkasıdır.

Fakat $\mathbb{Z}_2[u] / \langle u^2 - u \rangle$ halkasının ideallerinin latisi tek bir zincirden ibaret değildir.



Dolayısıyla $\mathbb{Z}_2[u] / \langle u^2 - u \rangle$ halkası bir zincir halkası değildir.

2.1.1 Halkalar için Çin Kalan Teoremi

Tanım 2.15 (Direkt çarpım) $\{R_1, R_2, \ldots, R_n\}$ birtakım halkalardan oluşan bir küme olsun. $r_i \in R_i$ olmak üzere $(r_1, r_2, \ldots, r_n)$ sıralı n-lilerinden oluşan kümeyi $R_1 \times R_2 \times \ldots \times R_n$ olarak gösterelim. Toplama ve çarpma işlemi bileşen bileşene (componentwise) tanımlandığında bu küme bir halka belirtir. Bu halka R_i halkalarının direkt çarpımı (dış direkt çarpımı) olarak adlandırılır.

Teorem 2.16 R bir halka ve $A_1, A_2, \ldots, A_n$, bu halkanın birtakım idealleri olsun.

i. $A_1 + A_2 + \ldots + A_n = R$,

ii. Her $k \in \{1, \ldots, n\}$ için $A_k \cap (A_1 + \ldots + A_{k-1} + A_{k+1} + \ldots + A_n) = 0$

şartları sağlanıyorsa $R \cong A_1 \times A_2 \times \ldots \times A_n$'dir.

Tanım 2.17 (Direkt toplam) R halkasının $A_1, A_2, \ldots, A_n$ idealleri yukarıdaki teoremde verilen şartları sağlıyorsa R halkası A_i ideallerinin bir direkt toplamıdır (iç direkt çarpımıdır) denir. $R = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ olarak gösterilir.

Aşağıda halkalar için Çin Kalan Teoremi verilmiştir.

Teorem 2.18 (Çin Kalan Teoremi) R halkasının $A_1, A_2, \ldots, A_n$ idealleri için aşağıdaki özellikler sağlanıyor olsun.

i. $R^2 + A_i = R$, $\forall i \in \{1, \ldots, n\}$,

ii. $A_i + A_j = R$, $\forall i \neq j$.

Bu durumda, herhangi $b_1, b_2, \ldots, b_n \in R$ için

$$b \equiv b_i \pmod{A_i} \quad (i = 1, 2, \ldots, n) \tag{2.3}$$

olacak şekilde bir $b \in R$ elemanı vardır. Ayrıca, b elemanı, mod $A_1 \cap A_2 \ldots \cap A_n$'e göre tek türlü belirlidir.

Eğer R halkası birimli bir halka ise $R^2 = R$ eşitliği sağlanır. Dolayısıyla R halkasının herhangi bir A ideali için $R^2 + A = R$ sağlanır.

Sonuç 2.19 $A_1, A_2, \ldots, A_n$, R halkasının idealleri olsun. Bu durumda

$$\Phi : R/(A_1 \cap A_2 \ldots \cap A_n) \to R/A_1 \times R/A_2 \times \ldots \times R/A_n \tag{2.4}$$

şeklinde bir halka homomorfizması mevcuttur. Eğer her i için $R^2 + A_i = R$ ve her $i \neq j$ için $A_i + A_j = R$ sağlanıyorsa Φ bir izomorfizmadır.

Aşağıdaki Teorem Çin Kalan Teoremi'nin bir sonucudur ve [33] nolu kaynakta egzersiz sorusu olarak verilmiştir (sayfa 135, soru 24). Bu teoremde $Z(R)$ halkanın merkezini ifade etmektedir.

Teorem 2.20 (Çin Kalan Teoremi'nin bir sonucu) R birimli bir halka ve $e_1, e_2, \ldots, e_n \in Z(R)$ olsun.

i. $e_i^2 = e_i$, $\forall i$,

ii. $e_i e_j = 0$, $\forall i \neq j$,

iii. $e_1 + e_2 + \ldots + e_n = 1_R$,

özellikleri sağlanıyorsa R halkası $e_i R$ ideallerinin direkt toplamı şeklinde yazılabilir, yani, $R = e_1 R \oplus e_2 R \oplus \ldots \oplus e_n R$ olarak yazılır.

İspat Öncelikle $e_1 + e_2 + \ldots + e_n = 1_R$ olduğundan $e_1 R + e_2 R + \ldots + e_n R = R$ elde edilir. Herhangi bir $k \in \{1, \ldots n\}$ için $a \in e_k R \bigcap \left(e_1 R + \ldots + e_{k-1} R + e_{k+1} R + \ldots + e_n R\right)$ alalım. Bu durumda,

$$a = e_k r_k = e_1 r_1 + \ldots + e_{k-1} r_{k-1} + e_{k+1} r_{k+1} + \ldots + e_n r_n \tag{2.5}$$

olacak şekilde $r_i \in R$ mevcuttur. $e_k r_k = e_1 r_1 + \ldots + e_{k-1} r_{k-1} + e_{k+1} r_{k+1} + \ldots + e_n r_n$ eşitliğinin her iki tarafını e_k ile çarptığımız takdirde, $k \neq j$ için $e_k e_j = 0$ ve $e_k^2 = e_k$ olduğundan $e_k r_k = 0$ elde edilir. Dolayısıyla $e_k R \bigcap \left(e_1 R + \ldots + e_{k-1} R + e_{k+1} R + \ldots + e_n R\right) = 0$ dır. Böylece Tanım 2.17 gereğince R halkası $e_i R$ ideallerinin bir direkt toplamıdır. ■

2.2 Sonlu cisimler

Bu başlık altındaki tanım ve teoremler [34] nolu kaynaktan yararlanılarak düzenlenmiştir.

Tanım 2.21 F boş olmayan bir küme ve bu kümenin elemanları arasında "+" ve "." şeklinde iki tane ikili işlem tanımlanmış olsun. $(F, +)$ ve $(F \setminus \{0\}, .)$ birer değişmeli grup ise $(F, +, .)$ üçlüsüne cisim denir.

Tanım 2.22 F bir cisim olmak üzere $p1_F = 0_F$ eşitliğini sağlayan en küçük pozitif p tam sayısına F cisminin karakteristiği denir. Böyle bir p tam sayısı olmadığı durumlarda karakteristik 0'dır.

Teorem 2.23 Bir cismin karakteristiği ya sıfırdır ya da bir asal sayıdır.

Teorem 2.24 Karakteristiği p olan sonlu bir cismin eleman sayısı, n pozitif bir tamsayı olmak üzere, p^n şeklindedir.

Not 2.25 $q = p^n$ elemanlı sonlu cisim kısaca F_q olarak gösterilir.

Teorem 2.26 $(F_q \setminus \{0\}, .)$ devirli bir gruptur.

Tanım 2.27 $F_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$ olacak şekildeki α elemanına F_q cisminin ilkel (primitive) elemanı denir. Aynı zamanda, ilkel eleman F_q cisminin çarpımsal grubunun üretecidir, yani $F_q^* = \langle \alpha \rangle$, $F_q^* = F_q \setminus \{0\}$.

Tanım 2.28 $\alpha \in F_q$ sıfırdan farklı bir eleman olsun. $\alpha^k = 1$ olacak şekilde en küçük pozitif k tamsayısına α'nın mertebesi denir ve $ord(\alpha) = k$ olarak gösterilir.

Önerme 2.29

i. F_q cisminin sıfırdan farklı bir α elemanının ilkel eleman olması için gerek ve yeter koşul mertebesinin $ord(\alpha) = q-1$ olmasıdır.

ii. Her sonlu cismin en az bir adet ilkel elemanı vardır.

2.3 Modül ve Alt Modüller

Bu başlık altında modül ve alt modüller ile ilgili temel bazı tanım ve toeremler [35] nolu kaynak esas alınarak düzenlenmiştir.

Tanım 2.30 $(M, +)$ bir değişmeli grup ve R bir halka olsun. M'deki elemanların, R'deki elemanlarla skaler çarpımı, $R \times M \to M$ fonksiyonu aşağıdaki koşulları sağlıyorsa, M'ye R üzerinde bir sol modül veya kısaca sol R-modül denir.

i. Her $r \in R$ ve her $m, m' \in M$ için $r(m + m') = rm + rm'$,

ii. Her $r, r' \in R$ ve her $m \in M$ için $(r + r')m = rm + r'm$,

iii. Her $r, r' \in R$ ve her $m \in M$ için $(rr')m = r(r'm)$.

Not 2.31 Yukarıdaki işlemler sağ taraftan tanımlandığında M bir sağ R-modüldür. Bu tezde modüller sol modül olarak ele alınacaktır.

Tanım 2.32 R bir halka, M bir R-modül ve $N \subseteq M$ boş olmayan bir alt küme olsun. N de kendi başına bir R-modül ise N'ye M'nin bir alt modülü veya R-alt modülü denir.

Önerme 2.33 R-modül M'nin boş olmayan bir $N \subseteq M$ alt kümesinin alt modül olması için gerek ve yeter koşul her $r, r' \in R$ ve her $m, m' \in N$ için $rm + r'm' \in N$ olmasıdır.

Tanım 2.34 M bir R-modül ve $m \in M$ olsun. m elemanının ürettiği alt modül

$$\langle m \rangle = Rm = \{ rm \mid r \in R \} \tag{2.6}$$

şeklinde tanımlanır. Eğer $M = \langle m \rangle$ olacak şekilde bir $m \in M$ bulunabilirse, M'ye devirli modül denir.

Tanım 2.35 R bir halka, M bir R-modül ve $S = \{ y_i \}_{i \in I} \subseteq M$ olsun. Her $m \in M$ elemanı, $r_i \in R$ olmak üzere $m = \sum_{i \in I} r_i y_i$ şeklinde sonlu bir toplam olarak yazılabiliyor ve bu toplam tek türlü oluyorsa, S kümesine M'nin bir bazı (tabanı) ve M modülüne de bir serbest modül denir.

2.4 Aykırı Polinom Halkaları

Aykırı (skew) polinom halkalarının teorisi ilk olarak Oystein Ore (1933) tarafından ortaya atılmış, Nathan Jacobson (1943) ve Bernard R. McDonald (1974) tarafından geliştirilmiştir [36], [37], [38].

q elemanlı bir sonlu cismi F_q ve F_q cisminin otomorfizmalar kümesini $Aut(F_q)$ olarak gösterelim. θ, F_q üzerinde tanımlı bir otomorfizma ($\theta \in Aut(F_q)$) ve θ'nın mertebesi $|\langle \theta \rangle| = m$ olsun. $q = p^t$ ise F_q cisminin θ otomorfizması tarafından sabit bırakılan alt cismi K, $p^{t/m}$ elemanlı sonlu cisimdir. Bu başlık altındaki tanımlarda ve teoremlerde bu notasyonlar kullanılacaktır.

Tanım 2.36 Katsayıları bir F_q cisminin elemanları olan

$$F_q[x;\theta]=\left\{a_0+a_1x+\ldots+a_nx^n \,\middle|\, a_i\in F_q, 0\le i\le n\right\} \tag{2.7}$$

polinomlarının kümesi, aykırı (skew) polinomlar kümesi olarak adlandırılır. $F_q[x;\theta]$ kümesi üzerinde toplama işlemi polinomlardaki toplama işlemi ve çarpma işlemi ise $(a_ix^i)(a_jx^j)=a_i\theta^i(a_j)x^{i+j}$ kuralı ile belirlidir [38].

Teorem 2.37 Toplama ve çarpma işlemlerinin yukarıdaki şekilde tanımlandığı $F_q[x;\theta]$ kümesi bir halka belirtir. θ birimden farklı ise $F_q[x;\theta]$ değişmeli olmayan bir halkadır. Bu halkaya aykırı (skew) polinom halkası denir [38].

Aykırı polinom halkasının bazı özellikleri aşağıda verilmiştir [38]. $f(x)$ polinomunun derecesi $der(f(x))$ ile gösterilmektedir.

i. $F_q[x;\theta]$ halkasının sıfır böleni yoktur.

ii. $F_q[x;\theta]$ halkasının birimselleri F_q cisminin birimselleridir.

iii. $f(x), g(x)\in F_q[x;\theta]$ olmak üzere

$$der(f(x)+g(x))\le \max\{der(f(x)), der(g(x))\},$$

ve $der(f(x)g(x))=der(f(x))+der(g(x))$'dir.

Teorem 2.38 (Bölme Algoritması) $F_q[x;\theta]$ halkasındaki herhangi iki polinom $f(x)\neq 0$ ve $g(x)$ için $g(x)=q(x)f(x)+r(x)$, $der(r(x))<der(f(x))$ veya $r(x)=0$ olacak şekilde $q(x)$, $r(x)\in F_q[x;\theta]$ vardır ve tek türlüdür [38].

Yukarıdaki teoremde $g(x)$ polinomu $f(x)$ polinomu ile sağdan bölünmüştür. Aynı teorem soldan bölme için de geçerlidir. Dolayısıyla $F_q[x;\theta]$ halkası için bölme algoritması sağdan ve soldan sağlanır.

I, $F_q[x;\theta]$ halkasının bir sol ideali ve I idealindeki en küçük dereceli sıfırdan farklı bir polinom $f(x)$ olsun. I idealindeki bir $g(x)$ polinomu için

$$g(x)=q(x)f(x)+r(x),\ der(r(x))<der(f(x)) \text{ veya } r(x)=0 \tag{2.8}$$

sağlanır. Ancak $r(x)=g(x)-q(x)f(x)\in I$ olması $f(x)$ polinomu idealdeki en küçük dereceye sahip olduğundan $r(x)=0$ olmalıdır. Dolayısıyla her $g(x)\in I$ için $g(x)=q(x)f(x)$ eşitliği sağlanır. Böylece I ideali $F_q[x;\theta]$ halkasında tek bir eleman tarafından üretilir, yani temel idealdir. $I=\langle f(x)\rangle$ şeklinde gösterilir. Benzer biçimde $F_q[x;\theta]$ halkasının tüm sağ idealleri temel idealdir [38].

Not 2.39 Bu çalışmada sol idealler üzerine yoğunlaşacağımız için, $I=\langle f(x)\rangle$ gösterimi $f(x)$ polinomu tarafından üretilen sol ideal kavramı için kullanılacaktır.

Tanım 2.40 $F_q[x;\theta]$ halkasının bir I ideali için $I=F_q[x;\theta]g(x)=f(x)F_q[x;\theta]$ eşitliğini sağlayan $f(x),g(x)\in F_q[x;\theta]$ varsa I idealine çift taraflı ideal veya kısaca ideal denir [38].

Teorem 2.41 $F_q[x;\theta]$ halkasında x^n-1 polinomunu tarafından üretilen sol ideal $\langle x^n-1\rangle$ ve $|\langle\theta\rangle|=m$ olsun. $\langle x^n-1\rangle$ idealinin çift taraflı ideal olması için gerek ve yeter koşul $m|n$ olmasıdır [28].

Teorem 2.42 F_q cisminin θ tarafından sabit bırakılan alt cismi K olsun.

$$Z\left(F_q[x;\theta]\right)=\left\{a_0+a_1x^m+\ldots+a_r\,x^{mr}\,\middle|\,a_i\in K,\,|\langle\theta\rangle|=m\right\} \tag{2.9}$$

kümesi $F_q[x;\theta]$ halkasının merkezidir [38].

Önerme 2.43 $h(x),g(x)\in F_q[x;\theta]$ olmak üzere $h(x)g(x)\in Z(F_q[x;\theta])$ ise $h(x)g(x)=g(x)h(x)$ sağlanır [29].

Yukarıdaki önermeden görüleceği üzere merkezdeki bir polinomun sol böleni aynı zamanda sağ bölenidir.

Sonuç 2.44 F_q cisminin mertebesi m olan bir otomorfizması θ ve $m|n$ olsun. $x^n-1=h(x)g(x)\in F_q[x;\theta]$ ise aynı zamanda $x^n-1=g(x)h(x)\in F_q[x;\theta]$ dir.

İspat $m|n$ olması durumunda x^n-1 polinomu $F_q[x;\theta]$ halkasının merkezindedir ve yukarıdaki önermenin bir sonucu olarak görülür. ■

2.5 Hata Düzelten Kodlar

Hata düzelten kodlar teorisi iletişim, veri depolama gibi dijital bilgi transferi esnasında kaynak ile alıcı arasında meydana gelebilecek hataların tespit edilmesi ve düzeltilmesi üzerinde çalışır. Bunun için transfer edilecek orijinal mesaja eklemeler yapılarak iletişim kanalından alıcıya aktarılır. Bu eklemelere kontrol biti adı verilir. Mümkün olan en doğru biçimde mesajın alıcıya ulaşacağı ve kanal verimliliğinin düşmeyeceği şekilde bu eklemeleri optimize etmek hata düzelten kodlar teorisinin temel amacıdır. Cebirsel kodlama teorisi ise kodlama teorisinin optimizasyon problemini cebirsel argümanlar yardımıyla çözmeyi amaçlar. Bu başlık altında kodlama teorisi ile ilgili bazı temel tanım ve teoremler [34] nolu kaynak esas alınarak düzenlenmiştir..

Tanım 2.45 $A=\{a_1,\ldots,a_q\}$ şeklinde q elemanlı bir küme olsun.

i. $\mathbf{w}=w_1w_2\ldots w_n \ \ (w_i\in A)$ şeklindeki diziye A kümesi üzerinde n uzunluğunda bir q-lu söz denir. $\mathbf{w}$ sözü aynı zamanda $\mathbf{w}=(w_1,w_2,\ldots,w_n)$ şeklinde vektör olarak da düşünülebilir.

ii. Boştan farklı bir $C\subseteq A^n$ kümesi, A üzerinde n uzunluğunda bir koddur. C'nin her bir elemanına C'nin kodsözü denir.

Tanım 2.46 $u=(u_1,u_2,...,u_n)$ ve $v=(v_1,v_2,...,v_n)$, n uzunluğunda birer söz olsun. u ile v arasındaki Hamming uzaklığı $d(u,v)=\left|\left\{i\,|u_i\neq v_i,1\leq i\leq n\right\}\right|$ şeklinde hesaplanır.

Tanım 2.47 C'nin farklı kodsözleri arasındaki en küçük Hamming uzaklığına C kodunun minimum Hamming uzaklığı denir ve $d(C)$ ile gösterilir.

Tanım 2.48 A; q elemanlı bir küme olsun. A üzerinde n uzunluğunda, eleman sayısı M ve minimum Hamming uzaklığı d olan bir kod kısaca $(n,\mathrm{M},d)_q$-kod olarak gösterilir. n, M ve d sayılarına kodun parametreleri denir.

2.5.1 Lineer Kodlar

F_q^n vektör uzayının bir F_q-alt vektör uzayına n uzunluğunda F_q üzerinde lineer kod denir.

Tanım 2.49 C, n uzunluğunda bir lineer kod ve $u=(u_1,u_2,...,u_n),\ v=(v_1,v_2,...,v_n)\in C$ olsun. u kodsözü için Hamming ağırlığı $wt(u)=\left|\left\{i\,|u_i\neq 0\right\}\right|$ olarak tanımlıdır. Ayrıca u ile v arasındaki Hamming uzaklığı $d(u,v)=wt(u-v)$ şeklinde hesaplanır. C'nin kodsözlerinin sıfırdan farklı en küçük Hamming ağırlığına C kodunun minimum Hamming ağırlığı denir ve $wt(C)$ ile gösterilir.

Teorem 2.50 C bir lineer kod ise $d(C)=wt(C)$ sağlanır.

Tanım 2.51 F_q üzerinde uzunluğu n, boyutu k ve minimum Hamming uzaklığı d olan bir C lineer kodu $[n,k,d]_q$-kod olarak gösterilir.

Tanım 2.52 $u=(u_0,u_1,\ldots,u_{n-1})$ ve $v=(v_0,v_1,\ldots,v_{n-1})\in F_q^n$ olsun. Aşağıda tanımlanan

$$\begin{aligned}\left\langle \cdot,\cdot \right\rangle &: F_q^n\times F_q^n\to F_q\\ (u,v)&\to\sum_{i=0}^{n-1}u_iv_i\end{aligned}\qquad(2.10)$$

fonksiyonu bir iç çarpım fonksiyondur ve Öklid iç çarpımı olarak adlandırılır. $C\subseteq F_q^n$ bir lineer kod olmak üzere $C^{\perp}=\left\{u\in F_q^n\,\middle|\,\text{Her } v\in C \text{ için } \left\langle u,v\right\rangle=0\right\}$ kümesine C kodunun duali denir.

