T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BAZI SONLU HALKALAR ÜZERİNDEKİ SKEW DEVİRLİ KODLAR VE KUANTUM KODLAR

Mohammad Kamal MKHALLALATI

Matematik Anabilim Dalı

Matematik Programı

DANIŞMAN
Doç. Dr. Fatma ÇALIŞKAN

Aralık, 2022

İSTANBUL

Bu çalışma 26.12.2022 tarihinde aşağıdaki jüri tarafından Matematik Anabilim Dalı Matematik Programında Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Jürisi

Doç. Dr. Fatma ÇALIŞKAN (Danışman)
İstanbul Üniversitesi
Fen Fakültesi

Prof. Dr. Ayten PEKİN
İstanbul Üniversitesi
Fen Fakültesi

Dr. Öğr. Üyesi Refia AKSOY
İstanbul Gedik Üniversitesi
Mühendislik Fakültesi

- **İntihal Programı Beyanı**

20.04.2016 tarihli resmi gazetede yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Suriye'deki olağanüstü durumlardan dolayı Türkiye'ye gelen bir öğrenci olarak asil Türk halkına her şey için teşekkürü borç bilirim. Yüksek lisans öğrenim sürecinde ve tez çalışmalarım boyunca bilgi ve tecrübesini benimle paylaşan, emek ve desteğini hiç esirgemeyen danışman hocam Doç. Dr. Fatma ÇALIŞKAN'a çok teşekkür ederim. Eğitim hayatım sürecinde yanımda olan bütün hocalarım ve arkadaşlarıma teşekkürlerimi sunarım. Kalbi ile her zaman yanımda duran değerli annem, babam ve kardeşlerime teşekkür ederim.

Aralık, 2022 Mohammad Kamal MKHALLALATI

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Simgeler	Açıklama
$\mathbb{C}$	: Karmaşık (Kompleks) sayılar kümesi
$GF(q)$	: Eleman sayısı q olan Galois cismi
$boy(V)$	: V vektör uzayının boyutu
$\|C\|$	: C kodunun eleman sayısı
$w(x)$	: x kod kelimesinin Hamming ağırlığı
$w_L(x)$	: x kod kelimesinin Lee ağırlığı
$w(C)$	: C kodunun Hamming ağırlığı
$w_L(C)$	: C kodunun Lee ağırlığı
$d(x,y)$	: x ile y arasındaki Hamming uzaklık
$d_L(x,y)$	: x ile y arasındaki Lee uzaklık
$[n, k, d]$	: Uzunluğu n, boyutu k ve minimum uzaklığı d olan bir kod
$C^{\perp}$	: C kodunun duali
$\|\|x\|\|$	: x vektörünün normu
$\|\cdot\rangle$	: Ket vektörü
$\langle\cdot\|$	: Bra vektörü
$A \otimes B$	: A ile B'nin tensör çarpımı
$\langle\varphi, \phi\rangle$	: φ ile ϕ vektörlerinin iç çarpımı
$R[x, \Theta]$	: R üzerindeki skew polinom halkası
$[[n, k, d]]_q$	: F_q üzerinde parametreleri n, k ve d olan kuantum hata düzelten kod

ÖZET

YÜKSEK LİSANS TEZİ

BAZI SONLU HALKALAR ÜZERİNDEKİ SKEW DEVİRLİ KODLAR VE KUANTUM KODLAR

Mohammad Kamal MKHALLALATI

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Danışman: Doç. Dr. Fatma ÇALIŞKAN

Lineer kodlar kuantum hata düzelten kodların elde edilmesinde önemli bir role sahiptir. Bu tez çalışmasında bazı sonlu halkalar üzerindeki skew devirli kodlar incelenmiş ve bir uygulama olarak skew devirli kodlardan kuantum hata düzelten kodların elde edilmesi araştırılmıştır.

Beş ana başlık altında toplanan bu çalışmanın ilk bölümünde kodlama teorisinin ana problemi ve literatür taramasının özeti verilmiştir. İkinci bölümde cebirsel yapılar ve cebirsel kodlama teorisi ile ilgili temel tanım ve teoremler üzerinde durulmuştur. Üçüncü bölümde $R = F_q[u]/(u^{k+1} - u)$ halkası ve bu halka üzerindeki skew polinom halkasının tanımı verilerek R halkası üzerinde tanımlı lineer kodların ve skew devirli kodların özellikleri incelenmiştir. Dördüncü bölümde ise R halkası üzerindeki skew devirli kodlardan kuantum kodların elde edilmesi araştırılmıştır. Beşinci bölümde tezin konusu ile ilgili tartışma ve sonuç verilmiştir.

Aralık 2022, 116 sayfa.

Anahtar kelimeler: Devirli kod, skew polinom halkası, skew devirli kod, kuantum kod

SUMMARY

M.Sc. THESIS

SKEW CYCLIC CODES OVER SOME FINITE RINGS AND QUANTUM CODES

Mohammad Kamal MKHALLALATI

İstanbul University

Institute of Graduate Studies in Sciences

Department of Mathematics

Supervisor: Assoc. Prof. Fatma ÇALIŞKAN

Linear codes have a significant role on constructing quantum error-correcting codes. In this thesis, we study skew cyclic codes over some finite rings. As an application, we construct quantum codes from skew cyclic codes.

This thesis consists of five chapters. Chapter 1 includes the main problem of the coding theory and the summary of the literature review are included. The basic definitions and the fundamental theorems of abstract algebra and algebraic coding theory are given in Chapter 2. Chapter 3 consists of the properties of the ring $R = F_q[u]/(u^{k+1} - u)$ and the skew polynomial ring. In this chapter, the properties of linear codes and skew cyclic codes over R are explained. Quantum codes over F_q are constructed from skew cyclic codes over R in Chapter 4. In the fifth chapter, the discussion and the conclusion about the subject of the thesis are given.

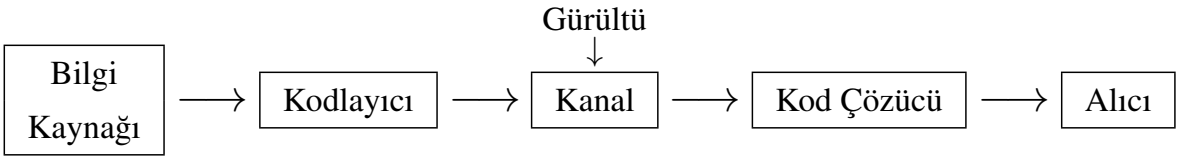
December 2022, 116 pages.

Keywords: Cyclic code, skew polynomial ring, skew cyclic code, quantum code.

1. GİRİŞ

Kodlama teorisinin ana konusu, kaynak alfabe simgelerini (harfler veya rakamlar olabilir), simgelerin farklı bir sistem ile (genellikle ikili sistem) temsil edilmesine dayanır ve bu temsile kodlama adı verilir. Diğer bir deyişle kodlama teorisi, gürültülü bir kanal boyunca verinin (kod kelimeleri) aktarılması ve bu sırada bozulan iletilerin belirlenmesi (error detection) ve düzeltilmesi (error correction) ile ilgilenmektedir. Bilginin daha kolay okunabilir hale gelmesiyle ilgilenen bu alan, bilginin daha zor okunmasını sağlamayı amaçlayan şifreleme (kriptoloji) ile karıştırılmamalıdır.

Hata tespiti, birçok farklı tekniğin uygulanabildiği yöntemlerin kullanılması ile hataların belirlenmesidir. İlk etapta, hatanın oluştuğu ve verilerin doğru şekilde iletilmediğinin bilinmesi gereklidir. Hatanın tespiti için iki durum söz konusudur. Bunlardan ilki, alıcı vericiye bir mesaj iletir ve verinin yeniden gelmesini sağlar, bu durum verinin orjinal hali gelene kadar sürer. Diğeri alıcı kendi bildiği bir teknik ve kod ile mesajı kodlayarak vericiye iletir ve kodu çözümleyerek hangi bitin hatalı olduğunu tespit eder ve düzeltir (**Şekil 1.1:**). Burada vericinin (göndericinin) kendi bildiği teknik ve kod aynı zamanda alıcının da uyguladığı teknik ve kod ile aynı olmalıdır. Yani bu işlem karşılıklı veri kodlama tekniğidir. Kısaca belirtmek gerekirse hata tespiti; alıcıya gönderilen verinin, gürültü ya da diğer faktörlerin neden olduğu bozulmaların belirlenmesi işlemidir. Hata düzeltme, alıcının gönderilen mesajlarda ya da verilerde oluşan bozulmaları gidererek orjinal mesajı (veriyi) elde etmesi işlemidir.



Şekil 1.1: İletişim Şeması

Bir konu ile ilgili verileri bir kanal boyunca iletirken hataları önlemek oldukça zordur. Verinin iletiminde ortaya çıkan hatalar insan ya da makine kaynaklı olabilir. Kodlama teorisinin asıl amacı bilgi iletiminin olabildiğince hızlı olmasını sağlamanın yanı sıra

meydana gelen hataları belirlemek ve düzeltmektir. Kodlama teorisi ile ilgili çalışmalarda matematiksel teknikler ve sonuçlar etkili bir şekilde kullanılır. Kodlama teorisinin ana problemi; boyutu ve minimum uzaklığı büyük olan kodların inşa edilmesidir. Boyut ve minimum uzaklık parametrelerinin aynı anda en yüksek değere sahip olması istense de bu durum pek de mümkün olmamaktadır. Verilen bir uzunluk için, minimum ağırlığı yüksek olan bir kod, oldukça az kod sözcüğü içerirken; kod sözcük sayısı maksimum olan bir kod en düşük minimum ağırlığa sahiptir. Bu yüzden kodlama teorisinde belirli bir uzunluğa sahip bir kod için boyutun ya da minimum ağırlığın bilinmesine göre bilinmeyen parametrenin alabileceği makul değer araştırılarak en iyi parametrelere sahip kodlar elde edilmeye çalışılır.

Cebirsel yapılar üzerindeki lineer kodlar matematikçiler tarafından uzun zamandır çalışılmaktadır. Cebirsel kodlama teorisinde ilk olarak iki elemanlı sonlu cisim olan F_2 üzerindeki kodlar ile çalışılmıştır, hatta günümüzde de çalışılmaya devam etmektedir. Daha sonra F_2 cisminin sonlu genişlemeleri ve eleman sayısı iki veya ikinin bir kuvveti olmayan sonlu cisimler üzerindeki kodlar incelenmiştir. 1994'de Hammons vd. tarafından literatüre kazandırılan çalışma ile, 4 elemanlı halka olan Z_4 üzerindeki kodların Gray görüntüleri olarak F_2 cismi üzerindeki bazı önemli lineer olmayan kodların elde edilebildiği gösterilmiştir. Bu önemli çalışmanın ardından araştırmacılar halkalar üzerindeki kodları araştırmaya başlamıştır. İlk zamanlar alfabe olarak sonlu zincir halkaları göz önüne alınırken daha sonra, Çin Kalan Teoremi (Chinese Remainder Theorem) yardımıyla, tüm sonlu değişmeli halkalar lokal halkaların direkt çarpımı olarak yazılabildiğinden lokal halkalar üzerindeki kodlar ile çalışılmıştır.

Son zamanlarda değişmeli olmayan bir yapıya sahip olan skew polinom halkaları üzerindeki kodlar araştırmacılar tarafından büyük ilgi görmektedir. Bu ilginin sebebi, skew polinom halkalarının değişmeli olmamasından kaynaklanmaktadır. Skew polinom halkaları üzerinde tanımlı olan çarpma işlemi değişme özelliğini sağlamadığından dolayı bu halkalar değişmeli değildir. Dolayısıyla skew polinom halkası üzerindeki bir polinomun çarpanlara ayrılışı tek türlü değildir. Böylece bir skew polinoma karşılık gelen kod sözcüğü sayısı, değişmeli polinom halkaları üzerindeki bir polinoma karşılık gelen kod sözcüğü sayısından daha fazladır. Bu sebeple farklı cebirsel yapılar üzerindeki skew devirli kodlar ile çalışmak var olan kodlardan daha iyi parametrelere sahip kodları elde etmek için oldukça önemlidir.

Kuantum bilgi işleme sürecinde klasik kodlamadaki bitler yerine kübitler kullanılır. Bitlerin

ortaya koyduğu 0 ve 1 durumunun bir karışımı olarak kübitler olasılıklar ile ifade edilir. İki kübit $00, 01, 10, 11$ gibi dört durumu ifade ederken üç kübit sekiz durumu ifade eder ki bunlar da $000, 001, 010, 100, 111, 110, 101, 011$ şeklindedir. Genel olarak n adet kübit 2^n tane durumu ifade edebilme kapasitesine sahiptir. İkiden fazla olası duruma sahip kuantum sistemler de olabileceği düşünüldüğünde daha yüksek seviyeli bilgi kodlama kapasitesinin ortaya çıkmasının mümkün olduğu görülür. Kuantum bilgi işlemeyi gerçekleştiren cihazlar, kuantum bilgisayarlar olarak bilinir. Kuantum bilgisayarlar belirli sorunları çözmek için klasik bilgisayarlardan daha verimli bir şekilde kullanılır. Kuantum hata düzeltme, kuantum bilgiyi olabilecek hatalardan korumak için kuantum hesaplamada kullanılır.

Literatürde kuantum hata düzelten kodlar genellikle devirli kodlar yardımıyla elde edilmiştir. Son zamanlarda skew devirli kodlardan kuantum hata düzelten kodların elde edilmesi üzerine çalışılmaktadır. Skew polinom halkası üzerinde çarpanlara ayrılış tek türlü olmadığı için skew devirli kodlar yardımıyla kuantum hata düzelten kodların elde edilmesi daha iyi parametreli kuantum hata düzelten kodların elde edilmesine olanak sağlamaktadır.

Bu çalışmada bazı sonlu halkalar üzerindeki skew devirli kodlardan kuantum hata düzelten kodların elde edildiğinin gösterilmesi hedeflenmektedir. Tez kapsamında ilk olarak bazı sonlu halkalar üzerindeki, birimden farklı bir otomorfi göz önüne alınarak elde edilen skew polinom halkalarının inşası ile ilgili detaylı bir araştırma yapılmıştır. Sonra skew polinom halkaları üzerindeki skew devirli kodlar ile ilgili tanım ve teoremler derinlemesine incelenip bu kodların cebirsel yapısının ve özelliklerinin çalışılması amaçlanmaktadır. Son olarak ise , kuantum hata düzelten kodlar çalışılarak bu kodların elde edilme yöntemleri incelenecek ve bazı sonlu halkalar üzerindeki skew devirli kodlardan kuantum kodların nasıl elde edildiği araştırılacaktır.

2. GENEL KISIMLAR

Bu bölümde, sonradaki bölümlerde kullanılacak olan cebirsel yapılarla ilgili bazı kavramlar verilecektir. İlk olarak cebirsel kodlama teorisi ile ilgili temel bilgiler, kavramlar ve teoremler ifade edilecektir. Daha sonra skew polinom halkasının inşası verilerek skew devirli kodlar tanıtılacaktır.

2.1. HALKA VE CİSİM KAVRAMI

Tanım 2.1.1. R boş olmayan bir küme ve R'nin elemanları arasında "$+$" ve "$\cdot$" ile göstereceğimiz iki tane ikili işlem tanımlanmış olsun. Aşağıdaki şartlar sağlanıyorsa, $(R,+,\cdot)$ cebirsel yapısına **halka** adı verilir:

- $(R,+)$ bir değişmeli grup,
- Her $a,b,c \in R$ için $a\cdot(b\cdot c)=(a\cdot b)\cdot c$,
- Her $a,b,c \in R$ için $a\cdot(b+c)=a\cdot b+a\cdot c$ ve $(a+b)\cdot c=a\cdot c+b\cdot c$.

Bundan sonra kolaylık için "$a\cdot b$" yerine "ab" kullanılacaktır.

Tanım 2.1.2. R bir halka ve $a,b \in R$ olsun. $0_R \in R$, yani R'nin sıfırı "$+$" işlemine göre birim (etkisiz) elemanı olarak alınsın. Bu takdirde

- Eğer $1_R a = a1_R = a$ olacak şekilde $1_R \in R$ elemanı var ise R'ye **birimli halka**,
- Eğer her $a,b \in R$ için $ab=ba$ ise R'ye **değişmeli halka**,
- Eğer $ab=0_R$ iken $a=0_R$ veya $b=0_R$ ise R'ye **tamlık bölgesi**,
- Eğer $(R\backslash\{0_R\},\cdot)$ cebirsel yapısı bir grup ise R'ye **yarı cisim**,
- Eğer R değişmeli bir yarı cisim ise R'ye **cisim**

denir.

Tanım 2.1.3. $(R,+,\cdot)$ bir halka ve S, R'nin boştan farklı bir alt kümesi olsun. Eğer S, R'deki "$+$" ve "$\cdot$" işlemlerine göre kapalı ise S'ye R'nin **alt halkası** denir.

Tanım 2.1.4. $(R,+,\cdot)$ bir halka ve J, R'nin boştan farklı bir alt kümesi olsun. Her $a \in J$ ve her $r \in R$ için eğer $ar \in J$ ise J'ye R'nin bir **sağ ideali** ve $ra \in J$ ise J'ye R'nin bir **sol ideali** denir. J, hem sağ hem sol ideal ise J'ye R'nin bir **ideali** denir.

Tanım 2.1.5. R değişmeli bir halka ve J, R'nin bir ideali olsun. $J = \langle a \rangle$ olacak şekilde bir $a \in R$ elemanı varsa J'ye R'nin **esas ideali** denir.

R bir halka ve R'nin bir ideali J olsun. $a,b \in R$ için:

$$"a \equiv b \Longleftrightarrow a-b \in J"$$

şeklinde tanımlanan "$\equiv$" bağıntısı R üzerinde bir denklik bağıntısıdır. Bu bağıntıyla ortaya çıkan bütün denklik sınıflarının kümesini $R/J = \{a+J \mid a \in R\}$ ile gösterelim. Bu küme üzerinde tanımlanan iki işlem "$+$" ve "$\cdot$" olmak üzere, her $a+J, b+J \in R/J$ için

$$(a+J)+(b+J) = (a+b)+J \tag{2.1}$$

$$(a+J)\cdot(b+J) = ab+J \tag{2.2}$$

şeklinde tanımlanır.

Tanım 2.1.6. R bir halka ve J, R'nin bir ideali olsun. R/J kümesi 2.1 ve 2.2'de tanımlanan işlemlere göre bir halkadır, bu halka **bölüm halkası** olarak adlandırılır. Eğer R birimli bir halka ve birimi 1_R ise R/J halkası da birimlidir ve birimi 1_R+J dır. Eğer R değişmeli ise R/J de değişmelidir.

Tanım 2.1.7. R birimli bir halka, R'nin birimi 1_R ve R'nin sıfırı 0_R olmak üzere $n \cdot 1_R = 0_R$ eşitliğini sağlayan en küçük pozitif n tam sayısına R halkasının **karakteristiği** denir. Böyle bir n tam sayısı yok ise R'nin karakteristiği sıfır olarak tanımlanır.

Teorem 2.1.8. Bir tamlık bölgesinin karakteristiği ya sıfırdır ya da asaldır.

Sonuç 2.1.9. Bir cismin karakteristiği ya sıfırdır ya da bir asal sayıdır.

Teorem 2.1.10. p bir asal sayı ve n bir doğal sayı olsun. Karakteristiği p olan bir cismin eleman sayısı $q = p^n$'dir ve bu cisim F_q ile gösterilir.

Önerme 2.1.11. F, karakteristiği p olan bir cisim ve $x, y \in F$ olsun. Bu durumda

i) $(x+y)^p = x^p + y^p$

ii) $(x-y)^p = x^p - y^p$

dır.

İspat. i) F, karakteristiği p olan bir cisim ve $x, y \in F$ olsun. Binom teoremine göre

$$(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j} \tag{2.3}$$

dır. Burada

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} \tag{2.4}$$

sayısı p'nin bir katıdır. $j = 1$ için

$$\binom{p}{j} = \binom{p}{1} = \frac{p!}{1!(p-1)!} = p$$

sağlanır.

$2 \leq j < p$ için $p \nmid j!$ dır. $p \mid j!$ olsa bu durumda $p \mid j(j-1)\dots 1$ olup bu durum $2 \leq j < p$ ve p'nin asal sayı olması ile çelişir. Dolayısıyla $p \nmid j!$ ve böylece $(p, j!) = 1$ dır. Bu durumda $\binom{p}{j}$ bir tam sayı olduğundan $\frac{(p-1)(p-2)\dots(p-j+1)}{j!}$ bir tam sayıdır. Üstelik $(p, j!) = 1$ olduğundan

$$1 = qp + j!r$$

olacak şekilde $q, r \in \mathbb{Z}$ vardır. Bu eşitliğin her iki tarafı $c_j := \frac{(p-1)(p-2)\dots(p-j+1)}{j!}$ ile çarpılırsa

$$c_j = qpc_j + j!rc_j$$

elde edilir. Buradan

$$c_j = q\binom{p}{j} + j!rc_j$$

olup

$$\begin{aligned}\binom{p}{j} &= \frac{1}{q}(c_j - c_j j!r) \\ &= \frac{c_j}{q}(1 - j!r) \\ &= \frac{c_j}{q}qp \\ &= pc_j\end{aligned}$$

elde edilir. Böylece $p \mid \binom{p}{j}$ olduğundan

$$\binom{p}{1}xy^{p-1} = pxy^{p-1} = 0$$

ve

$$\sum_{j=2}^{p-1}\binom{p}{j}x^j y^{p-j} = \sum_{j=2}^{p-1} pc_j x^j y^{p-j} = 0$$

olup 2.3 eşitliğinden

$$(x+y)^p = x^p + y^p$$

elde edilir.

ii) $x - y = x + (-y)$ olarak yazılabildiğinden

$$(x-y)+y = \big(x+(-y)\big)+y = x+\big((-y)+y\big) = x$$

olup i) kısmından

$$\big((x-y)+y\big)^p = x^p \Rightarrow (x-y)^p + y^p = x^p \Rightarrow (x-y)^p = x^p - y^p$$

elde edilir.

Tanım 2.1.12. F bir cisim olsun ve $\theta : F \longrightarrow F$ fonksiyonu verilsin. Eğer her $a, b \in F$ için

$\theta(a+b) = \theta(a) + \theta(b)$.

$$\theta(ab) = \theta(a)\theta(b).$$

ise θ'ya bir **cisim homomorfizması** denir. Eğer θ homomorfizması birebir ve örten ise θ'ya bir **cisim otomorfizması** denir. Her $a \in F$ için $\theta^m(a) = a$ şartını sağlayan en küçük m pozitif tam sayısına ise θ'nın mertebesi denir ve kısaca $|\langle\theta\rangle| = m$ ile gösterilir. F cisminin θ tarafından sabit bırakılan elemanlarının kümesi, yani

$$K = \{a \in F \mid \theta(a) = a\} \tag{2.5}$$

kümesi F'nin bir alt cismidir.

Teorem 2.1.13. F, karakteristiği p olan bir cisim olsun. Her $x \in F$ için $\theta(x) = x^p$ şeklinde tanımlanan fonksiyon F'nin bir otomorfizmasıdır. Bu otomorfizmaya F'nin **Frobenius otomorfizması** denir.

İspat. $x, y \in F$ olsun. Bu durumda:

$$\theta(x+y) = (x+y)^p = x^p + y^p = \theta(x) + \theta(y)$$

ve

$$\theta(xy) = (xy)^p = \underbrace{(xy)(xy)\dots(xy)}_{p\text{-tane}} = x^p y^p = \theta(x)\theta(y)$$

olduğundan θ bir cisim homomorfizmasıdır. Her $x, y \in F$ için $\theta(x) = \theta(y) \Rightarrow x^p = y^p \Rightarrow x^p - y^p = 0 \Rightarrow (x-y)^p = 0 \Rightarrow x - y = 0 \Rightarrow x = y \Rightarrow$ θ birebirdir. θ birebir ve F sonlu olduğundan θ örtendir. θ bir cisim otomorfizmasıdır. Özel olarak bu otomorfizmaya **Frobenius otomorfizması** denir.

Tanım 2.1.14. F, birimi 1_F olan bir cisim ve V bir değişmeli grup olsun. $* : F \times V \longrightarrow V$ skaler çarpımı aşağıdaki koşulları sağlıyorsa, V'ye F üzerinde bir **vektör uzayı** denir. Her $f, f_1, f_2 \in F$ ve her $v, v_1, v_2 \in V$ için

- $f * v \in V$,
- $f * (v_1 + v_2) = f * v_1 + f * v_2$
  $(f_1 + f_2) * v = f_1 * v + f_2 * v$,

- $(f_1 f_2) * v = f_1 * (f_2 v)$,
- $1_F * v = v$.

V kümesi bir vektör uzayı ise V'nin bir elemanı vektör olarak adlandırılır.

Tanım 2.1.15. R, birimi 1_R olan bir halka ve M bir değişmeli grup olsun. $\star : R \times M \longrightarrow M$ skaler çarpımı aşağıdaki koşulları sağlıyorsa, M'ye R üzerinde bir **sol modül** veya **sol R-modül** denir. Her $r, r_1, r_2 \in R$ ve her $m, m_1, m_2 \in M$ için

- $r \star m \in M$,
- $r \star (m_1 + m_2) = r \star m_1 + r \star m_2$
  $(m_1 + m_2) \star r = m_1 \star r + m_2 \star r$,
- $(r_1 \star r_2) \star m = r_1 \star (r_2 \star m)$,
- $1_R \star m = m$.

Her cisim bir halka olduğundan, her vektör uzayını da bir modül olarak kabul edebiliriz. Bundan sonra kolaylık için "$r \star m$" yerine "rm" ve "$f * v$" yerine "fv" kullanılacaktır.

Tanım 2.1.16. R bir halka, M bir R-modül ve $N \subseteq M$ olsun. Eğer N bir R-modül ise N'ye M'nin bir **alt modülü** denir.

Önerme 2.1.17. R bir halka, M bir R-modül ve $N \subseteq M$ olsun. N'nin, M'nin bir alt modülü olması için gerek ve yeter koşul $r_1, r_2 \in R$ ve $n_1, n_2 \in N$ için

$$r_1 n_1 + r_2 n_2 \in N$$

olmasıdır.

Tanım 2.1.18. M bir R-modül ve $m \in M$ olmak üzere m elemanının ürettiği alt modül

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

dir. Eğer $M = \langle m \rangle$ olacak şekilde bir $m \in M$ var ise M'ye devirli modül denir.

Tanım 2.1.19. R bir halka, M bir R-modül ve $S \subseteq M$ olsun.

- $x_1, x_2, \ldots, x_n \in S$, $i, j \in \{1, 2, \ldots, n\}$ ve $i \neq j$ için $x_i \neq x_j$ olsun. $r_i \in R$ olmak üzere

  $$r_1 x_1 + r_2 x_2 + \cdots + r_n x_n = 0$$

  denkleminin tek çözümü $r_i = 0$ $(i = 1, 2, \ldots, n)$ ise S kümesine lineer bağımsız bir küme denir.

- $i = 1, 2, \ldots, n$ için $r_i \in R$ ve $x_i \in S$ olmak üzere her $m \in M$ için

  $$m = \sum_{i=1}^{n} r_i x_i$$

  sağlanıyorsa S, M'yi üretir denir.

Bu iki koşulu sağlayan bir S kümesine M'nin bir bazı denir. Bazı olan R-modüllere de **serbest modül** denir.

Örnek 2.1.20.

i) F bir cisim olmak üzere F^n, F- vektör uzayı bir serbest F-modüldür.

ii) Sıfır bölen içermeyen bir R halkası, bir serbest R-modüldür.

2.2. SONLU CİSİMLER ÜZERİNDE TANIMLI VEKTÖR UZAYI

Tanım 2.2.1. F_q, eleman sayısı q olan bir cisim olsun. Bu durumda uzunluğu n olan vektörlerin kümesi F_q^n olmak üzere

$$F_q^n = \{(v_1, v_2, \ldots, v_n) \mid v_i \in F_q,\ 0 \leq i \leq n\} \tag{2.6}$$

şeklinde gösterilir. F_q^n üzerinde iki işlem şu şekilde tanımlanır: $v = (v_1, v_2, \ldots, v_n), w = (w_1, w_2, \ldots, w_n) \in F_q^n$ ve $\lambda \in F_q$ olmak üzere toplama ve skaler ile çarpma işlemleri sırasıyla

- $v + w = (v_1 + w_1,\ v_2 + w_2,\ \ldots,\ v_n + w_n) \in F_q$
- $\lambda v = (\lambda v_1,\ \lambda v_2,\ \ldots,\ \lambda v_n) \in F_q$

dır. Tanımlanan bu işlemler altında F_q^n, F_q üzerinde bir vektör uzayıdır [6].

İspat. $v=(v_1,v_2,\ldots,v_n)$, $w=(w_1,w_2,\ldots,w_n)\in F_q^n$ ve $\alpha,\beta\in F_q$ olsun.

$(F_q,+)$ değişmeli bir gruptur.

$$\begin{aligned}(\alpha\beta)v &= ((\alpha\beta)v_1,(\alpha\beta)v_2,\ldots,(\alpha\beta)v_n)\\ &= (\alpha(\beta v_1),\alpha(\beta v_2),\ldots,\alpha(\beta v_n))\\ &= \alpha(\beta v_1,\beta v_2,\ldots,\beta v_n)\\ &= \alpha(\beta v)\end{aligned}$$

$$\begin{aligned}\alpha(v+w) &= \alpha(v_1+w_1,v_2+w_2,\ldots,v_n+w_n)\\ &= (\alpha(v_1+w_1),\alpha(v_2+w_2),\ldots,\alpha(v_n+w_n))\\ &= (\alpha v_1+\alpha w_1,\alpha v_2+\alpha w_2,\ldots,\alpha v_n+\alpha w_n)\\ &= (\alpha v_1,\alpha v_2,\ldots,\alpha v_n)+(\alpha w_1,\alpha w_2,\ldots,\alpha w_n)\\ &= \alpha v+\alpha w\end{aligned}$$

$$\begin{aligned}(\alpha+\beta)v &= ((\alpha+\beta)v_1,(\alpha+\beta)v_2,\ldots,(\alpha+\beta)v_n)\\ &= (\alpha v_1+\beta v_1,\alpha v_2+\beta v_2,\ldots,\alpha v_n+\beta v_n)\\ &= (\alpha v_1,\alpha v_2,\ldots,\alpha v_n)+(\beta v_1,\beta v_2,\ldots,\beta v_n)\\ &= \alpha v+\beta v\end{aligned}$$

$1\in F_q$ için $1(v_1,v_2,\ldots,v_n)=(v_1,v_2,\ldots,v_n)$ dir.

Tanım 2.2.2. V, F_q üzerinde bir vektör uzayı ve $\varnothing\neq C\subseteq V$ olsun. Bu takdirde

- Her $x,y\in C$ için $x+y\in C$,
- Her $\lambda\in F_q$ ve her $x\in C$ için $\lambda x\in C$

koşulları sağlanıyorsa C kümesine V'nin bir alt vektör uzayı denir [6].

Tanım 2.2.3.

i) V, F_q üzerine bir vektör uzayı ve $\lambda_1,\lambda_2,\ldots,\lambda_n\in F_q$ olsun. $v_1,v_2,\ldots,v_n\in V$ vektörlerinin bir lineer kombinasyonu $\lambda_1v_1+\lambda_2v_2+\cdots+\lambda_nv_n$ şeklinde yazılır.

ii) $\lambda_1v_1+\lambda_2v_2+\cdots+\lambda_nv_n=0$ denkleminin tek çözümü $\lambda_1=\lambda_2=\ldots=\lambda_n=0$ ise $\{v_1,v_2,\ldots,v_n\}$ kümesi lineer bağımsızdır.

iii) $S = \{v_1, v_2, \ldots, v_n\} \subseteq V$ olsun. S'nin bütün lineer kombinasyonları kümesi $\langle S \rangle$ ile gösterilir ve

$$\langle S \rangle = \{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \mid \lambda_1, \lambda_2, \ldots, \lambda_n \in F_q\} \tag{2.7}$$

şeklinde ifade edilir. $\langle S \rangle$ uzayına S'nin ürettiği alt vektör uzayı denir. Üstelik S kümesi $\langle S \rangle$ uzayının bir üreteç kümesidir [6].

Önerme 2.2.4. S kümesi V'nin bir alt vektör uzayı ise $\langle S \rangle = S$ dir.

Tanım 2.2.5. V, F_q üzerinde bir vektör uzayı olsun.

- $A = \{v_1, v_2, \ldots, v_n\}$ kümesi lineer bağımsız ve $V = \langle A \rangle$ ise A kümesine V vektör uzayının bir bazı denir.
- A bazının eleman sayısına V'nin boyutu denir ve $boy(V)$ ile gösterilir. A sonsuz eleman içeriyor ise $boy(V) = \infty$ olarak gösterilir [6].

Teorem 2.2.6. V, F_q üzerinde bir vektör uzayı olsun. $boy(V) = k$ ise

- V'deki vektörlerin sayısı tam olarak q^k'dır.
- V'nin tam $\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$ tane farklı bazı vardır.

koşulları sağlanır [8].

Tanım 2.2.7. $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in F_q^n$ olsun.

- x ile y vektörlerinin Öklid iç çarpımı veya standart iç çarpımı

$$\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \tag{2.8}$$

şeklinde tanımlanır.

- $\langle x, y \rangle = 0$ ise x ve y vektörleri birbirine diktir, denir.
- S, F_q^n'nin bir alt kümesi olmak üzere $S^{\perp} = \{x \in F_q^n \mid \langle x, s \rangle = 0\,, \forall s \in S\}$ kümesine S'nin dik tümleyeni denir.

NOT: $S \subseteq F_q^n$ herhangi bir küme olsun. $S^\perp$ kümesi her zaman F_q^n'nin bir alt uzayıdır. Ayrıca $\langle S \rangle^\perp = S^\perp$'dir [8].

Teorem 2.2.8. $S \subseteq F_q^n$ olmak üzere, $boy(\langle S \rangle) + boy(S^\perp) = n$'dir [8].

2.3. SKEW POLİNOM HALKASI

Skew polinom halkasının küme olarak bildiğimiz normal polinom halkasından temel farkı çarpma işlemidir. Polinom halkasında üzerinde tanımlanan çarpma işlemi değişmelidir ancak skew polinom halkasındaki çarpma işlemi değişmeli değildir. Değişmeli olmayan bu skew polinom halkaları ilk olarak 1933'te Oystein Ore tarafından çalışmıştır [10].

K sonlu bir cisim ve θ da K'nın, mertebesi m olan bir otomorfizması olsun, yani $|\langle \theta \rangle| = m$'dir. θ tarafından sabit bırakılan alt cisimi K_0 ile gösterirsek $K_0 = \{x \in K \mid \theta(x) = x\}$ şeklinde ifade edilir, bu durumda $m = [K : K_0]$ olur. Üstelik, p bir asal sayı ve $q = p^t$ olmak üzere eğer $K_0 = GF(q)$ eleman sayısı q olan sonlu cisim ise, bu durumda $K = |K_0|^m = GF(q^m)$'dir.

K üzerinde tanımlı

$$K[x,\theta] = \{a_0 + a_1 x + \cdots + a_n x^{n-1} \mid a_i \in K,\ 0 \leq i \leq n-1\} \tag{2.9}$$

polinom kümesini göz önüne alalım. $K[x,\theta]$ üzerinde toplama işlemi olarak normal polinom halkası üzerinde tanımlı toplama işlemini, çarpma işlemi olarak

$$\alpha x^i \beta x^j = \alpha \theta^i(\beta) x^{i+j} \tag{2.10}$$

Şeklinde tanımlanan çarpma işlemini göz önüne alalım. Tanımlanan bu işlem değişmeli değildir ve $K[x,\theta]$ kümesi adi toplama işlemi ve bu şekilde tanımlanan çarpma işlemi ile bir halka oluşturur ve bu halka **skew polinom halkası** olarak adlandırılır. $Aut(K)$, K cisminin otomorfileri kümesi olmak üzere $\theta \in Aut(K)$ özel olarak birim otomorfizma alınırsa elde edilen skew polinom halkası K üzerindeki normal polinom halkasına karşılık gelir, çünkü $\alpha x^i \beta x^j = \alpha \theta^i(\beta) x^{i+j} = \alpha \beta x^{i+j}$ olup polinomlar üzerinde tanımlı adi çarpma işlemine karşılık gelir, yani "$K[x,\theta] = K[x]$" olur. Ayrıca $K[x,\theta]$ halkası sıfır bölensizdir ve $K[x,\theta]$'nın birimleri kümesi K'dır [9].

$a_n \neq 0$ olmak üzere $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x,\theta]$ olsun. $f(x)$'e derecesi n olan bir polinom denir ve $\deg f(x) = n$ yazılır. Özel olarak sıfır polinomun derecesi eksi sonsuz olup "$\deg 0 = -\infty$" şeklinde ifade edilir.

Önerme 2.3.1. $f(x), g(x) \in K[x,\theta]$ olsun. Bu durumda

i) $\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$,

ii) $\deg(f(x)\,g(x)) = \deg f(x) + \deg g(x)$'dir [9].

Örnek 2.3.2. $F_4 = \{0,\, 1,\, \alpha,\, 1+\alpha\} = F_2[\alpha]/(\alpha^2+\alpha+1)$ karakteristiği 2 olan dört elemanlı cisimi alalım. F_4 üzerinde tanımlı Frobenius otomorfizması

$$\begin{aligned} \theta : F_4 &\longrightarrow F_4 \\ a &\longmapsto \theta(a) = a^2 \end{aligned}$$

şeklinde tanımlanır. Özel olarak

$$\begin{aligned} \theta(0) &= 0 \\ \theta(1) &= 1 \\ \theta(\alpha) &= \alpha^2 \equiv 1+\alpha \pmod{\alpha^2+\alpha+1} \\ \theta(1+\alpha) &= (1+\alpha)^2 = 1+2\alpha+\alpha^2 = 1+\alpha^2 \equiv \alpha \pmod{\alpha^2+\alpha+1} \end{aligned}$$

olarak elde edilir. F_4 üzerinde θ otomorfisi ile tanımlanan $F_4[x,\theta]$ skew polinom halkası

$$F_4[x,\theta] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in F_4,\ 0 \leq i \leq n-1\}$$

şeklinde ifade edilir. θ tarafından sabit bırakılan alt cisimi ise

$$K_0 = \{x \in F_4 \mid \theta(x) = x\} = \{0,1\}$$

olup θ'nın mertebesi $|\langle\theta\rangle| = 2$ olduğundan $[F_4 : K_0] = 2$ dir. Ayrıca

$$\begin{aligned} \alpha x \alpha^2 x &= \alpha\theta(\alpha^2)x^2 = \alpha\alpha x^2 = \alpha^2x^2 \\ \alpha^2 x \alpha x &= \alpha^2\theta(\alpha)x^2 = \alpha^2(1+\alpha)x^2 = \alpha x^2 \end{aligned}$$

olup çarpma işlemi değişmeli değildir.

Teorem 2.3.3. $K[x,\theta]$ skew polinom halkası ve $0 \neq f(x), g(x) \in K[x,\theta]$ herhangi iki polinom olsun. Bu durumda

$$g(x) = q(x)f(x) + r(x)\,;\ \deg r(x) \leq \deg f(x)$$

olacak şekilde tek türlü belirli $q(x)$, $r(x) \in K[x,\theta]$ vardır [9].

İspat. $\alpha_i, \beta_i \in K$ olmak üzere $K[x,\theta]$'daki $g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_t x^t$ ve $f(x) = \beta_0 + \beta_1 x + \cdots + \beta_s x^s$ polinomları için

$$\deg g(x) < \deg f(x)$$

ise $q(x) = 0$ ve $r(x) = g(x)$ olarak alınırsa

$$g(x) = q(x)f(x) + r(x)$$

sağlanır. Eğer

$$\deg g(x) \geq \deg f(x)$$

ise ispat $\deg g(x)$ üzerinden tümevarım ile yapılır. $\deg g(x) = 0$ için $g(x) = \alpha_0$ olur. Bu durumda $q(x) = 1$, $f(x) = \alpha_0$ ve $r(x) = 0$ alınırsa

$$g(x) = q(x)f(x) + r(x)$$

sağlanır. Şimdi $\deg g(x) \leq t-1$ için iddianın doğru olduğunu varsayalım ve $\deg g(x) = t$ için iddianın doğru olduğunu ispat edelim.

$$q(x) = \alpha_t \theta^{t-s}(\beta_s^{-1})x^{t-s}$$
$$r(x) = g(x) - q(x)f(x)$$

olarak alırsak, bu durumda

$$\begin{aligned} r(x) &= g(x) - q(x)f(x) \\ &= (\alpha_0 + \alpha_1 x + \cdots + \alpha_t x^t) - q(x)(\beta_0 + \beta_1 x + \cdots + \beta_s x^s) \\ &= (\alpha_0 + \alpha_1 x + \cdots + \alpha_{t-1} x^{t-1} + \alpha_t x^t) - q(x)\beta_0 - q(x)\beta_1 x - \cdots - q(x)\beta_{s-1} x^{s-1} - q(x)\beta_s x^s \\ &= (\alpha_0 + \alpha_1 x + \cdots + \alpha_{t-1} x^{t-1} + \alpha_t x^t) - q(x)\beta_0 - q(x)\beta_1 x - \cdots - q(x)\beta_{s-1} x^{s-1} \\ &\quad - \alpha_t \theta^{t-s}(\beta_s^{-1}) x^{t-s} \beta_s x^s \end{aligned}$$

$$\begin{aligned} &= (\alpha_0 + \alpha_1 x + \cdots + \alpha_{t-1} x^{t-1} + \alpha_t x^t) - q(x)\beta_0 - q(x)\beta_1 x - \cdots - q(x)\beta_{s-1} x^{s-1} \\ &\quad - \alpha_t \theta^{t-s}(\beta_s^{-1}) \theta^{t-s}(\beta_s) x^{s+t-s} \\ &= \alpha_0 + \alpha_1 x + \cdots + \alpha_{t-1} x^{t-1} + \underline{\alpha_t x^t} - q(x)\beta_0 - q(x)\beta_1 x - \cdots - q(x)\beta_{s-1} x^{s-1} - \underline{\alpha_t x^t} \\ &= \delta_0 + \delta_1 x + \cdots + \delta_{t-1} x^{t-1} \end{aligned}$$

olup $\deg r(x) = t - 1$ olur. Tümevarım hopitezine göre $r(x)$ için teoremin ifadesi doğru olduğundan

$$r(x) = q_1(x)f(x) + r_1(x);\ \deg r_1(x) \leq \deg f(x)$$

olacak şekilde tek türlü belirli $q_1(x), r_1(x) \in K[x,\theta]$ vardır. Kabulden $q(x) = \alpha_t \theta^{t-s}(\beta_s^{-1}) x^{t-s}$ ve $r(x) = g(x) - q(x)f(x)$ olduğundan

$$\begin{aligned} g(x) &= q(x)f(x) + r(x) \\ &= (\alpha_t \theta^{t-s}(\beta_s^{-1}) x^{t-s}) f(x) + q_1(x)f(x) + r_1(x) \\ &= \left(\alpha_t \theta^{t-s}(\beta_s^{-1}) x^{t-s} + q_1(x)\right) f(x) + r_1(x);\ \deg r_1(x) \leq \deg f(x) \end{aligned}$$

elde edilir. Şimdi bu yazılışın tek türlü olduğunu ispat edelim. $q(x)$, $q_1(x)$, $r(x)$, $r_1(x) \in K[x,\theta]$ için

$$\begin{aligned} g(x) &= q(x)f(x) + r(x);\ \deg r(x) \leq \deg f(x) \\ &= q_1(x)f(x) + r_1(x);\ \deg r_1(x) \leq \deg f(x),\ q(x) \neq q_1(x) \end{aligned}$$

şeklinde iki farklı yazılış olsa

$$\big(q(x)-q_1(x)\big)f(x)=r_1(x)-r(x)$$

olup $\deg\big(\big(q(x)-q_1(x)\big)f(x)\big)=\deg\big(r_1(x)-r(x)\big)$ olurdu, buradan

$$\deg\big(q(x)-q_1(x)\big)+\deg f(x)=\deg\big(r_1(x)-r(x)\big)\leq\max\{\deg r(x),\deg r_1(x)\}$$

çelişkisi elde edilirdi. O halde bu yazılış tek türlüdür.