Tanım 2.53 $C\subseteq F_q^n$ bir lineer kod olsun.

- **i.** C, F_q^n uzayının bir alt vektör uzayı olduğundan bir bazı vardır. C'nin baz vektörlerini satır kabul eden matrise C'nin üreteç matrisi denir.
- **ii.** Her $u\in C$ için $Hu^T=0$ eşitliğini sağlayan H matrisine C'nin kontrol matrisi denir. H matrisi aynı zamanda $C^{\perp}$ kodunun üreteç matrisidir.

2.5.2 Devirli Kodlar

Devirli kodlar, lineer kodların özel bir alt ailesidir. Devirli kodlar ilk olarak Eugene Prange tarafından 1957 yılında ortaya konulmuştur [39]. Bu çalışma, cebirsel kodlama teorisi alanında çok önemli gelişmelere yol açmıştır. Devirli kodlar özellikle verimli kodlama ve dekodlama algoritmaları sağlaması açısından avantajlıdır. n uzunluğunda

k boyutlu bir lineer kodu temsil edebilmek için $k \times n$'lik bir matrise ihtiyaç duyulurken, aynı parametrelere sahip bir devirli kod sadece derecesi $n-k$ olan bir polinom tarafından temsil edilebilmektedir. Hamming kodlar, Golay kodlar, BCH kodlar gibi önemli kod aileleri devirli kodlardır.

Tanım 2.54 C, n uzunluğunda bir lineer kod ve her $c=(c_0,c_1,...,c_{n-1}) \in C$ için $\sigma(c)=(c_{n-1},c_0,...,c_{n-2}) \in C$ ise C'ye devirli kod denir. σ dönüşümüne ise devirsel öteleme (cyclic shift) denir.

Önerme 2.55 Kodlar polinomlar cinsinden ifade edilebilir.

$$\pi_1 : F_q^n \to F_q[x] \Big/ \langle x^n - 1 \rangle, \quad c=(c_0,c_1,...,c_{n-1}) \to c(x)=c_0+c_1x+...+c_{n-1}x^{n-1} \qquad (2.11)$$

Yukarıda tanımlanan π_1 fonksiyonu bir lineer dönüşümdür. Bu durumda $c \in C$ kodsözünün polinom yazımında devirsel ötelemesi, $F_q[x] \Big/ \langle x^n - 1 \rangle$ bölüm halkasında $x.c(x)$ polinomuna tekabül eder. Yukarıdaki lineer dönüşüm vasıtasıyla devirli kodlar idealler cinsinden ifade edilebilir.

Teorem 2.56 $C \subseteq F_q^n$ lineer kodunun devirli kod olması için gerek ve yeter koşul $\pi_1(C)$'nin $F_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının bir ideali olmasıdır.

Teorem 2.57 $F_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının sıfırdan farklı bir ideali I ve $g(x)$ polinomu da I idealindeki sıfırdan farklı en küçük dereceye sahip monik (baş katsayısı 1 olan) polinom olsun. Bu durumda $g(x)$ polinomu I idealinin bir üretecidir ve x^n-1'i böler.

$C \subseteq F_q^n$ bir devirli kod ve $\pi_1(C)=\langle g(x) \rangle$ ise $g(x)$ polinomuna C kodunun üreteç polinomu denir ve $C=\langle g(x) \rangle$ olarak gösterilir.

Teorem 2.58 $F_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının sıfırdan farklı herhangi bir I idealindeki sıfırdan farklı en küçük dereceli monik polinom tektir.

Örnek 2.59 $C=\{0000,1010,0101,1111\}$ kodu F_2 cismi üzerinde bir devirli koddur. C'nin kod sözlerine karşılık gelen polinomların kümesi $\pi_1(C)=\{0,1+x^2,x+x^3,1+x+x^2+x^3\}$'dir. $\pi_1(C)$, $F_2[x] \Big/ \langle x^4 - 1 \rangle$ halkasının bir

idealidir. $\pi_1(C)$ idealindeki en küçük dereceli monik polinom x^2+1, $\pi_1(C)$ idealini üretir. Böylece x^2+1 polinomu C kodunun üreteç polinomudur, yani $C=\langle x^2+1\rangle$'dir.

Teorem 2.60 $F_q[x]$ halkasında x^n-1 polinomunun her bir monik böleni F_q üzerinde tanımlı bir devirli kod üretir.

Teorem 2.61 $g(x)\in F_q[x]$, $g(x)\,|\,x^n-1$ ve $der(g(x))=k$ olsun. Bu durumda $g(x)$ tarafından üretilen ideale karşılık gelen kod n uzunluğunda boyutu $n-k$ olan devirli bir koddur.

Tanım 2.62 $f(x)=a_0+a_1x+a_2x^2+\ldots+a_kx^k\in F_q[x]$, derecesi k olan bir polinom olsun. $f(x)$'in ters sıralı polinomu (reciprocal) $f^t(x):=x^kf(1/x)=\sum_{i=0}^{k}a_{k-i}x^i$ şeklinde tanımlıdır.

Önerme 2.63 $x^n-1=h(x)g(x)\in F_q[x]$ ve $C=\langle g(x)\rangle$, F_q üzerinde n uzunluğunda bir devirli kod olsun. Bu durumda C'nin duali $h^t(x)$ polinomu tarafından üretilen devirli koddur, yani $C^{\perp}=\langle h^t(x)\rangle$ dir.

Not 2.64 $h(x)=h_0+h_1x+\ldots+h_kx^k$ iken $h^t(x)$ polinomu monik olmayabilir. Bu durumda $h_0\neq 0$ iken $h_0^{-1}h^t(x)$ polinomu monik bir polinomdur. $h^t(x)$ polinomunun ürettiği ideal ile $h_0^{-1}h^t(x)$ polinomunun ürettiği ideal eşit olacağından, $C^{\perp}=\langle h^t(x)\rangle$ yazılır.

Teorem 2.65 $x^n-1=h(x)g(x)\in F_q[x]$ ve $C=\langle g(x)\rangle$, F_q üzerinde n uzunluğunda bir devirli kod olsun.

i. $g(x)=g_0+g_1x+\ldots+g_{n-k}x^{n-k}$ ve $der(g(x))=n-k$ olmak üzere

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

matrisi C kodunun üreteç matrisidir.

ii. $h(x)=h_0+h_1x+\ldots+h_kx^k$ ve $der(h(x))=k$ olmak üzere

$$H=\begin{bmatrix} h^t(x) \\ xh^t(x) \\ \vdots \\ x^{n-k-1}h^t(x) \end{bmatrix}=\begin{bmatrix} h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ \vdots & & & \ddots & & & & & \vdots \\ 0 & 0 & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 \end{bmatrix}$$

matrisi C kodunun kontrol matrisidir. H matrisi aynı zamanda $C^{\perp}$ kodunun üreteç matrisidir.

Örnek 2.66 $g(x)=1+x+x^2+x^4$ polinomu, $F_2[x]$ halkasında x^7-1 polinomunun bir bölenidir. Bu durumda $g(x)$ polinomu $n=7$ uzunluğunda boyutu $n-k=7-4=3$ olan devirli bir kod üretir. $C=\langle g(x)\rangle$ devirli kodu için üreteç matrisi,

$$G=\begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \tag{2.12}$$

şeklindedir. C kodunun parametreleri $[7,3,4]_2$'dir. $h(x)=(x^7-1)/g(x)=1+x+x^3$ ve $h^t(x)=1+x^2+x^3$ dir. Bu durumda $C^{\perp}=\langle h^t(x)\rangle$ ve $C^{\perp}$ kodunun üreteç matrisi,

$$H=\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{2.13}$$

şeklindedir.

2.5.3 Aykırı Devirli Kodlar

Aykırı (skew) devirli kodlar ilk olarak Boucher vd. tarafından 2007 yılında tanımlanmıştır [26]. Bu çalışmada aykırı polinom halkaları kullanılarak devirli kodların bir genellemesi elde edilmiştir. Bazı çalışmalarda bu aile aykırı devirli kodlar yerine θ-devirli kodlar olarak adlandırılmıştır [29], [40]. Aykırı polinom halkalarının cebirsel özellikleri nedeniyle aykırı devirli kodlar optimal kod bulma açısından devirli kodlara göre daha avantajlıdır. Bu cebirsel özellikler kısaca aykırı polinom halkalarında sağ ve

sol bölme algoritmasının sağlanıyor olması ve çarpanlara ayırmanın tek türlü olmamasıdır.

Tanım 2.67 C kodu, F_q üzerinde n uzunluğuna sahip bir lineer kod ve θ, F_q cismi üzerinde tanımlı bir otomorfizma olsun. Her $c=(c_0,c_1,....,c_{n-1})\in C$ için

$$\sigma(c)=\left(\theta\left(c_{n-1}\right),\theta\left(c_0\right),....,\theta\left(c_{n-2}\right)\right)\in C \tag{2.14}$$

sağlanıyorsa C koduna n uzunluğunda aykırı devirli (skew cyclic) kod denir. σ dönüşümüne aykırı devirsel öteleme (skew cyclic shift) denir [26].

Eğer θ birim ise C bir devirli koddur. Dolayısıyla aykırı devirli kod ailesi devirli kodlar ailesini kapsar.

C kodunun kodsözlerini polinomlar cinsinden aşağıdaki gibi ifade edebiliriz.

$$\begin{aligned}\pi:\ C &\to\ F_q[x;\theta]\big/(x^n-1)\\ c=(c_0,c_1,.....,c_{n-1}) &\to c(x)=c_0+c_1x+.....+c_{n-1}x^{n-1}\end{aligned} \tag{2.15}$$

olarak tanımlanan π dönüşümü bir izomorfizmadır. $c\in C$ kodsözünün aykırı devirsel ötelenmiş hali $\sigma(c)$, polinom yazılımında $xc(x)=\theta(c_{n-1})+\theta(c_0)x+....+\theta(c_{n-2})x^{n-1}$ ye karşılık gelir.

C, F_q üzerinde tanımlı n uzunluğunda devirli kod iken $\pi_1(C)$'nin $F_q[x]\big/\left\langle x^n-1\right\rangle$ halkasının bir ideali olduğu gösterilmişti. Aykırı devirli kodlar tanımlanırken iki durum ile karşılaşılır.

C, F_q üzerinde tanımlı n uzunluğunda aykırı devirli kod ve $\left|\left\langle\theta\right\rangle\right|=m$ olsun.

i. $m|n$ ise $F_q[x;\theta]\big/\left\langle x^n-1\right\rangle$ bir halka belirtir. Bu durumda $\pi(C)$, $F_q[x;\theta]\big/\left\langle x^n-1\right\rangle$ halkasının bir idealidir [26].

ii. $m\nmid n$ olması durumunda $F_q[x;\theta]\big/\left\langle x^n-1\right\rangle$ halka belirtmez. Fakat $F_q[x;\theta]\big/\left\langle x^n-1\right\rangle$ bir sol $F_q[x;\theta]$-modüldür. Herhangi bir n değeri için $\pi(C)$, $F_q[x;\theta]\big/\left\langle x^n-1\right\rangle$'in bir sol $F_q[x;\theta]$-alt modülü olarak ele alınabilir [27].

Teorem 2.68 C, F_q üzerinde tanımlı n uzunluğunda bir lineer kod olsun. C kodunun aykırı devirli kod olması için gerek ve yeter koşul C'nin $F_q[x;\theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$-alt modülü olmasıdır [27].

Önerme 2.69 C, $F_q[x;\theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$-alt modülü olsun. Bu durumda C devirli alt modüldür ve C'deki sıfırdan farklı en küçük dereceli monik polinom tarafından üretilir [27].

Teorem 2.70 C, $F_q[x;\theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$-alt modülü olsun ve $f(x)$ polinomu C'deki sıfırdan farklı en küçük dereceli monik polinom olsun. Bu durumda $f(x)$ polinomu x^n-1'in bir sağ bölenidir [27].

Teorem 2.71 $F_q[x;\theta]$ halkasında $x^n-1=h(x)g(x)$ ve $der(g(x))=r$ olsun. $C=\langle g(x)\rangle$, $F_q[x;\theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $F_q[x;\theta]$-alt modülü olsun. Bu durumda C bir serbest sol F_q-altmodüldür. C'nin bir bazı $\beta=\{g(x),xg(x),\ldots,x^{n-r-1}g(x)\}$ şeklindedir. Yani her $c\in C$ elemanı, $\alpha_i\in F_q$ olmak üzere $c=\sum_{i=0}^{n-r-1}\alpha_i x^i g(x)$ şeklinde sonlu toplam olarak yazılabilir ve bu yazılış tek türlüdür [27].

Sonuç olarak; x^n-1'in sağ bölenleri $F_q[x;\theta]\Big/\langle x^n-1\rangle$ modülünde birer sol $F_q[x;\theta]$-alt modül üretir ve $F_q[x;\theta]\Big/\langle x^n-1\rangle$ modülünün sol $F_q[x;\theta]$-alt modülleri birer aykırı devirli koda karşılık gelir. x^n-1'in derecesi $n-k$ olan her bir sağ böleni, n uzunluğunda boyutu k olan bir aykırı devirli kod üretir.

Teorem 2.72 $g(x)=g_0+g_1x+\ldots+g_{n-k}x^{n-k}$ polinomu $F_q[x;\theta]$ halkasında x^n-1'in bir sağ böleni ve $der(g(x))=n-k$ olsun. Bu durumda n uzunluğunda $C=\langle g(x)\rangle$ aykırı devirli kodunun üreteç matrisi aşağıdaki gibidir [41].

$$G=\begin{bmatrix} g(x)\\ xg(x)\\ \vdots\\ x^{k-1}g(x)\end{bmatrix}=\begin{bmatrix} g_0 & g_1 & \ldots & \ldots & g_{n-k} & 0 & 0 & \ldots & 0\\ 0 & \theta(g_0) & \theta(g_1) & \ldots & \ldots & \theta(g_{n-k}) & 0 & \ldots & 0\\ \vdots & & & \ddots & & & & & \vdots\\ 0 & 0 & \ldots & 0 & \theta^k(g_0) & \theta^k(g_1) & \ldots & \ldots & \theta^{k-1}(g_{n-k})\end{bmatrix}.$$

$F_q[x;\theta]$ halkasında polinomların çarpanlara ayrılışı tek türlü değildir. Çarpanlara ayrılışın tek türlü olmaması daha fazla sayıda sağ bölen bulmamıza ve daha fazla sayıda kod üretmemize olanak sağlar. Böylece daha iyi parametrelere sahip kod bulunması açısından avantajlıdır.

Örnek 2.73 $\theta \in Aut(F_4)$ ve $\theta(a) = a^2$ olsun. F_4 üzerinde uzunluğu 4, boyutu 2 olan aykırı devirli kod bulmak için öncelikle $x^4 - 1 \in F_4[x;\theta]$ polinomunun derecesi 2 olan sağ böleni bulunmalıdır. $x^4 - 1$'in $F_4[x;\theta]$ halkasında derecesi 2 olan tüm sağ bölenleri aşağıda verilmiştir.

$$\begin{aligned} x^4 - 1 &= (x^2+1)(x^2+1) \\ &= (x^2+\alpha x+\alpha)(x^2+\alpha x+\alpha^2) \\ &= (x^2+\alpha^2 x+\alpha^2)(x^2+\alpha^2 x+\alpha) \\ &= (x^2+\alpha^2 x+\alpha)(x^2+\alpha^2 x+\alpha^2) \\ &= (x^2+x+\alpha^2)(x^2+x+\alpha) \\ &= (x^2+x+\alpha)(x^2+x+\alpha^2) \\ &= (x^2+\alpha x+\alpha^2)(x^2+\alpha x+\alpha). \end{aligned} \tag{2.16}$$

$g_1(x) = x^2 + \alpha x + \alpha^2$ polinomu $[4,2,3]_4$ parametrelerine sahip, aykırı devirli kod üretir.

$C = \langle g_1(x) \rangle$ aykırı devirli kodunun üreteç matrisi $G_1 = \begin{bmatrix} \alpha^2 & \alpha & 1 & 0 \\ 0 & \alpha & \alpha^2 & 1 \end{bmatrix}$ şeklindedir.

$F_4[x] \big/ \langle x^4 - 1 \rangle$ değişmeli polinom halkasında $x^4 - 1$ polinomunun derecesi 2 olan böleni sadece $g_2(x) = x^2 + 1$ polinomudur. $g_2(x)$ tarafından üretilen ideal F_4 üzerinde $[4,2,2]_4$ parametrelerine sahip devirli bir koda karşılık gelir. $F_4[x] \big/ \langle x^4 - 1 \rangle$ halkasında $x^4 - 1$'in ikinci dereceden başka böleni olmadığından bu şekilde başka bir devirli kod yoktur. Brouwer'in tablosuna göre F_4 üzerinde $[4,2,3]_4$ parametrelerine sahip kodlar optimaldir [42]. Bu örnekte de görüldüğü üzere aykırı devirli kod ailesi devirli kodlar ailesine göre optimal kodlar elde etme açısından daha avantajlıdır.

Şimdi aykırı devirli kodların dualleri hakkında bazı önemli teoremleri verelim**.**

Tanım 2.74 $f(x)=a_0+a_1x+a_2x^2+\ldots+a_tx^t\in F_q[x;\theta]$ ve $a_t\neq 0$ olmak üzere $f(x)$ polinomunun aykırı ters sıralısı (skew reciprocal) $f^R(x)=\sum_{i=0}^{t}x^ia_{t-i}=\sum_{i=0}^{t}\theta^i(a_{t-i})x^i$ olarak tanımlıdır.

Not 2.75 $f(x)=a_0+a_1x+a_2x^2+\ldots+a_tx^t\in F_q[x;\theta]$ polinomunun aykırı ters sıralısı kolayca şu şekilde hesaplanır;

$$\begin{aligned} f^R(x) &= x^t(a_0+x^{-1}a_1+x^{-2}a_2+\ldots+x^{-t}a_t) \\ &= \theta^t(a_0)+\theta^{t-1}(a_1)x^{t-1}+\theta^{t-2}(a_2)x^{t-2}+\ldots+a_t. \end{aligned} \tag{2.17}$$

Önerme 2.76 θ'nın mertebesi m ve $m\,|\,n$ olsun. $x^n-1=h(x)g(x)\in F_q[x;\theta]$ ve $C=\langle g(x)\rangle$, F_q üzerinde n uzunluğunda bir aykırı devirli kod olsun. Bu durumda C'nin duali $h^R(x)$ polinomu tarafından üretilen aykırı devirli koddur, yani $C^{\perp}=\langle h^R(x)\rangle$'tir [29].

Teorem 2.77 C, F_q üzerinde tanımlı n uzunluğunda bir aykırı devirli kod ve $|\langle\theta\rangle|=m$ olsun. $(m,n)=1$ ise C bir devirli koddur [27].

Teorem 2.78 $F_q[x;\theta]$ halkasında $g(x)$ polinomu x^n-1'in bir sağ böleni ve F_q cisminin θ tarafından sabit bırakılan alt cismi K olsun. $(m,n)=1$ ise $g(x)\in K[x]$ tir [32].

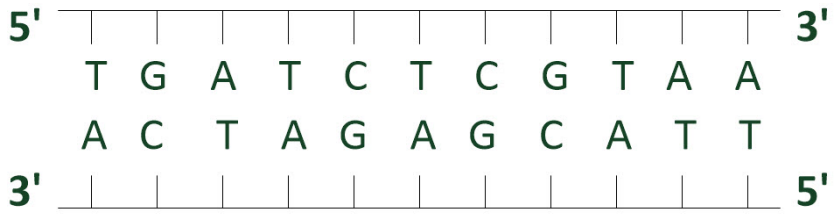
Teorem 2.79 $k\leq n$, $g(x),\ h(x)\in F_q[x;\theta]$ ve $der(h(x))=k$, $der(g(x))=n-k$ olsun. Bu durumda, $\theta^n(g(x))=\theta^n(g_0)+\theta^n(g_1)x+\ldots+\theta^n(g_{n-k})x^{n-k}$ olmak üzere, $x^n-1=h(x)g(x)$ olması için gerek ve yeter koşul $x^n-1=\theta^n(g(x))h(x)$ olmasıdır [41].