Teorem 2.3.3'te verilen ifade $g(x)$ polinomunun $f(x)$ polinomu ile sağdan bölünmesi olarak adlandırılır. Soldan bölme de benzer olarak şu şekilde tanımlanır:

$$g(x)=f(x)q(x)+r(x);\ \deg r(x)\leq\deg f(x)$$

olacak şekilde tek türlü belirli $q(x),r(x)\in K[x,\theta]$ vardır.

Teorem 2.3.4. $K[x,\theta]$'nın herhangi bir sol (sağ) ideali esaes sol (sağ) idealdir [9].

İspat. I, $K[x,\theta]$'ın bir sol ideali ve $g(x)\in I$ herhangi bir polinom olsun. I'da derecesi en küçük olan sıfırdan farklı polinom $f(x)$ olmak üzere Teorem 2.3.3'e göre

$$g(x)=q(x)f(x)+r(x);\ \deg r(x)\leq\deg f(x)$$

olacak şekilde tek türlü belirli $q(x),r(x)\in K[x,\theta]$ vardır. Buradan

$$r(x)=g(x)-q(x)f(x)\in I$$

olup $f(x)$, I da derecesi en küçük, sıfırdan farklı bir polinomu olduğundan

$$r(x)=0$$

elde edilir. Böylece

$$g(x)=q(x)f(x)$$

bulunur ve

$$I = \{q(x)f(x) \mid q(x) \in K[x,\theta]\} = K[x,\theta]f(x)$$

elde edilir. Yani I ideali $K[x,\theta]$ halkasında bir esas sol idealdir. Benzer şekilde $K[x,\theta]$'nın sağ idealleri de esas ideallerdir.

O halde $K[x,\theta]$, değişmeli olmayan esas ideal bölgesidir. $K[x,\theta]$'nın bir ideali hem sağ hem sol ideal ise iki taraflı ideal olarak adlandırılır.

Önerme 2.3.5. $K[x,\theta]$'nın iki taraflı bir ideali I olsun. O halde

$$I = \{q(x)g(x) \mid q(x) \in K[x,\theta]\} = K[x,\theta]g(x)$$

$$I = \{f(x)q(x) \mid q(x) \in K[x,\theta]\} = f(x)K[x,\theta]$$

şeklinde olup $g(x) = sf(x)$ olacak şekilde K'da bir s aritmetik birim vardır [9].

İspat. I, $K[x,\theta]$'nın bir iki taraflı ideali olsun. Bu durumda

$$I = f(x)K[x,\theta] = K[x,\theta]g(x)$$

olduğundan

$$g(x) = f(x)s$$

ve

$$f(x) = tg(x)$$

olacak şekilde $s,t \in K[x,\theta]$ vardır.

$$tf(x) = t\big(tg(x)\big) \in I$$

olduğu için

$$tf(x) = f(x)t'$$

olacak şekilde bir $t' \in K[x,\theta]$ vardır. O halde

$$f(x) = tg(x) = tf(x)s = f(x)t's$$

olduğundan

$$f(x) - f(x)t's = 0 \Rightarrow f(x)\left(1 - t's\right) = 0$$

bulunur. $K[x,\theta]$ sıfır bölensiz ve $f(x) \neq 0$ olduğu için

$$1 - t's = 0 \Rightarrow t's = 1$$

olup s'nin bir aritmetik birim eleman olduğu elde edilir. Benzer şekilde t de bir aritmetik birim elemandır. Dolayısıyla

$$f(x) = tg(x)$$

elde edilir.

Teorem 2.3.6. $K[x,\theta]$ skew polinom halkası için $|\langle\theta\rangle| = m$, θ'nın sabit bıraktığı alt cisim K_0 ve $I = \langle f(x)\rangle$, $K[x,\theta]$'nın iki taraflı bir ideali olsun. Bu durumda $a_i \in K_0$, $a_0 \neq 0$ ve $t \in \mathbb{Z}^+ \cup \{0\}$ olmak üzere

$$f(x) = (a_0 + a_1x^m + a_2x^{2m} + \cdots + a_nx^{nm})x^t$$

şeklindedir.

İspat. $f(x) = a_0x^t + a_1x^{1+t} + a_2x^{2+t} + \cdots + a_nx^{n+t}$ şeklinde olduğunu varsayalım. Bu durumda

$$f(x) = (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)x^t = q(x)x^t$$

şeklinde ifade edilebilir, burada $q(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ olarak alınır. İlk olarak, x^t'nin ürettiği ideal çift taraflıdır çünkü $\delta \in K$ için $x^t\delta = \theta^t(\delta)x^t$ dır. İkinci olarak, $q(x)$'in ürettiği ideal çift taraflı olsun. Bu durumda her $\beta \in K$ için

$$\beta q(x) = q(x)\gamma$$

olacak şekilde uygun bir $\gamma \in K$ vardır, buradan

$$\begin{aligned}\beta q(x) &= \beta(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) \\ &= \beta a_0 + \beta a_1x + \beta a_2x^2 + \cdots + \beta a_nx^n\end{aligned}$$

ve

$$\begin{aligned}q(x)\gamma &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)\gamma \\ &= a_0\gamma + a_1x\gamma + a_2x^2\gamma + \cdots + a_nx^n\gamma \\ &= \gamma a_0 + \theta(\gamma)a_1x + \theta^2(\gamma)a_2x^2 + \cdots + \theta^n(\gamma)a_nx^n\end{aligned}$$

olup katsayıların karşılaştırılması ile

$$\beta = \gamma = \theta(\gamma) = \theta^2(\gamma) = \ldots = \theta^n(\gamma) \tag{2.11}$$

elde edilir. β elemanı keyfi olduğundan γ da keyfidir. $|\langle\theta\rangle| = m$ olduğundan Eşitlik 2.11'in gerçekleşmesi için x'in derecelerinin m'nin bir katı olması gerekir. O halde $q(x) \in K[x^m]$ olur, yani $q(x) = a_0 + a_1x^m + a_2x^{2m} + \cdots + a_nx^{nm}$ yazılır. Böylece x^t ve $q(x) = a_0 + a_1x^m + a_2x^{2m} + \cdots + a_nx^{nm}$'nin ürettikleri idealler çift taraflı olduğundan dolayısıyla, $q(x)x^t = f(x)$'in ürettiği ideal de çift taraflıdır.

Önerme 2.3.7. $K[x,\theta]$ skew polinom halkası için $|\langle\theta\rangle| = m$ ve θ'nın sabit bıraktığı alt cisim K_0 olsun. Bu durumda, skew polinom halkasının merkezi

$$Z(K[x,\theta]) = \{f(x) \in K[x,\theta] \mid f(x)g(x) = g(x)f(x)\,,\ g(x) \in K[x,\theta]\} = K_0[x^m] \tag{2.12}$$

şeklindedir [9].

İspat. $a(x) = a_0 + a_1x^m + \cdots + a_rx^{rm} \in K_0[x^m]$ ve $q(x) = q_0 + q_1x + \cdots + q_nx^n \in K[x,\theta]$ olsun. Bu durumda $|\langle\theta\rangle| = m$ olduğundan $t \in \mathbb{Z}$ ve $0 \leq i \leq n$ için $\theta^{mt}(q_i) = q_i$ dir. Üstelik $0 \leq i \leq r$ için

$$\theta(a_i) = \theta^2(a_i) = \ldots = \theta^n(a_i) = a_i$$

olur. Buradan

$$\begin{aligned}
a(x)q(x) &= (a_0 + a_1x^m + \cdots + a_rx^{rm})(q_0 + q_1x + \cdots + q_nx^n) \\
&= a_0q_0 + a_0q_1x + \cdots + a_0q_nx^n + a_1x^mq_0 + a_1x^mq_1x + \cdots + a_1x^mq_nx^n \\
&\quad + \cdots + a_rx^{rm}q_0 + a_rx^{rm}q_1x + \cdots + a_rx^{rm}q_nx^n \\
&= a_0q_0 + a_0q_1x + \cdots + a_0q_nx^n + a_1\theta^m(q_0)x^m + a_1\theta^m(q_1)x^{m+1} + \cdots + a_1\theta^m(q_n)x^{m+n} \\
&\quad + \cdots + a_r\theta^{rm}(q_0)x^{rm} + a_r\theta^{rm}(q_1)x^{rm+1} + \cdots + a_r\theta^{rm}(q_n)x^{rm+n} \\
&= a_0q_0 + a_0q_1x + \cdots + a_0q_nx^n + a_1q_0x^m + a_1q_1x^{m+1} + \cdots + a_1q_nx^{m+n} \\
&\quad + \cdots + a_rq_0x^{rm} + a_rq_1x^{rm+1} + \cdots + a_rq_nx^{rm+n}
\end{aligned}$$

bulunur. Benzer şekilde

$$\begin{aligned}
q(x)a(x) &= (q_0 + q_1x + \cdots + q_nx^n)(a_0 + a_1x^m + \cdots + a_rx^{rm}) \\
&= q_0a_0 + q_0a_1x^m + \cdots + q_0a_rx^{rm} + q_1xa_0 + q_1xa_1x^m + \cdots + q_1xa_rx^{rm} \\
&\quad + \cdots + q_nx^na_0 + q_nx^na_1x^m + \cdots + q_nx^na_rx^{rm} \\
&= q_0a_0 + q_0a_1x^m + \cdots + q_0a_rx^{rm} + q_1\theta(a_0)x + q_1\theta(a_1)x^{1+m} + \cdots + q_1\theta(a_r)x^{1+rm} \\
&\quad + \cdots + q_n\theta^n(a_0)x^n + q_n\theta^n(a_1)x^{n+m} + \cdots + q_n\theta^n(a_r)x^{n+rm} \\
&= q_0a_0 + q_0a_1x^m + \cdots + q_0a_rx^{rm} + q_1a_0x + q_1a_1x^{1+m} + \cdots + q_1a_rx^{1+rm} \\
&\quad + \cdots + q_na_0x^n + q_na_1x^{n+m} + \cdots + q_na_rx^{n+rm} \\
&= q_0a_0 + q_1a_0x + \cdots + q_na_0x^n + q_0a_1x^m + q_1a_1x^{1+m} + \cdots + q_na_1x^{n+m} \\
&\quad + \cdots + q_0a_rx^{rm} + q_1a_rx^{1+rm} + \cdots + q_na_rx^{n+rm}
\end{aligned}$$

elde edilir. O halde $a(x)q(x) = q(x)a(x)$ olup $Z(K[x,\theta])$'nın tanımından

$$K_0[x^m] \subseteq Z(K[x,\theta]) \tag{2.13}$$

elde edilir. Şimdi her $b(x) = b_0 + b_1x + \cdots + b_nx^n \in Z(K[x,\theta])$ ve her $a \in K[x,\theta]$ elemanı için $b(x)a = ab(x)$ olduğundan

$$\begin{aligned}
(b_0 + b_1x + \cdots + b_nx^n)a &= a(b_0 + b_1x + \cdots + b_nx^n) \\
b_0a + b_1xa + \cdots + b_nx^na &= ab_0 + ab_1x + \cdots + ab_nx^n \\
b_0a + b_1\theta(a)x + \cdots + b_n\theta^n(a)x^n &= ab_0 + ab_1x + \cdots + ab_nx^n
\end{aligned}$$

olup buradan

$$\theta(a) = \theta^2(a) = \ldots = \theta^n(a) = a$$

elde edilir. Bu durum ancak $b(x) \in K[x^m]$ olmasıyla gerçeklenir. Şimdi $x \in K[x,\theta]$ için $b(x)x = xb(x)$ olduğundan

$$\begin{aligned}
(b_0 + b_1x + \cdots + b_nx^n)x &= x(b_0 + b_1x + \cdots + b_nx^n) \\
b_0x + b_1x^2 + \cdots + b_nx^{n+1} &= xb_0 + xb_1x + \cdots + xb_nx^n \\
b_0x + b_1x^2 + \cdots + b_nx^{n+1} &= \theta(b_0)x + \theta(b_1)x^2 + \cdots + \theta(b_n)x^{n+1}
\end{aligned}$$

olur, böylece

$$\begin{aligned}
\theta(b_0) &= b_0 \\
\theta(b_1) &= b_1 \\
&\vdots \\
\theta(b_n) &= b_n
\end{aligned}$$

elde edilir. O halde $b_i \in K_0$ elde edilir ve $b(x) \in K[x^m]$ olduğundan $b(x) \in K_0[x^m]$ olup

$$Z(K[x,\theta]) \subseteq K_0[x^m] \tag{2.14}$$

bulunur. Sonuç olarak $Z(K[x,\theta]) = K_0[x^m]$ elde edilir.

Sonuç 2.3.8. $x^n - 1 \in K[x,\theta]$ ve $|\langle\theta\rangle| = m$ olsun. Bu durumda

i) $x^n - 1$'in ürettiği idealin çift taraflı olması için gerek ve yeter koşul $m \mid n$ olmasıdır,

ii) $x^n - 1 \in Z(K[x,\theta])$ olması için gerek ve yeter koşul $m \mid n$ olmasıdır

ifadeleri geçerlidir [5].

İspat. $x^n - 1 \in K[x,\theta]$, $|\langle\theta\rangle| = m$ ve $t \in \mathbb{Z}$ olmak üzere $x^t \in K[x,\theta]$ olsun.

i) Teorem 2.3.6'dan

$$\begin{aligned}\langle x^n-1\rangle \text{ çift taraflı bir idealdir } &\Leftrightarrow\ x^n-1\in K[x^m]x^t\\ &\Leftrightarrow\ x^n-1\in K[x^m]\\ &\Leftrightarrow\ n=rm,\ r\in\mathbb{N}\\ &\Leftrightarrow\ m\mid n\end{aligned}$$

elde edilir.

ii) Önerme 2.3.7'den

$$\begin{aligned}x^n-1\in Z(K[x,\theta])=K_0[x^m] &\Leftrightarrow\ x^n-1=x^{bm}-1 \text{ olacak şekilde bir } b \text{ tam sayı vardır}\\ &\Leftrightarrow\ n=bm\\ &\Leftrightarrow\ m\mid n\end{aligned}$$

elde edilir.

Örnek 2.3.9. Örnek 2.3.2'de alınan dört elemanlı cisim üzerinde tanımlı skew polinom halkası

$$F_4[x,\theta]=\{a_0+a_1x+\cdots+a_nx^n \mid a_i\in F_4\,,\ 0\le i\le n\}$$

olup yukarıdaki sonuca göre
n çifttir $\Leftrightarrow x^n-1$'in ürettiği ideal çift taraflıdır ve $x^n-1\in Z(F_4[x,\theta])$'dır.
n tektir $\Leftrightarrow x^n-1$'in ürettiği ideal çift taraflı değildir ve $x^n-1\notin Z(F_4[x,\theta])$'dır.

Örneğin x^2-1'in ürettiği ideal çift taraflıdır, çünkü $\alpha x^2+x+1\in F_4[x,\theta]$ için

$$\begin{aligned}(x^2-1)(\alpha x^2+x+1) &= x^2\alpha x^2+x^3+x^2-\alpha x^2-x-1\\ &= \theta^2(\alpha)x^4+x^3+x^2-\alpha x^2-x-1\\ &= \alpha x^4+x^3+x^2-\alpha x^2-x-1\end{aligned}$$

olup

$$\begin{aligned}(\alpha x^2+x+1)(x^2-1) &= \alpha x^2x^2-\alpha x^2+x^3-x+x^2-1\\ &= \alpha x^4+x^3+x^2-\alpha x^2-x-1\\ &= (x^2-1)(\alpha x^2+x+1)\end{aligned}$$

elde edilir. Diğer yandan x^5-1'in ürettiği ideal çift taraflı değildir, çünkü $\alpha x^2+x+1 \in F_4[x,\theta]$ için

$$\begin{aligned}(x^5-1)(\alpha x^2+x+1) &= x^5\alpha x^2+x^6+x^5-\alpha x^2-x-1\\ &= \theta^5(\alpha)x^7+x^6+x^5-\alpha x^2-x-1\\ &= \alpha^2x^7+x^6+x^5-\alpha x^2-x-1\end{aligned}$$

olup

$$\begin{aligned}(\alpha x^2+x+1)(x^5-1) &= \alpha x^2x^5-\alpha x^2+x^6-x+x^5-1\\ &= \alpha x^7+x^6+x^5-\alpha x^2-x-1\\ &\neq (x^5-1)(\alpha x^2+x+1)\end{aligned}$$

elde edilir.

2.4. CEBİRSEL KODLAMA TEORİSİ

$A=\{a_1,a_2,\ldots,a_q\}$ kümesini göz önüne alalım. Burada A kümesi **kod alfabesi**, A kümesinin bir elemanı bir **bit** olarak adlandırılır. $w_1,w_2,\ldots,w_n \in A$ olmak üzere $w=w_1w_2\ldots w_n$ şeklindeki bir diziye n uzunluklu q-lu bir kelime denir. w aynı zamanda $(w_1,w_2,\ldots,w_n)$ veya $(w_1w_2\ldots w_n)$ vektörü olarak da düşünülebilir.

Aynı n uzunluğa sahip q-lu kelimelerin boş olmayan bir C alt kümesine **q-lu blok kod** denir. C kümesinin her elemanına ise **kod kelimesi** adı verilir. C içindeki kod kelimelerinin sayısına C'nin büyüklüğü (size) denir ve $|C|$ ile gösterilir. Uzunluğu n ve eleman sayısı M olan bir kod (n,M) **kod** şeklinde ifade edilir.

Kod alfabesi olarak, q elemanlı bir sonlu cismin alındığını varsayalım ve bu cismi $F_q=$

$\{0,1,\ldots,q-1\}$ ile n uzunluklu q-lu elemanların kümesini de

$$F_q^n = \{(a_1a_2\ldots a_n) \mid a_i \in F_q,\ 1 \leq i \leq n\} \tag{2.15}$$

ile gösterelim. F_q^n kümesinin elemanları vektör veya kod kelimesi olarak adlandırılır. Bu kümenin eleman sayısı

$$|F_q^n| = |F_q|^n = q^n$$

dır. C, F_q^n kümesinin bir alt kümesi ise C'ye q-lu bir kod denir. Özel olarak iki elemanlı cisim olan $F_2 = \{0,1\}$ kod alfabesi üzerinde tanımlanan koda **ikili kod** (**binary code**) denir. Üç elemanlı $F_3 = \{0,1,2\}$ cismi alfabe olarak alınırsa, F_3 üzerindeki koda **üçlü kod** (**ternary code**) denir.

Örnek 2.4.1.

i) $C_1 = \{00,\ 01,\ 10,\ 00\} \subseteq F_2^2$ bir $(2,\ 4)$-kodudur.

ii) $C_2 = \{000,\ 011,\ 110,\ 101\} \subseteq F_2^3$ bir $(3,\ 4)$-kodudur.

iii) $C_3 = \{00000,\ 01101,\ 10110,\ 11011\} \subseteq F_2^5$ bir $(5,\ 4)$-kodudur.

Bir A alfabesi üzerinde n uzunluklu x ve y gibi iki kelime alalım. x ile y arasındaki **Hamming uzaklık**, x ve y'nin birbirinden farklı basamak sayısı olarak tanımlanır ve $d(x,y)$ şeklinde gösterilir. Buna göre $x = x_1x_2\ldots x_n$ ile $y = y_1y_2\ldots y_n$ arasındaki Hamming uzaklık

$$d(x,y) = d(x_1,y_1) + d(x_2,y_2) + \cdots + d(x_n,y_n)\ ;\quad d(x_i,y_i) = \begin{cases} 1, & x_i \neq y_i \\ 0, & x_i = y_i \end{cases}\ ;\quad 1 \leq i \leq n$$

şeklinde ifade edilebilir. Örnek 2.4.1'de verilen F_2^5 üzerindeki C_3 kodunun 01101 ile 11011 kod kelimelerinin arasındaki Hamming uzaklık

$$d(01101,\ 11011) = 1+0+1+1+0 = 3$$

iken F_2^3 üzerindeki C_2 kodunun 011 ile 101 kod kelimelerinin arasındaki Hamming uzaklık

$$d(011,\ 101) = 1+1+0 = 2$$

dir.

Önerme 2.4.2. x, y ve z bir A alfabesi üzerinde uzunluğu n olan kelimeler olsun. Buna göre, Hamming uzaklık bir metrik fonksiyonudur, yani

i) $d(x,y) = 0 \Leftrightarrow x = y$

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

iii) $d(x,y) \leq d(x,z) + d(z,y)$ (Üçgen eşitsizliği)

koşulları sağlanır.

İspat. Hamming uzaklık fonksiyonunun i), ii) ve iii) koşullarını gerçeklediğini gösterelim: x, y, z bir A alfabesi üzerinde uzunluğu n olan kelimeler olmak üzere

i) $$\begin{aligned} d(x,y) = 0 &\Leftrightarrow d(x_1,y_1) + d(x_2,y_2) + \cdots + d(x_n,y_n) = 0 \\ &\Leftrightarrow d(x_1,y_1) = 0, d(x_2,y_2) = 0, \ldots, d(x_n,y_n) = 0 \\ &\Leftrightarrow x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n \\ &\Leftrightarrow x = y \end{aligned}$$

ii) $$\begin{aligned} d(x,y) &= d(x_1,y_1) + d(x_2,y_2) + \cdots + d(x_n,y_n) \\ &= d(y_1,x_1) + d(y_2,x_2) + \cdots + d(y_n,x_n) \\ &= d(y,x) \end{aligned}$$

iii) $x = y \Rightarrow d(x,y) = 0 \leq d(x,z) + d(z,y).$

$x \neq y$ ise $x_i \neq y_i$ olacak şekilde en azından bir $i \in \{1,2,\ldots,n\}$ vardır. O halde üç farklı durum vardır, bu durumlar

$$\begin{cases} x_i \neq z_i \text{ ve } y_i \neq z_i \\ x_i \neq z_i \text{ ve } y_i = z_i \\ x_i = z_i \text{ ve } y_i \neq z_i \end{cases} \Longrightarrow d(x_i,y_i) = 1 \leq \begin{cases} 1+1 = 2 = d(x_i,z_i) + d(y_i,z_i) \\ 1+0 = 1 = d(x_i,z_i) + d(y_i,z_i) \\ 0+1 = 1 = d(x_i,z_i) + d(y_i,z_i) \end{cases}$$

şeklinde incelenir. Buradan

$$d(x,y) \leq d(x,z) + d(z,y)$$

elde edilir.

C, A alfabesi üzerinde bir kod ve C kodunun içinde en az iki kod kelimesi olsun. C kodun **minimum Hamming uzaklığı** $d(C)$ ile gösterilir ve

$$d(C) = \min \{d(x,y) \mid x,y \in C,\ x \neq y\} \tag{2.16}$$

olarak tanımlanır. Uzunluğu n, eleman sayısı M ve minimum Hamming uzaklığı d olan bir kod (n,M,d)-kodu olarak ifade edilir. Burada n, M ve d kodun parametreleri olarak adlandırılır.

s bir pozitif tam sayı ve C bir kod olsun. Eğer bir kod kelimesinde s veya s'den daha az sayıda hata meydana geldiğinde, ortaya çıkan kelime C'nin bir kod kelimesi değilse C koduna s **hata fark edebilen** bir kod adı verilir. Eğer C kodu s hata fark edip $s+1$ hatayı fark edemiyorsa C koduna **tam** s **hata fark edebilen** kod denir.

t bir pozitif tam sayı ve C bir kod olsun. Minimum uzaklık kodlaması t veya t'den daha az hatayı doğrulayabiliyorsa C koduna t **hata düzelten** kod adı verilir. Eğer t hata düzeltip $t+1$ hatayı düzeltemiyor ise, C koduna **tam** t **hata düzelten** kod adı verilir.

Örnek 2.4.1'de verilen C_1, C_2 ve C_3 kodlarında C_2 tam 1 hata fark edebilen koddur çünkü C_2'deki her kod kelimesinde 1 hata gelirse elde edilen kelime C_2'nin bir elemanı değildir. C_3 tam 1 hata düzelten koddur, çünkü C_3'teki her kod kelimesinde 1 hata meydana gelirse elde edilen kelime C_3'ün başka bir kod kelimesinden'1 hata ile elde edilememektedir.

Teorem 2.4.3. Bir C kodunun s hata fark edebilen kod olması için gerek ve yeter koşul $d(C) \geqslant s+1$ olmasıdır, yani eğer $d(C) = d$ ise C kodu tam $d-1$ hata fark edebilir.

İspat. $d(C) \geqslant s+1$ olduğunu varsayalım. $x \in C$ olsun. x kod kelimesinin en fazla s hata ile x' olarak iletildiğini varsayalım. Bu durumda

$$1 \leq d(x,x') \leq s < d(C) \ \Rightarrow\ d(x,x') < d(C)$$

olur. Aynı zamanda $d(C)$'nin tanımından

$$x' \notin C$$

elde edilir. O halde C kodu s hata fark edebilir.

Diğer yandan eğer $d(C) < s+1$, yani $d(C) \leq s$ ise

$$1 \leq d(c_1, c_2) = d(C) \leq s$$

olacak şekilde c_1, $c_2 \in C$ vardır. Bu durumda c_1 kod kelimesi $d(C)$ hatanın meydana gelmesi ile c_2 olarak, yani C'deki diğer bir kod kelimesi olarak ulaşabilir. Böylece C, s hata fark edebilen kod değildir. Dolayısıyla C kodu s hata fark edebiliyorsa $d(C) \geqslant s+1$ dir.

$d(C) = d$ ve x kod kelimesinin tam d hata ile gönderildiğini varsayarsak

$$d(x, x') = d = d(C)$$

olacağından x' elemanının C'nin elemanı olup olmadığı belirlenemez. Dolayısıyla C kodu tam $d-1$ hata fark edebilen koddur.

Teorem 2.4.4. Bir C kodunun t hata düzelten kod olması için gerek ve yeter koşul $d(C) \geqslant 2t+1$ olmasıdır, yani eğer $d(C) = d$ ise C kodu tam $\lfloor | \frac{d-1}{2} | \rfloor$ hata düzelten koddur.

İspat. $d(C) \geqslant 2t+1$ olduğunu varsayalım. $x \in C$ olsun. x gönderilirken en fazla t hata meydana geldiğini ve x' olarak elde edildiğini varsayalım. Bu durumda $d(x, x') \leq t$. Bu durumda $y \in C \backslash \{x\}$ kod kelimesi için üçgen eşitsizliğinden

$$d(x, y) \leq d(x, x') + d(x', y)$$

olup

$$2t+1 \leq d(x, y) \leq t + d(x', y)$$

bulunur. Buradan

$$2t+1 \leq t + d(x', y)$$

$\Rightarrow\ t+1 \leq d(x',y)$

$\Rightarrow\ d(x,x') \leq t < d(x',y)$

elde edilir. Böylece, eğer minimum uzaklık kodlaması kullanılıyorsa, x', x olarak (yani doğru olarak) düzeltilecektir. O halde C kodu t hata düzeltir.

2.4.1. Lineer Kodlar

q bir asal sayının kuvveti, F_q alfabe kümesi q elemanlı $GF(q)$ Galois cismi ve $V(n,q)$ vektör uzayı F_q^n sıralı n-lilerin kümesi olarak göz önüne alınsın. Ayrıca bir $(x_1,x_2,\ldots,x_n)$ vektörü $x_1x_2\ldots x_n$ olarak yazılacaktır. $GF(q)$ üzerindeki bir **lineer kod** bir n pozitif tam sayısı için $V(n,q)$ vektör uzayının bir alt uzayıdır. Dolayısıyla bir lineer kodun bir elemanı, kod kelimesi yerine vektör olarak da adlandırılabilir. C kümesi $V(n,q)$ vektör uzayının boştan farklı bir alt kümesi olsun. Bu durumda $\varnothing \neq C \subseteq F_q^n$ alt kümesinin bir lineer kod olabilmesi için gerek ve yeter koşul

i) Her $x,y \in C$ için $x+y \in C$,

ii) Her $x \in C$ ve her $\lambda \in F_q$ için $\lambda x \in C$

olmasıdır. Özel olarak $F_2 = \{0,1\}$ kümesinin elemanları ile oluşturulan bir ikili kodun lineer olması için gerek ve yeter koşul kümedeki herhangi iki kod kelimesinin toplamının yine o kümenin içindeki bir kod kelimesi olmasıdır.

Eğer C, $V(n,q)$ vektör uzayının k boyutlu bir alt uzayı ise, C lineer koduna $[n,\ k]$ kod denir. Üstelik bu gösterilişe kodun minimum uzaklığı olan d eklenmek istenirse o halde C kodu $[n,\ k,\ d]$ ile gösterilir.

Eğer C, $V(n,q)$ vektör uzayının bir alt uzayı ise C tam olarak q^k tane vektör içerdiğinden q-lu bir $[n,\ k,\ d]$ kodu aslında q-lu $(n,\ q^k,\ d)$ kodudur. Fakat tersi doğru olmayabilir. Örneğin; $(11,\ 24,\ 5)$ kodu lineer değildir, çünkü 24 sayısı herhangi bir asalın kuvveti şeklinde yazılamaz.

Herhangi bir $x = x_1x_2\ldots x_n \in C$ kod kelimesi için $w(x)$ ile gösterilen x'in **Hamming ağırlığı**

x'in sıfırdan farklı bileşen sayısıdır ve

$$w(x) = |\{x_i \neq 0 \mid 0 \leq i \leq n\}| \tag{2.17}$$

şeklinde ifade edilir. Bir lineer kodun sıfırdan farklı kod kelimelerinin en küçük Hamming ağırlığına **kodun Hamming ağırlığı** denir ve

$$w(C) = \min\{w(x) \mid x \in C \backslash \{0\}\} \tag{2.18}$$

şeklinde ifade edilir. Lineer kodların en kullanışlı özeliklerinden biri, bir lineer kodun minimum Hamming uzaklığının verilen kodun Hamming ağırlığına eşit olmasıdır, yani

$$d(C) = w(C)$$

olmasıdır. Bu eşitliği ispatlamadan önce aşağıdaki sonucu ispatlayalım.

Önerme 2.4.1.1. $x, y \in F_q^n$ için $d(x,y) = w(x-y)$ dir.

İspat. $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in F_q^n$ olsun. $1 \leq i \leq n$ için

$$\begin{aligned} d(x_i, y_i) = &\begin{cases} 1 & ; x_i \neq y_i \\ 0 & ; x_i = y_i \end{cases} \\ =&w(x_i - y_i) \end{aligned}$$

olduğundan

$$\begin{aligned} d(x,y) &= d(x_1,y_1) + d(x_2,y_2) + \cdots + d(x_n,y_n) \\ &= w(x_1 - y_1) + w(x_2 - y_2) + \cdots + w(x_n - y_n) \\ &= w(x-y) \end{aligned}$$

elde edilir.

Teorem 2.4.1.2. Bir C lineer kodu için $d(C) = w(C)$ dir.

İspat. Bir kodun minimum Hamming uzaklığı tanımından $d(C) = d(x,y)$ olacak şekilde $x, y \in C$ vardır. Önerme 2.4.1.1'e göre $d(C) = d(x,y) = w(x-y) \geq w(C)$ dir. Diğer yandan

$w(C) = w(z) = d(z,0) \geq d(C)$ olacak şekilde bir $z \in C$ vardır. O halde $d(C) \geq w(C)$ ve $w(C) \geq d(C)$ olduğundan $d(C) = w(C)$ elde edilir.

Tanım 2.4.1.3. C, F_q üzerinde tanımlı lineer bir $[n, k]$ kodu olsun. Satırları C kodunun bir bazı olan matrise C kodunun bir **üreteç matrisi** denir ve genellikle G ile gösterilir. C bir $[n, k]$ lineer kod ise C'nin her üreteç matrisi $k \times n$ boyutlu olur.

Örnek 2.4.1.4.

i) Örnek 2.4.1'de verilen F_2^3 üzerindeki C_2 kodu için bir üreteç matrisi

$$G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

dir.

ii) F_q üzerinde tanımlı uzunluğu n olan tekrarlı kod (repetition code), üreteç matrisi

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}_{1\times n}$$

olan bir $[n, 1, n]$ koddur.

Bir vektör uzayının birden fazla bazı olduğundan ve bir lineer kodun kendisi de vektör uzayı olduğundan dolayı bir lineer kodun birden fazla üreteç matrisi de olabilir. Eğer sabit bir baz seçilirse, bu baz ile ifade edilen üreteç matrisinin satırlarının permütasyonu ile farklı üreteç matrisleri elde edilebilir. Bir lineer kodun üreteç matrisinin satırlarına sütunlarına elemanter satır-sütun işlemi yapılarak üreteç matrisi $[I_k \mid A]$ şeklinde özel bir forma getirilebilir ve oluşturulan bu forma **standart üreteç matrisi** denir, burada I_k, k boyutlu birim matris ve A, $k \times (n-k)$ formunda bir matristir.

Örnek 2.4.1.5. Örnek 2.4.1'de verilen F_2^3 üzerindeki $C_2 = \{000, 011, 110, 101\}$ kodu için bir üreteç matrisi

$$G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

ile verilir. G_2 üreteç matrisinin satırlarının yerleri değiştirildiğinde elde edilen üreteç matrisi

$$G_2' = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

standart üreteç matrisidir.

2.4.2. Dual Kod ve Kontrol Matrisi

C, F_q^n üzerinde tanımlı bir $[n, k]$ lineer kod olsun. F_q^n kümesinden alınan herhangi iki eleman $x = x_1x_2\ldots x_n$ ve $y = y_1y_2\ldots y_n$ olsun. Denklem 2.8'de verilen, x ile y'nin iç çarpımı olan

$$\begin{aligned} \langle x, y\rangle &= \sum_{i=1}^{n} x_i y_i \\ &= x_1y_1 + x_2y_2 + \cdots + x_ny_n \end{aligned}$$

skaleri göz önüne alalım. C'nin dual kodu $C^{\perp}$ ile gösterilir ve

$$C^{\perp} = \{x \in F_q^n \mid \langle x, y\rangle = 0\ ,\ \forall y \in C\} \tag{2.19}$$

şeklinde ifade edilir. F_q^n üzerinde tanımlı bir C lineer kodu için

- $C \subseteq C^{\perp}$ ise C'ye **kendine dik** (self-orthogonal) kod denir ve $dim(C) \leq \frac{n}{2}$ dir,
- $C = C^{\perp}$ ise C'ye **kendine dual** (self-dual) kod denir ve $dim(C) = \frac{n}{2}$ dir.

Önerme 2.4.2.1. C, F_q üzerinde tanımlı, üreteç matrisi G olan bir $[n, k]$ kod ve $x = x_1x_2\ldots x_n \in F_q^n$ bir vektör olsun. Bu durumda

$$x \in C^{\perp} \Leftrightarrow x\,G^T = 0$$

dır, burada G^T, G matrisinin transpozunu göstermektedir [6].

Teorem 2.4.2.2. C, F_q üzerinde tanımlı bir $[n, k]$ lineer kod olsun. Bu durumda $C^{\perp}$, F_q üzerinde $[n, n-k]$ lineer koddur [6].

Örnek 2.4.2.3. $C = \{0000, 0011, 1100, 1111\}$, F_2 üzerinde tanımlı, üreteç matrisi

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

olan bir $[4, 2]$ koddur. $C = C^{\perp}$ olup C kendine dual koddur.

$C^{\perp}$ dual kodunun üreteç matrisi H ile gösterilir ve H'ye C'nin **kontrol matrisi** denir. Bu matris dual kodun üreteci olduğundan dolayı standart formu da mevcuttur ve bu form $[B \mid I_{n-k}]$ şeklinde gösterilip B bir $(n-k) \times n$ formunda bir matristir.

Teorem 2.4.2.4. C, F_q üzerinde tanımlı ve standart üreteç matrisi $[I_k \mid A]$ şeklinde bir $[n, k]$ kod olsun. Bu durumda C'nin kontrol matrisi $[-A^T \mid I_{n-k}]$ şeklindedir [6].

Teorem 2.4.2.5. C, F_q^n üzerinde tanımlı bir lineer kod olsun. Bu durumda

- $|C| = q^{dim(C)}$
- $C^{\perp}$ bir lineer koddur ve $dim(C) + dim(C^{\perp}) = n$
- $(C^{\perp})^{\perp} = C$

dir [8].

2.4.3. Devirli Kodlar

Devirli kodlar, en önemli kod sınıflarından biri olup teorik açıdan zengin bir cebirsel yapıya sahiptirler. Bir devirli kodun bir polinom ile temsil edilebilmesi uygulamada oldukça önemli faydalar sağlamaktadır. Üstelik ikili Hamming kodlar, Golay kodlar ve BCH kodlar gibi birçok önemli kod, devirli kodlara denktir.

Tanım 2.4.3.1. Uzunluğu n olan bir C kodu için

i) C lineer kod,

ii) Her $x_1x_2 \ldots x_n \in C$ için $x_nx_1 \ldots x_{n-1} \in C$

koşulları sağlanıyorsa C'ye **devirli kod** denir.

Örnek 2.4.3.2.

i) $C = \{000, 011, 110, 101\}$

şeklinde verilen kod F_2 üzerinde bir devirli koddur.

ii) $C = \{0000, 1001, 0110, 1111\}$

şeklinde verilen kod F_2 üzerinde devirli kod değildir, çünkü $0110 \in C$ olmasına rağmen $0011 \notin C$ dir.

iii) $C = \left\{ \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \mid x_1, x_2 \in F_3 \right\}$
$= \{0000, 0112, 0221, 1011, 1120, 1202, 2022, 2101, 2210\}$

şeklinde verilen kod F_3 üzerinde bir devirli kod değildir, çünkü $0112 \in C$ olmasına rağmen $2011 \notin C$'dir.

Tanım 2.4.3.3. F bir cisim ve $a(x), b(x) \neq 0 \in F[x]$ herhangi iki polinom olsun. Bu durumda

$$a(x) = q(x)b(x) + r(x)\,;\ \deg r(x) \leq \deg b(x)$$

olacak şekilde tek türlü belirli $q(x), r(x) \in F[x]$ vardır [6].

Örnek 2.4.3.4. $a(x) = x^3 + x + 1,\ b(x) = x^2 + x + 1 \in F_2[x]$ olsun. $a(x)$ ile $b(x)$'e bölme algoritması uygulanırsa

$$x^3 + x + 1 = (x^2 + x + 1)(x - 1) + (x + 2)\ ;\ \deg(x + 2) = \deg(x - 1)$$

elde edilir.

Tanım 2.4.3.5. $g(x), h(x), f(x) \in F[x]$ olsun. Eğer $f(x) \mid g(x) - h(x)$ ise $g(x)$ ve $h(x)$ modülo $f(x)$ denktir denir ve

$$g(x) \equiv h(x) \pmod{f(x)} \tag{2.20}$$

şeklinde gösterilir.

F cismi olarak q elemanlı F_q sonlu cismi alınsın ve $f(x) \in F_q[x]$ ve $\deg f(x) = n$ olsun. Bu

durumda

$$\begin{aligned} F_q[x]/f(x) &= \{a(x) \in F_q[x] \mid \deg a(x) < n\} \\ &= \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_i \in F_q\,,\ 0 \le i \le n-1\} \end{aligned} \tag{2.21}$$

kümesini göz önüne alalım. Bu küme üzerinde

$$\begin{array}{rcl} +: \big(F_q[x]/f(x)\big) \times \big(F_q[x]/f(x)\big) & \longrightarrow & F_q[x]/f(x) \\ \big(a(x), b(x)\big) & \longmapsto & a(x)+b(x) \pmod{f(x)} \end{array}$$

ve

$$\begin{array}{rcl} \cdot: \big(F_q[x]/f(x)\big) \times \big(F_q[x]/f(x)\big) & \longrightarrow & F_q[x]/f(x) \\ \big(a(x), b(x)\big) & \longmapsto & a(x)b(x) \pmod{f(x)} \end{array}$$

şeklinde tanımlı işlemlere göre $F_q[x]/f(x)$, eleman sayısı q^n olan bir halkadır [6].

Örnek 2.4.3.6. $F_2[x]$ polinom halkasını ve x^2+x+1 polinomunu göz önüne alalım.

$$\begin{aligned} F_2[x]/(x^2+x+1) &= \{a(x) \in F_2[x] \mid \deg a(x) < 2\} \\ &= \{a_0 + a_1 x \mid a_0, a_1 \in F_2\} \\ &= \{0,\ 1,\ x,\ 1+x\} \end{aligned}$$

olur. $F_2[x]/(x^2+x+1)$ üzerinde tanımlanan toplama ve çarpma işlemlerine göre işlem tabloları aşağıdaki gibidir:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

$F_2[x]/(x^2+x+1)$ sadece bir halka değil aynı zamanda bir cisimdir, çünkü bu kümedeki sıfırdan farklı her elemanın çarpmaya göre tersi vardır.

Teorem 2.4.3.7. F bir cisim, F üzerindeki polinomların kümesi $F[x]$ ve $f(x) \in F[x]$ olsun. Bu durumda $F[x]/f(x)$ bölüm halkasının bir cisim olması için gerek ve yeter koşul $f(x)$ polinomunun indirgenemez olmasıdır [6].

Şimdi

$$F_q[x]/(x^n-1) = \{a(x) \in F_q[x] \mid \deg a(x) < n\}$$

kümesini göz önüne alalım, burada

$$\begin{aligned} x^n \equiv 1 \pmod{x^n-1} &\Rightarrow x^{n+1} \equiv x \pmod{x^n-1} \\ &\Rightarrow x^{n+2} \equiv x^2 \pmod{x^n-1} \\ &\dots \end{aligned}$$

dir. $f(x) = 5x^8 + 6x^5 + x^4$ polinomunun $\pmod{x^5-1}$ hangi kalan sınıfında olduğunu bulalım: $x^5 \equiv 1 \pmod{x^5-1}$, $x^6 \equiv x \pmod{x^5-1}$, $x^7 \equiv x^2 \pmod{x^5-1}$ ve $x^8 \equiv x^3 \pmod{x^5-1}$ olduğu kullanılarak

$$f(x) = 5x^8 + 6x^5 + x^4 \equiv 5x^3 + 6 + x^4 \pmod{x^5-1}$$

elde edilir.

Devirli kodların karşılık geldiği cebirsel yapı için

$$\pi : F_q^n \longrightarrow F_q[x]/(x^n-1)$$

olmak üzere

$$(a_0, a_1, \dots, a_{n-1}) \longmapsto a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$$

şeklinde verilen π tasviri göz önüne alınır. π tasviri bir F_q-lineer dönüşümdür. Bu tasvir ile F_q^n'deki bir

$$a = (a_0, a_1, \dots, a_{n-1})$$

vektörü yerine $F_q[x]/(x^n-1)$ deki

$$a(x) = \sum_{i=0}^{n-1} a_i x^i = a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$$

polinomu karşılık gelir [8].

Şimdi $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ polinomu x ile çarpıldığında

$$\begin{aligned} xa(x) &= x(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \\ &= a_0x + a_1x^2 + \cdots + a_{n-1}x^n \\ &= a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} \\ &= (a_{n-1}, a_0, \ldots, a_{n-2}) \end{aligned}$$

eşitliği elde edilir. Yani bu polinoma $(a_0, a_1, \ldots, a_{n-1})$ vektörü karşılık gelirken bu polinom x ile çarpıldığında elde edilen polinoma $(a_{n-1}, a_0, \ldots, a_{n-2})$ vektörü karşılık gelir. Dolayısıyla bir polinomu x ile çarpmak tek bir devirsel ötelemeye karşılık gelir ve benzer şekilde x^m ile çarpmak m tane devirsel ötelemeye karşılık gelir.