Teorem 2.80 $\theta\in Aut(F_q)$, $|\langle\theta\rangle|=m$ ve F_q cisminin θ tarafından sabit bırakılan alt cismi K olsun. $(m,n)=1$ olması durumunda, x^n-1 polinomunun $F_q[x;\theta]$ halkasındaki ayrışımı $K[x]$ değişmeli halkasındaki ayrışımından ibarettir.

İspat Teorem 2.78 ve Teorem 2.79'un sonucu olarak görülür. ■

2.6 DNA ile ilgili Temel Bilgiler ve DNA Kodlar

DNA; hücrelerin fonksiyonlarını sürdürebilmesi için gerekli bilgileri taşıyan moleküldür. DNA dizileri; Adenin (A), Guanin (G), Sitozin (C) ve Timin (T) olarak adlandırılan dört temel bazdan (nükleotid) oluşur. Bu bazlar DNA molekülünün şeker ve fosfattan oluşan iskeletine tutunarak, molekülün bir iplikçiğini oluştururlar. İki DNA iplikçiği birbirine WCC (Watson Crick complement) özelliğine göre bağlanır ve DNA çift sarmalını oluşturur. WCC özelliğine göre A ile T ve G ile C birbirinin tamlayanıdır ve $A^c = T$ ve $G^c = C$ olarak gösterilir. A ile T ikili hidrojen bağı, G ile C ise üçlü hidrojen bağı kurarak DNA çift sarmal yapısını oluştururlar. Birbirinin tamlayanı olan uygun DNA parçalarının bir araya gelerek ikili sarmal oluşturmasına DNA hibridizasyonu denir.



Şekil 2.1 DNA bazlarının karşılıklı dizilimi

Bir DNA iplikçiğinin (DNA dizisi) uç noktaları kimyasal farklılıklarından dolayı $3'$-ucu ve $5'$-ucu olarak adlandırılır. Genel olarak bir iplikli DNA ve RNA dizileri yazılırken $5'$-ucundan $3'$-ucuna doğru yazılır ve hibridizasyon esnasında $3'$-ucu ve $5'$-ucu birbirini tamamlar. Bu yazıma göre bir DNA dizisi ile ters sıralı tamlayanı DNA çift sarmalını oluşturur. Örneğin $5'-TGATCTCGTAA-3'$ ile $5'-TTACGAGATCA-3'$ DNA dizileri WCC kuralına göre birbirine bağlanarak DNA çift zincirini oluştururlar (Şekil 2.1). Bir DNA k-bazı (k-mer) kısaca k uzunluğunda bir DNA dizilimidir. Örneğin, $ATGGC$ bir DNA 5-bazıdır.

Tanım 2.81 (DNA kod) Bileşenleri $\{A,T,G,C\}$ kümesinin elemanları olan n uzunluğundaki vektörler(kelimeler)den oluşan kümeye DNA kod adı verilir. DNA kodun elemanlarına kodsöz denir.

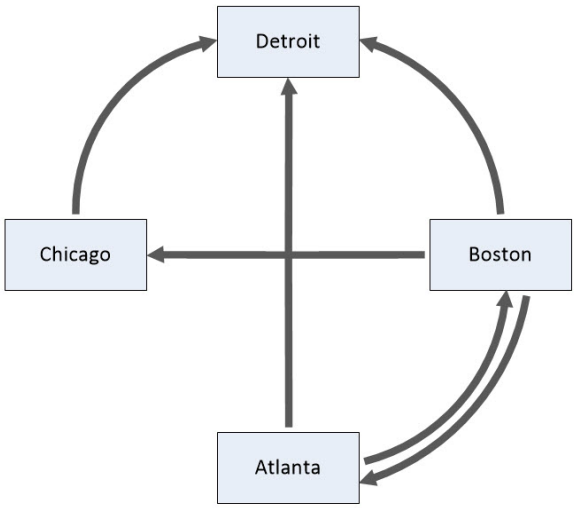
Tanım 2.82 D DNA kod ve $u \in D$ olsun. u kodsözünün ters sıralısı (reverse) u^r, tamlayanı (complement) u^c ve ters sıralı tamlayanı (reverse-complement) u^{rc} olarak gösterilir.

Örnek 2.83 $u = ATGCTATT$ şeklinde bir DNA kodsözünün ters sıralısı $u^r = TTATCGTA$, tamlayanı $u^c = TACGATAA$ ve ters sıralı tamlayanı $u^{rc} = AATAGCAT$ şeklindedir.

Adleman, Hamilton yolu problemini 7 düğüm için sentetik DNA dizilerinin WCC özelliğinden yararlanılarak deney tüpünde manipüle edilmesi ile çözmüştür. Bu çalışma ile birlikte DNA molekülleri hesaplama işlemlerinde kullanılmaya başlanmıştır.

Hamilton yolu problemi kısaca, yönlü veya yönsüz bir graf verildiğinde her bir düğümü tam olarak bir defa geçerek tüm düğümlere uğrayan bir yol olup olmadığıdır. Adleman'ın deneyini 4 düğüm için örneklendirelim.

Örnek 2.84 [43] Şekil 2.2'de şehirler arasındaki uçuşlar yönlü graf olarak verilmiştir. Buna göre, Chicago'dan Detroit'e uçuş var iken Detroit'ten Chicago'ya uçuş yoktur.



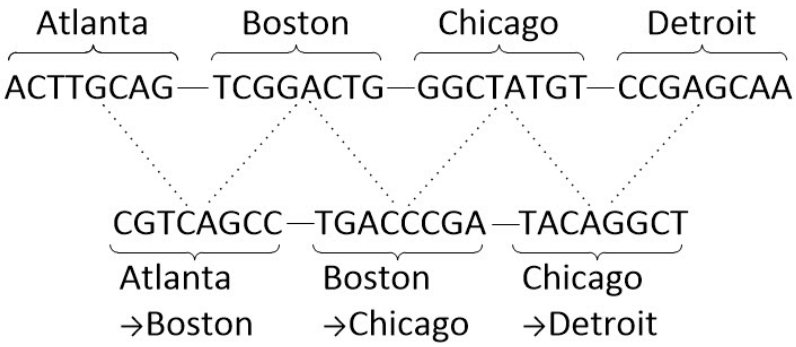
Şekil 2.2 Şehirler arası uçuşlar

Şekil 2.2'ye göre Atlanta'dan başlayıp Detroit'e her bir şehire tam olarak 1 kez uğrayarak varan Hamilton yolunu bulalım. Bunun için her bir şehir 8 uzunluğunda bir sentetik DNA dizisi ile kodlanır. Şehirler arasındaki uçuşlar(yollar) ise kalkış şehrini temsil eden DNA dizisinin son 4-bazının tamlayanı ile varış şehrinin ilk 4-bazının tamlayanı şeklinde kodlanır (Çizelge 2.1).

Çizelge 2.1 Şehirler, uçuşlar ve DNA karşılıkları

Şehirler	DNA karşılığı
Atlanta	ACTT GCAG
Boston	TCGG ACTG
Chicago	GGCT ATGT
Detroit	CCGA GCAA
Uçuşlar	DNA karşılığı
Atlanta $\rightarrow$ Boston	CGTC AGCC
Atlanta $\rightarrow$ Detroit	CGTC GGCT
Boston $\rightarrow$ Chicago	TGAC CCGA
Boston $\rightarrow$ Detroit	TGAC GGCT
Boston $\rightarrow$ Atlanta	TGAC TGAA
Chicago $\rightarrow$ Detroit	TACA GGCT

Yollara karşılık gelen DNA dizileri çoğaltılarak bir deney tüpüne şehirlere karşılık gelen DNA dizileri ise çoğaltılarak bir başka bir deney tüpüne konulur. Bu iki deney tüpü ortak bir kapta gerekli enzimler ile karıştırılarak hibridizasyonların gerçekleşmesi sağlanır. Daha sonra ayrıştırma yöntemleri kullanılarak elde edilen DNA çift zincirlerinden ilk etapta uzunluğu 4'ten küçük olanlar daha sonra Atlanta ile başlayıp Detroit ile bitenler haricindekiler ayrıştırılır. Neticede kalan DNA dizileri okunarak her bir şehre uğrayan dizisi çözüm olarak elde edilir (Şekil 2.3).



Şekil 2.3 Örnek 2.84'ün çözümü

Yukarıdaki örnekte de görüldüğü üzere DNA hesaplamalarında önemli adımlardan biri problemin sentetik DNA dizilerine uygun bir aktarımını (DNA-kodlamasını) bulmaktır. Böylelikle hibridizasyon süreci neticesinde istenen sonuç elde edilmiş olacaktır. Fakat DNA dizileri arasında istenmeyen hibridizasyonların gerçekleşmesi mümkündür. Bu durum problemin çözümünü engeller ve verimi düşürür. Tasarlanan DNA dizileri arasında hatalı hibridizasyon oluşma ihtimalini minimuma indirgemek için DNA kodlara bazı kombinatöryel kısıtlar uygulanır [10], [11]. D bir DNA kod ve d bir pozitif tamsayı olsun.

i. **Hamming uzaklığı kısıtı:** Her $u, v \in D$ ($u \neq v$) için $d(u,v) \geq d$.

ii. **Ters sıra kısıtı:** Her $u, v \in D$ için $d(u^r, v) \geq d$.

iii. **Ters sıra tamlayan kısıtı:** Her $u, v \in D$ için $d(u^{rc}, v) \geq d$.

iv. GC**-miktar kısıtı:** Her $u \in D$ kodsözünün içerdiği G ve C bazlarının toplam sayısının eşit olmasıdır.

Tanım 2.85 (Ters sıralı DNA kod) D bir DNA kod olsun. Her $u \in D$ için $u^r \in D$ sağlanıyorsa, D bir ters sıralı DNA koddur.

Tanım 2.86 (Ters sıralı tamlayan DNA kod) D DNA kod olsun. Her $u \in D$ için $u^{rc} \in D$ sağlanıyorsa, D bir ters sıralı tamlayan DNA koddur.

Doğal olarak ters sıralı DNA kodlar ters sıra kısıtını sağlar. Ayrıca ters sıralı DNA kodlardan ters sıra tamlayan DNA kod elde etmek oldukça kolaydır. Aşağıdaki teorem [16] çalışmasında verilen Teorem 4.1'in bir sonucu olarak görülür.

Teorem 2.87 D, uzunluğu n olan ters sıralı bir DNA kod olsun. $n = 2k$ şeklinde bir çift sayı ise, $x_i \in D$ elemanları $x_i = a_i b_i$ şeklinde uzunluğu k olan a_i ve b_i vektörü olarak ifade edildiğinde; $\left\{ y_i = a_i b_i^c \right\}$ kümesi bir ters sıralı tamlayan DNA koddur.

İspat D bir ters sıralı DNA kod ve $n = 2k$ olsun**.** $x_i \in D$ elemanları $x_i = a_i b_i$ şeklinde yazılsın. $D' = \left\{ y_i = a_i b_i^c \right\}$ olsun. $(b_i^c)^c = b_i$ olduğundan $y_i^{rc} = b_i^r a_i^{rc}$ elde edilir.

$$\begin{aligned} x_i = a_i b_i \in D \;&\Rightarrow\; x_i^r = b_i^r a_i^r \in D, \\ b_i^r a_i^r \in D \;&\Rightarrow\; b_i^r a_i^{rc} \in D'. \end{aligned} \tag{2.18}$$

Böylece $y_i^{rc} = b_i^r a_i^{rc} \in D'$ elde edilir. Dolayısıyla D' kümesi bir ters sıralı tamlayan koddur. ■

Örnek 2.88 $D = \left\{ AAAA, TTTT, GCAT, TACG \right\}$ kümesi çift uzunluklu bir ters sıralı DNA koddur.

$$\begin{aligned} x_1 = AA\,AA \;&\Rightarrow y_1 = AATT, \\ x_2 = TT\,TT \;&\Rightarrow y_2 = TT\,AA, \\ x_3 = GC\,AT \;&\Rightarrow y_3 = GC\,TA, \\ x_4 = TACG \;&\Rightarrow y_4 = TAGC. \end{aligned} \tag{2.19}$$

$y_1^{rc} = y_1$, $y_2^{rc} = y_2$, $y_3^{rc} = y_4$ ve $y_4^{rc} = y_3$ olduğundan $D' = \{y_1, y_2, y_3, y_4\}$ kümesi bir ters sıralı tamlayan DNA koddur.

2.6.1 Ters sıralılık problemi

Abualrub vd. tarafından [17] nolu çalışmada $F_4 = \{0, 1, \alpha, \alpha^2\}$ cisminin elemanları ile DNA bazları arasında birebir eşleme verilmiştir. Bu eşlemeye göre; A, C, G ve T bazları sırasıyla $0, \alpha, \alpha^2$ ve 1 elemanları ile eşleştirilmiştir. Benzer şekilde bir halka veya cismin elemanları ile DNA k-bazlarını ilişkilendirerek ters sıralı DNA kodlar bulmak için bazı çalışmalar yapılmıştır [19], [21], [22]. Bu çalışmalarda karşılaşılan ters sıralılık problemini (reversibility problem) kısaca şu şekilde açıklayabiliriz. F_{16} cisminin elemanları ile DNA bazlarını ilişkilendirmek için F_{16} cisminin her bir elemanını bir DNA

2-bazı ile eşleştirmek gerekmektedir, örneğin, $\alpha \in F_{16}$ için $\alpha \to AT$ şeklinde eşleştirilir.

$a_1, a_2, a_3 \in F_{16}$ ve $a_1 \to AC,\ a_2 \to AG,\ a_3 \to TC$ olsun.

(a_1, a_2, a_3) kodsözünün DNA karşılığı $ACAGTC$ elde edilir. Bu durumda (a_1, a_2, a_3) kodsözünün ters sıralısı (a_3, a_2, a_1) olup DNA karşılığı $TCAGAC$ dir. Fakat $TCAGAC$ DNA dizilimi (string), $ACAGTC$ diziliminin ters sıralısı değildir.

BÖLÜM 3

F_q CİSMİ ÜZERİNDE TERS SIRALI DNA KODLAR

Cisimler veya farklı cebirsel yapılar üzerinde DNA kodlar tanımlanırken ortaya çıkan ters sıralılık problemi Bölüm 2.6.1'de açıklanmıştı. Bu bölümde $q = 4^{2s}$ iken F_q cismi üzerinde DNA kodlar için ters sıralılık problemi, aykırı devirli kodlar yardımıyla çözülecektir. Önceki çalışmalarda ([21],[22]) F_q üzerinde ters sıralı DNA kodlar, değişmeli $F_q[x]$ polinom halkası kullanılarak özel üreteç kümeleri tarafından belirlenen lineer kodlardan elde edilmiştir. Bu çalışmada öncekilerin aksine, değişmeli olmayan $F_q[x;\theta]$ aykırı polinom halkası kullanılacak ve $x^n - 1$ polinomunun bu halkadaki bölenlerinin özelliklerinden yararlanılarak aykırı devirli kodlardan direkt olarak ters sıralı DNA kodlar elde edilecektir. Ayrıca bu kodların dualinin de ters sıralı DNA kod olduğu gösterilecektir.

Çizelge 3.1'de F_{16} cisminin elemanları ile DNA baz çiftleri arasında her bir eleman ve 4. kuvveti birbirinin DNA ters sıralısı olacak şekilde bir eşleştirme verilmiştir [21]. Çizelge 3.1'de verilen eşleştirme, [22] nolu çalışmada genelleştirilmiştir. Bunun için $q = 4^{2s}$ iken F_q cisminin elemanları ile DNA 2s-bazlar arasında her bir cisim elemanı ile 4^s inci kuvveti birbirinin DNA ters sıralısı olacak şekilde bir eşleştirme tablosu oluşturmak için gerekli algoritma verilmiştir. Aşağıda verilen ϕ dönüşümü bu kurala göre cisim elemanlarını DNA 2s-bazlarına eşler.

$$\begin{aligned} \phi:\ F_{4^{2s}} &\to \{A,T,G,C\}^{2s} \\ \alpha &\to (b_0, b_1, \ldots, b_{2s-1}) \end{aligned} \qquad (3.1)$$

Bu dönüşüm doğal olarak $F_{4^{2s}}^{n}$ vektör uzayına genişletilebilir; ϕ: $F_{4^{2s}}^{n} \to \{A,T,G,C\}^{2sn}$ ve $\phi((c_0,c_1,\ldots,c_{n-1})) = (b_0,b_1,\ldots,b_{2sn-1})$.

Çizelge 3.1 F_{16} cisminin elemanları ile DNA 2-bazlarının eşleştirme tablosu [21]

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

Örnek 3.1 $F_{256}^{*} = \langle\alpha\rangle$ olsun. $q = 256 = 4^4$ olduğundan F_{256} cisminin her bir elemanı bir DNA 4-bazı ile eşlenir. Ayrıca her bir eleman ile 4^2 inci kuvveti birbirinin DNA ters sıralısıdır [22]. Örneğin,

- $\phi(\alpha^2) = (AAAG)$ ve $\phi(\alpha^{32}) = (GAAA)$,
- $\phi(\alpha^2,\alpha^{20},\alpha^{135},\alpha^{219}) = (AAAG\ ATAC\ CGAC\ TAGA)$,

- $\phi(\alpha^3,\alpha^4,\alpha)=(AAAC\ AATA\ AAAT)$ ve $\phi(\alpha^{16},\alpha^{64},\alpha^{48})=(TAAA\ ATAA\ CAAA)$.

$C\subseteq F_{4^{2s}}^n$ ve $c=(c_0,c_1,\ldots,c_{n-1})\in C$ olsun. $\phi(c)$ DNA kodsözünün ters sıralısı aşağıda verilmiştir.

$$\phi(c)^r=\phi((c_{n-1}^{4^s},c_{n-2}^{4^s},\ldots,c_0^{4^s})). \tag{3.2}$$

C, $F_{4^{2s}}$ üzerinde n uzunluğunda bir kod olsun. Bu durumda, $\phi(C)$ DNA kodunun uzunluğu $2sn$'dir. Eğer $\phi(C)$ ters sıralı DNA kod ise Teorem 2.87'de görüldüğü üzere $\phi(C)$ kodundan bir ters sıralı tamlayan DNA kod kolayca elde edilir.

Tanım 3.2 $f(x)=a_0+a_1x+\ldots+a_tx^t\in F_q[x;\theta]$ ve θ; F_q üzerinde mertebesi 2 olan bir otomorfizma olsun. Eğer $f(x)$ polinomunun katsayıları için $a_i=a_{t-i}$ $(i\in\{0,1,\ldots,t\})$ eşitliği sağlanıyorsa palindromik polinom, $a_i=\theta(a_{t-i})$ $(i\in\{0,1,\ldots,t\})$ eşitliği sağlanıyorsa θ-palindromik polinom denir.

Örnek 3.3 $F_{16}^*=\langle\alpha\rangle$ ve $\theta(\alpha)=\alpha^4$ $(\theta\in Aut(F_{16}))$olmak üzere;

- $f_1(x)=\alpha+\alpha^2x+x^2+x^4+\alpha^2x^5+\alpha x^6\in F_{16}[x;\theta]$ bir palindromik polinom,
- $f_2(x)=\alpha+\alpha^2x+x^2+x^4+\alpha^8x^5+\alpha^4x^6\in F_{16}[x;\theta]$ bir θ-palindromik polinomdur.

Teorem 2.77'de görüldüğü üzere θ otomorfizmasının mertebesi m, ile n aralarında asal ise F_q üzerinde n uzunluğundaki aykırı devirli kodlar aynı zamanda devirli koddur. Ayrıca, Teorem 2.80'de $(m,n)=1$ ise $F_q[x;\theta]$ halkasında x^n-1 polinomunun çarpanlara ayrılışının tek türlü olduğu görülür.

Bu çalışmada, $q=4^{2s}$ ve $\theta(a)=a^{4^s}$ olarak tanımlı $F_q[x;\theta]$ aykırı polinom halkalarını kullanacağız. Bu durumda, θ otomorfizmasının mertebesi 2 olduğundan n tek iken x^n-1 polinomunun çarpanlara ayrılışı tek türlüdür. Bu yüzden tek ve çift uzunluklu kodların durumunu ayrı olarak inceleyeceğiz. Bu başlık altında aksi belirtilmedikçe $q=4^{2s}$ ve $\theta(a)=a^{4^s}$ olarak kullanacağız.