Teorem 2.4.3.8. $R_n = F_q[x]/(x^n - 1)$ halkası üzerindeki bir C kodunun devirli olabilmesi için gerek ve yeter koşul

i) $a(x), b(x) \in C$ için $a(x) + b(x) \in C$,

ii) $a(x) \in C$ ve $r(x) \in R_n$ için $r(x)a(x) \in C$

koşullarının sağlanmasıdır. Diğer bir deyişle, i) ve ii) koşulları $R_n = F_q[x]/(x^n - 1)$ halkası üzerindeki bir C kodunun devirli olabilmesi için gerek ve yeter koşulun C'nin R_n'nin bir ideali olması gerektiğini ifade eder.

İspat. $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in C$ ve $r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \in R_n$ olsun. C'nin R_n üzerinde devirli kod olduğunu varsayalım. O halde C bir lineer koddur ve i) koşulu sağlanır. C devirli olduğundan $xa(x) \in C, x(xa(x)) = x^2a(x) \in C, \ldots$ dır. Böylece

$$\begin{aligned} r(x)a(x) &= (r_0 + r_1x + \cdots + r_{n-1}x^{n-1})a(x) \\ &= r_0a(x) + r_1xa(x) + \cdots + r_{n-1}x^{n-1}a(x) \in C \end{aligned}$$

olup ii) koşulu da sağlanır.

Şimdi *i*) ve *ii*) koşullarının sağlandığını varsayıp $r(x) = x$ olarak alınırsa

$$\begin{aligned} r(x)a(x) &= xa(x) \\ &= x(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \\ &= a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} \in C \end{aligned}$$

elde edilir. Dolayısıyla $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$ dir, yani C kodu devirli koddur.

Teorem 2.4.3.9. $f(x) \in R_n$ olsun. Bu takdirde $f(x)$ polinomu tarafından üretilen polinomların kümesi

$$\langle f(x) \rangle = \{a(x)f(x) \mid a(x) \in R_n\}$$

bir devirli koda karşılık gelir.

İspat. $a(x), b(x) \in \langle f(x) \rangle$ ve $r(x) \in R_n$ olsun. Bu durumda $a(x) = r_1(x)f(x)$ ve $b(x) = r_2(x)f(x)$ olacak şekilde $r_1(x), r_2(x) \in R_n$ vardır. Buradan

i) $a(x) + b(x) = r_1(x)f(x) + r_2(x)f(x) = \big(r_1(x) + r_2(x)\big)f(x) \in \langle f(x) \rangle$

ii) $r(x)a(x) = r(x)\big(r_1(x)f(x)\big) = \big(r(x)r_1(x)\big)f(x) \in \langle f(x) \rangle$

elde edilir. Teorem 2.4.3.8'e göre $\langle f(x) \rangle$ bir devirli koda karşılık gelir.

Örnek 2.4.3.10. $R_3 = F_2[x]/(x^3 - 1)$ halkası üzerinde $1 + x^2$ polinomu ile üretilen devirli kodu bulalım.

$$\begin{aligned} R_3 = F_2[x]/(x^3 - 1) &= \{a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in F_2\} \\ &= \{0,\ 1,\ x,\ 1+x,\ x^2,\ 1+x^2,\ x+x^2,\ 1+x+x^2\} \end{aligned}$$

polinomlarına karşılık gelen vektörlerin kümesi

$$\begin{aligned} F_2^3 &= \{(a_0, a_1, a_2) \mid a_0, a_1, a_2 \in F_2\} \\ &= \{000, 001, 010, 011, 100, 101, 110, 111\} \end{aligned}$$

dir. Şimdi

$$\begin{aligned} C &= \langle 1+x^2 \rangle \\ &= \{a(x)(1+x^2) \mid a(x) \in R_3\} \end{aligned}$$

kümesini bulalım.

F_2^3	$a(x) \in R_3$	$a(x)(1+x^2) \pmod{x^3-1}$
000	0	0
001	x^2	$x^2+x^4 \equiv x+x^2$
010	x	$x+x^3 \equiv 1+x$
011	$x+x^2$	$x+x^3+x^2+x^4 \equiv 1+2x+x^2 \equiv 1+x^2$
100	1	$1+x^2$
101	$1+x^2$	$x^4+2x^2+1 \equiv 1+2x^2+x \equiv 1+x$
110	$1+x$	$1+x^2+x+x^3 \equiv 2+x+x^2 \equiv x+x^2$
111	$1+x+x^2$	$1+x+x^2+x^2+x^3+x^4 \equiv 0$

Tablo 2.1: $1+x^2$ polinomu ile üretilen, uzunluğu 3 olan ikili devirli kodun elemanları

Tablo 2.1'den

$$\begin{aligned} C = \langle 1+x^2 \rangle &= \{0,\, 1+x,\, 1+x^2,\, x+x^2\} \\ &= \{000,\, 011,\, 110,\, 101\} \end{aligned}$$

elde edilir. Teorem 2.4.3.9'a göre $C = \langle 1+x^2 \rangle$ bir devirli koddur.

Teorem 2.4.3.11. *C, R_n üzerinde sıfırdan farklı bir devirli kod olsun. Bu takdirde*

i) *C'de $g(x)$ ile gösterilen tek türlü belirli en küçük dereceli bir monik polinom vardır,*

ii) $C = \langle g(x) \rangle$,

iii) $g(x) \mid (x^n-1)$

dir [6].

İspat.

i) C'de $g(x)$ ve $h(x)$ en küçük dereceli iki monik polinom olsun. O halde $g(x)-h(x) \in C$ ve $\deg(g(x)-h(x)) < \deg g(x)$ dır. Eğer $g(x)-h(x) \neq 0$ ise uygun bir skaler ile $g(x)-$

$h(x)$ çarpılarak bir monik polinom elde edilebilir, bu ise $g(x)$'in en küçük dereceli olması ile çelişir.

ii) $a(x) \in C$ olsun. Bölme algoritmasına göre

$$a(x) = q(x)g(x) + r(x);\ \deg r(x) < \deg g(x)$$

olacak şekilde $q(x), r(x) \in R_n$ vardır. $r(x) = a(x) - q(x)g(x) \in C$ ve $\deg r(x) < \deg g(x)$ olduğundan $r(x) = 0$ elde edilir. O halde $a(x) = q(x)g(x)$ ve böylece $C = \langle g(x) \rangle$ elde edilir.

iii) Bölme algoritmasına göre

$$x^n - 1 = q_1(x)g(x) + r_1(x);\ \deg r_1(x) < \deg g(x)$$

olacak şekilde $q_1(x), r_1(x) \in R_n$ vardır. $r_1(x) = (x^n - 1) - q_1(x)g(x) \in C$ ve $\deg r_1(x) < \deg g(x)$ olduğundan $r_1(x) = 0$ elde edilir. Buradan $x^n - 1 = q_1(x)g(x)$ olup ve $g(x) \mid (x^n - 1)$ elde edilir.

Sonuç 2.4.3.12. F_q^n'de her devirli koda karşılık gelen, F_q üzerinde monik ve $x^n - 1$'i bölen bir polinom vardır.

Tanım 2.4.3.13. C, R_n üzerinde sıfırdan farklı bir devirli kod olsun. Teorem 2.4.3.11'de belirtilen $g(x)$ polinomuna C kodunun **üreteç polinomu** denir.

Bir C devirli kodunu, üreteç polinomundan farklı polinomlar da üretebilir, yani aynı kod birden çok polinom ile de üretilebilir, ancak Teorem 2.4.3.11'de verilen üreteç polinomu tektir.

Örnek 2.4.3.14. Örnek 2.4.3.10'da verilen C kodu, $1+x^2$ tarafından üretilir, ancak aşağıdaki tablo C kodunun $1+x$ polinomu ile de üretildiğini gösterir.

$$\begin{aligned} C = \langle 1+x^2 \rangle &= \langle 1+x \rangle \\ &= \{0,\ 1+x,\ 1+x^2,\ x+x^2\} \\ &= \{000,\ 011,\ 110,\ 101\} \end{aligned}$$

F_2^3	$a(x) \in R_3$	$a(x)(1+x) \pmod{x^3-1}$
000	0	0
001	x^2	$x^2+x^3 \equiv 1+x^2$
010	x	$x+x^2$
011	$x+x^2$	$x+x^2+x^2+x^3 = x+2x^2+x^3 \equiv 1+x$
100	1	$1+x$
101	$1+x^2$	$1+x+x^2+x^3 = 1+x+x^2+1 \equiv x+x^2$
110	$1+x$	$1+2x+x^2 \equiv 1+x^2$
111	$1+x+x^2$	$1+x+x^2+x+x^2+x^3 \equiv 0$

Tablo 2.2: $1+x$ polinomu ile üretilen, uzunluğu 3 olan ikili devirli kodun elemanları

Yani C'yi hem $1+x$ hem de $1+x^2$ üretir. Teorem 2.4.3.11'e göre derecesi en küçük olan monik polinom üreteç polinomu olarak adlandırılır ve tektir, buradaki C kodu için üreteç polinomu $g(x) = 1+x$ dir. Aynı zamanda $x^2+1 = (1+x)(x-1)$ sağlanır, yani $(x-1) \mid (x^2+1)$ tir.

Teorem 2.4.3.11'in iii) şıkkı, uzunluğu n olan bütün devirli kodların bulunabilmesi için bir yöntem verir. Bu yöntem için x^n-1 polinomunun çarpanlara ayrılışını bulmak yeterlidir.

Örnek 2.4.3.15. F_2 üzerinde, uzunluğu 3 olan bütün devirli kodları bulalım.

$$\begin{aligned} R_3 = F_2[x]/(x^3-1) &= \{a_0+a_1x+a_2x^2 \mid a_0,a_1,a_2 \in F_2\} \\ &= \{0,\ 1,\ x,\ 1+x,\ x^2,\ 1+x^2,\ x+x^2,\ 1+x+x^2\} \end{aligned}$$

x^3-1 polinomunun F_2 üzerindeki çarpanlara ayrılışı

$$x^3-1 = (x+1)(x^2+x+1)$$

şeklindedir. Bu durumda, F_2 üzerinde, uzunluğu 3 olan bütün devirli kodların üreteç polinomları

$$\begin{aligned} g_1(x) &= 1 \\ g_2(x) &= x+1 \\ g_3(x) &= x^2+x+1 \\ g_4(x) &= x^3-1 \end{aligned}$$

dir. Bu polinomlar ile üretilen devirli kodlar aşağıdaki tabloda verilmiştir:

Üreteç Polinomu	$C_i = \langle g_i(x) \rangle$	$C_i \subseteq F_2^3$
$g_1(x) = 1$	$C_1 = R_3$	$C_1 = \{000, 001, 010, 011, 100, 101, 110, 111\}$
$g_2(x) = x+1$	$C_2 = \{0,\ 1+x,\ 1+x^2,\ x+x^2\}$	$C_2 = \{000, 011, 110, 101\}$
$g_3(x) = x^2+x+1$	$C_3 = \{0, 1+x+x^2\}$	$C_3 = \{000, 111\}$
$g_4(x) = x^3-1$	$C_4 = \{0\}$	$C_4 = \{000\}$

Tablo 2.3: F_2 üzerinde, uzunluğu 3 olan tüm devirli kodlar

Teorem 2.4.3.16. $x^n - 1 \in F_q[x]$ polinomunun indirgenemez monik ayrılışı

$$\begin{aligned} x^n - 1 &= \prod_{i=1}^{r} P_i^{m_i}(x) \\ &= P_1^{m_1}(x) P_2^{m_2}(x) \cdots P_r^{m_r}(x) \end{aligned}$$

şeklindedir, burada $1 \leq i \leq r$ için $m_i \geq 0$ dır ve $P_i(x)$ monik indirgenemez polinomlardır. Teorem 2.4.3.11 ve Teorem 2.4.3.16'ya göre, F_q üzerinde, uzunluğu n olan tam olarak

$$\prod_{i=1}^{r}(m_i+1) = (m_1+1)(m_2+1)\cdots(m_r+1)$$

devirli kod vardır [8].

Lemma 2.4.3.17. r bir tam sayı olamk üzere, $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ uzunluğu n olan bir devirli kodun üreteç polinomu olsun. Bu durumda $g_0 \neq 0$ dır.

İspat. $g(x)$ üreteç polinomu olduğundan kod kelimelerine karşılık gelen polinom kümesindeki derecesi en küçük olan monik polinom $g(x)$ dir. $x^n \equiv 1 \pmod{x^n - 1}$ olduğundan $x^{n-1} \equiv x^{-1} \pmod{x^n - 1}$ olur. Eğer $g_0 = 0$ olsaydı,

$$\begin{aligned} x^{n-1} g(x) &= x^{-1} g(x) \\ &= x^{-1}(g_1 x + g_2 x^2 \cdots + g_r x^r) \\ &= g_1 + g_2 x + \cdots + g_r x^{r-1} \in C \end{aligned}$$

olurdu ki, $\deg(x^{n-1} g(x)) \leq r - 1 < r = \deg g(x)$ çelişkisi elde edilirdi. Dolayısıyla $g_0 \neq 0$ dır.

Teorem 2.4.3.18. C, F_q üzerinde, uzunluğu n olan bir devirli kod ve C'nin üreteç polinomu

$g(x) = g_0 + g_1 x + \cdots + g_r x^r$ olsun. Bu durumda $dim(C) = n - r$ dir ve C'nin üreteç matrisi

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & & g_r & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & & g_r \end{pmatrix}_{(n-r)\times n} = \begin{pmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ \vdots \\ x^{n-r-1} g(x) \end{pmatrix} \quad (2.22)$$

şeklindedir.

İspat. C kodu F_q üzerinde vektör uzayı olduğundan ve üreteç matrisinin satırları C'nin bazı olduğundan G'nin satırlarının lineer bağımsız olduğu ve C'yi ürettiği gösterilmelidir. İlk olarak G'nin satırlarının lineer bağımsız bir küme olduğunu ispat edip sonra bu kümenin F_q üzerinde C'yi ürettiğini ispat edelim.

Satırlardaki g_0'ların altındaki elemanlar 0 olduğundan G matrisi satır eşelon formdadır ve G'nin satırları lineer bağımsızdır.

Eğer $a(x) \in C$ ise $a(x) = q(x)g(x)$ olacak şekilde bir $q(x) \in F_q[x]$ polinomu vardır ve kod kelimelerinin uzunluğu n olduğundan $\deg a(x) < n$ dir. F_q cisim olduğundan

$$\deg a(x) = \deg q(x) + \deg g(x)$$

olur ve böylece

$$\begin{aligned} &\deg q(x) + \deg g(x) < n \\ &\Rightarrow \deg q(x) < n - \deg g(x) \\ &\Rightarrow \deg q(x) < n - r \end{aligned}$$

elde edilir. Buradan

$$\begin{aligned} a(x) &= q(x)g(x) \\ &= (q_0 + q_1 x + \cdots + q_{n-r-1} x^{n-r-1}) g(x) \\ &= q_0 \underline{g(x)} + q_1 \underline{xg(x)} + q_2 \underline{x^2 g(x)} + \cdots + q_{n-r-1} \underline{x^{n-r-1} g(x)} \end{aligned}$$

bulunur. O halde G'nin satrları C'yi üretir. Dolayısıyla, G matrisi, C'nin üreteç matrisidir ve

üreteç matrisinin satırlarının sayısı C'nin boyutu olduğundan $dim(C) = n - r$ dir.

Örnek 2.4.3.19. F_3 üzerinde, uzunluğu 4 olan bütün devirli kodları bulup bu kodların üreteç matrislerini yazalım.

$x^4 - 1$ polinomunun F_3 üzerinde çarpanlara ayrılışı

$$\begin{aligned} x^4 - 1 &= (x-1)(x^3 + x^2 + x + 1) \\ &= (x-1)(x-2)(x^2+1) \end{aligned}$$

şeklindedir. Uzunluğu 4 olan devirli kodların üreteç polinomları ve karşılık gelen üreteç matrisleri aşağıdaki tabloda verilmiştir.

Üreteç Polinomu	Üreteç Matrisi
$g_1(x) = 1$	$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I_4$
$g_2(x) = x - 1$	$G_2 = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$
$g_3(x) = x + 1$	$G_3 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$
$g_4(x) = x^2 + 1$	$G_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$
$g_5(x) = (x-1)(x+1) = x^2 - 1$	$G_5 = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$
$g_6(x) = (x-1)(x^2+1) = x^3 - x^2 + x - 1$	$G_6 = \begin{pmatrix} -1 & 1 & -1 & 1 \end{pmatrix}$
$g_7(x) = (x+1)(x^2+1) = x^3 + x^2 + x + 1$	$G_7 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$
$g_8(x) = x^4 - 1 = 0$	$G_8 = \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$

Tablo 2.4: Uzunluğu 4 olan devirli kodların üreteç polinomları ve karşılık gelen üreteç matrisleri

Örneğin **Tablo 2.4**'e göre

$$\begin{aligned} C_1 &= \left\{ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix} I_4 \mid a_i \in F_3\,,\ 1 \le i \le 4 \right\} \\ &= \left\{ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix} \mid a_i \in F_3\,,\ 1 \le i \le 4 \right\} \\ &= F_3^4 \end{aligned}$$

$$\begin{aligned} C_5 &= \left\{ \begin{pmatrix} a_1 & a_2 \end{pmatrix} G_5 \mid a_1, a_2 \in F_3 \right\} \\ &= \left\{ \begin{pmatrix} -a_1 & -a_2 & a_1 & a_2 \end{pmatrix} \mid a_1, a_2 \in F_3 \right\} \\ &= \{0000, 0201, 0102, 2010, 2211, 2112, 1020, 1221, 1122\} \end{aligned}$$

şeklinde yazılır.

Tanım 2.4.3.20. C bir $[n, k]$ devirli kod ve C'nin üreteç polinomu $g(x)$ olsun. Bu durumda, $g(x) \mid (x^n - 1)$ olduğundan

$$x^n - 1 = g(x)h(x)$$

olacak şekilde bir $h(x)$ polinomu vardır. $g(x)$ monik olduğundan, $h(x)$ polinomu da monik polinomdur. $\deg g(x) = n - k$ olduğundan $\deg h(x) = k$ dır. Bu şekilde tanımlanan $h(x)$ polinomu C'nin **kontrol polinomu** olarak adlandırılır.

Teorem 2.4.3.21. C, R_n üzerinde bir devirli kod, C'nin üreteç polinomu $g(x)$, C'nin kontrol polinomu $h(x)$ ve R_n'nin bir elemanı $c(x)$ olsun. Bu durumda

$$c(x) \in C \Leftrightarrow c(x)h(x) = 0$$

dır.

İspat. C, üreteç polinomu $g(x)$ ve kontrol polinomu $h(x)$ olan bir devirli kod olduğundan

$$x^n - 1 = g(x)h(x) \equiv 0 \pmod{x^n - 1}$$

dir. Bir $c(x) \in C$ elemanı için

$$c(x) = a(x)g(x)$$

olacak şekilde bir $a(x) \in R_n$ vardır. Buradan

$$c(x)h(x) = a(x)g(x)h(x) = a(x)0 = 0$$

elde edilir. Diğer taraftan, $c(x) \in R_n$ için $c(x)h(x) = 0$ olduğunu varsayalım. $c(x)$'in $g(x)$'e bölümü ile

$$c(x) = q(x)g(x) + r(x)\,;\ \deg r(x) < \deg g(x) = n-k$$

olacak şekilde tek türlü belirli $q(x)$, $r(x) \in R_n$ polinomları vardır. Buradan

$$\deg\left(r(x)h(x)\right) = \deg r(x) + \deg h(x) < n-k+k$$

olduğundan

$$\deg\left(r(x)h(x)\right) < n$$

elde edilir. Hipotez gereği $c(x)h(x) = 0$ olduğundan

$$\big(q(x)g(x) + r(x)\big)h(x) = q(x)g(x)h(x) + r(x)h(x) = 0$$

elde edilir. Buradan

$$q(x)(x^n - 1) + r(x)h(x) = 0$$

olup

$$r(x)h(x) \equiv 0 \pmod{x^n - 1}$$

bulunur. $\deg\left(r(x)h(x)\right) < n$ olduğundan

$$r(x)h(x) = 0$$

dır. $h(x) \neq 0$ ve $F_q[x]$ sıfır bölensiz olduğu için $r(x) = 0$ elde edilir. Bu durumda

$$c(x) = q(x)g(x) \in C$$

olup ispat bitmiş olur.

Teorem 2.4.3.22. C devirli $[n, k]$ kod ve C'nin kontrol polinomu $h(x) = h_0 + h_1x + \cdots + h_kx^k$ olsun. Bu durumda C'nin kontrol matrisi

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & & h_0 & 0 & \dots & 0 \\ & & \ddots & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & & h_0 \end{pmatrix}_{(n-k)\times n} \tag{2.23}$$

şeklindedir. Üstelik $C^{\perp}$, üreteç polinomu

$$\bar{h}(x) = h_k + h_{k-1}x + \cdots + h_0x^k$$

olan bir devirli koddur.