3.1 Çift Uzunluklu Ters Sıralı DNA Kodlar

Bu başlık altında n çift iken x^n-1'in $F_q[x;\theta]$ halkasındaki sağ bölenleri ile ilgileneceğiz. C, uzunluğu n olan F_q üzerinde θ otomorfizmasına göre bir aykırı devirli kod ve $g(x)$ polinomu bu kodun içerisindeki en küçük dereceye sahip monik polinom olsun. Bu durumda C kodu $g(x)$ tarafından üretilir ve $g(x)$ polinomu $F_q[x;\theta]$ halkasında x^n-1'in bir sağ bölenidir [26]. $\beta \in F_q^*$ olmak üzere $F_q[x;\theta]$ halkasında $\langle g(x)\rangle$ ve $\langle \beta g(x)\rangle$ sol ideallerinin eşit olduğu kolaylıkla görülür. Ayrıca $x^n-1=h(x)g(x)\in F_q[x;\theta]$ ise $x^n-1=h(x)\beta^{-1}\beta g(x)\in F_q[x;\theta]$ dir, yani $g(x)$ polinomu x^n-1'in bir sağ böleni ise $\beta g(x)$ polinomu da x^n-1'in bir sağ bölenidir. Dolayısıyla C'nin üreteç polinomu monik polinom olmak zorunda değildir. Aşağıdaki teoremler için C kodunun üreteç polinomunu, monikliği gözetmeden, kodun içerisindeki en küçük dereceli bir polinom $g(x)=g_0+g_1x+\ldots+g_wx^w$ olarak alacağız.

Teorem 3.4 $F_q[x;\theta]$ halkasında $x^n-1=h(x)g(x)$ ve $g(x)$ polinomunun derecesi çift olsun. Bu durumda $C=\langle g(x)\rangle$ aykırı devirli kodunun DNA karşılığı $\phi(C)$'nin ters sıralı DNA kod olması için gerek ve yeter koşul $g(x)$ polinomunun palindromik polinom olmasıdır.

İspat $g(x)$ derecesi çift olan bir palindromik polinom ve $k=n-der(g(x))$ olsun. Bu durumda k bir çift tamsayıdır. Her $c\in C$ için $\phi(c)^r\in\phi(C)$ olduğunu göstermemiz gerekiyor. Öncelikle $\phi(g)^r\in\phi(C)$ olduğunu göstermekle başlayalım.

$g(x)$ polinomunun kodsöz karşılığı $g=(g_0,g_1,\ldots,g_{n-k},\overbrace{0,0,\ldots,0}^{k-1})$ olsun. Eşitlik (3.2)'den $\phi(g)$ DNA kodsözünün ters sıralısı

$$\phi(g)^r=\phi((\overbrace{0,0,\ldots,0}^{k-1},g_{n-k}^{4^s},g_{n-k-1}^{4^s},\ldots,g_0^{4^s}))=\phi((\overbrace{0,0,\ldots,0}^{k-1},\theta(g_{n-k}),\theta(g_{n-k-1}),\ldots,\theta(g_0))).$$

$g(x)$ palindromik olduğundan $\phi(g)^r=\phi((\overbrace{0,0,\ldots,0}^{k-1},\theta(g_0),\theta(g_1),\ldots,\theta(g_{n-k})))$ yazılabilir. $c'=(\overbrace{0,0,\ldots,0}^{k-1},\theta(g_0),\theta(g_1),\ldots,\theta(g_{n-k}))$ tam olarak $x^{k-1}g(x)$ polinomunun

vektör karşılığıdır. $x^{k-1}g(x) \in C$ olduğundan $c' \in C$ elde edilir. Ayrıca $g(x)$ polinomunun bir $\beta \in F_q^*$ skaler katı $\beta g(x) \in C$ dir. $\beta g(x)$ polinomuna karşılık gelen kodsöz ve DNA ters sıralısı aşağıdaki gibidir.

$$\begin{aligned} v &= (\beta g_0, \beta g_1, \ldots, \beta g_{n-k}, \overbrace{0,0,\ldots,0}^{k-1}) \Rightarrow \\ \phi(v)^r &= (\overbrace{0,0,\ldots,0}^{k-1}, \beta^{4^s} g_{n-k}^{4^s}, \beta^{4^s} g_{n-k-1}^{4^s}, \ldots, \beta^{4^s} g_0^{4^s})) \\ &= \phi((\overbrace{0,0,\ldots,0}^{k-1}, \theta(\beta g_{n-k}), \theta(\beta g_{n-k-1}), \ldots, \theta(\beta g_0))) \\ &= \phi((\overbrace{0,0,\ldots,0}^{k-1}, \theta(\beta g_0), \theta(\beta g_1), \ldots, \theta(\beta g_{n-k}))). \end{aligned} \tag{3.3}$$

$k-1$ tek bir tamsayı ve θ'nın mertebesi 2 olduğundan $\theta^{k-1}(\beta) = \theta(\beta)$ sağlanır. Dolayısıyla, $v' = (\overbrace{0,0,\ldots,0}^{k-1}, \theta(\beta g_0), \theta(\beta g_1), \ldots, \theta(\beta g_{n-k}))$ vektörü tam olarak $x^{k-1}\beta g(x)$ polinomuna karşılık gelir ve $x^{k-1}\beta g(x) \in C$ olduğundan $v' \in C$ elde edilir. Böylece her $\beta g(x) \in C$ için $\phi(\beta g(x))^r = \phi(\theta(\beta) x^{k-1} g(x))$ olduğu görülür. Teorem 2.71'de görüldüğü üzere C'nin elemanları $\beta_i \in F_q$ olmak üzere $\sum_{i=0}^{k-1} \beta_i x^i g(x)$ şeklindedir. Yukarıdaki argümanlar kullanılarak

$$\phi\left(\sum_{i=0}^{k-1} \beta_i x^i g(x)\right)^r = \phi\left(\sum_{i=0}^{k-1} \theta(\beta_i) x^{k-1-i} g(x)\right) \tag{3.4}$$

olduğu görülür. $\sum_i \theta(\beta_i) x^{k-1-i} g(x) \in C$ olduğundan $\phi(C)$ bir ters sıralı DNA koddur.

Tersine, $C = \langle g(x) \rangle$ aykırı devirli kodunun DNA karşılığı $\phi(C)$, bir ters sıralı DNA kod ve

$$a(x) = g_w^{-1} g(x) = a_0 + a_1 x + \ldots + a_{w-1} x^{w-1} + x^w, \qquad a_i = g_w^{-1} g_i \tag{3.5}$$

olsun. Bu durumda, $a(x)$ polinomu C kodunun içerisindeki sıfırdan farklı en küçük dereceli monik polinomdur. w ve n çift sayı olduğundan $n-w-1$ bir tek sayıdır ve $x^{n-w-1} a_i = \theta(a_i) x^{n-w-1} = a_i^{4^s} x^{n-w-1}$ dir.

Bu durumda; $c_1(x) = x^{n-w-1}a(x) = a_0^{4^s}x^{n-w-1} + a_1^{4^s}x^{n-w} + \ldots + a_{w-1}^{4^s}x^{n-2} + x^{n-1} \in C$'dir. $c_2(x) = 1 + a_{w-1}x + \ldots + a_1x^{w-1} + a_0x^w$ olmak üzere, $\phi(c_1)^r = \phi(c_2)$ ve $\phi(c_1)^r \in \phi(C)$ olduğundan $c_2(x)$ de C'nin bir elemanıdır. Dolayısıyla,

$$c_3(x) = a(x) - a_0^{-1}c_2(x) = (a_0 - a_0^{-1}) + (a_1 - a_0^{-1}a_{w-1})x + \ldots + (a_{w-1} - a_0^{-1}a_1)x^{w-1} \in C \qquad (3.6)$$

ve $der(c_3(x)) < der(g(x)) = w$ elde edilir, ki bu da $c_3(x) \neq 0$ olması durumunda $g(x)$'in derecesinin minimal olması ile çelişir. Böylece $c_3(x) = 0$ olmalıdır. Dolayısıyla $a_0 - a_0^{-1} = 0$ ve $a_0 = 1$ elde edilir. Aynı zamanda $a_1 - a_0^{-1}a_{w-1} = 0$ olacağından $a_1 - a_{w-1} = 0$ ve $a_1 = a_{w-1}$'dir.

Bu şekilde devam edildiğinde, her $i \in \{0,1,\ldots,w\}$ için $a_i = a_{w-i}$ elde edilir. Bu ise $a(x)$'in palindromik polinom olduğunu kanıtlar. Ayrıca,

$$g(x) = g_w a(x) \qquad (3.7)$$

olduğundan $g(x)$ polinomu da palindromiktir. ■

Örnek 3.5 α; F_{16} cisminin bir ilkel elemanı ve $\alpha^4 = \alpha + 1$ olmak üzere, $F_{16}[x;\theta]$ halkasında $x^{10} - 1$'in bir ayrışımı

$$\begin{aligned} x^{10} - 1 &= h(x)g(x) \\ &= (1 + \alpha x + \alpha^3 x^2 + \alpha x^3 + x^4)(1 + \alpha x + \alpha^{11}x^2 + \alpha^{11}x^4 + \alpha x^5 + x^6). \end{aligned} \qquad (3.8)$$

$C = \langle g(x) \rangle$ aykırı devirli kodunun üreteç matrisi

$$G = \begin{bmatrix} 1 & \alpha & \alpha^{11} & 0 & \alpha^{11} & \alpha & 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha^4 & \alpha^{14} & 0 & \alpha^{14} & \alpha^4 & 1 & 0 & 0 \\ 0 & 0 & 1 & \alpha & \alpha^{11} & 0 & \alpha^{11} & \alpha & 1 & 0 \\ 0 & 0 & 0 & 1 & \alpha^4 & \alpha^{14} & 0 & \alpha^{14} & \alpha^4 & 1 \end{bmatrix} \qquad (3.9)$$

ve parametreleri $[10,4,6]_{16}$ dır. G matrisinin i inci satırı s_i olmak üzere, her bir satırın DNA karşılıkları aşağıda verilmiştir.

$$\begin{aligned}
&\phi(s_1) = (TT\ AT\ CT\ AA\ CT\ AT\ TT\ AA\ AA\ AA)\\
&\phi(s_4) = (AA\ AA\ AA\ TT\ TA\ TC\ AA\ TC\ TA\ TT)\\
&\phi(s_2) = (AA\ TT\ TA\ TC\ AA\ TC\ TA\ TT\ AA\ AA)\\
&\phi(s_3) = (AA\ AA\ TT\ AT\ CT\ AA\ CT\ AT\ TT\ AA).
\end{aligned} \tag{3.10}$$

Görüldüğü üzere $\phi(s_1)^r = \phi(s_4)$ ve $\phi(s_2)^r = \phi(s_3)$'tür. Aynı zamanda $g(x)$ polinomunun derecesi çift ve palindromik olduğundan $\phi(C)$ bir ters sıralı DNA koddur. $\phi(C)$ DNA kodunun parametreleri ise $(20, 4^8, 8)_4$ olarak elde edilir.

Teorem 3.6 $F_q[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ ve $g(x)$ polinomunun derecesi tek olsun. $C = \langle g(x) \rangle$ bir aykırı devirli koddur. Bu durumda, $g(x)$ polinomu θ-palindromik ise $\phi(C)$ bir ters sıralı DNA koddur. Diğer yandan, $\phi(C)$ ters sıralı DNA kod ise C kodu bir θ-palindromik polinom tarafından üretilir.

İspat $g(x)$ bir θ-palindromik polinom ve $k = n - der(g(x))$ olsun. Bu durumda k bir tek tamsayıdır. $g(x)$ polinomunun kodsöz karşılığı ve $\phi(g)^r$ aşağıdaki gibidir.

$$\begin{aligned}
&g = (g_0, g_1, \ldots, g_{n-k}, \overbrace{0,0,\ldots,0}^{k-1}) \in C,\\
&\phi(g)^r = \phi((\overbrace{0,0,\ldots,0}^{k-1}, g_{n-k}^{4^s}, g_{n-k-1}^{4^s}, \ldots, g_0^{4^s}))\\
&\quad = \phi((\overbrace{0,0,\ldots,0}^{k-1}, \theta(g_{n-k}), \theta(g_{n-k-1}), \ldots, \theta(g_0))).
\end{aligned} \tag{3.11}$$

$g(x)$ polinomu θ-palindromik olduğundan $\phi(g)^r = ((\overbrace{0,0,\ldots,0}^{k-1}, g_0, g_1, \ldots, g_{n-k}))$ dir. Burada, $c' = (\overbrace{0,0,\ldots,0}^{k-1}, g_0, g_1, \ldots, g_{n-k})$ tam olarak $x^{k-1}g(x)$ polinomunun vektör karşılığıdır. Dolayısıyla, $c' \in C$ ve $\phi(g)^r \in \phi(C)$ elde edilir. Herhangi $\beta \in F_q^*$ için $\beta g(x) \in C$'dir. $\beta g(x)$ polinomuna karşılık gelen kodsöz v olsun.

$$\begin{aligned}
&v = (\beta g_0, \beta g_1, \ldots, \beta g_{n-k}, \overbrace{0,0,\ldots,0}^{k-1}) \Rightarrow\\
&\quad \phi(v)^r = (\overbrace{0,0,\ldots,0}^{k-1}, \beta^{4^s} g_{n-k}^{4^s}, \beta^{4^s} g_{n-k-1}^{4^s}, \ldots, \beta^{4^s} g_0^{4^s}))\\
&\quad\quad = \phi((\overbrace{0,0,\ldots,0}^{k-1}, \theta(\beta g_{n-k}), \theta(\beta g_{n-k-1}), \ldots, \theta(\beta g_0)))\\
&\quad\quad = \phi((\overbrace{0,0,\ldots,0}^{k-1}, \theta(\beta) g_0, \theta(\beta) g_1, \ldots, \theta(\beta) g_{n-k})).
\end{aligned} \tag{3.12}$$

Dolayısıyla, $v' = (\overbrace{0,0,\ldots,0}^{k-1}, \theta(\beta)g_0, \theta(\beta)g_1, \ldots, \theta(\beta)g_{n-k})$ vektörü tam olarak $\theta(\beta)x^{k-1}g(x)$ polinomuna karşılık gelir ve $\theta(\beta)x^{k-1}g(x) \in C$ olduğundan $v' \in C$ elde edilir. Böylece her $\beta g(x) \in C$ için $\phi(\beta g(x))^r = \phi(\theta(\beta)x^{k-1}g(x))$ olduğu görülür. Teorem 2.71'de görüldüğü üzere C'nin elemanları $\beta_i \in F_q$ olmak üzere $\sum_{i=0}^{k-1} \beta_i x^i g(x)$ şeklindedir. Böylece, her $c \in C$ için $\phi(c) \in \phi(C)$ DNA kodsözünün ters sıralısı aşağıdaki eşitlikten bulunur. $\beta_i \in F_q$ olmak üzere,

$$\phi\left(\sum_{i=0}^{k-1} \beta_i x^i g(x)\right)^r = \phi\left(\sum_{i=0}^{k-1} \theta(\beta_i) x^{k-1-i} g(x)\right) \tag{3.13}$$

$\sum_i \theta(\beta_i)x^{k-1-i}g(x) \in C$ olduğundan $\phi(C)$ bir ters sıralı DNA koddur.

Tersine, $\phi(C)$ bir ters sıralı DNA kod ve

$$a(x) = g_w^{-1}g(x) = a_0 + a_1 x + \ldots + a_{w-1}x^{w-1} + x^w, \quad a_i = g_w^{-1}g_i \tag{3.14}$$

olsun. Bu durumda, $a(x)$ polinomu C kodunun içerisindeki sıfırdan farklı en küçük dereceli monik polinomdur. w tek ve n çift sayı olduğundan $n-w-1$ bir çift sayıdır ve $x^{n-w-1}a_i = \theta^{n-w-1}(a_i)x^{n-w-1} = a_i x^{n-w-1}$ olur. Bu durumda;

$$c_1(x) = x^{n-w-1}a(x) = a_0 x^{n-w-1} + a_1 x^{n-w} + \ldots + a_{w-1}x^{n-2} + x^{n-1} \in C. \tag{3.15}$$

$c_2(x) = 1 + a_{w-1}^{4^s}x + \ldots + a_1^{4^s}x^{w-1} + a_0^{4^s}x^w$ olsun. $\phi(c_1)^r = \phi(c_2)$ olduğundan, $c_2(x)$ de C'nin bir elemanıdır. Dolayısıyla,

$$c_3(x) = a(x) - a_0^{-4^s}c_2(x) = (a_0 - a_0^{-4^s}) + (a_1 - a_0^{-4^s}a_{w-1}^{4^s})x + \ldots + (a_{w-1} - a_0^{-4^s}a_1^{4^s})x^{w-1} \in C$$

ve $der(c_3(x)) < der(g(x)) = w$ elde edilir, ki bu da $c_3(x) \neq 0$ olması durumunda $g(x)$'in derecesinin minimal olması ile çelişir. Böylece, α elemanı F_q cisminin bir ilkel elemanı ve j bir pozitif tam sayı olmak üzere,

$$c_3(x) = 0 \Rightarrow a_0 - a_0^{-4^s} = 0 \Rightarrow a_0^{4^s+1} = 1 \Rightarrow a_0 = \alpha^{(4^s-1)j}. \tag{3.16}$$

Ayrıca, $a_{w-1} - a_0^{-4^s}a_1^{4^s} = 0 \Rightarrow a_{w-1} = \alpha^{(4^s-1)j}a_1^{4^s}$ elde edilir.

Bu şekilde devam edildiğinde, $a_0 = \alpha^{(4^s-1)j}$ olmak üzere,

$$a(x) = \sum_{i=0}^{(w-1)/2} (a_i x^i + \alpha^{(4^s-1)j} a_i^{4^s} x^{w-i}) \tag{3.17}$$

olduğu görülür. $a(x)$ polinomunu α^j ile çarpalım.

$$\alpha^j a(x) = \sum_{i=0}^{(w-1)/2} (\alpha^j a_i x^i + \alpha^{(4^s)j} a_i^{4^s} x^{w-i}) \in C. \tag{3.18}$$

Böylece, $\alpha^j a(x) = \alpha^j g_w^{-1} g(x)$ bir θ-palindromik polinomdur. $\alpha^j a(x)$ tarafından üretilen sol ideal $C = \langle g(x) \rangle$'e eşit olduğundan C kodu bir θ-palindromik polinom tarafından üretilir. ■

Örnek 3.7 F_{16} cisminin bir ilkel elemanı α ve $\alpha^4 = \alpha + 1$ olmak üzere, $F_{16}[x;\theta]$ halkasında $x^6 - 1 = (1 + \alpha^7 x + \alpha^7 x^2 + x^3)(1 + \alpha^7 x + \alpha^{13} x^2 + x^3)$ tür.

$g(x) = 1 + \alpha^7 x + \alpha^{13} x^2 + x^3$ polinomu tarafından üretilen $C = \langle g(x) \rangle$ aykırı devirli kodunun üreteç matrisi

$$G = \begin{bmatrix} 1 & \alpha^7 & \alpha^{13} & 1 & 0 & 0 \\ 0 & 1 & \alpha^{13} & \alpha^7 & 1 & 0 \\ 0 & 0 & 1 & \alpha^7 & \alpha^{13} & 1 \end{bmatrix} \tag{3.19}$$

ve parametreleri $[6,3,4]_{16}$'dır. G matrisinin i inci satırı s_i olmak üzere, her bir satırın DNA karşılıkları aşağıda verilmiştir.

$$\begin{aligned} \phi(s_1) &= (TT\ GT\,TG\,TT\ AA\,AA) \\ \phi(s_3) &= (AA\,AA\ TT\,GT\,TG\,TT) \\ \phi(s_2) &= (AATT\,TG\,GT\,TT\ AA). \end{aligned} \tag{3.20}$$

Dolayısıyla $\phi(s_1)^r = \phi(s_3)$ ve $\phi(s_2)^r = \phi(s_2)$ olduğu görülür. $g(x)$ polinomunun derecesi tek ve θ-palindromik olduğundan $\phi(C)$ bir ters sıralı DNA koddur. $\phi(C)$ DNA kodunun parametreleri ise $(12, 4^6, 5)_4$'tür.