İspat. $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_kx^k + c_{k+1}x^{k+1} + \cdots + c_{n-1}x^{n-1} \in C$ olsun. Teorem 2.4.3.21'e göre

$$c(x) \in C \Leftrightarrow c(x)h(x) = 0$$

olduğundan

$$\begin{aligned} c(x)h(x) = {} & c_0h_0 + c_0h_1x + c_0h_2x^2 + \cdots + c_0h_{k-1}x^{k-1} + \underline{c_0h_kx^k} \\ & + c_1h_0x + c_1h_1x^2 + c_1h_2x^3 + \cdots + \underline{c_1h_{k-1}x^k} + \underline{\underline{c_1h_kx^{k+1}}} \\ & + c_2h_0x^2 + c_2h_1x^3 + c_2h_2x^4 + \cdots + \underline{\underline{c_2h_{k-1}x^{k+1}}} + c_2h_kx^{k+2} \\ & \vdots \\ & + \underline{c_kh_0x^k} + \underline{\underline{c_kh_1x^{k+1}}} + c_kh_2x^{k+2} + \cdots + c_kh_{k-1}x^{2k-1} + c_kh_kx^{2k} \\ & + \underline{\underline{c_{k+1}h_0x^{k+1}}} + c_{k+1}h_1x^{k+2} + c_{k+1}h_2x^{k+3} + \cdots + c_{k+1}h_{k-1}x^{2k} + c_{k+1}h_kx^{2k+1} \\ & \vdots \\ & + c_{n-1}h_0x^{n-1} + c_{n-1}h_1x^n + c_{n-1}h_2x^{n+1} + \cdots + c_{n-1}h_{k-1}x^{n+k-2} + c_{n-1}h_kx^{n+k-1} \\ & = 0 \end{aligned}$$

bulunur. Çarpımın sonucu sıfır olduğundan, özel olarak $x^k, x^{k+1}, \ldots, x^{n-1}$ terimlerinin katsayıları da sıfırdır. Bu katsayılar sırasıyla,

$$\begin{aligned}
c_0h_k + c_1h_{k-1} + \cdots + c_{k-1}h_1 + c_kh_0 &= 0 \longrightarrow \quad c \text{ ile } H\text{'nin birinci satırın iç çarpımı} \\
c_1h_k + c_2h_{k-1} + \cdots + c_kh_1 + c_{k+1}h_0 &= 0 \longrightarrow \quad c \text{ ile } H\text{'nin ikinci satırın iç çarpımı} \\
\vdots & \quad \vdots \\
c_{n-k-1}h_k + c_{n-k}h_{k-1} + \cdots + c_{n-2}h_1 + c_{n-1}h_0 &= 0 \longrightarrow \quad c \text{ ile } H\text{'nin } (n-k). \text{ satırın iç çarpımı}
\end{aligned}$$

olarak ifade edilir. Yani herhangi bir $(c_0, c_1, \ldots, c_{n-1}) \in C$ kod kelimesi H matrisinin satırları ile ortogonaldır. Buradan $C^{\perp}$'in tanımından H'nin satırlarının $C^{\perp}$'in kod kelimeleri olduğu elde edilir. Üstelik, $h(x)$, derecesi k olan bir monik polinom olup H'nin satırlarındaki h_k'ların bulunduğu sütunlarda h_k'nın altındaki elemanlar 0 olduğundan H matrisi satır eşelon formdadır. Dolayısıyla H'nin satırları lineer bağımsızdır. H matrisinin satır sayısı $n-k$ olup, $dim(C^{\perp}) = n-k$ olduğundan H, $C^{\perp}$'in bir üreteç matrisidir. Yani H, C için bir kontrol matrisidir.

Şimdi

$$\begin{aligned}
x^k h(x^{-1}) &= x^k(h_0 + h_1x^{-1} + \cdots + h_kx^{-k}) \\
&= h_0x^k + h_1x^{k-1} + \cdots + h_kx^0 \\
&= h_k + h_{k-1}x + \cdots + h_0x^k \\
&= \bar{h}(x)
\end{aligned}$$

olduğunu göz önüne alalım. $x^n - 1 = h(x)g(x)$ olduğundan

$$(x^{-1})^n - 1 = h(x^{-1})g(x^{-1})$$

olur ve eşitliğin her iki tarafı x^n ile çarpılarak

$$x^n(x^{-n} - 1) = x^k h(x^{-1})x^{n-k}g(x^{-1})$$

bulunur, buradan

$$1 - x^n = \bar{h}(x)x^{n-k}g(x^{-1})$$

olup $\bar{h}(x) \mid (x^n - 1)$ sonucu elde edilir. Teorem 2.4.3.18'e göre $\langle \bar{h}(x) \rangle$ bir devirli kod olup üreteç polinomu $\bar{h}(x)$ ve üreteç matrisi H'dir.

2.4.4. Kuantum Kodlar

Bu alt bölümde kuantum kodların daha iyi bir şekilde ifade edilebilmesi için gerekli bazı temel kavramlar verilecektir.

Tanım 2.4.4.1. K, $\mathbb{R}$ veya $\mathbb{C}$ olmak üzere X kümesi K üzerinde bir vektör uzayı olsun.

$$\langle \cdot, \cdot \rangle : X \times X \longrightarrow K$$

dönüşümü $x, y, z \in X$ ve $\alpha \in K$ için

- $\langle x, x \rangle \geq 0 \quad$ ve $\quad \langle x, x \rangle = 0 \Leftrightarrow x = 0$
- $\langle x, y \rangle = \overline{\langle y, x \rangle} \quad$ kompleks eşleniği
- $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$
- $\langle x + y,\, z \rangle = \langle x, z \rangle + \langle y, z \rangle$

özelliklerine sahip ise $\langle \cdot, \cdot \rangle$'ye X üzerinde bir iç çarpım ve $(X, \langle \cdot, \cdot \rangle)$ ikilisine de **iç çarpım uzayı** veya (**ön Hilbert uzayı**) denir.

Tanım 2.4.4.2. $(X, \langle \cdot, \cdot \rangle)$ iç çarpım uzayı ve $x \in X$ herhangi bir eleman olsun. Bu $x \in X$ vektörünün **normu**

$$\|x\| = \sqrt{\langle x, x \rangle}$$

şeklinde tanımlanır.

Tanım 2.4.4.3. Bir $(X, \langle \cdot, \cdot \rangle)$ iç çarpım uzayı yukarıda tanımlanan norma göre tam ise, yani $(X, \langle \cdot, \cdot \rangle)$ içindeki her Cauchy dizisi yukarıda tanımlanan norma göre bu uzayda yakınsak ise, bu iç çarpım uzayına **Hilbert uzayı** denir.

Kuantum kodlar kompleks sayılar cismi üzerinde tanımlı sonlu boyutlu Hilbert uzayları üzerinde tanımlanır. Klasik lineer kodların temel birimi bitler iken, kuantum kodların temel birimi kübitlerdir. q bir p asalının kuvveti olmak üzere bir kübit, q boyutlu kompleks vektör

uzayındaki bir vektör ile temsil edilir. q boyutlu Hilbert uzayı olarak $\mathbb{C}^q$ kompleks vektör uzayı göz önüne alınırsa $|\cdot\rangle$ notasyonu bir sütun vektörünü temsil etmek üzere bir kübit

$$|x\rangle = \begin{pmatrix} a_i \end{pmatrix}_{q\times 1} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_q \end{pmatrix}_{q\times 1}$$

şeklinde yazılır, burada $1 \leq i \leq q$ olmak üzere $a_i \in \mathbb{C}$ dır.

Bir $|x\rangle \in \mathbb{C}^q$ kübitinin kendisinden farklı $|y\rangle \in \mathbb{C}^q$ kübitine dönüşmesine kuantum hata denir.

Bir sütun vektörünü gösteren "$|\cdot\rangle$" notasyonu **ket** diye okunur. "$\langle\cdot|$" notasyonu ise ket vektörünün eşlenik transpozesidir ve **bra** diye okunur.

Bundan sonra $|\psi\rangle$ ile bir Hilbert uzayındaki bir vektör belirtilecektir. Hilbert uzaylarını daha iyi ifade edebilmek için matrislerin tensör çarpımının bilinmesi gerekir.

Tanım 2.4.4.4. A bir $m \times n$ matris ve B bir $r \times s$ matris olmak üzere A ile B matrislerinin **tensör çarpımı**, A'nın her bileşeninin B matrisi ile çarpımı olarak tanımlanır ve

$$A \otimes B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}$$

şeklinde gösterilir. $A \otimes B$ tensör çarpımı $mr \times ns$ tipinde bir matristir.

Örneğin, $\mathbb{C}^2$ Hilbert uzayı için

$$|x\rangle = \begin{pmatrix} 1+i \\ 1 \end{pmatrix} \implies \langle x| = \begin{pmatrix} 1-i & 1 \end{pmatrix}$$

olur. Bir boyutlu kompleks Hilbert uzayı kompleks sayılar kümesine karşılık gelir. İki

boyutlu Hilbert uzayının elemanları, bileşenleri kompleks sayılar olan

$$H = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \mid a,b \in \mathbb{C} \right\}$$

olarak gösterilen 2×1 şeklindeki sütun vektörleridir.

Boyutu 2 olan H Hilbert uzayı için ortonormal bir baz seçilebilir. Örneğin $a,b \in \mathbb{C}$ için her $\begin{pmatrix} a \\ b \end{pmatrix} \in H$ vektörü

$$\begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

şeklinde yazılabildiğinden $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ vektörleri, boyutu 2 olan H Hilbert uzayının bir bazıdır. Burada

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{ve} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

olarak alınırsa $\{|0\rangle, |1\rangle\}$ kümesi H Hilbert uzayı için bir baz olur. Bu durumda H Hilbert uzayı

$$H = \{a|0\rangle + b|1\rangle \mid a,b \in \mathbb{C}\}$$

şeklinde ifade edilir.

Örnek 2.4.4.5. $A = \begin{pmatrix} 1 & 3 \\ i & 2 \end{pmatrix}_{2\times 2}$ ve $B = \begin{pmatrix} 1 \\ i \end{pmatrix}_{2\times 1}$ olsun. A ile B'nin tensör çarpımı

$$A \otimes B = \begin{pmatrix} 1 & 3 \\ i & 2 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 1\binom{1}{i} & 3\binom{1}{i} \\ i\binom{1}{i} & 2\binom{1}{i} \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ i & 3i \\ i & 2 \\ -1 & 2i \end{pmatrix}_{4\times 2}$$

şeklindedir.

Genel olarak, $|\varphi\rangle$ ile $|\phi\rangle$ vektörlerinin tensör çarpımı için

$$|\varphi\rangle \otimes |\phi\rangle = |\varphi\rangle|\phi\rangle = |\varphi\phi\rangle$$

notasyonları kullanılabilir.

Örnek 2.4.4.6. $|0\rangle = \binom{1}{0}$ ve $|1\rangle = \binom{0}{1}$ olsun. Bu durumda

$$|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = \binom{1}{0} \otimes \binom{1}{0} = \begin{pmatrix} 1\binom{1}{0} \\ 0\binom{1}{0} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

$$|0\rangle \otimes |1\rangle = |0\rangle|1\rangle = \binom{1}{0} \otimes \binom{0}{1} = \begin{pmatrix} 1\binom{0}{1} \\ 0\binom{0}{1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

$$|1\rangle \otimes |0\rangle = |1\rangle|0\rangle = \binom{0}{1} \otimes \binom{1}{0} = \begin{pmatrix} 0\binom{1}{0} \\ 1\binom{1}{0} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

$$|1\rangle \otimes |1\rangle = |1\rangle|1\rangle = \binom{0}{1} \otimes \binom{0}{1} = \begin{pmatrix} 0\binom{0}{1} \\ 1\binom{0}{1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

olur.

$n = 2$ olmak üzere $2^n = 4$ boyutlu Hilbert uzayının elemanları, bileşenleri kompleks sayılar olan 4×1 şeklindeki sütun vektörleridir. Bu durumda bu uzayın elemanları $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$ olmak üzere $\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$ şeklindedir. Her $\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} \in \mathbb{C}^4$ için

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} = a_{00}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_{01}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_{10}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_{11}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

olarak yazılabildiğinden ve

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \; |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

olduğundan $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ vektörleri 2^2 boyutlu Hilbert uzayı için bir bazdır. Dolayısıyla bu uzay

$$H = \left\{ a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \mid a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C} \right\}$$

şeklinde ifade edilebilir. 2^n boyutlu Hilbert uzayda $|0\rangle$ ve $|1\rangle$ vektörlerinin tensör çarpımı aşağıdaki gibi genelleştirilebilir:

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle = |\overbrace{00\ldots00}^{n\text{-tane}}\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{2^n \times 1}$$

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle = |\overbrace{00\ldots01}^{n\text{-tane}}\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{2^n \times 1}$$

ve benzer şekilde

$$|1\rangle \otimes |1\rangle \otimes \cdots \otimes |0\rangle = |\overbrace{11\ldots10}^{n\text{-tane}}\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}_{2^n \times 1}$$

$$|1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle = |\overbrace{11\ldots11}^{n\text{-tane}}\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}_{2^n \times 1}$$

olarak ifade edilebilir. Herhangi bir $n > 0$ için 2^n boyutlu Hilbert uzayının bir bazı

$$\{\overbrace{|00\ldots00\rangle}^{n\text{-tane}}, \overbrace{|00\ldots01\rangle}^{n\text{-tane}}, \ldots, \overbrace{|11\ldots10\rangle}^{n\text{-tane}}, \overbrace{|11\ldots11\rangle}^{n\text{-tane}}\}$$

şeklindedir. Bu durumda 2^n boyutlu Hilbert uzayı

$$H = \{a_1|00\ldots00\rangle + a_2|00\ldots01\rangle + \cdots + a_{2^n-1}|11\ldots10\rangle + a_{2^n}|11\ldots11\rangle \mid a_i \in \mathbb{C},\ 1 \leq i \leq 2^n\}$$

şeklinde ifade edilebilir.

Tanım 2.4.4.7. $H = (X, \langle\cdot,\cdot\rangle)$ bir Hilbert uzayı ve $|\psi\rangle, |\phi\rangle \in H$ olsun. Bu durumda

- $|\psi\rangle$ ile $|\phi\rangle$ vektörlerin iç çarpımı $\langle\psi||\phi\rangle = \langle\psi|\phi\rangle$ şeklinde tanımlanır.
- Eğer $\langle\psi|\phi\rangle = 0$ ise $|\psi\rangle,\ |\phi\rangle$ ye diktir, denir.
- $|\psi\rangle$ vektörünün normu $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$ şeklinde gösterilir.
- Eğer $\||\psi\rangle\| = 1$ ise $|\psi\rangle$ vektörüne birim vektör denir.

Tanım 2.4.4.8. H bir Hilbert uzayı ve $B = \{|b_m\rangle\}$ kümesi H Hilbert uzayının bir bazı olsun.

Her $|b_n\rangle, |b_m\rangle \in B$ için

$$\langle b_n|b_m\rangle = \delta_{n,m} = \begin{cases} 0, & n \neq m \\ 1, & n = m \end{cases}$$

şartını sağlayan $B = \{|b_m\rangle\}$ kümesine H Hilbert uzayının bir **ortonormal bazı** denir [7].

Örnek 2.4.4.9. 2^2 boyutlu Hilbert uzayı için

$$\begin{aligned} B &= \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \\ &= \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\} \end{aligned}$$

kümesi bir ortonormal bazdır. Çünkü B kümesinden aldığımız her iki vektörün iç çarpımı 0 ve her vektörün normu 1 dir [7].

Tanım 2.4.4.10. H bir vektör uzayı olsun. $T : H \to H$ lineer dönüşümüne H vektör uzayı üzerinde tanımlı bir lineer operatör denir.

Örnek 2.4.4.11. H iki boyutlu Hilbert uzayı olsun.

$$\begin{aligned} T : H &\longrightarrow H \\ a|0\rangle + b|1\rangle &\longmapsto a|1\rangle + b|0\rangle \end{aligned}$$

şeklinde tanımlanan dönüşüm bir lineer dönüşüm olduğundan H vektör uzayı üzerinde bir lineer operatördür. Sonlu boyutlu bir vektör uzayında her lineer dönüşüm bir matris tarafından ifade edilebildiğinden T lineer operatörüne karşılık gelen matris $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ şeklindedir.

Yukarıda iki elemanlı F_2 sonlu cismi üzerinde yapılan inceleme q elemanlı F_q sonlu cismne de genişletilebilir. Dolayısıyla F_q üzerindeki bir kuantum kod tanımı aşağıdaki gibi verilir:

Tanım 2.4.4.12. q bir p asalının kuvveti olmak üzere q elemanlı sonlu cisim olarak F_q ve q boyutlu Hilbert uzayı olarak $\mathbb{C}^q$ kompleks vektör uzayı göz önüne alınsın. Her i için $x_i \in F_q$

olmak üzere $|x_1 x_2 \ldots x_n\rangle$, $\mathbb{C}^q$'nun bir ortonormal bazını göstersin. $(\mathbb{C}^q)^{\otimes n}$, $\mathbb{C}^q$'nun n-li tensör çarpımını göstersin, yani

$$(\mathbb{C}^q)^{\otimes n} = \underbrace{\mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_{n-\text{tane}}.$$

Bu durumda $(\mathbb{C}^q)^{\otimes n}$, q^n boyutlu bir Hilbert uzayıdır. F_q üzerinde uzunluğu n boyutu k olan bir kuantum kod $(\mathbb{C}^q)^{\otimes n}$'nin q^k boyutlu alt uzayı olarak tanımlanır ve $[[n,k]]_q$ ile gösterilir. Eğer kodun minimum uzaklığı d ise, yani kod en fazla $\lfloor \frac{d-1}{2} \rfloor$ hata düzeltebiliyorsa, bu kuantum hata düzelten kod $[[n,k,d]]_q$ ile gösterilir.

3. MALZEME VE YÖNTEM

Bu bölümde ilk olarak $R = F_q[u]/(u^{k+1} - u)$ halkasının temel özellikleri ve cebirsel yapısı incelenecektir. Sonra R halkası üzerinde tanımlı skew polinom halkası tanıtılacaktır. Daha sonra R halkası üzerindeki lineer kodlar ve skew devirli kodlar incelenecektir. Bu bölümde sunulan kavramlar ile ilgili daha ayrıntılı bilgi için [5]'de verilen çalışmaya bakılabilir.

3.1. R HALKASININ ÖZELLİKLERİ

k bir tam sayı, p tek bir asal ve $k \mid (p-1)$ olsun. Bu takdirde uygun bir m doğal sayısı için $q = p^m$ olmak üzere $R = F_q[u]/(u^{k+1} - u)$ şeklinde verilen kümeyi göz önüne alalım. Bu küme

$$\begin{aligned} R &= F_q[u]/(u^{k+1} - u) \\ &= F_q + uF_q + \cdots + u^k F_q \\ &= \{a_0 + ua_1 + \cdots + u^k a_k \mid a_i \in F_q\,, 0 \le i \le k\,,\ u^{k+1} = u\} \end{aligned} \tag{3.1}$$

şeklinde de ifade edilebilir. Polinomlardaki adi toplama ve çarpma işlemlerine göre R, karakteristiği p ve eleman sayısı q^{k+1} olan bir değişmeli halkadır.

Örnek 3.1.1. $p = 3$ olsun. $k \mid (p-1)$ olduğundan $k \in \{1,2\}$ dir. $m = 1$ ve $k = 1$ alırsak, bu durumda

$$\begin{aligned} R = F_3[u]/(u^2 - u) &= F_3 + uF_3 \\ &= \{a_0 + ua_1 \mid a_0, a_1 \in F_3\,,\ u^2 = u\} \\ &= \{0,\ 1,\ 2,\ u,\ 1+u,\ 2+u,\ 2u,\ 1+2u,\ 2+2u\} \end{aligned}$$

kümesi elde edilir. R, karakteristiği 3 ve eleman sayısı $3^2 = 9$ olan bir değişmeli halkadır. R halkasının işlem tabloları aşağıdaki gibidir:

$+ \pmod 3$	0	1	2	u	$1+u$	$2+u$	$2u$	$1+2u$	$2+2u$
0	0	1	2	u	$1+u$	$2+u$	$2u$	$1+2u$	$2+2u$
1	1	2	0	$1+u$	$2+u$	u	$1+2u$	$2+2u$	$2u$
2	2	0	1	$2+u$	u	$1+u$	$2+2u$	$2u$	$1+2u$
u	u	$1+u$	$2+u$	$2u$	$1+2u$	$2+2u$	0	1	2
$1+u$	$1+u$	$2+u$	u	$1+2u$	$2+2u$	$2u$	1	2	0
$2+u$	$2+u$	u	$1+u$	$2+2u$	$2u$	$1+2u$	2	0	1
$2u$	$2u$	$1+2u$	$2+2u$	0	1	2	u	$1+u$	$2+u$
$1+2u$	$1+2u$	$2+2u$	$2u$	1	2	0	$1+u$	$2+u$	u
$2+2u$	$2+2u$	$2u$	$1+2u$	2	0	1	$2+u$	u	$1+u$

Tablo 3.1: $F_3[u]/(u^2-u)$'nun toplam tablosu

$\cdot \pmod 3$	0	1	2	u	$2u$	$1+u$	$2+u$	$1+2u$	$2+2u$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	u	$2u$	$1+u$	$2+u$	$1+2u$	$2+2u$
2	0	2	1	$2u$	u	$2+2u$	$1+2u$	$2+u$	$1+u$
u	0	u	$2u$	u	$2u$	$2u$	0	0	u
$2u$	0	$2u$	u	$2u$	u	u	0	0	$2u$
$1+u$	0	$1+u$	$2+2u$	$2u$	u	1	$2+u$	$1+2u$	2
$2+u$	0	$2+u$	$1+2u$	0	0	$2+u$	$1+2u$	$2+u$	$1+2u$
$1+2u$	0	$1+2u$	$2+u$	0	0	$1+2u$	$2+u$	$1+2u$	$2+u$
$2+2u$	0	$2+2u$	$1+u$	u	$2u$	2	$1+2u$	$2+u$	1

Tablo 3.2: $F_3[u]/(u^2-u)$'nun çarpım tablosu

Örnek 3.1.2. $p=7$ olsun. $k \mid (p-1)$ olduğundan $k \in \{1,2,3,6\}$ dir. $m=2$ ve $k=3$ alırsak, bu durumda

$$\begin{aligned} R &= F_{49}[u]/(u^4-u) \\ &= F_{49} + uF_{49} + u^2F_{49} + u^3F_{49} \\ &= \{a_0 + ua_1 + u^2a_2 + u^3a_3 \mid a_0,a_1,a_2,a_3 \in F_{49},\ u^4 = u\} \end{aligned}$$

kümesi elde edilir. R, karakteristiği 7 ve eleman sayısı $49^4 = 5764801$ olan bir değişmeli halkadır.