Teorem 3.8 $F_q[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ ve $g(x)$ polinomunun derecesi çift olsun. Eğer $h(x)$ palindromik polinom ise $g(x)$ polinomu da palindromiktir.

İspat $h(x)=h_0+h_1x+\ldots+h_{2k}x^{2k}$, $g(x)=g_0+g_1x+\ldots+g_{2r}x^{2r}$ ve $n=2k+2r$ olsun. $h(x)$ polinomunun palindromik olduğunu, yani her $i\in\{0,1,\ldots,k\}$ için $h_i=h_{2k-i}$ olduğunu kabul edelim. $h(x)g(x)$ polinomunda x^i nin katsayısını a_i olarak adlandıralım. Herhangi $t<n/2$ için $h(x)g(x)$ çarpımında

$$\begin{aligned} &i<0 \text{ veya } i>2k \Rightarrow h_i=0,\\ &j<0 \text{ veya } j>2r \Rightarrow g_j=0, \end{aligned} \tag{3.21}$$

olmak üzere x^t'nin katsayısı

$$a_t=\sum_{j=0}^{t}h_j\theta^j(g_{t-j}) \tag{3.22}$$

ve x^{n-t}'nin katsayısı $a_{n-t}=\sum_{j=0}^{t}h_{2k-j}\theta^{2k-j}(g_{2r-(t-j)})$ dir.

$x^n-1=h(x)g(x)$ olduğundan $a_0=a_n=1$ ve her $i\in\{1,\ldots,n-1\}$ için $a_i=0$'dır. Tümevarım yöntemini kullanarak her $i\in\{0,1,\ldots,r-1\}$ için $g_i=g_{2r-i}$ olduğunu yani $g(x)$ polinomunun palindromik olduğunu göstereceğiz.

$i=0$ için; $a_0=h_0\theta^0(g_0)=h_0g_0$ ve $a_n=h_{2k}\theta^{2k}(g_{2r})=h_{2k}g_{2r}$ dir. Ayrıca $a_0=a_n=1$ ve $h_0=h_{2k}$ olduğundan $g_0=g_{2r}$ elde edilir.

$l<r$ olmak üzere her $0\le i<l$ için $g_i=g_{2r-i}$ eşitliğinin sağlandığını kabul edelim. Şimdi a_l ve a_{n-l} katsayılarını inceleyelim.

$$\begin{aligned} a_l&=\sum_{j=0}^{l}h_j\theta^j(g_{l-j})=\sum_{j=1}^{l}h_j\theta^j(g_{l-j})+h_0g_l,\\ a_{n-l}&=\sum_{j=0}^{l}h_{2k-j}\theta^{2k-j}(g_{2r-(l-j)})=\sum_{j=1}^{l}h_{2k-j}\theta^{2k-j}(g_{2r-(l-j)})+h_{2k}g_{2r-l}. \end{aligned} \tag{3.23}$$

θ otomorfizmasının mertebesi 2 olduğundan her $a\in F_q$ ve $j\in\{1,\ldots,l\}$ için $\theta^j(a)=\theta^{2k-j}(a)$'dır. Ayrıca, $h_j=h_{2k-j}$ ve $g_{l-j}=g_{2r-(l-j)}$ olduğundan $h_j\theta^j(g_{l-j})=h_{2k-j}\theta^{2k-j}(g_{2r-(l-j)})$ elde edilir.

Dolayısıyla, $\sum_{j=1}^{l} h_j \theta^j(g_{l-j}) = \sum_{j=1}^{l} h_{2k-j}\theta^{2k-j}(g_{2r-(l-j)})$ dir. Ayrıca, $a_l = a_{n-l} = 0$ bilgisini kullanarak, $h_0 g_l = h_{2k} g_{2r-l} = h_0 g_{2r-l}$ elde edilir. Böylece $g_l = g_{2r-l}$'dir. ■

Önerme 2.43 ve Teorem 3.8'in bir sonucu aşağıda verilmiştir.

Sonuç 3.9 $F_q[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ ve $der(g(x))$ çift olsun. Eğer $g(x)$ bir palindromik polinom ise $h(x)$ polinomu da palindromiktir.

Teorem 3.10 $F_q[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ ve $g(x)$ polinomunun derecesi tek olsun. Eğer $g(x)$ bir θ-palindromik polinom ise $h(x)$ polinomu palindromiktir.

İspat $h(x) = h_0 + h_1 x + \ldots + h_{2k-1}x^{2k-1}$, $g(x) = g_0 + g_1 x + \ldots + g_{2r-1}x^{2r-1}$ ve $n = 2k + 2r - 2$ olsun. $g(x)$ polinomunun $\theta-$palindromik olduğunu, yani her $i \in \{0,1,\ldots,r-1\}$ için $g_i = \theta(g_{2r-1-i})$ olduğunu kabul edelim. $h(x)g(x)$ polinomunda x^i'nin katsayısını a_i olarak adlandıralım. Herhangi $t < n/2$ için $h(x)g(x)$ çarpımında

$$\begin{aligned} &i < 0 \text{ veya } i > 2k-1 \Rightarrow h_i = 0, \\ &j < 0 \text{ veya } j > 2r-1 \Rightarrow g_j = 0, \end{aligned} \tag{3.24}$$

x^t'nin katsayısı $a_t = \sum_{j=0}^{t} h_j \theta^j(g_{t-j})$ ve x^{n-t}'nin katsayısı ise

$$a_{n-t} = \sum_{j=0}^{t} h_{2k-1-j}\theta^{2k-1-j}(g_{2r-1-(t-j)}). \tag{3.25}$$

$h(x)g(x) = x^n - 1$ olduğundan $a_0 = a_n = 1$ ve her $i \in \{1,\ldots,n-1\}$ için $a_i = 0$'dır. Tümevarım yöntemini kullanarak her $i \in \{0,1,\ldots,k-1\}$ için $h_i = h_{2k-1-i}$ olduğunu yani $h(x)$ polinomunun palindromik olduğunu göstereceğiz.

$i = 0$ için; $a_0 = h_0\theta^0(g_0) = h_0 g_0$ ve $a_n = h_{2k-1}\theta^{2k-1}(g_{2r-1}) = h_{2k-1}\theta(g_{2r-1})$ dir. Ayrıca $a_0 = a_n = 1$ ve $g_0 = \theta(g_{2r-1})$ olduğundan $h_0 = h_{2k-1}$ elde edilir.

$l \le k-1$ olmak üzere her $0 \le i < l$ için $h_i = h_{2k-1-i}$ eşitliğinin sağlandığını kabul edelim. Şimdi a_l ve a_{n-l} katsayılarını inceleyelim.

$$a_l = \sum_{j=0}^{l} h_j \theta^j(g_{l-j}) = \sum_{j=0}^{l-1} h_j \theta^j(g_{l-j}) + h_l \theta^l(g_0),$$

$$a_{n-l} = \sum_{j=0}^{l} h_{2k-1-j} \theta^{2k-1-j}(g_{2r-1-(l-j)}) \tag{3.26}$$

$$= \sum_{j=0}^{l-1} h_{2k-1-j} \theta^{2k-1-j}(g_{2r-1-(l-j)}) + h_{2k-1-l} \theta^{2k-1-l}(g_{2r-1}).$$

θ otomorfizmasının mertebesi 2 olduğundan her $a \in F_q$ ve $j \in \{1,\ldots,l-1\}$ için $\theta^j(a) = \theta^{2k-1-j}(\theta(a))$ dır. Ayrıca $h_j = h_{2k-1-j}$ ve $g_{l-j} = \theta(g_{2r-(l-j)})$ olduğundan

$$\theta^j(g_{l-j}) = \theta^{2k-1-j}(\theta(g_{l-j})) = \theta^{2k-1-j}(g_{2r-1-(l-j)}) \tag{3.27}$$

ve böylece $h_j \theta^j(g_{l-j}) = h_{2k-1-j} \theta^{2k-1-j}(g_{2r-1-(l-j)})$ elde edilir.

Dolayısıyla, $\sum_{j=0}^{l-1} h_j \theta^j(g_{l-j}) = \sum_{j=0}^{l-1} h_{2k-1-j} \theta^{2k-1-j}(g_{2r-1-(l-j)})$ dir. Ayrıca, $a_l = a_{n-l} = 0$ bilgisini kullanarak, $h_l g_0 = h_{2k-1-l} \theta(g_{2r-1})$ elde edilir. Böylece $h_l = h_{2k-1-l}$ dir, dolayısıyla $h(x)$ palindromiktir. ■

Teorem 3.11 $h(x) \in F_q[x;\theta]$ derecesi t olan bir palindromik polinom olsun.

1. Eğer t tek tamsayı ise $h^R(x)$ polinomu θ-palindromiktir.
2. Eğer t çift tamsayı ise $h^R(x)$ polinomu palindromiktir.

İspat $h(x) = h_0 + h_1 x + \ldots + h_t x^t \in F_q[x;\theta]$ polinomu bir palindromik polinom olsun. Bu durumda her $i \in \{0,1,\ldots,t\}$ için $h_i = h_{t-i}$ ve $h^R(x) = \sum_{i=0}^{t} a_i x^i = \sum_{i=0}^{t} \theta^i(h_{t-i}) x^i$ dir.

1. t bir tek sayı olsun. Eğer i tek sayı ise $t-i$ çifttir. Bu durumda $a_i = \theta^i(h_{t-i}) = \theta(h_{t-i}) = \theta(h_i)$ ve $a_{t-i} = \theta^{t-i}(h_i) = h_i$. Böylece $a_i = \theta(a_{t-i})$ olduğu görülür. Benzer şekilde i çift iken de $a_i = \theta(a_{t-i})$ olduğu görülür. Dolayısıyla $h^R(x)$ bir θ-palindromik polinomdur.
2. t bir çift sayı olsun. Eğer i tek sayı ise $t-i$ tektir. Bu durumda $a_i = \theta^i(h_{t-i}) = \theta(h_{t-i}) = \theta(h_i)$ ve $a_{t-i} = \theta^{t-i}(h_i) = \theta(h_i)$. Böylece $a_i = a_{t-i}$ olduğu

görülür. Benzer şekilde i çift iken de $a_i = a_{t-i}$ olduğu görülür. Dolayısıyla $h^R(x)$ bir palindromik polinomdur.■

Teorem 3.12 C, $x^n - 1$'in $F_q[x;\theta]$ halkasındaki bir sağ böleni tarafından üretilen aykırı devirli kod olsun. Eğer $\phi(C)$ ters sıralı DNA kod ise, $\phi(C^\perp)$ de ters sıralı DNA koddur.

İspat C bir aykırı devirli kod ve $g(x)$ polinomu C'nin içinde en küçük dereceli sıfırdan farklı bir polinom olsun. Bu durumda $C = \langle g(x) \rangle$ ve $g(x)$ polinomu $F_q[x;\theta]$ halkasında $x^n - 1$'in bir sağ bölenidir [26]. $\phi(C)$'nin bir ters sıralı DNA kod olduğunu kabul edelim.

1. Eğer $g(x)$ polinomunun derecesi çift ise Teorem 3.4'te görüldüğü üzere $g(x)$ polinomu palindromiktir. $x^n - 1 = h(x)g(x) \in F_q[x;\theta]$ ise $h^R(x)$ polinomunun derecesi çifttir ve Sonuç 3.9 ile Teorem 3.11'in bir sonucu olarak $h^R(x)$ palindromik polinomdur. Böylece, Teorem 3.4'ten, $\phi(C^\perp)$ bir ters sıralı DNA koddur.
2. Eğer $g(x)$ polinomunun derecesi tek ise Teorem 3.6'da görüldüğü üzere C bir $g'(x)$, θ-palindromik polinomu tarafından üretilir ve bu polinom $g(x)$'in bir skaler katıdır. Dolayısıyla $g'(x)$ polinomu $F_q[x;\theta]$ halkasında $x^n - 1$'in bir sağ bölenidir. Eğer $x^n - 1 = h'(x)g'(x) \in F_q[x;\theta]$ ise $h'^R(x)$ polinomunun derecesi tek ve Teorem 3.10 ile Teorem 3.11'in bir sonucu olarak $h'^R(x)$ bir θ-palindromik polinomdur. Böylece, Teorem 3.6'dan, $\phi(C^\perp)$ bir ters sıralı DNA koddur. ■

Örnek 3.13 $F_{16}[x;\theta]$ halkasında $x^6 - 1$ polinomunun bazı çarpanları aşağıda verilmiştir.

$$\begin{aligned} x^6 - 1 &= h_1(x)g_1(x) = (1 + \alpha^3 x + \alpha^3 x^3 + x^4)(1 + \alpha^3 x + x^2) \\ &= h_2(x)g_2(x) = (1 + \alpha^{14} x + \alpha^{14} x^2 + x^3)(1 + \alpha^{14} x + \alpha^{11} x^2 + x^3). \end{aligned} \tag{3.28}$$

- $g_1(x)$ polinomu palindromik iken $h_1(x)$ de palindromiktir.

  $h_1^R(x) = x^4(1 + x^{-1}\alpha^3 + x^{-3}\alpha^3 + x^{-4}) = x^4 + \alpha^{12}x^3 + \alpha^{12}x + 1$ palindromik polinom ve derecesi çift olduğundan $C^\perp = \langle h_1^R(x) \rangle$ aykırı devirli kodunun DNA karşılığı

$\phi(C^{\perp})$, bir ters sıralı DNA koddur. $C^{\perp}$ kodunun parametreleri $[6,2,4]_{16}$ ve $\phi(C^{\perp})$ DNA kodunun parametreleri $(12,4^4,4)_4$ tür.

- $g_2(x)$ polinomu θ-palindromik iken $h_2(x)$ palindromiktir.

  $h_2^R(x) = x^3(1+x^{-1}\alpha^{14} + x^{-2}\alpha^{14} + x^{-3}) = x^3 + \alpha^{14}x^2 + \alpha^{11}x + 1$ θ-palindromik ve derecesi tek olduğundan $C^{\perp} = \langle h_2^R(x) \rangle$ aykırı devirli kodunun DNA karşılığı $\phi(C^{\perp})$, bir ters sıralı DNA koddur. $C^{\perp}$ kodunun parametreleri $[6,3,4]_{16}$ ve $\phi(C^{\perp})$ DNA kodunun parametreleri $(12,4^6,4)_4$ tür.

3.2 Tek Uzunluklu Ters Sıralı DNA Kodlar

Bu çalışmada $\theta(a) = a^{4^s}$ olduğundan $F_{4^{2s}}$ cisminin θ tarafından sabit bırakılan alt cismi F_{4^s}'dir. θ'nın mertebesi $m = 2$ olduğu için aşağıdaki önerme Teorem 2.80'in özel halidir.

Önerme 3.14 n bir tek sayı ve $g(x)$ polinomu $F_{4^{2s}}[x;\theta]$ halkasında $x^n - 1$'in bir monik sağ böleni olsun. Bu durumda $g(x) \in F_{4^s}[x]$ ve $x^n - 1$'in $F_{4^{2s}}[x;\theta]$ halkasındaki çarpanlara ayrılışı $F_{4^s}[x]$ değişmeli halkasındaki çarpanlara ayrılışından ibarettir.

Teorem 3.15 $F_{4^{2s}}[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ ve n tek olsun. Bu durumda $C = \langle g(x) \rangle$ aykırı devirli koddur. $\phi(C)$'nin ters sıralı DNA kod olması için gerek ve yeter koşul $g(x)$ polinomunun palindromik olmasıdır. Aynı zamanda eğer $\phi(C)$ ters sıralı DNA kod ise $\phi(C^{\perp})$ de ters sıralı DNA koddur.

İspat $F_{4^{2s}}[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ ve n tek olsun. Önerme 3.14'te görüldüğü üzere $g(x) \in F_{4^s}[x]$'tir. $der(g(x)) = r$ ve $g(x)$ polinomu palindromik bir polinom ise $i \in \{0,1,\ldots,r\}$ için $g_i = g_{r-i}$ ve $g_i = \theta(g_{r-i})$ elde edilir. Dolayısıyla, $g(x)$ polinomu aynı zamanda θ-palindromik bir polinomdur. Çift uzunluklu DNA kodlar için kullanılan argümanlar yardımıyla ispatlanır. ■

Örnek 3.16 α ; F_{16} cisminin bir ilkel elemanı olsun. F_{16} cisminin, $\theta(a)=a^4$ olarak tanımlı θ otomorfizması altında sabit kalan alt cismi $F_4=\{0,1,\alpha^5,\alpha^{10}\}$'dur. Bu durumda $F_{16}[x;\theta]$ halkasında $x^5-1=(x-1)(x^2+\alpha^5x+1)(x^2+\alpha^{10}x+1)$ olarak tek türlü çarpanlarına ayrılır.

$g(x)=x^2+\alpha^{10}x+1$ polinomu tarafından üretilen C aykırı devirli kodunun üreteç matrisi

$$G=\begin{bmatrix}1 & \alpha^{10} & 1 & 0 & 0\\ 0 & 1 & \alpha^{10} & 1 & 0\\ 0 & 0 & 1 & \alpha^{10} & 1\end{bmatrix} \tag{3.29}$$

şeklindedir. C kodunun parametreleri $[5,3,3]_{16}$'dır. G matrisinin satırlarına karşılık gelen DNA kodsözleri sırasıyla aşağıda verilmiştir.

$$\begin{aligned}&\phi(s_1)=(TT\,GG\,TT\;\;AA\,AA),\\ &\phi(s_2)=(AA\;TT\,GG\,TT\;\;AA),\\ &\phi(s_1)=(AA\,AA\,TT\;GG\,TT\,).\end{aligned} \tag{3.30}$$

$g(x)$ polinomu palindromik olduğundan $\phi(C)$ bir ters sıralı DNA koddur. $\phi(C)$'nin parametreleri ise $(10,4^6,3)_4$ olarak elde edilir.

Aynı zamanda $h(x)=h^R(x)=x^3+\alpha^{10}x^2+\alpha^{10}x+1$ polinomu da palindromik polinom olduğundan $\phi(C^{\perp})$ de ters sıralı DNA koddur. $C^{\perp}$ kodunun ve $\phi(C^{\perp})$ kodunun parametreleri sırasıyla $[5,2,4]_{16}$ ve $(10,4^4,4)_4$ olarak elde edilir.

BÖLÜM 4

$F_{16}+uF_{16}+vF_{16}+uvF_{16}$ HALKASI ÜZERİNDE TERS SIRALI DNA KODLAR

Bu bölümde $F_{16}+uF_{16}+vF_{16}+uvF_{16}$ halkası üzerinde aykırı devirli kodlar tanımlanacak ve $F_{16}+uF_{16}+vF_{16}+uvF_{16}$ halkasının elemanları ile DNA 8-bazları eşlenerek ters sıralı DNA kodlar elde edilecektir.

$R_{16}=F_{16}+uF_{16}+vF_{16}+uvF_{16}$ halkası $u^2=u$, $v^2=v$ ve $uv=vu$ olmak üzere birimli ve değişmeli bir halkadır ve karakteristiği 2'dir. $R_{16}=\{a+bu+cv+duv \mid a,b,c,d\in F_{16}\}$ halkasının $16^4=65536$ adet elemanı vardır ve ideal yapısını belirlemek kolay değildir. Aşağıda R_{16} halkasında uv ve $v+uv$ elemanlarının ürettiği idealler verilmiştir.

$$\begin{aligned} uvR_{16}&=\langle uv\rangle=\{auv \mid a\in F_{16}\}\\ (v+uv)R_{16}&=\langle v+uv\rangle=\{av+auv \mid a\in F_{16}\}. \end{aligned} \tag{4.1}$$

Görüldüğü üzere her iki ideal de 16 elemanlıdır ve birbirini içermez. Dolayısıyla R_{16} bir zincir halkası değildir.

R_{16} halkasının idempotent elemanlarından oluşan küme aşağıda verilmiştir.

$$\begin{aligned} \{a+bu+cv+duv \mid a,b,c,d\in\{0,1\}\}=\{&0,1,u,v,uv,v+uv,u+uv,u+v,u+v+uv,1+u,\\ &1+v,1+uv,1+v+uv,1+u+uv,1+u+v,1+u+v+uv\}. \end{aligned}$$

$e_1=uv$, $e_2=v+uv$, $e_3=u+uv$ ve $e_4=1+u+v+uv$ olarak seçelim. Bu durumda $i\neq j$ ve $i,j\in\{1,2,3,4\}$ iken $e_ie_j=0$ olduğu kolayca görülür. Ayrıca, $e_1+e_2+e_3+e_4=1$ dir. Dolayısıyla; Teorem 2.20 gereğince R_{16} halkası

$$R_{16}=uvR_{16}\oplus(v+uv)R_{16}\oplus(u+uv)R_{16}\oplus(1+u+v+uv)R_{16} \tag{4.2}$$

olarak ayrışır. Yukarıda görüldüğü üzere uvR_{16} ideali uvF_{16}'ya eşittir. Benzer şekilde

$$\begin{aligned}&(v+uv)R_{16}=(v+uv)F_{16},\ (u+uv)R_{16}=(u+uv)F_{16}\text{ ve}\\&(1+u+v+uv)R_{16}=(1+u+v+uv)F_{16}\end{aligned}\tag{4.3}$$

olduğundan

$$R_{16}=uvF_{16}\oplus(v+uv)F_{16}\oplus(u+uv)F_{16}\oplus(1+u+v+uv)F_{16}\tag{4.4}$$

elde edilir. Bu ayrışıma göre

$$\begin{aligned}&\phi:R_{16}\to F_{16}^{4}\\&a+ub+vc+uvd\ \to(a+b+c+d,a+c,a+b,a)\end{aligned}\tag{4.5}$$

dönüşümü R_{16} halkasından F_{16}^{4} vektör uzayına bir Gray dönüşümüdür. R_{16} halkası üzerinde aykırı devirli kodların tanımlanabilmesi için bu halka üzerinde bir otomorfizma tanımlanması gerekmektedir.

$$\begin{aligned}&\theta:\ \ R_{16}\to R_{16}\\&a+ub+vc+uvd\to a^{4}+(1+u)b^{4}+(1+v)c^{4}+(1+u)(1+v)d^{4}\\&\qquad\qquad=(a+b+c+d)^{4}+u(b+d)^{4}+v(c+d)^{4}+uvd^{4}\end{aligned}\tag{4.6}$$

Yukarıda tanımladığımız θ dönüşümü R_{16} halkası üzerinde mertebesi 2 olan bir otomorfizmadır. Doğal olarak $R_{16}[x;\theta]$ bir aykırı polinom halkasıdır ve R_{16} halkası üzerinde tanımlı n uzunluğunda bir C aykırı devirli kodu $R_{16}[x;\theta]$-modül $R_{16}[x;\theta]\big/\langle x^{n}-1\rangle$'in bir sol alt modülüne karşılık gelir.

Çizelge 3.1'de F_{16} cisminin elemanları ile DNA baz çiftleri arasında her bir eleman ve 4. kuvveti birbirinin DNA ters sıralısı olacak şekilde bir eşleştirme verilmişti. Çizelge 3.1'deki dönüşümü τ olarak adlandıralım. Bu dönüşüm F_{16}^{4}'ten DNA 8-bazlarına olan bir dönüşüme aşağıdaki gibi genişletilebilir.

$$\begin{aligned}&\tau_{2}:\ F_{16}^{4}\to\{A,T,G,C\}^{8}\\&\ \ (a,b,c,d)\to(\tau(a),\tau(b),\tau(c),\tau(d)).\end{aligned}\tag{4.7}$$

R_{16} halkasının elemanları ile DNA 8-bazlarını eşleştirmek için $\varphi=\tau_{2}\circ\phi$ dönüşümünü tanımlayalım. Bu durumda herhangi $a+ub+vc+uvd\in R_{16}$ için

$\varphi(a+ub+vc+uvd)=\tau_2(\phi(a+ub+vc+uvd))=(\tau(a+b+c+d),\tau(a+c),\tau(a+b),\tau(a))$ şeklindedir.

Önerme 4.1 Herhangi $\rho=a+ub+vc+uvd\in R_{16}$ için $\varphi(\rho)^r=\varphi(\theta(\rho))$'dur.

İspat $\theta(\rho)=(a+b+c+d)^4+u(b+d)^4+v(c+d)^4+uvd^4$ ve

$$\begin{aligned}\varphi(\theta(\rho))&=\varphi((a+b+c+d)^4+u(b+d)^4+v(c+d)^4+uvd^4)\\&=\tau_2(\phi((a+b+c+d)^4+u(b+d)^4+v(c+d)^4+uvd^4))\\&=\tau_2(a^4,(a+b)^4,(a+c)^4,(a+b+c+d)^4)\\&=(\tau(a^4),\tau((a+b)^4),\tau((a+c)^4),\tau((a+b+c+d)^4)).\end{aligned}\tag{4.8}$$

Ayrıca $\varphi(\rho)=(\tau(a+b+c+d),\tau(a+c),\tau(a+b),\tau(a))$ ve $\varphi(\rho)$ nin ters sıralısı $\varphi(\rho)^r=(\tau(a)^r,\tau(a+b)^r,\tau(a+c)^r,\tau(a+b+c+d)^r)$ şeklindedir. Çizelge 3.1'de $\tau(a)$ ile $\tau(a^4)$ birbirinin ters sıralısı olduğundan $\tau(a)^r=\tau(a^4)$'tür. Böylece $\varphi(\rho)^r=\varphi(\theta(\rho))$ olduğu görülür. ■

Yukarıdaki φ dönüşümü doğal olarak n-koordinata genişletilebilir. Herhangi $c=(c_0,c_1,\ldots,c_{n-1})\in R_{16}^n$ için $\varphi(c)=(\varphi(c_0),\varphi(c_1),\ldots,\varphi(c_{n-1}))$ şeklindedir. Önerme 4.1'in n-koordinata genişletimiş hali aşağıda verilmiştir.

Önerme 4.2 $c=(c_0,c_1,\ldots,c_{n-1})\in R_{16}^n$ ve $\theta(c^r)=(\theta(c_{n-1}),\theta(c_{n-2}),\ldots,\theta(c_1),\theta(c_0))$ olsun. Bu durumda, $\varphi(c)^r=\varphi(\theta(c^r))$ sağlanır.

Örnek 4.3 $F_{16}^*=\langle\alpha\rangle$ ve $\alpha^4+\alpha+1=0$ olmak üzere, $\beta=\alpha+u+\alpha^3v+\alpha^2uv\in R_{16}$ alalım. Bu durumda $\varphi(\beta)=(\tau(\alpha^{12}),\tau(\alpha^9),\tau(\alpha^4),\tau(\alpha))=(GA,CA,TA,AT)$ elde edilir. Aynı zamanda $\varphi(\theta(\beta))=\tau_2(\alpha^4,\alpha,\alpha^6,\alpha^3)=(TA,AT,AC,AG)$ dir. Böylece $\varphi(\beta)^r=\varphi(\theta(\beta))$ olduğu görülür.

Tanım 4.4 $f(x)=a_0+a_1x+\ldots+a_tx^t\in R_{16}[x;\theta]$ olsun. Eğer $f(x)$ polinomunun katsayıları için $a_i=a_{t-i}$ ($i\in\{0,1,\ldots,t\}$) eşitliği sağlanıyorsa palindromik polinom, $a_i=\theta(a_{t-i})$ ($i\in\{0,1,\ldots,t\}$) eşitliği sağlanıyorsa θ-palindromik polinom denir.

Örnek 4.5 $R_{16}[x;\theta]$ halkasında;

- $f_1(x)=\alpha+\alpha^2x+x^2+x^4+\alpha^2x^5+\alpha x^6$ bir palindromik polinom,

- $f_2(x) = \alpha + \alpha^2 x + x^2 + x^4 + \alpha^8 x^5 + \alpha^4 x^6$ bir θ-palindromik polinomdur.

Teorem 4.6 $R_{16}[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ olsun. $C = \langle g(x) \rangle$, R_{16} üzerinde $g(x)$ polinomu tarafından üretilen aykırı devirli kod olsun. Eğer $n - der(g(x))$ çift ve $g(x)$ polinomu bir palindromik polinom ise $\varphi(C)$ bir ters sıralı DNA koddur.

İspat $g(x)$ bir palindromik polinom ve $k = n - der(g(x))$ olsun. φ dönüşümü kod sözlerin DNA kodsözü karşılığını verir. Her $c \in C$ için $\varphi(c)$ DNA kodsözünün ters sıralısı aşağıdaki eşitlikten bulunur, $\beta_i \in R_{16}$ olmak üzere,

$$\varphi\left(\sum_{i=0}^{k-1} \beta_i x^i g(x)\right)^r = \varphi\left(\sum_{i=0}^{k-1} \theta(\beta_i) x^{k-1-i} g(x)\right). \tag{4.9}$$

$\sum_i \theta(\beta_i) x^{k-1-i} g(x) \in C$ olduğundan $\varphi(C)$ bir ters sıralı DNA koddur. ■

Örnek 4.7 $R_{16}[x;\theta]$ halkasında $x^6 - 1$ in bir ayrışımı;

$$\begin{aligned} &x^6 - 1 = h(x)g(x), \\ &h(x) = (1 + (\alpha^3 + \alpha^2(u+v))x + x^2), \\ &g(x) = (1 + (\alpha^3 + \alpha^2(u+v))x + (\alpha^3 + \alpha^2(u+v))x^3 + x^4) \end{aligned} \tag{4.10}$$

şeklindedir. Bu durumda $C = \langle g(x) \rangle$, R_{16} üzerinde $[6,4,4]_q$ parametrelerine sahip aykırı devirli koddur ($q = 16^4$). Ayrıca $g(x)$ polinomu palindromik ve $n - der(g(x))$ çift olduğundan $\varphi(C)$ bir ters sıralı DNA koddur.

Teorem 4.8 $R_{16}[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ olsun. $C = \langle g(x) \rangle$, R_{16} üzerinde $g(x)$ polinomu tarafından üretilen aykırı devirli kod olsun. Eğer $n - der(g(x))$ tek ve $g(x)$ polinomu bir θ-palindromik polinom ise $\varphi(C)$ bir ters sıralı DNA koddur.

İspat $g(x)$ bir θ-palindromik polinom ve $k = n - der(g(x))$ olsun. φ dönüşümü kod sözlerin DNA kodsözü karşılığını verir. Her $c \in C$ için $\varphi(c)$ DNA kodsözünün ters sıralısı aşağıdaki eşitlikten bulunur, $\beta_i \in R_{16}$ olmak üzere,

$$\varphi\left(\sum_{i=0}^{k-1} \beta_i x^i g(x)\right)^r = \varphi\left(\sum_{i=0}^{k-1} \theta(\beta_i) x^{k-1-i} g(x)\right). \tag{4.11}$$

$\sum_i \theta(\beta_i)x^{k-1-i}g(x) \in C$ olduğundan $\varphi(C)$ bir ters sıralı DNA koddur. ■

Örnek 4.9 $R_{16}[x;\theta]$ halkasında x^6-1 polinomunun bir ayrışımı aşağıda verilmiştir.

$$\begin{aligned} &x^6-1 = h(x)g(x), \\ &h(x) = (1+(\alpha^7+\alpha(u+v))x+(\alpha^7+\alpha(u+v))x^2+x^3), \\ &g(x) = (1+(\alpha^7+\alpha(u+v))x+(\alpha^{13}+\alpha^4(u+v))x^2+x^3). \end{aligned} \tag{4.12}$$

Bu durumda $C=\langle g(x)\rangle$, R_{16} üzerinde $[6,3,4]_q$ parametrelerine sahip aykırı devirli koddur ($q=16^4$). Ayrıca $n-der(g(x))$ tek ve $g(x)$ polinomu θ-palindromik olduğundan $\varphi(C)$ bir ters sıralı DNA koddur.

Not 4.10 Teorem 4.6 ve Teorem 4.8'in ispatlarını somut bir örnek üzerinde açıklayalım. $C=\langle g(x)\rangle$, R_{16} halkası üzerinde 8 uzunluğunda bir aykırı devirli kod olsun. Farz edelim ki $g(x)$ derecesi 5 olan bir θ-palindromik polinom olsun. Bu durumda $g(x)$ polinomu, $g_0, g_1, g_2 \in R_{16}$ olmak üzere,

$$g(x) = g_0 + g_1x + g_2x^2 + \theta(g_2)x^3 + \theta(g_1)x^4 + \theta(g_0)x^5 \tag{4.13}$$

formundadır.

Vektör gösteriminde $g(x)$ polinomuna karşılık gelen kodsöz c olsun.

$$c = (g_0, g_1, g_2, \theta(g_2), \theta(g_1), \theta(g_0), 0, 0) \in C, \tag{4.14}$$

$$\begin{aligned} \varphi(c)^r &= (\varphi(g_0), \varphi(g_1), \varphi(g_2), \varphi(\theta(g_2)), \varphi(\theta(g_1)), \varphi(\theta(g_0)), \varphi(0), \varphi(0))^r \\ &= (\varphi(0), \varphi(0), \varphi(g_0), \varphi(g_1), \varphi(g_2), \varphi(\theta(g_2)), \varphi(\theta(g_1)), \varphi(\theta(g_0))) \\ &= \varphi(c'). \end{aligned} \tag{4.15}$$

Yukarıda verilen c' vektörü $c' = (0, 0, g_0, g_1, g_2, \theta(g_2), \theta(g_1), \theta(g_0))$ dır. c' vektörü $x^2g(x)$ polinomuna karşılık geldiğinden $c' \in C$ dir. Böylece $g(x)$ ve $x^2g(x)$ polinomlarına karşılık gelen DNA kodsözleri birbirinin ters sıralısıdır. Benzer şekilde, herhangi $\beta \in R_{16}$ için, $\beta g(x)$ ve $\theta(\beta)x^2g(x)$ polinomlarına karşılık gelen DNA kodsözleri birbirinin ters sıralısıdır.

Not 4.11 C, R_{16} üzerinde n uzunluğunda bir kod olsun. Bu durumda, $\varphi(C)$ DNA kodunun uzunluğu $8n$'dir. Eğer $\varphi(C)$ ters sıralı DNA kod ise Teorem 2.87'de görüldüğü üzere $\varphi(C)$ kodundan bir ters sıralı tamlayan DNA kod kolayca elde edilir.

BÖLÜM 5

$R_{k,s}$ HALKASI ÜZERİNDE TERS SIRALI DNA KODLAR

Bu bölümde, bir önceki bölümde tanımlamış olduğumuz $F_{16}+uF_{16}+vF_{16}+uvF_{16}$ halkası üzerinde aykırı devirli kodlar ve ters sıralı DNA kodların genellemesi $R_{k,s}=F_{4^{2k}}[u_1,\ldots,u_s]\Big/\left\langle {u_1}^2-u_1,\ldots,{u_s}^2-u_s\right\rangle$ halkası üzerinden yapılacaktır.

$R_{k,s}=F_{4^{2k}}[u_1,\ldots,u_s]\Big/\left\langle {u_1}^2-u_1,\ldots,{u_s}^2-u_s\right\rangle$ halkası, $k,s\geq 1$ olmak üzere, karakteristiği 2, eleman sayısı $4^{2k2^s}=4^{2^{s+1}k}$ olan değişmeli bir halkadır, zincir halkası değildir. $R_{k,s}$ halkası üzerinde aykırı devirli kodları tanımlamak için aşağıdaki otomorfizmayı kullanacağız.

$$\begin{aligned}&\theta: R_{k,s}\to R_{k,s}\\ &\quad a \to a^{4^k} \quad \forall a\in F_{4^{2k}},\\ &\quad u_i \to u_i+1 \ \forall i\in\{1,\ldots,s\},\end{aligned} \tag{5.1}$$

olarak tanımlı θ dönüşümü $R_{k,s}$ halkası üzerinde mertebesi 2 olan bir otomorfizmadır. Doğal olarak $R_{k,s}[x;\theta]$ bir aykırı polinom halkasıdır ve $R_{k,s}$ halkası üzerinde tanımlı n uzunluğunda bir C aykırı devirli kodu $R_{k,s}[x;\theta]\Big/\left\langle x^n-1\right\rangle$'in bir sol $R_{k,s}[x;\theta]$-alt modülüne karşılık gelir.

5.1 $R_{k,s}$ Halkasının Çin Kalan Teoremi'ne Göre Ayrışımı

$R_{k,s}$ halkası ile DNA kodları ilişkilendirilebilmek için, $R_{k,s}$ halkasının her elemanını bir DNA $2^{s+1}k$-sıralı bazı ile eşleştirmemiz gerekmektedir. Bunun için öncelikle $R_{k,s}$

halkasının elemanlarını bir sıralamaya göre tek türlü yazacağız. $R_{k,s}$ halkasındaki idempotent elemanların yardımıyla Çin Kalan Teoremi'ni kullanarak halkanın bir ayrışımını elde edeceğiz. Ardından bu ayrışımın yardımıyla $R_{k,s}$ halkasından $F_{4^{2k}}^{2^s}$ üzerine bir Gray dönüşümü tanımlayarak halka elemanlarının DNA karşılıklarını tanımlayacağız.

$R_{k,s}$ halkasının $u_1^{r_1}u_2^{r_2}\ldots u_s^{r_s}$ tipindeki elemanlarını sıralayalım. Bu tipteki elemanların kümesi, $A=\left\{u_1^{r_1}u_2^{r_2}\ldots u_s^{r_s}\,\middle|\, r_i\in\{0,1\},\ 1\le i\le s\right\}$, eleman sayısı 2^s olan bir kümedir.

$$\begin{aligned}&\mu: A\to\mathbb{Z}^s\\ &u_1^{r_1}u_2^{r_2}\ldots u_s^{r_s}\ \to(r_1,r_2,\ldots,r_s).\end{aligned}\qquad(5.2)$$

Yukarıda tanımlanan μ dönüşümü A kümesinin elemanlarını, s bileşenli vektörlere (s-tuples) eşler. $(r_1,r_2,\ldots,r_s)$ formundaki s-bileşenli vektörlerin sıralaması için birçok metod geliştirilmiştir. Biz sözlüksel (lexicographic) sıralamayı kullanacağız.

Tanım 5.1 [44] $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_s)$, $\beta=(\beta_1,\beta_2,\ldots,\beta_s)\in\mathbb{Z}_{\ge 0}^s$ olsun. Eğer $\alpha-\beta$ farkının sıfırdan farklı en soldaki elemanı pozitif ise α elemanı β elemanından sözlüksel sıralamaya göre büyüktür denir ve $\alpha>_{lex}\beta$ olarak gösterilir. Ayrıca $\alpha>_{lex}\beta$ ise $u_1^{\alpha_1}u_2^{\alpha_2}\ldots u_s^{\alpha_s}>_{lex}u_1^{\beta_1}u_2^{\beta_2}\ldots u_s^{\beta_s}$ dir.

Örneğin; $u_1,u_2\in R_{1,3}$ elemanlarını sıralayalım. $\mu(u_1)=(1,0,0)$ ve $\mu(u_2)=(0,1,0)$ olduğu görülür. Ayrıca $(1,0,0)-(0,1,0)=(1,-1,0)$ olduğundan $u_1>_{lex}u_2$ elde edilir.

Şimdi, $A=\left\{u_1^{r_1}u_2^{r_2}\ldots u_s^{r_s}\,\middle|\, r_i\in\{0,1\},\ 1\le i\le s\right\}$ kümesinin elemanlarını yeniden adlandıralım;

1. İlk olarak A kümesinin

   $A_j=\left\{u_1^{r_1}u_2^{r_2}\ldots u_s^{r_s}\,\middle|\,\text{tam olarak } j \text{ adet } r_i\ 1,\ \text{diğerleri } 0\right\},\ 0\le j\le s$

   şeklindeki özel alt kümelerini ele alalım. Bu durumda, $A_0=\{1\}$, $A_1=\{u_1,u_2,\ldots,u_s\}$, $A_2=\{u_1u_2,u_1u_3\ldots,u_{s-1}u_s\}$ ve $A_s=\{u_1u_2\ldots u_s\}$.

2. A_j kümesininin elemanlarının sözlüksel sıralamaya göre büyükten küçüğe doğru sıralanmış dizisini B_j olarak adlandıralım. $B_0=[1]$, $B_1=[u_1,u_2,\ldots,u_s]$.
3. B_j dizilerini birleştirerek B dizisini oluşturalım; $B=[B_0,B_1,\ldots,B_s]$.
4. B dizisininin i. elemanını U_i olarak adlandıralım. Örneğin, $U_0=1$, $U_1=u_1$, $U_{2^s-1}=u_1u_2\ldots u_s$ gibi.