Şimdi R halkasının yapısını inceleyelim. $0 \le i \le k$ olmak üzere $B_i \subseteq R$ alt kümelerini göz önüne alalım. Bu alt kümeler için $\oplus$ ve $\otimes$ işlemleri

$$B_0 \oplus B_1 \oplus \cdots \oplus B_k = \{b_0 + b_1 + \cdots + b_k \mid b_i \in B_i,\ 0 \le i \le k\} \tag{3.2}$$

$$B_0 \otimes B_1 \otimes \cdots \otimes B_k = \{(b_0, b_1, \ldots, b_k) \mid b_i \in B_i,\ 0 \leq i \leq k\} \tag{3.3}$$

şeklinde tanımlansın. R halkasının tanımında hipotez gereği k bir tam sayı, $p > 2$ bir asal sayı ve $k \mid (p-1)$ dir, bu durumda $p-1 = kt$ olacak şekilde bir t tam sayısı vardır. Buradan

$$\begin{aligned} u^{p-1} - 1 &= (u^k)^t - 1 \\ &= (u^k - 1)\left((u^k)^{t-1} + (u^k)^{t-2} + \cdots + 1\right) \end{aligned}$$

olup $f(u) = (u^k)^{t-1} + (u^k)^{t-2} + \cdots + 1$ alınırsa

$$\begin{aligned} u^{p-1} - 1 = (u^k - 1)f(u) \qquad &\Rightarrow \qquad u^p - u = (u^{k+1} - u)f(u) \\ &\Rightarrow \qquad (u^{k+1} - u) \mid (u^p - u) \end{aligned}$$

elde edilir. $F_p^* = F_p \backslash \{0\}$ kümesi çarpma işlemine göre, eleman sayısı $p-1$ olan bir grup olduğundan her $a \in F_p^*$ için $a^{p-1} = 1$ dir. Böylece her $a \in F_p$ için $a^p = a$ dır. Buradan her $a \in F_p$ için

$$(u-a) \mid (u^p - u)$$

dır. Dolayısıyla $0 \leq i \leq p-1$ olmak üzere $u_i \in F_p$ için

$$u^p - u = (u-u_0)(u-u_1)\ldots(u-u_{p-1})$$

yazılır. $u^p - u$, F_p'de lineer çarpanlarına ayrılabilir ve $(u^{k+1} - u) \mid (u^p - u)$ olduğundan $u^{k+1} - u$ da F_p üzerinde lineer çarpanlarına ayrılabilir, yani $0 \leq i \leq k$ için $v_i \in F_p$ ve $v_i \neq v_j$ olmak üzere

$$u^{k+1} - u = (u-v_0)(u-v_1)(u-v_2)\ldots(u-v_k) \tag{3.4}$$

şeklinde yazılabilir. Şimdi $0 \leq i \leq k$ için

$$e_i = \frac{u^{k+1} - u}{u - v_i} = \frac{(u-v_0)(u-v_1)(u-v_2)\ldots(u-v_k)}{u - v_i} \tag{3.5}$$

şeklinde tanımlansın. Bu durumda

$$e_0 = \frac{u^{k+1}-u}{u-v_0} = (u-v_1)(u-v_2)\dots(u-v_k) \in F_p[u] \tag{3.6}$$

$$e_1 = \frac{u^{k+1}-u}{u-v_1} = (u-v_0)(u-v_2)\dots(u-v_k) \in F_p[u] \tag{3.7}$$

$$\vdots$$

$$e_k = \frac{u^{k+1}-u}{u-v_k} = (u-v_0)(u-v_1)\dots(u-v_{k-1}) \in F_p[u] \tag{3.8}$$

e_i ve $u-v_i$ arasında ortak bölen olmadığı için, e_i ve $u-v_i$ aralarında asal polinomlardır ve

$$(e_i, u-v_i) = 1$$

şeklinde yazılır. En büyük ortak bölen, lineer kombinasyon olarak yazılabildiğinden

$$A_i e_i + B_i(u-v_i) = 1 \tag{3.9}$$

olacak şekilde $A_i, B_i \in F_p[u]$ vardır. Şimdi

$$\gamma_i := A_i e_i$$

olarak alınırsa

$$\begin{aligned}
\gamma_i^2 &= A_i e_i [1 - B_i(u-v_i)] \\
&= A_i e_i - A_i e_i B_i (u-v_i) \\
&= A_i e_i - A_i B_i (u^{k+1}-u) \\
&\equiv A_i e_i \pmod{u^{k+1}-u} \\
&= \gamma_i
\end{aligned} \tag{3.10}$$

elde edilir. Aynı zamanda $i \neq j$ için

$$\begin{aligned}\gamma_i\gamma_j &= A_i e_i A_j e_j \\ &= A_i \frac{u^{k+1}-u}{u-v_i} A_j \frac{u^{k+1}-u}{u-v_j} \\ &= A_i A_j \frac{u^{k+1}-u}{u-v_i}\frac{u^{k+1}-u}{u-v_j} \\ &\equiv 0 \pmod{u^{k+1}-u}\end{aligned} \tag{3.11}$$

elde edilir. Üstelik (3.10) ve (3.11) denklemlerinden

$$\begin{aligned}\prod_{i=0}^{k}(1-\gamma_i) &= (1-\gamma_0)(1-\gamma_1)\dots(1-\gamma_k) \\ &= 1-\sum_{i=0}^{k}\gamma_i\end{aligned}$$

olur. Diğer yandan

$$\begin{aligned}\prod_{i=0}^{k}(1-\gamma_i) &= \prod_{i=0}^{k}(1-A_i e_i) \\ &= \prod_{i=0}^{k} B_i(u-v_i) \\ &= (u^{k+1}-u)\prod_{i=0}^{k} B_i \\ &\equiv 0 \pmod{u^{k+1}-u}\end{aligned}$$

bulunur. Dolayısıyla

$$\prod_{i=0}^{k}(1-\gamma_i) = 1-\sum_{i=0}^{k}\gamma_i \equiv 0 \pmod{u^{k+1}-u}$$

olup

$$\sum_{i=0}^{k}\gamma_i \equiv 1 \pmod{u^{k+1}-u} \tag{3.12}$$

elde edilir. Bu durumda $\{\gamma_0, \gamma_1, \dots, \gamma_k\}$ kümesi, R'nin (3.12) özelliği sağlanacak şekilde

ikişer ikişer ortogonal ve idempotent olan sıfırdan farklı elemanların kümesidir. Dolayısıyla

$$R = \bigoplus_{i=0}^{k} \gamma_i R = \gamma_0 R \oplus \gamma_1 R \oplus \cdots \oplus \gamma_k R \tag{3.13}$$

elde edilir [5]. Şimdi $0 \leq i \leq k$ için $\gamma_i = A_i e_i$'nin modülo $u^{k+1} - u$ tek türlü belirli olduğunu gösterelim. Eğer $\gamma_i \neq \gamma_i'$ olacak şekilde $\gamma_i' = A_i' e_i$ olsaydı

$$A_i e_i + B_i(u - v_i) = 1$$

ve

$$A_i' e_i + B_i'(u - v_i) = 1$$

olacağından

$$(A_i - A_i')e_i - (B_i' - B_i)(u - v_i) = 0$$

veya buna denk olarak

$$(A_i - A_i')e_i = (B_i' - B_i)(u - v_i) \Rightarrow e_i \mid (B_i' - B_i)(u - v_i)$$

olurdu. $(e_i, u - v_i) = 1$ ve $e_i \mid (B_i' - B_i)(u - v_i)$ olduğundan $B_i' - B_i = e_i f$ olacak şekilde bir $f \in F_p[u]$ vardır. Böylece

$$\begin{aligned}(A_i - A_i')e_i &= e_i f(u - v_i) \\ &= \frac{u^{k+1} - u}{u - v_i} f(u - v_i) \\ &= (u^{k+1} - u)f \\ &\equiv 0 \pmod{u^{k+1} - u}\end{aligned}$$

bulunur ki buradan

$$A_i e_i \equiv A_i' e_i \pmod{u^{k+1} - u}$$

olup

$$\gamma_i \equiv \gamma_i' \pmod{u^{k+1}-u}$$

elde edilirdi. O halde tüm γ_i ler modülo $u^{k+1}-u$ tek türlü belirlidir.

Örnek 3.1.3. R halkası olarak

$$\begin{aligned} R =& F_9[u]/(u^3-u) \\ =& F_9 + uF_9 + u^2F_9 \\ =& \{a_0 + a_1u + a_2u^2 \mid a_i \in F_9\,,\, 0 \le i \le 2\} \end{aligned}$$

kümesini göz önüne alalım. $k=2,\ p=3$ durumunda $k \mid (p-1)$ olur. u^3-u polinomu F_3 üzerinde

$$u^3-u = u(u-1)(u-2)$$

şeklinde çarpanlarına ayrılır. $v_0=0$, $v_1=1$, $v_2=2$ için

- $e_0 = \dfrac{u^3-u}{u} = (u-1)(u-2) = u^2-2u-u+2 = u^2-1$
- $e_1 = \dfrac{u^3-u}{u-1} = u(u-2) = u^2-2u$
- $e_2 = \dfrac{u^3-u}{u-2} = u(u-1) = u^2-u$

olur. O halde $i=0,1,2$ için $A_ie_i + B_i(u-v_i) = 1$ olacak şekilde A_i, B_i leri hesaplayabiliriz.

$$\begin{aligned} * A_0 = 2 \in F_3[u] \text{ için } &\Longrightarrow A_0e_0 + B_0(u-v_0) = 1 \\ &\Longrightarrow 2(u^2-1) + B_0u = 1 \\ &\Longrightarrow 2u^2 - 2 + B_0u = 1 \\ &\Longrightarrow B_0u = 1+2-2u^2 \\ &\Longrightarrow B_0u = 3+u^2 \\ &\Longrightarrow B_0u = u^2 \\ &\Longrightarrow B_0 = u \in F_3[u] \end{aligned}$$

$$
\begin{aligned}
*\, A_1 = 2 \in F_3[u] \text{ için } &\Longrightarrow A_1 e_1 + B_1(u - v_1) = 1 \\
&\Longrightarrow 2(u^2 - 2u) + B_1(u-1) = 1 \\
&\Longrightarrow 2u^2 - 4u + B_1(u-1) = 1 \\
&\Longrightarrow B_1(u-1) = 1 + 4u - 2u^2 \\
&\Longrightarrow B_1(u-1) = u^2 + u + 1 \\
&\Longrightarrow B_1(u-1) = (u-1)(u-1) \\
&\Longrightarrow B_1 = u - 1 \in F_3[u]
\end{aligned}
$$

$$
\begin{aligned}
*\, A_2 = 2 \in F_3[u] \text{ için } &\Longrightarrow A_2 e_2 + B_2(u - v_2) = 1 \\
&\Longrightarrow 2(u^2 - u) + B_2(u-2) = 1 \\
&\Longrightarrow 2u^2 - 2u + B_2(u-2) = 1 \\
&\Longrightarrow B_2(u-2) = 1 + 2u - 2u^2 \\
&\Longrightarrow B_2(u-2) = u^2 + 2u + 1 \\
&\Longrightarrow B_2(u-2) = (u+1)(u+1) \\
&\Longrightarrow B_2(u-2) = (u-2)(u-2) \\
&\Longrightarrow B_2 = u - 2 \in F_3[u]
\end{aligned}
$$

elde edilir. Şimdi $i = 0,1,2$ için $\gamma_i = A_i e_i$ olmak üzere $\{\gamma_0, \gamma_1, \gamma_2\}$ kümesini inceleyelim. İlk olarak bu kümenin elemanları

$$
\begin{aligned}
\gamma_0 &= A_0 e_0 = 2(u^2 - 1) = 2u^2 - 2 \\
\gamma_1 &= A_1 e_1 = 2(u^2 - 2u) = 2u^2 - 4u = 2u^2 - u \\
\gamma_2 &= A_2 e_2 = 2(u^2 - u) = 2u^2 - 2u
\end{aligned}
$$

şeklindedir. Buradan

- $\gamma_i^2 \equiv \gamma_i \pmod{u^3 - u}$
  - $\gamma_0^2 = (2u^2-2)(2u^2-2) = 4u^4 - 8u^2 + 4 \equiv 2u^2 - 2 \pmod{u^3 - u}$.
  - $\gamma_1^2 = (2u^2-u)(2u^2-u) = 4u^4 - 4u^3 + u^2 \equiv 2u^2 - u \pmod{u^3 - u}$.
  - $\gamma_2^2 = (2u^2-2u)(2u^2-2u) = 4u^4 - 8u^3 + 4u^2 \equiv 2u^2 - 2u \pmod{u^3 - u}$

- $0 \leq i, j \leq 2$ ve $i \neq j$ için $\gamma_i \gamma_j \equiv 0 \pmod{u^3 - u}$ dır.
  - $\gamma_0\gamma_1 = (2u^2-2)(2u^2-u) = (1-u^2)(-u^2-u) = -u^2-u+u^4+u^3 = -u^2-u+u^2+u \equiv 0 \pmod{u^3-u}$
  - $\gamma_0\gamma_2 = (2u^2-2)(2u^2-2u) = (1-u^2)(u-u^2) = u-u^2-u^3+u^4 = u-u^2-u+u^2 \equiv 0 \pmod{u^3-u}$
  - $\gamma_1\gamma_2 = (2u^2-u)(2u^2-2u) = (-u^2-u)(u-u^2) = u^4-u^2 \equiv 0 \pmod{u^3-u}$
- $\sum_{i=0}^{2} \gamma_i = \gamma_0+\gamma_1+\gamma_2 = (2u^2-2)+(2u^2-u)+(2u^2-2u) \equiv 1 \pmod{u^3-u}$

özellikleri sağlanır. O halde $\{2u^2-2,\ 2u^2-u,\ 2u^2-2u\}$ kümesi ikişerli ortogonal ve idempotent elemanlardan oluşur.

Örnek 3.1.4. R halkası olarak

$$\begin{aligned} R &= F_{49}[u]/(u^4-u) \\ &= F_{49} + uF_{49} + u^2F_{49} + u^3F_{49} \\ &= \{a_0 + a_1u + a_2u^2 + a_3u^3 \mid a_i \in F_{49},\ 0 \leq i \leq 3\} \end{aligned}$$

kümesini göz önüne alalım. $k = 3,\ p = 7$ durumunda $k \mid (p-1)$ olur. u^4-u polinomu F_7 üzerinde

$$\begin{aligned} u^4-u &= u(u^3-1) \\ &= u(u-1)(u^2+u+1) \\ &= u(u-1)(u^2-6u+8) \\ &= u(u-1)(u-2)(u-4) \end{aligned}$$

şeklinde çarpanlarına ayrılır. $v_0 = 0$, $v_1 = 1$, $v_2 = 2$, $v_3 = 4$ için

- $e_0 = \dfrac{u^4-u}{u} = (u-1)(u-2)(u-4) = u^3-1$
- $e_1 = \dfrac{u^4-u}{u-1} = u(u-2)(u-4) = u^3+u^2+u$
- $e_2 = \dfrac{u^4-u}{u-2} = u(u-1)(u-4) = u^3-4u^2-u^2+4u = u^3-5u^2+4u = u^3+2u^2+4u$

- $e_3 = \dfrac{u^4-u}{u-4} = u(u-1)(u-2) = u^3-2u^2-u^2+2u = u^3-3u^2+2u = u^3+4u^2+2u$

olur. O halde $i = 0,1,2,3$ için $A_i e_i + B_i(u-v_i) = 1$ olacak şekilde A_i, B_i leri hesaplayabiliriz.

$$
\begin{aligned}
* A_0 = 6 \in F_7[u] \text{ için } &\Longrightarrow A_0 e_0 + B_0(u-v_0) = 1 \\
&\Longrightarrow 6(u^3-1) + B_0 u = 1 \\
&\Longrightarrow B_0 u = 1 - 6u^3 + 6 \\
&\Longrightarrow B_0 u = u^3 \\
&\Longrightarrow B_0 = u^2 \in F_7[u]
\end{aligned}
$$

$$
\begin{aligned}
* A_1 = 5 \in F_7[u] \text{ için } &\Longrightarrow A_1 e_1 + B_1(u-v_1) = 1 \\
&\Longrightarrow 5(u^3+u^2+u) + B_1(u-1) = 1 \\
&\Longrightarrow B_1(u-1) = 1 - 5u^3 - 5u^2 - 5u \\
&\Longrightarrow B_1(u-1) = 2u^3 + 2u^2 + 2u + 1 \\
&\Longrightarrow B_1(u-1) = (u-1)(2u^2+4u+6) \\
&\Longrightarrow B_1 = 2u^2 + 4u + 6 \in F_7[u]
\end{aligned}
$$

$$
\begin{aligned}
* A_2 = 5 \in F_7[u] \text{ için } &\Longrightarrow A_2 e_2 + B_2(u-v_2) = 1 \\
&\Longrightarrow 5(u^3+2u^2+4u) + B_2(u-2) = 1 \\
&\Longrightarrow B_2(u-2) = 1 - 5u^3 - 10u^2 - 20u \\
&\Longrightarrow B_2(u-2) = 2u^3 - 3u^2 + u + 1 \\
&\Longrightarrow B_2(u-2) = (u-2)(2u^2+u+3) \\
&\Longrightarrow B_2 = 2u^2 + u + 3 \in F_7[u]
\end{aligned}
$$

$$
\begin{aligned}
* A_3 = 5 \in F_7[u] \text{ için } &\Longrightarrow A_3e_3 + B_3(u - v_3) = 1 \\
&\Longrightarrow 5(u^3 + 4u^2 + 2u) + B_3(u-4) = 1 \\
&\Longrightarrow B_3(u-4) = 1 - 5u^3 - 20u^2 - 10u \\
&\Longrightarrow B_3(u-4) = 2u^3 + u^2 - 3u + 1 \\
&\Longrightarrow B_3(u-4) = (u-4)(2u^2 + 2u + 5) \\
&\Longrightarrow B_3 = 2u^2 + 2u + 5 \in F_7[u]
\end{aligned}
$$

elde edilir. Şimdi $i = 0,1,2,3$ için $\gamma_i = A_i e_i$ olmak üzere $\{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$ kümesini inceleyelim. İlk olarak bu kümenin elemanları

$$
\begin{aligned}
\gamma_0 &= A_0 e_0 = 6(u^3 - 1) = 6u^3 - 6 = 1 - u^3 \\
\gamma_1 &= A_1 e_1 = 5(u^3 + u^2 + u) = 5u^3 + 5u^2 + 5u \\
\gamma_2 &= A_2 e_2 = 5(u^3 + 2u^2 + 4u) = 5u^3 + 10u^2 + 20u = 5u^3 + 3u^2 - u \\
\gamma_3 &= A_3 e_3 = 5(u^3 + 4u^2 + 2u) = 5u^3 + 20u^2 + 10u = 5u^3 - u^2 + 3u
\end{aligned}
$$

şeklindedir.

- $\gamma_i^2 \equiv \gamma_i \pmod{u^4 - u}$ olduğunu gösterelim:
  - $\gamma_0^2 = (1-u^3)(1-u^3) = 1 - 2u^3 + u^6 \equiv 1 - u^3 \pmod{u^4 - u}$
  - $\gamma_1^2 = 5(u^3 + u^2 + u)5(u^3 + u^2 + u) = 25(u^6 + 2u^5 + 3u^4 + 2u^3 + u^2) = 25(3u^3 + 3u^2 + 3u) = 75(u^3 + u^2 + u) \equiv 5(u^3 + u^2 + u) \pmod{u^4 - u}$
  - $\gamma_2^2 = (5u^3 + 3u^2 - u)(5u^3 + 3u^2 - u) = u^2(5u^2 + 3u - 1)(5u^2 + 3u - 1) = u^2(2u^3 - u^2 - 2u + 1) = 2u^5 - u^4 - 2u^3 + u^2 = 2u^2 - u - 2u^3 + u^2 \equiv 5u^3 + 3u^2 - u \pmod{u^4 - u}$
  - $\gamma_3^2 = (5u^3 - u^2 + 3u)(5u^3 - u^2 + 3u) = u^2(4u^3 + 3u^2 - 2u + 2) = 4u^5 + 3u^4 - 2u^3 + 2u^2 = 4u^2 + 3u - 2u^3 + 2u^2 = -2u^3 - u^2 + 3u \equiv 5u^3 - u^2 + 3u \pmod{u^4 - u}$.
- $0 \leq i, j \leq 3$ ve $i \neq j$ için $\gamma_i \gamma_j \equiv 0 \pmod{u^4 - u}$ dır. Örneğin
  - $\gamma_0 \gamma_1 = (1-u^3)(5u^3 + 5u^2 + 5u) = 5u^3 + 5u^2 + 5u - 5u^3 u^3 - 5u^2 u^3 - 5uu^3 = 5u^3 + 5u^2 + 5u - 5u^3 - 5u^2 - 5u \equiv 0 \pmod{u^4 - u}$

- $\sum_{i=0}^{3}\gamma_i = \gamma_0+\gamma_1+\gamma_2+\gamma_3 = (6u^3-6)+(5u^3+5u^2+5u)+(5u^3+3u^2-u)+(5u^3-u^2+3u) = 21u^3+7u^2+7u-6 \equiv 1 \pmod{u^4-u}$

özelliği sağlanır. O halde $\{1-u^3,\ 5u^3+5u^2+5u,\ 5u^3+3u^2-u,\ 5u^3-u^2+3u\}$ kümesi ikişerli ortogonal ve idempotent elemanlardan oluşur.

Sonuç 3.1.5. p bir asal sayı, $k \mid (p-1)$ ve m bir doğal sayı olmak üzere $q = p^m$ olsun.

$$R = F_q[u]/(u^{k+1}-u) = F_q + uF_q + \cdots + u^kF_q = \{a_0+ua_1+\cdots+u^ka_k \mid a_i \in F_q\,, 0 \le i \le k\,,\ u^{k+1}=u\}$$

halkasının yukarıda tanımlanan $\{\gamma_0,\ \gamma_1,\ \ldots,\ \gamma_k\}$ alt kümesi için

$$R = \bigoplus_{i=0}^{k}\gamma_i R \cong \bigoplus_{i=0}^{k}\gamma_i F_q$$

dır. Bu durumda her $r \in R$ elemanı

$$r = \sum_{i=0}^{k}\gamma_i r_i = \gamma_0 r_0 + \gamma_1 r_1 + \cdots + \gamma_k r_k$$

olacak şekilde yazılır, burada $0 \le i \le k$ için $r_i \in F_q$ dur [4, Lemma 2.3].

3.1.1. R Üzerinde Tanımlı Skew Polinom Halkası

Bölüm 2.3.'te skew polinom halkasının cisimler üzerindeki inşası verildi. Bu alt bölümde özel olarak $R = F_q[u]/(u^{k+1}-u)$ halkası üzerinde tanımlı skew polinom halkasının inşası verilecektir.