$R_{k,s}$ halkasının sıralı s-bileşenlerinin dizisini

$$T=\left[\mu(U_0),\mu(U_1),\ldots,\mu\left(U_{2^s-1}\right)\right]=\left[T_0,T_1,\ldots,T_{2^s-1}\right] \tag{5.3}$$

olarak tanımlayalım. Bu durumda, $0\le i\le 2^s-1$ iken

$\mu(U_i)+\mu\left(U_{2^s-1-i}\right)=T_i+T_{2^s-1-i}=(1,1,\ldots,1)$ olduğu görülür.

Örnek 5.2 $R_{1,3}=F_{16}[u_1,u_2,u_3]\Big/\left\langle {u_1}^2-u_1,{u_2}^2-u_2,{u_3}^2-u_3\right\rangle$ halkasını ele alalım. $R_{1,3}$ halkası için A kümesi;

$$A=\{1,u_1,u_2,u_3,u_2u_3,u_1u_3,u_1u_2,u_1u_2u_3\} \tag{5.4}$$

ve A_j alt kümeleri;

$$\begin{aligned}&A_0=\{1\},\quad A_1=\{u_1,u_2,u_3\},\\&A_2=\{u_2u_3,u_1u_3,u_1u_2\},\ A_3=\{u_1u_2u_3\}\end{aligned} \tag{5.5}$$

ve B_j dizileri;

$$\begin{aligned}&B_0=[1],\quad B_1=[u_1,u_2,u_3],\\&B_2=[u_1u_2,u_1u_3,u_2u_3],\ B_3=[u_1u_2u_3]\end{aligned} \tag{5.6}$$

olarak elde edilir. Böylece $B=[1,u_1,u_2,u_3,u_1u_2,u_1u_3,u_2u_3,u_1u_2u_3]=[U_0,U_1,\ldots,U_7]$ dir. Ayrıca $R_{1,3}$ halkasının sıralı 3-bileşenlerinin dizisi;

$$T=\left[T_0,T_1,\ldots T_7\right]=\left[(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,1,1),(1,1,1)\right] \tag{5.7}$$

şeklindedir ve $T_i+T_{7-i}=(1,1,1)$ eşitliğinin sağlandığı kolayca görülür. Örneğin;

$$\begin{aligned}&T_0+T_7=\mu(U_0)+\mu(U_7)=\mu(1)+\mu(u_1u_2u_3)=(0,0,0)+(1,1,1)=(1,1,1),\\&T_3+T_4=\mu(U_3)+\mu(U_4)=\mu(u_3)+\mu(u_1u_2)=(0,0,1)+(1,1,0)=(1,1,1).\end{aligned} \tag{5.8}$$

$R_{k,s}$ halkasının Teorem 2.20'yi sağlayan idempotent elemanlarından oluşan I kümesini oluşturacağız. Bunun için $R_{k,s}$ halkasının bazı elemanları ile T_i sıralı s-bileşenlerini ilişkilendireceğiz. Her $T_i = (r_1, r_2, \ldots, r_s)$ için $I_i = \theta^{r_1}(u_1)\theta^{r_2}(u_2)\ldots\theta^{r_s}(u_s)$ olarak tanımlayalım.

Örneğin; $T_0 = (0,0,0)$, $T_1 = (1,0,0)$, ve $T_4 = (1,1,0)$ iken $I_0 = u_1u_2u_3$, $I_1 = \theta(u_1)u_2u_3 = (u_1+1)u_2u_3$ ve $I_4 = \theta(u_1)\theta(u_2)u_3 = (u_1+1)(u_2+1)u_3$'tür.

Teorem 5.3 $I = \left\{ I_i = \theta^{r_1}(u_1)\theta^{r_2}(u_2)\ldots\theta^{r_s}(u_s) \middle| T_i = (r_1, r_2, \ldots, r_s), 0 \le i \le 2^s - 1 \right\}$ olsun. Bu durumda I kümesi Teorem 2.20'yi sağlar ve $R_{k,s} = I_0F_{4^{2k}} \oplus I_1F_{4^{2k}} \oplus \ldots \oplus I_{2^s-1}F_{4^{2k}}$ olarak yazılır.

İspat i) $I_i^2 = I_i$.

Her I_i elemanı $(u_{j_1}+1)\ldots(u_{j_d}+1)u_{j_{d+1}}\ldots u_{j_s}$ formundadır öyle ki $\{j_1, j_2, \ldots, j_s\} = \{1, 2, \ldots, s\}$ dir. $(u_{j_e}+1)^2 = (u_{j_e}+1)$ ve $u_{j_f}^2 = u_{j_f}$ olduğundan $I_i^2 = I_i$ eşitliği sağlanır.

ii) $i \ne j$ ve $0 \le i, j \le 2^s - 1$ iken $I_iI_j = 0$.

$$\begin{aligned} &I_i = \theta^{r_1}(u_1)\theta^{r_2}(u_2)\ldots\theta^{r_s}(u_s) \to T_i = (r_1, r_2, \ldots, r_s), \\ &I_j = \theta^{m_1}(u_1)\theta^{m_2}(u_2)\ldots\theta^{m_s}(u_s) \to T_j = (m_1, m_2, \ldots, m_s) \end{aligned} \tag{5.9}$$

olsun. $i \ne j$ olduğundan T_i ile T_j'nin en az bir koordinatı farklıdır, yani $r_e \ne m_e$ olacak şekilde en az bir $e \in \{1, \ldots, s\}$ vardır. Genelliği bozmadan $r_e = 0$ ve $m_e = 1$ olarak kabul edebiliriz. Bu durumda $\theta^{r_e}(u_e) = u_e$ ve $\theta^{m_e}(u_e) = u_e + 1$ dir. $u_e(u_e+1) = 0$ olduğundan, $I_iI_j = 0$ olarak elde edilir.

iii) $\sum_{i=0}^{2^s-1} I_i = 1$.

Tümevarım kullanılarak ispatlanır. $s = 0$ için $I_0 = 1$'dir. Her $0 \le j < l$ için $\sum_{i=0}^{2^j-1} I_i = 1$ eşitliğinin sağlandığını kabul edelim. $s = l$ durumunu inceleyelim.

$I=\{I_0,I_1,\ldots,I_{2^l-1}\}$ kümesinin elemanlarının tam olarak yarısı u_l'yi bir çarpan olarak içerirken diğer yarısı u_l+1'i çarpan olarak içerir. I kümesinin u_l'yi bir çarpan olarak içeren elemanlarının alt kümesini alalım ve bu elemanların her birinden u_l çarpanını silelim. Oluşan yeni küme tam olarak $R_{k,l-1}$ halkasının idempotent kümesidir. Bu kümeyi $\{V_0,V_1,\ldots,V_{2^{l-1}-1}\}$ olarak gösterelim. Tümevarım hipotezi gereği $\sum_{i=0}^{2^{l-1}-1}V_i=1$ olduğu görülür.

I kümesinin u_l+1'i bir çarpan olarak içeren elemanlarının alt kümesini alalım ve aynı şekilde her elemandan u_l+1 çarpanını silelim. Elde ettiğimiz yeni küme yine $R_{k,l-1}$ halkasının idempotent kümesidir. Böylece;

$$\begin{aligned}\sum_{i=0}^{2^l-1}I_i &= u_l\sum_{i=0}^{2^{l-1}-1}V_i+(u_l+1)\sum_{i=0}^{2^{l-1}-1}V_i \\ &= u_l+(u_l+1)=1.\end{aligned} \tag{5.10}$$

Dolayısıyla, Teorem 2.20'nin sonucu olarak $R_{k,s}=I_0R_{k,s}\oplus I_1R_{k,s}\oplus\ldots\oplus I_{2^s-1}R_{k,s}$ şeklinde ideallerin direkt toplamı olarak yazılabilir. Şimdi $I_iR_{k,s}$ ideallerini inceleyelim. Her $i\in\{0,\ldots,2^s-1\}$ için $I_i=\theta^{r_1}(u_1)\theta^{r_2}(u_2)\ldots\theta^{r_s}(u_s)$ elemanı $a=u_1^{e_1}u_2^{e_2}\ldots u_s^{e_s}$ formunda bir eleman ile çarpıldığında en az bir $j\in\{0,1,\ldots,2^s-1\}$ pozisyonunda $r_j=e_j=1$ olması durumunda $(u_j+1)u_j=0$ olduğundan $aI_i=0$ elde edilecektir. r_j ve e_j'nin diğer durumları aşağıda listelenmiştir.

$$\begin{aligned}&r_j=0,e_j=0 \text{ ise } u_j(u_j^0)=u_j,\\ &r_j=1,e_j=0 \text{ ise}(1+u_j)(u_j^0)=1+u_j,\\ &r_j=0,e_j=1 \text{ ise}\,u_j(u_j^1)=u_j^2=u_j.\end{aligned} \tag{5.11}$$

Sonuç olarak hiçbir pozisyonda $r_j=e_j=1$ durumu yoksa $aI_i=I_i$ elde edilir. Dolayısıyla $I_iR_{k,s}=\{aI_i\,|\,a\in R_{k,s}\}$ idealinin elemanları $I_iF_{4^{2k}}=\{aI_i\,|\,a\in F_{4^{2k}}\}$ kümesinden ibarettir ve

$$R_{k,s}=I_0F_{4^{2k}}\oplus I_1F_{4^{2k}}\oplus\ldots\oplus I_{2^s-1}F_{4^{2k}} \tag{5.12}$$

olarak yazılır. ■

Örnek 5.4 $R_{1,3}$ halkası için I kümesini oluşturalım. Örnek 5.2'de T kümesi

$$T=\left[T_0,T_1,\ldots T_7\right]=\left[(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,1,1),(1,1,1)\right] \quad (5.13)$$

olarak belirlenmişti. Bu durumda

$$\begin{aligned}
I_0&=u_1u_2u_3,\\
I_1&=(u_1+1)u_2u_3,\\
I_2&=u_1(u_2+1)u_3,\\
I_3&=u_1u_2(u_3+1),\\
I_4&=(u_1+1)(u_2+1)u_3,\\
I_5&=(u_1+1)u_2(u_3+1),\\
I_6&=u_1(u_2+1)(u_3+1),\\
I_7&=(u_1+1)(u_2+1)(u_3+1),
\end{aligned}$$

elde edilir. Yukarıda listelenen I_i elemanlarının Teorem 2.20'yi sağladığı görülür. Örneğin ;

$$\begin{aligned}
&I_1^2=\left[(u_1+1)u_2u_3\right]^2=(u_1^2+1)u_2^2u_3^2=(u_1+1)u_2u_3=I_1,\\
&I_1I_3=\left[(u_1+1)u_2u_3\right]\left[u_1u_2(u_3+1)\right]=0
\end{aligned} \quad (5.14)$$

ve $\sum_{i=0}^{7}I_i=1$'dir.

Teorem 5.3'teki ayrışım kullanılarak $R_{k,s}$ halkasının her α elemanı, $\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1}\in F_{4^{2k}}$ olmak üzere, $\alpha=\alpha_0I_0+\alpha_1I_1+\ldots+\alpha_{2^s-1}I_{2^s-1}$ biçiminde tek türlü yazılır. Bu yazımı kullanarak Gray dönüşümünü tanımlayalım;

$$\begin{aligned}
&\phi:R_{k,s}\to F_{4^{2k}}^{2^s}\\
&\alpha=\alpha_0I_0+\alpha_1I_1+\ldots+\alpha_{2^s-1}I_{2^s-1}\ \to(\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1}).
\end{aligned} \quad (5.15)$$

ϕ dönüşümü birebir ve örten bir dönüşümdür ve n-bileşenli vektörlere doğal olarak genişletilebilir. Yani, $\beta=(\beta_1,\beta_2,\ldots\beta_n)\in R_{k,s}^n$ için $\phi(\beta)=(\phi(\beta_1),\phi(\beta_2),\ldots,\phi(\beta_n))\in R_{k,s}^n$ şeklindedir.

Aşağıdaki önerme $\alpha=b_0U_0+b_1U_1+\ldots+b_{2^s-1}U_{2^s-1}\in R_{k,s}$ formundaki elemanların Gray dönüşümü altındaki görüntüsünü belirlememize yardımcı olur. Önermede kullanılan

noktasal çarpım "·" kısaca $\mathbb{Z}$ üzerinde bileşen bileşene çarpım olarak tanımlıdır. Örneğin; $(0,1,0)\cdot(1,0,0)=(0,0,0)$'dır.

Önerme 5.5 $b_0,\ldots,b_{2^s-1}\in F_{4^{2k}}$ ve $\alpha=b_0U_0+b_1U_1+\ldots+b_{2^s-1}U_{2^s-1}\in R_{k,s}$ olsun. Bu durumda $\phi(\alpha)=(\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1})$ ise her α_i için $\alpha_i=\sum_j b_j$ sağlanır, öyle ki $0\le j\le 2^s-1$ ve j, $T_i\cdot T_j=(0,0,\ldots,0)$ eşitliğini sağlar.

İspat $\alpha=b_0U_0+b_1U_1+\ldots+b_{2^s-1}U_{2^s-1}\in R_{k,s}$ ve $\phi(\alpha)=(\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1})$ olsun. Bu durumda, $\alpha=\alpha_0I_0+\alpha_1I_1+\ldots+\alpha_{2^s-1}I_{2^s-1}$ dir. $i\neq j$ iken $I_iI_j=0$ ve $I_i^2=I_i$ olduğundan

$$\begin{aligned} &I_i\alpha=\alpha_iI_i=I_i(b_0U_0+b_1U_1+\ldots+b_{2^s-1}U_{2^s-1})\\ &\rightarrow \alpha_iI_i=b_0U_0I_i+b_1U_1I_i+\ldots+b_{2^s-1}U_{2^s-1}I_i. \end{aligned} \tag{5.16}$$

$0\le j\le 2^s-1$ için U_jI_i'yi belirleyelim. I_i elemanı için T_i sıralı s-bileşeni $T_i=(r_1,r_2,\ldots,r_s)$ ve U_j elemanı için T_j sıralı s-bileşeni $T_j=(e_1,e_2,\ldots,e_s)$ olsun. Herhangi $k\in\{1,2,\ldots,s\}$ için $r_k=e_k=1$ ise I_i elemanını (u_k+1)'i, U_j elemanı u_k'yı çarpan olarak içerir ve dolayısıyla $U_jI_i=0$'dır. Bunun anlamı; $I_i\alpha$ çarpımında $b_jU_jI_i=0$ olduğundan b_j gözükmez.

Diğer taraftan, her $k\in\{1,2,\ldots,s\}$ için $r_k=e_k=0$ veya $r_k\neq e_k$ ise $U_jI_i\neq 0$'dır. Dolayısıyla $I_i\alpha$ çarpımında b_j gözükür.

Her $k\in\{1,2,\ldots,s\}$ için $r_k=e_k=0$ veya $r_k\neq e_k$ olması durumunda $T_i\cdot T_j=(0,0,\ldots,0)$ dir. Sonuç olarak; $0\le j\le 2^s-1$ ve $T_i\cdot T_j=(0,0,\ldots,0)$ eşitliğini sağlayan j tam sayıları için $\alpha_i=\sum_j b_j$'dir. ■

5.2 $R_{k,s}$ Halkası Üzerinde Tanımlı Ters Sıralı DNA Kodlar

Bu başlık altında ϕ Gray dönüşümünden yararlanarak $R_{k,s}$ halkası üzerindeki aykırı devirli kodlardan ters sıralı DNA kodlar elde edeceğiz.

E. Öztaş vd. (2015) [22] nolu çalışmada $F_{4^{2k}}$ cisminin elemanları ve DNA $2k$-bazları arasında birebir eşleme yapmayı sağlayan bir algoritma vermiştir. Bu algoritmaya göre

her β ve $\beta^{4^k} \in F_{4^{2k}}$ elemanlarının DNA karşılıkları birbirinin ters sıralısıdır. $F_{4^{2k}}$ cisminden DNA $2k$-bazlarına tanımlanan eşlemeyi τ dönüşümü olarak adlandıralım. τ dönüşümü 2^s koordinata aşağıdaki gibi genişletilebilir.

$$\begin{aligned} \tau_2 : F_{4^{2k}}^{2^s} &\to \{A,T,G,C\}^{2^{s+1}k} \\ (\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1}) &\to (\tau(\alpha_0),\tau(\alpha_1),\ldots,\tau(\alpha_{2^s-1})). \end{aligned} \tag{5.17}$$

Bizim çalışmamızda her $\beta \in F_{4^{2k}}$ için $\beta^{4^k} = \theta(\beta)$ olduğundan $\tau(\beta)$ ile $\tau(\theta(\beta))$ birbirinin ters sıralısıdır. Kısaca β ve $\theta(\beta)$ birbirinin DNA ters sıralısıdır diyebiliriz. $\alpha \in R_{k,s}$ elemanının Gray dönüşümü altındaki görüntüsü $\phi(\alpha) = (\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1})$ olsun. $R_{k,s}$ halkasının elemanları ile DNA $2^{s+1}k$-sıralı bazlarını eşleştirmek için $\varphi = \tau_2 \circ \phi$ dönüşümünü tanımlayalım. Bu durumda α elemanına karşılık gelen DNA $2^{s+1}k$-bazı

$$\varphi(\alpha) = \tau_2(\phi(\alpha)) = \tau_2(\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1}) = (\tau(\alpha_0),\tau(\alpha_1),\ldots,\tau(\alpha_{2^s-1})) \tag{5.18}$$

ve ters sıralısı

$$\varphi(\alpha)^r = (\tau(\theta(\alpha_{2^s-1})),\ldots,\tau(\theta(\alpha_1)),\tau(\theta(\alpha_0))) \tag{5.19}$$

şeklindedir.

Önerme 5.6 $j \in \{0,1,\ldots,2^s-1\}$ olmak üzere, $\theta(I_j) = I_{2^s-1-j}$ sağlanır.

İspat $T_j = (r_1,r_2,\ldots,r_s)$ olsun. $T_j + T_{2^s-1-j} = (1,1,\ldots,1)$ olduğundan

$$T_{2^s-1-j} = (1-r_1,1-r_2,\ldots,1-r_s)\text{'dir.} \tag{5.20}$$

Böylece, $I_j = \theta^{r_1}(u_1)\theta^{r_2}(u_2)\ldots\theta^{r_s}(u_s) \Rightarrow \theta(I_j) = \theta^{1-r_1}(u_1)\theta^{1-r_2}(u_2)\ldots\theta^{1-r_s}(u_s) = I_{2^s-1-j}$. ■

Teorem 5.7 $\alpha \in R_{k,s}$ olsun. Bu durumda $\varphi(\alpha)$'nın ters sıralısı $\varphi(\theta(\alpha))$'dır, yani $\varphi(\alpha)^r = \varphi(\theta(\alpha))$'dır.

İspat $\alpha = \alpha_0 I_0 + \alpha_1 I_1 + \ldots + \alpha_{2^s-1} I_{2^s-1} \in R_{k,s}$ olsun. Bu durumda $\phi(\alpha) = (\alpha_0,\alpha_1,\ldots,\alpha_{2^s-1})$ ve $\varphi(\alpha) = (\tau(\alpha_0),\tau(\alpha_1),\ldots,\tau(\alpha_{2^s-1}))$ şeklindedir.

$$\begin{aligned}\theta(\alpha) &= \theta(\alpha_0)\theta(I_0) + \theta(\alpha_1)\theta(I_1) + \ldots + \theta(\alpha_{2^s-1})\theta(I_{2^s-1}) \\ &= \theta(\alpha_0)I_{2^s-1} + \theta(\alpha_1)I_{2^s-2} + \ldots + \theta(\alpha_{2^s-1})I_0 \\ &= \theta(\alpha_{2^s-1})I_0 + \theta(\alpha_{2^s-2})I_1 + \ldots + \theta(\alpha_0)I_{2^s-1}.\end{aligned} \tag{5.21}$$

Böylece $\varphi(\theta(\alpha)) = (\tau(\theta(\alpha_{2^s-1})), \ldots, \tau(\theta(\alpha_1)), \tau(\theta(\alpha_0)))$ elde edilir ve bu da tam olarak $\varphi(\alpha)$'nın ters sıralısıdır. ■

Örnek 5.8. Örnek 5.2'deki $R_{1,3}$ halkasını ele alalım. β elemanı F_{16} cisminin ilkel elemanı ve $\beta^4 + \beta + 1 = 0$ olmak üzere

$$\alpha = \beta^2 I_0 + \beta I_1 + \beta^5 I_2 + \beta^3 I_3 + I_4 + \beta^7 I_6 + I_7 \in R_{1,3} \tag{5.23}$$

olsun. Bu durumda

$$\phi(\alpha) = (\beta^2, \beta, \beta^5, \beta^3, 1, 0, \beta^7, 1). \tag{5.24}$$

Çizelge 3.1'i kullanarak α elemanına karşılık gelen DNA 16-bazı aşağıdaki gibidir.

$$\begin{aligned}\varphi(\alpha) &= \tau_2(\beta^2, \beta, \beta^5, \beta^3, 1, 0, \beta^7, 1) \\ &= (\tau(\beta^2), \tau(\beta), \tau(\beta^5), \tau(\beta^3), \tau(1), \tau(0), \tau(\beta^7), \tau(1)) \\ &= (GC, AT, CC, AG, TT, AA, GT, TT).\end{aligned} \tag{5.25}$$

Ayrıca,

$$\begin{aligned}&\theta(\alpha) = I_0 + \beta^{13} I_1 + I_3 + \beta^{12} I_4 + \beta^5 I_5 + \beta^4 I_6 + \beta^8 I_7, \\ &\phi(\theta(\alpha)) = (1, \beta^{13}, 0, 1, \beta^{12}, \beta^5, \beta^4, \beta^8) \text{ ve} \\ &\varphi(\theta(\alpha)) = \tau_2(1, \beta^{13}, 0, 1, \beta^{12}, \beta^5, \beta^4, \beta^8) = (TT, TG, AA, TT, GA, CC, TA, CG).\end{aligned} \tag{5.26}$$

Böylece $\varphi(\alpha)$ ve $\varphi(\theta(\alpha))$'nın birbirinin DNA ters sıralısı, $\varphi(\alpha)^r = \varphi(\theta(\alpha))$ olduğu görülür.

Herhangi bir $f(x) = a_0 + a_1 x + \ldots + a_t x^t \in R_{k,s}[x;\theta]$ polinomu için palindromik ve θ-palindromik tanımı Tanım 4.4'te olduğu gibi yapılır. Teorem 4.6 ve Teorem 4.8'in $R_{k,s}[x;\theta]$ halkasındaki genelleştirilmesi aşağıdaki teoremde verilmiştir. Teorem 4.6 ve 4.8'deki yöntemler kullanılarak ispatlanır.

Teorem 5.9 $R_{k,s}[x;\theta]$ halkasında $x^n - 1 = h(x)g(x)$ olsun. $C = \langle g(x) \rangle$, $R_{k,s}$ üzerinde $g(x)$ polinomu tarafından üretilen aykırı devirli kod olsun.

1. Eğer $n-der(g(x))$ tek ve $g(x)$ polinomu bir θ-palindromik polinom ise $\varphi(C)$ bir ters sıralı DNA koddur.
2. Eğer $n-der(g(x))$ çift ve $g(x)$ polinomu bir palindromik polinom ise $\varphi(C)$ bir ters sıralı DNA koddur.

Örnek 5.10 $R_{1,3}$ halkasını ele alalım. β elemanı F_{16} cisminin ilkel elemanı olsun. x^6-1 polinomunun $R_{1,3}[x;\theta]$ halkasında bir ayrışımı,

$$x^6-1=h(x)g(x)=[1+(\beta^{14}+u_1+u_2)x+x^2] \\ [1+(\beta^{14}+u_1+u_2)x+(\beta^{14}+u_1+u_2)x^3+x^4]. \tag{5.27}$$

$C=\langle g(x)\rangle$ olsun. $g(x)=1+(\beta^{14}+u_1+u_2)x+(\beta^{14}+u_1+u_2)x^3+x^4$ polinomu bir palindromik polinom ve $n-der(g(x))$ çift olduğundan $\varphi(C)$ bir ters sıralı DNA koddur.

Örnek 5.11 $R_{1,3}$ halkasını ele alalım. β elemanı F_{16} cisminin ilkel elemanı olsun. x^6-1 polinomunun $R_{1,3}[x;\theta]$ halkasında bir ayrışımı,

$$x^6-1=h(x)g(x)=[1+(\beta(u_2+u_3)+\beta^7)x+(\beta(u_2+u_3)+\beta^7)x^2+x^3] \\ [1+(\beta(u_2+u_3)+\beta^7)x+(\beta^4(u_2+u_3)+\beta^{13})x^2+x^3]. \tag{5.28}$$

$C=\langle g(x)\rangle$ olsun. $g(x)=1+(\beta(u_2+u_3)+\beta^7)x+(\beta^4(u_2+u_3)+\beta^{13})x^2+x^3$ polinomu bir θ-palindromik polinom ve $n-der(g(x))$ tek olduğundan $\varphi(C)$ bir ters sıralı DNA koddur.

Not 5.12 C, $R_{k,s}$ üzerinde n uzunluğunda bir kod olsun. Bu durumda, $\varphi(C)$ DNA kodunun uzunluğu $2^{s+1}kn$'dir. Eğer $\varphi(C)$ ters sıralı DNA kod ise Teorem 2.87'de görüldüğü üzere $\varphi(C)$ kodundan bir ters sıralı tamlayan DNA kod kolayca elde edilir.

BÖLÜM 6

SONUÇ VE ÖNERİLER

Bu tezde, literatürde ilk olarak, değişmeli olmayan aykırı polinom halkaları ile DNA kodlar ilişkilendirilmiştir. DNA kodlar için ters sıralılık problemi aykırı devirli kodlar yardımıyla çözülmüştür. F_q cismi ($q = 4^{2s}$) üzerinde tanımlı bir C aykırı devirli kodunun DNA karşılığının ters sıralı DNA kod olması için gerek ve yeter şartlar belirlenmiştir. Ayrıca C kodunun DNA karşılığı ters sıralı DNA kod ise bu kodun duailinin de ters sıralı DNA koda karşılık geldiği gösterilmiştir. Daha sonra, $F_{16} + uF_{16} + vF_{16} + uvF_{16}$ halkasının elemanları ile DNA 8-bazları arasındaki uygun eşleme belirlenerek $F_{16} + uF_{16} + vF_{16} + uvF_{16}$ halkası üzerindeki aykırı devirli kodlardan ters sıralı DNA kodlar elde edilmiştir. Son bölümde ise zincir halkası olmayan $R_{k,s}$ halka ailesi incelenmiştir. Bu halka üzerinde tanımlanan bir θ otomorfizması sayesinde $R_{k,s}$ halkasının Çin Kalan Teoremi'ne göre ayrışımı belirlenmiştir. Daha sonra tanımladığımız Gray dönüşümü vasıtasıyla $R_{k,s}$ halkası üzerindeki aykırı devirli kodlardan ters sıralı DNA kodlar elde edilmiştir. Ayrıca çift uzunluğa sahip ters sıralı DNA kodlardan, ters sıralı tamlayan DNA kodların kolayca elde edilebileceğine dair bir teorem verilmiştir. Her üç bölümde de elde edilen ters sıralı DNA kodlar çift uzunluğa sahip olduğundan aynı zamanda ters sıralı tamlayan DNA kodlara karşılık gelmektedir.

GC-miktar kısıtını sağlayan DNA kodların aykırı devirli kodlar yardımıyla elde edilmesi ve farklı metriklerde (Levenshtein uzaklığı vb.) iyi parametrelere sahip DNA kodların bulunması açık bir problemdir. Ayrıca elde edilen DNA kodların canlılara ait gerçek gen parçaları ile karşılaştırılması da önemli bir problemdir.

KAYNAKLAR

[1] Adleman, L.M., (1994). "Molecular Computation of Solutions to Combinatorial Problems", Science, 266: 1021-1024.

[2] Wang, X., Bao, Z., Hu, J., Wang, S. ve Zhan, A., (2008). "Solving the SAT Problem Using a DNA Computing Algorithm Based on Ligase Chain Reaction", Biosystems, 91(1):117–125.

[3] Darehmiraki M., (2010). "A Semi-General Method to Solve the Combinatorial Optimization Problems Based on Nanocomputing", International Journal of Nanoscience, 9(05):391–398.

[4] Adleman, L.M., Rothemund, P.W.K., Roweis, S. ve Winfree, E., (1999). "On Applying Molecular Computation to the Data Encryption Standard", Journal of Computational Biology, 6(1): 53-63.

[5] Boneh, D., Dunworth, C. ve Lipton, R., (1995). "Breaking DES Using Molecular Computer", Princeton CS Tech-Report, Number CS-TR-489-95, 1995.

[6] Frutos, A.G., Liu, Q., Thiel, A.J., Sanner, A.M.W., Condon, A.E., Smith, L.M. ve Corn, R.M., (1997). "Demonstration of a Word Design Strategy for DNA Computing on Surfaces", Nucleic Acids Research, 25: 4748-4757.

[7] Mansuripur, M., Khulbe, P.K., Kuebler, S.M., Perry, J.W., Giridhar, M.S. ve Peyghambarian, N., (2003). "Information Storage and Retrieval Using Macromolecules as Storage Media", Vancouver, BC: Optical Society of America.

[8] Bystrykh, L. V. (2012). "Generalized DNA Barcode Design Based on Hamming Codes," PloS one, vol. 7(5): e36852.

[9] Limbachiya, D., Rao, B. ve Gupta, M.K., "The Art of DNA Strings: Sixteen Years of DNA Coding Theory", arXiv:1607.00266.

[10] Aboluion, N., Smith, D.H. ve Perkins, S., (2012). "Linear and Nonlinear Constructions of DNA Codes with Hamming Distance d, Constant GC-Content and a Reverse-Complement Constraint", Discrete Mathematics, 312: 1062-1075.

[11] Gaborit, P. ve King, O.D., (2005). "Linear Constructions for DNA Codes", Theoretical Computer Science, 334:99-113.

[12] Tulpan, D.C., Hoos, H.H. ve Condon, A.E., (2003). “Stochastic Local Search Algorithms for DNA Word Design”, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2568: 229-241.

[13] Deaton, R., Murphy, R.C., Rose, J.A., Garzon, M., Franceschetti, D.R. ve Stevens, S.E., (1997). “A DNA Based Implementation of an Evolutionary Search for Good Encodings for DNA Computation”, Proceedings of 1997 IEEE International Conference on Evolutionary Computation (ICEC '97), 267-271.

[14] Deaton, R., Garzon, M., Murphy, R.C., Franceschetti, D.R. ve Stevens, S.E., (1996). “Genetic Search of Reliable Encoding for DNA Based Computation”, First Conference on Genetic Programming GP-96, Stanford University, 9-15.

[15] King, O.D., (2003). “Bounds for DNA Codes with Constant GC-Content”, Electronic Journal of Combinatorics, 10:R33.

[16] Marathe, A., Condon, A.E. ve Corn, R.M., (2001). “On Combinatorial DNA Word Design”, Journal of Computational Biology, 8: 201-219.

[17] Abualrub, T., Ghrayeb, A. ve Nian Zeng, X., (2006). “Construction of Cyclic Codes Over $GF(4)$ for DNA Computing”, Journal of the Franklin Institute, 343: 448-457.

[18] Şiap, İ., Abualrub, T. ve Ghrayeb, A., (2009). “Cyclic DNA Codes Over the Ring $F_2[u]/(u^2-1)$ Based on the Deletion Distance”, Journal of the Franklin Institute-Engineering and Applied Mathematics, 346: 731-740.

[19] Yıldız, B. ve Şiap, İ., (2012). “Cyclic Codes Over $F_2[u]/(u^4-1)$ and Applications to DNA Codes”, Computers & Mathematics with Applications, 63: 1169-1176.

[20] Bayram, A., Öztas, E.S. ve Şiap, İ., (2016). “Codes Over F_4+vF_4 and Some DNA Applications”, Designs, Codes and Cryptography, 80(2): 379-393.

[21] Öztaş, E.S. ve Şiap, İ., (2013). “Lifted Polynomials Over F_{16} and Their Applications to DNA Codes”, Filomat, 27(3): 459–466.

[22] Öztaş, E.S. ve Şiap, İ., (2015). “On a Generalization of Lifted Polynomials Over Finite Fields and Their Applications to DNA Codes”, International Journal of Computer Mathematics, 92(9): 1976-1988.

[23] Faria, L.C.B., Rocha, A.S.L., Kleinschmidt, J.H., Silva-Filho, M.C., Bim, E., Herai, R.H., Yamagishi, M.E.B. ve Palazzo Jr., R., (2012). “Is a genome a codeword of an error-correcting code?”, PloS ONE, 7(5): e36644.

[24] Lichtenberg, J., Yilmaz, A., Welch, J.D., Kurz, K., Liang, X.Y., Drews, F., Ecker, K., Lee, S.S., Geisler, M., Grotewold, E. ve Welch, L.R., (2009). “The Word Landscape of the Non-Coding Segments of the Arabidopsis Thaliana Genome”, Bmc Genomics, 10:463.

[25] Hammons, A.R. Jr., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A. ve Solé, P., (1994). "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes", IEEE Transactions on Information Theory, 40:301-319.

[26] Boucher, D., Geiselmann, W. ve Ulmer, F., (2007). "Skew Cyclic Codes", Applicable Algebra in Engineering, Communication and Computing, 18(4):379-389.

[27] Şiap, İ., Abualrub, T., Aydin, N. ve Seneviratne, P., (2011). "Skew Cyclic Codes of Arbitrary Length", International Journal of Information and Coding Theory, 2:10-20.

[28] Abualrub, T., Ghrayeb, A., Aydin, N. ve Şiap, İ., (2010). "On the Construction of Skew Quasi-Cyclic Codes", IEEE Transactions on Information Theory, 56:2080-2090.

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

[30] Boucher, D., Solé P. ve Ulmer, F., (2008). "Skew Constacyclic Codes Over Galois Rings", Advances in Mathematics of Communications, 2:273-292.

[31] Jitman, S., Ling, S. ve Udomkavanich, P., (2010). "Skew Constacyclic Codes Over Finite Chain Rings", Advances in Mathematics of Communications, 6(1):39-63.

[32] Gürsoy, F., Şiap, İ. ve Yıldız, B., (2014). "Construction of Skew Cyclic Codes Over $F_q + vF_q$", Advances in Mathematics of Communications, 8(3):313–322.

[33] Hungerford, T. W., (1974). Algebra, Springer-Verlag, New York.

[34] Ling, S. ve Xing, C. (2004). Coding Theory: A First Course, First Edition, Cambridge University Press, New York.

[35] Çallıalp, F. ve Tekir, Ü., (2009). Değişmeli Halkalar ve Modüller, Birinci Baskı, Birsen Yayınevi, İstanbul.

[36] Ore, O., (1933). "Theory of Non-Commutative Polynomials", Annals of Mathematics, 34:480–508.

[37] Jacobson, N., (1943). The Theory of Rings, American Mathematical Society, New York.

[38] McDonald, B.R., (1974). Finite Rings with Identity, Marcel Dekker Inc., New York.

[39] Prange, E., (1957). Cyclic Error correcting Codes in Two Symbols, Air Force Cambridge Res. Center, AFCRC-TN-57-103, Cambridge, MA.

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

[41] Boucher, D. ve Ulmer, F., (2011). "A Note on the Dual Codes of Module Skew Codes", Lecture Notes in Computer Science, 7089:230-243.

[42] Grassl, M., Bounds on the Minimum Distance of Linear Codes and Quantum Codes", http://www.codetables.de, 1 Nisan 2019.

[43] Adleman, L., (1998). "Computing with DNA", Scientific American, August:54-61.

[44] Cox, D.A., Little, J. ve O'Shea, D., (2007). Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Third Edition, Springer, New York.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Fatmanur GÜRSOY

Doğum Tarihi ve Yeri : 28.06.1989, Denizli

Yabancı Dili : İngilizce

E-posta : fnurgursoy@gmail.com

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Matematik	Yıldız Teknik Üniversitesi	2013
Lisans	Matematik (İng)	Fatih Üniversitesi	2010
Lise	Fen Bilimleri	Yesevi Lisesi	2006

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2012-2019	Yıldız Teknik Üniversitesi	Araştırma Görevlisi
2011-2012	İstanbul Medeniyet Üniversitesi	Araştırma Görevlisi

YAYINLARI

Makale

1. Gürsoy, F., Şiap, İ. ve Yıldız, B., (2014). "Construction of Skew Cyclic Codes Over $F_q + vF_q$", Advances in Mathematics of Communications, 8(3):313–322.

2. Gürsoy, F., Öztaş, E. S. ve Şiap, İ., (2017). "Reversible DNA Codes Using Skew Polynomial Rings", Applicable Algebra in Engineering, Communication and Computing, 28(4):311-320.

3. Gürsoy, F., Öztaş, E. S. ve Şiap, İ., (2017). "Reversible DNA codes over $F_{16} + uF_{16} + vF_{16} + uvF_{16}$", Advances in Mathematics of Communications, 11(2):307–312.

4. Aydoğdu İ., Gürsoy F., (2019). "Z2Z4Z8-Cyclic Codes", Journal of Applied Mathematics and Computing, 60(1-2):327-341.

Bildiri

1. Gürsoy, F., Şiap, İ. ve Yıldız, B. (2013). "Skew Cyclic Codes over a Special Non-Chain Ring", IWBCMS, 30 Mayıs - 1 Haziran 2013, Elbasan, Albania.

2. Gürsoy, F., Şiap, İ. ve Yıldız, B. (2013). "Idempotent Generators of Skew Cyclic Codes over F_q", IECMSA-II, 26-29 Ağustos 2013, Sarajevo, Bosnia and Herzegovina.

3. Gürsoy, F., Öztaş, E. S. ve Şiap, İ. (2015). "Reversible DNA Codes using Skew Polynomial Rings", ICCC 2015, International Conference on Coding and Cryptography, 2-5 Kasım 2015, Algiers, Algeria.

4. Aydoğdu, İ., Gürsoy, F. ve Şiap, İ. (2016). "On $\mathbb{Z}_2\mathbb{Z}_4[\xi]$ Skew Cyclic Codes", Analysis, Topology, Algebra: Theory and Applications, 6-9 Temmuz 2016, Čačak, Serbia.

5. Gürsoy, F., Öztaş, E. S. ve Şiap, İ. (2016). "Reversible DNA codes over $F_{16} + uF_{16} + vF_{16} + uvF_{16}$", Workshop on Mathematics in Communications (WMC'2016), 6-8 Temmuz 2016, Santander, Spain.

6. Aydoğdu İ. ve Gürsoy F., (2017). "The structure of $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-codes", International Conference on Mathematics and Engineering, 10-12 Mayıs 2017, İstanbul, Türkiye.

7. Bedir S., Gürsoy F. (2018). "A Note on Dual Codes of Pseudo-cyclic Codes", International Conference on Mathematical Advances and Applications (ICOMAA2018), 11-13 Mayıs 2018, İstanbul, Türkiye.

8. Gürsoy, F., Öztaş E. S. (2018). “Reversible DNA Codes by Extending a Chain Ring” International Conference On Mathematics “An Istanbul Meeting for World Mathematicians”, 3-6 July 2018, İstanbul, Türkiye.

9. Gürsoy, F., Özkan A. (2019). “Reversible DNA Codes over a Non-chain Ring via Skew Cyclic Codes”, 2nd International Conference on Mathematical Advances and Applications, 3-5 Mayıs 2019, İstanbul, Türkiye.

Proje

1. “Değişmeli Olmayan Halkalar Üzerinde Tanımlı Devirli Kodlar”, YTÜ BAP, Proje no: 2012-01-03-YL01. (Araştırmacı)

ÖDÜLLERİ

1. YTÜ Yayın Teşvik Ödülü (2014, 2018)
2. TÜBİTAK UBYT Yayın Teşvik Ödülü (2014, 2018)
3. TÜBİTAK Yurtiçi Doktora Bursu
4. TÜBİTAK Yurtiçi Yüksek Lisans Bursu
5. TÜBİTAK Yurtiçi Lisans Bursu