Önerme 3.1.1.1. $0 \le i \le k$ için $r_i \in F_q$ olmak üzere $r_0+r_1u+\cdots+r_ku^k \in R$ ve $\theta \in Aut(F_q)$ olsun. Bu durumda

$$\begin{aligned} \Theta : R &\longrightarrow R \\ r_0+r_1u+\cdots+r_ku^k &\longmapsto \theta(r_0)+\theta(r_1)u+\cdots+\theta(r_k)u^k \end{aligned}$$

şeklinde tanımlı tasvir R'nin bir otomorfisidir. Bu şekilde tanımlanan $\Theta \in Aut(R)$, $\theta \in Aut(F_q)$'nun genişlemesidir.

İspat. $r = r_0+r_1u+\cdots+r_ku^k$, $b = b_0+b_1u+\cdots+b_ku^k \in R$ ve $\theta \in Aut(F_q)$ olsun. Bu durumda $0 \le i \le k$ için $r_i, b_i \in F_q$ olduğundan $\theta(r_i), \theta^{-1}(r_i), \theta(b_i), \theta^{-1}(b_i) \in F_q$

sağlanır.Ayrıca

$$u^{k+1} = u \Rightarrow u^{k+2} = u^2 \Rightarrow \cdots \Rightarrow u^{2k} = u^k$$

olduğunu göz önüne alarak Θ'nın R'nin bir otomorfisi olduğunu gösterelim.

i) $r = b \Leftrightarrow r_0 + r_1u + \cdots + r_ku^k = b_0 + b_1u + \cdots + b_ku^k$

$\Leftrightarrow 0 \leq i \leq k$ için $r_i = b_i$

$\Leftrightarrow \theta(r_i) = \theta(b_i)\ ;\ 0 \leq i \leq k$

$\Leftrightarrow \theta(r_0) + \theta(r_1)u + \cdots + \theta(r_k)u^k = \theta(b_0) + \theta(b_1)u + \cdots + \theta(b_k)u^k$

$\Leftrightarrow \Theta(r_0 + r_1u + \cdots + r_ku^k) = \Theta(b_0 + b_1u + \cdots + b_ku^k)$

$\Leftrightarrow \Theta(r) = \Theta(b)$

Yani Θ, iyi tanımlı ve birebir bir fonksiyondur.

ii) $r = r_0 + r_1u + \cdots + r_ku^k \in R$ olsun. $0 \leq i \leq k$ için $r_i \in F_q$ ve $\theta \in Aut(F_q)$ olduğundan $\theta^{-1}(r_i) \in F_q$ dir. Böylece $\theta^{-1}(r_0) + \theta^{-1}(r_1)u + \cdots + \theta^{-1}(r_k)u^k \in R$ elde edilir. Bu eleman için

$$\begin{aligned}\Theta\big(\theta^{-1}(r_0) + \theta^{-1}(r_1)u + \cdots + \theta^{-1}(r_k)u^k\big) &= \theta\big(\theta^{-1}(r_0)\big) + \theta\big(\theta^{-1}(r_1)\big)u + \ldots \\ &\quad + \theta\big(\theta^{-1}(r_k)\big)u^k \\ &= r_0 + r_1u + \cdots + r_ku^k = r\end{aligned}$$

elde edilir. Böylece Θ, örten bir fonksiyonudur.

iii) $\begin{aligned}\Theta(r+b) &= \Theta(r_0 + r_1u + \cdots + r_ku^k + b_0 + b_1u + \cdots + b_ku^k) \\ &= \Theta\big((r_0 + b_0) + (r_1 + b_1)u + \cdots + (r_k + b_k)u^k\big) \\ &= \theta(r_0 + b_0) + \theta(r_1 + b_1)u + \cdots + \theta(r_k + b_k)u^k \\ &= \big(\theta(r_0) + \theta(b_0)\big) + \big(\theta(r_1) + \theta(b_1)\big)u + \cdots + \big(\theta(r_k) + \theta(b_k)\big)u^k \\ &= \theta(r_0) + \theta(r_1)u + \cdots + \theta(r_k)u^k + \theta(b_0) + \theta(b_1)u + \cdots + \theta(b_k)u^k \\ &= \Theta(r_0 + r_1u + \cdots + r_ku^k) + \Theta(b_0 + b_1u + \cdots + b_ku^k) \\ &= \Theta(r) + \Theta(b).\end{aligned}$

O halde Θ, toplama işlemini korur.

$$\begin{aligned}
\text{iv)}\quad rb &= (r_0+r_1u+\cdots+r_ku^k)(b_0+b_1u+\cdots+b_ku^k)\\
&= r_0b_0+r_0b_1u+\cdots+r_0b_ku^k+r_1b_0u+r_1b_1u^2+\cdots+r_1b_ku^{k+1}\\
&\quad+\cdots+r_kb_0u^k+r_kb_1u^{k+1}+\cdots+r_kb_ku^{2k}\\
&= r_0b_0+r_0b_1u+\cdots+r_0b_ku^k+r_1b_0u+r_1b_1u^2+\cdots+r_1b_ku\\
&\quad+\cdots+r_kb_0u^k+r_kb_1u+\cdots+r_kb_ku^k\\
&= r_0b_0+(r_0b_1+r_1b_0+r_1b_k+r_kb_1)u+\cdots+(r_0b_k+r_kb_0+r_kb_k)u^k
\end{aligned}$$

elemanı için

$$\begin{aligned}
\Theta(rb) &= \Theta\big[r_0b_0+(r_0b_1+r_1b_0+r_1b_k+r_kb_1)u+\cdots+(r_0b_k+r_kb_0+r_kb_k)u^k\big]\\
&= \theta\big[r_0b_0\big]+\theta\big[r_0b_1+r_1b_0+r_1b_k+r_kb_1\big]u+\cdots+\theta\big[r_0b_k+r_kb_0+r_kb_k\big]u^k\\
&= \big[\theta(r_0)\theta(b_0)\big]+\big[\theta(r_0)\theta(b_1)+\theta(r_1)\theta(b_0)+\theta(r_1)\theta(b_k)+\theta(r_k)\theta(b_1)\big]u\\
&\quad+\cdots+\big[\theta(r_0)\theta(b_k)+\theta(r_k)\theta(b_0)+\theta(r_k)\theta(b_k)\big]u^k\\
&= \theta(r_0)\theta(b_0)+\theta(r_0)\theta(b_1)u+\cdots+\theta(r_0)\theta(b_k)u^k+\theta(r_1)\theta(b_0)u+\theta(r_1)\theta(b_1)u^2\\
&\quad+\cdots+\theta(r_1)\theta(b_k)u+\cdots+\theta(r_k)\theta(b_0)u^k+\theta(r_k)\theta(b_1)u+\cdots+\theta(r_k)\theta(b_k)u^k\\
&= \theta(r_0)\theta(b_0)+\theta(r_0)\theta(b_1)u+\cdots+\theta(r_0)\theta(b_k)u^k+\theta(r_1)\theta(b_0)u+\theta(r_1)\theta(b_1)u^2\\
&\quad+\cdots+\theta(r_1)\theta(b_k)u^{k+1}+\cdots+\theta(r_k)\theta(b_0)u^k+\theta(r_k)\theta(b_1)u^{k+1}+\cdots+\theta(r_k)\theta(b_k)u^{2k}\\
&= \big(\theta(r_0)+\theta(r_1)u+\cdots+\theta(r_k)u^k\big)\big(\theta(b_0)+\theta(b_1)u+\cdots+\theta(b_k)u^k\big)\\
&= \Theta(r_0+r_1u+\cdots+r_ku^k)\Theta(b_0+b_1u+\cdots+b_ku^k)\\
&= \Theta(r)\Theta(b)
\end{aligned}$$

elde edilir. Dolayısıyla Θ, çarpma işlemini korur. Böylece i), ii), iii) ve iv) den, Θ dönüşümünün R'nin bir otomorfizması olduğu elde edilir.

R'nin tüm otomorfilerin kümesi $Aut(R)$ ve R'nin birim otomorfisi Θ_0 olmak üzere $\Theta \in Aut(R)\backslash\{\Theta_0\}$ olsun. R üzerindeki skew polinom halkası aşağıdaki gibi tanımlanır:

$$R[x,\Theta] = \{a_0+a_1x+\cdots+a_nx^n \mid a_i \in R,\ 0 \le i \le n\} \tag{3.14}$$

polinom kümesini göz önüne alalım. $R[x,\Theta]$ kümesi üzerinde toplama işlemi olarak $R[x]$

polinom halkası üzerinde tanımlı adi toplama işlemini ve çarpma işlemi olarak $i,\ j \in \mathbb{N}$ ve $\alpha, \beta \in R$ olmak üzere

$$\alpha x^i \beta x^j = \alpha \Theta^i(\beta) x^{i+j} \tag{3.15}$$

şeklinde tanımlanır. Bu şekilde tanımlı toplama ve çarpma işlemlerine göre $R[x,\Theta]$ kümesi R üzerindeki skew polinom halkası olarak adlandırılır. Θ, birim otomorfi olmadıkça bu halka değişmeli değildir, üstelik bu halka sıfır bölensizdir ve birimleri R'nin birimleridir. Θ özel olarak birim otomorfi olarak alınırsa, elde edilen skew polinom halkası, normal polinom halkasına denk gelir, çünkü çarpma işlemi $\alpha x^i \beta x^j = \alpha \Theta_0^i(\beta) x^{i+j} = \alpha\beta x^{i+j}$ şeklinde olup polinomların adi çarpma işlemine karşılık gelir, dolayısıyla $R[x,\Theta_0] = R[x]$ elde edilir [5].

Örnek 3.1.1.2. Skew polinom halkası tek türlü çarpanlara ayrılış bölgesi değildir. Örneğin $F_9[x,\theta]$ üzerinde x^8-1 polinomunun bazı çarpanlara ayrılışı

$$\begin{aligned} x^8-1 &= (1+x)(2+x)(w+x)(w^7+x)(1+w^3x+x^2)(1+w^7x+x^2) \\ &= (1+x)(2+x)(w+x)(w^7+x)(1+wx+x^2)(1+w^5x+x^2) \\ &= (w^3+x)(w^5+x)(w^6+x)^2(2+w^2x+x^2)(2+w^6x+x^2) \\ &= (w^2+x)^2(w^3+x)(w^5+x)(1+w^3x+x^2)(1+w^7x+x^2) \\ &= (1+x)(2+x)(w^3+x)(w^5+x)(w^6+x^2)(w^2+x^2) \end{aligned}$$

şeklindedir, burada her $a \in F_9$ için $\theta(a) = a^3$ otomorfisi göz önüne alınmıştır.

3.2. R ÜZERİNDEKİ LİNEER KODLAR

Bu bölümde $R = F_q + uF_q + \cdots + u^k F_q$ halkası üzerindeki lineer kodlar incelenecektir.

Tanım 3.2.1. R sonlu ve değişmeli bir halka, $\varnothing \neq C \subseteq R^n$ bir küme olmak üzere

- $C \subseteq R^n$ ise C'ye R üzerinde, uzunluğu n olan bir **kod** denir,
- $C \subseteq R^n$ alt kümesi bir R-alt modül ise C'ye R üzerinde, uzunluğu n olan bir **lineer kod** denir.

Tanım 3.2.2. R halkası üzerinde, uzunluğu n olan bir lineer kod C olsun. Eğer

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

koşulu sağlanıyor ise C'ye **devirli kod** denir.

Şimdi R halkası üzerindeki Gray dönüşümü verelim. λ, F_q'nun sıfırdan farklı bir elemanı olmak üzere $MM^T = \lambda I_{k+1}$ olacak şekilde bir $M \in GL_{k+1}(F_q)$ matrisini göz önüne alalım, burada M^T, M matrisinin transpozunu ve I_{k+1}, mertebesi $k+1$ olan birim matrisi göstermektedir. R üzerinde bir Gray dönüşüm

$$\phi : R \longrightarrow F_q^{k+1} \tag{3.16}$$

olmak üzere $r = \gamma_0 r_0 + \gamma_1 r_1 + \cdots + \gamma_k r_k \in R$ için

$$\phi(\gamma_0 r_0 + \gamma_1 r_1 + \cdots + \gamma_k r_k 1 = (r_0, r_1, \ldots, r_k)M \tag{3.17}$$

şeklinde tanımlanır. Herhangi bir $r = \gamma_0 r_0 + \gamma_1 r_1 + \cdots + \gamma_k r_k \in R$ elemanı için r'nin **Lee ağırlığı** $w_L(r) = w_H(\phi(r))$ olarak tanımlanır, burada $w_H(\phi(r))$, $\phi(r)$'nin F_q üzerindeki Hamming ağırlığını gösterir. r, $r' \in R$ elemanları arasındaki **Lee uzaklığı**

$$d_L(r, r') = w_L(r - r') = w_H(\phi(r - r'))$$

olarak tanımlanır. ϕ tasviri bir lineer dönüşümdür ve R^n'den $F_q^{(k+1)n}$'ye bileşenler üzerinden genişletilebilir. R üzerinde, uzunluğu n olan bir lineer C kodu için

- $C_0 = \{a_0 \in F_q^n \mid \gamma_0 a_0 + \gamma_1 a_1 + \cdots + \gamma_k a_k \in C,\ a_1, a_2, \ldots, a_k \in F_q^n\}$
- $C_1 = \{a_1 \in F_q^n \mid \gamma_0 a_0 + \gamma_1 a_1 + \cdots + \gamma_k a_k \in C,\ a_0, a_2, \ldots, a_k \in F_q^n\}$

  $\vdots$

- $C_k = \{a_k \in F_q^n \mid \gamma_0 a_0 + \gamma_1 a_1 + \cdots + \gamma_k a_k \in C,\ a_0, a_1, \ldots, a_{k-1} \in F_q^n\}$

tanımlansın, burada $i = 0, 1, \ldots, k$ için C_i'ler, F_q üzerinde, uzunluğu n olan lineer kodlardır.

Böylece R üzerinde, uzunluğu n olan bir lineer C kodu

$$C = \gamma_0 C_0 \oplus \gamma_1 C_1 \oplus \cdots \oplus \gamma_k C_k$$

olacak şekilde tek türlü ifade edilebilir. $i = 0, 1, \ldots, k$ için G_i'ler q-lu lineer C_i kodlarının üreteç matrisleri ise, bu durumda C'nin üreteç matrisi

$$G = \begin{pmatrix} \gamma_0 G_0 \\ \gamma_1 G_1 \\ \vdots \\ \gamma_k G_k \end{pmatrix}$$

şeklinde ve $\phi(C)$'nin üreteç matrisi

$$\phi(G) = \begin{pmatrix} \phi(\gamma_0 G_0) \\ \phi(\gamma_1 G_1) \\ \vdots \\ \phi(\gamma_k G_k) \end{pmatrix}$$

şeklindedir [5].

Örnek 3.2.3. $R = F_9[u]/(u^2 - u)$ halkasını göz önüne alalım. Burada $k = 1$ ve $p = 3$ dir.

$$M = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in GL_2(F_9)$$

şeklinde verilen 2×2 tipindeki matrisi göz önüne alalım. M^T, M matrisinin transpozunu ve I_2, mertebesi 2 olan birim matrisi göstermek üzere M matrisi için

$$MM^T = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = 2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2I_2$$

sağlanır. O halde $r = \gamma_0 r_0 + \gamma_1 r_1 \in R$ olmak üzere R halkası üzerindeki Gray dönüşüm

$$\begin{aligned} \phi : R &\longrightarrow F_9^2 \\ \gamma_0 r_0 + \gamma_1 r_1 &\longmapsto (r_0, r_1)M = (r_0 + r_1, -r_0 + r_1) \end{aligned}$$

şeklinde tanımlanır.

Örnek 3.2.4. $R = F_{25}[u]/(u^3 - u)$ halkasını göz önüne alalım. Burada $k = 2$ ve $p = 5$ dir.

$$M = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{pmatrix} \in GL_3(F_{25})$$

şeklinde verilen 3×3 tipindeki matrisi göz önüne alalım. M^T, M matrisinin transpozunu ve I_3, mertebesi 3 olan birim matrisi göstermek üzere M matrisi için

$$MM^T = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 2 & -2 \\ 2 & 1 & 2 \\ 2 & -2 & -1 \end{pmatrix} = 9 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 9I_3$$

sağlanır. O halde $r = \gamma_0 r_0 + \gamma_1 r_1 + \gamma_2 r_2 \in R$ olmak üzere R halkası üzerindeki Gray dönüşüm

$$\phi : R \longrightarrow F_{25}^3$$

olmak üzere

$$\begin{aligned} \phi(\gamma_0 r_0 + \gamma_1 r_1 + \gamma_2 r_2) &= (r_0, r_1, r_2)M \\ &= (r_0 + 2r_1 - 2r_2,\, 2r_0 + r_1 + 2r_2,\, 2r_0 - 2r_1 - r_2) \end{aligned}$$

şeklinde tanımlanır.

Örnek 3.2.5. $R = F_{49}[u]/(u^4 - u)$ halkasını göz önüne alalım. Burada $k = 3$ ve $p = 7$ dir.

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \in GL_4(F_{49})$$

matrisini göz önüne alalım, burada M^T, M matrisinin transpozunu ve I_4, mertebesi 4 olan

birim matrisi göstermek üzere

$$MM^T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = 4 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = 4I_4$$

sağlanır. O halde $r = \gamma_0 r_0 + \gamma_1 r_1 + \gamma_2 r_2 + \gamma_3 r_3 \in R$ olmak üzere R halkası üzerindeki Gray dönüşüm

$$\phi : R \longrightarrow F_{49}^4$$

olmak üzere

$$\begin{aligned} \phi(\gamma_0 r_0 + \gamma_1 r_1 + \gamma_2 r_2 + \gamma_3 r_3) &= (r_0, r_1, r_2, r_3)M \\ &= (r_0 + r_1 + r_2 + r_3,\ r_0 - r_1 + r_2 - r_3,\ r_0 + r_1 - r_2 - r_3,\ r_0 - r_1 - r_2 + r_3) \end{aligned}$$

şeklinde tanımlanır.

Önerme 3.2.6. ϕ, R üzerinde (3.16)'da verilen Gray dönüşüm olsun. Bu durumda aşağıdaki özellikler sağlanır:

1. ϕ, R^n'den (Lee uzaklık) $F_q^{(k+1)n}$'ye (Hamming uzaklık) tanımlanan, F_q-lineer uzaklığı koruyan bir dönüşümüdür.

2. Eğer C, R üzerinde bir $[n, k', d_L]$ lineer kod ise, bu durumda $\phi(C)$, F_q üzerinde bir $[n(k+1), k', d_H]$ lineer koddur.

İspat.

1. $0 \leq i \leq k$ için $a_i, b_i \in F_q^n$ olmak üzere $\alpha \in F_q$ ve $x_1 = \gamma_0 a_0 + \gamma_1 a_1 + \cdots + \gamma_k a_k$ ve $x_2 = \gamma_0 b_0 + \gamma_1 b_1 + \cdots + \gamma_k b_k \in R^n$ olsun. Bu durumda

$$\begin{aligned} \phi(x_1 + x_2) &= ((a_0 + b_0)M,\ (a_1 + b_1)M,\ \ldots,\ (a_k + b_k)M) \\ &= (a_0 M,\ a_1 M,\ \ldots,\ a_k M) + (b_0 M,\ b_1 M,\ \ldots,\ b_k M) \\ &= \phi(x_1) + \phi(x_2) \end{aligned}$$

ve

$$\begin{aligned}\phi(\alpha x_1) &= (\alpha a_0 M,\, \alpha a_1 M,\, \ldots,\, \alpha a_k M)\\ &= \alpha\phi(x_1)\end{aligned}$$

elde edilir. Yani ϕ, F_q-lineer dönüşümdür. Şimdi uzaklığı koruyan bir dönüşüm olduğunu gösterelim.

$$\begin{aligned}d_L(x_1,x_2) = w_L(x_1-x_2) &= w_H(\phi(x_1-x_2))\\ &= w_H(\phi(x_1)-\phi(x_2))\\ &= d_H(\phi(x_1),\phi(x_2)).\end{aligned}$$

2. ϕ Gray dönüşümü birebir, örten ve F_q-lineer olduğundan

$$|C| = |\phi(C)| = q^{k'}$$

sağlanır. Aynı zamanda ϕ, uzaklık koruyan bir dönüşüm olduğundan

$$d_L(C) = d_H(\phi(C))$$

olur. O halde C, R üzerinde bir $[n,\, k',\, d_L]$ lineer kod ise, bu durumda $\phi(C)$ de F_q üzerinde bir $[n(k+1),\, k',\, d_H]$ lineer koddur.

Önerme 3.2.7. $C = \gamma_0 C_0 \oplus \gamma_1 C_1 \oplus \cdots \oplus \gamma_k C_k$, R üzerinde, uzunluğu n olan bir lineer kod olsun. Bu durumda C'nin duali

$$C^{\perp} = \gamma_0 C_0^{\perp} \oplus \gamma_1 C_1^{\perp} \oplus \cdots \oplus \gamma_k C_k^{\perp}$$

olup R üzerinde, uzunluğu n olan bir lineer koddur.

İspat. R üzerinde, uzunluğu n olan lineer C kodunun

$$C^{\perp} = \{x \in R \mid \langle x, c\rangle = 0\ ,\ \forall\, c \in C\}$$

dualini göz önüne alalım. $0 \le i \le k$ için $a_i \in F_q$ ve $b_i \in C_i$ olmak üzere $x = \sum_{i=0}^{k} \gamma_i a_i \in C^{\perp}$ ve

$c = \sum_{i=0}^{k} \gamma_i b_i \in C$ elemanları için

$$\langle x, c \rangle = \langle \sum_{i=0}^{k} \gamma_i a_i, \sum_{i=0}^{k} \gamma_i b_i \rangle = 0$$

olup $0 \leq i,\ j \leq k$ ve $i \neq j$ için $\gamma_j^2 = \gamma_j,\ \gamma_i \gamma_j = 0$ özelliklerinden

$$\sum_{i=0}^{k} \gamma_i \langle a_i, b_i \rangle = 0$$

elde edilir. Buradan $0 \leq i \leq k$ için $\langle a_i, b_i \rangle = 0$ olduğundan $a_i \in C_i^{\perp}$ bulunur. Dolayısıyla

$$C^{\perp} = \gamma_0 C_0^{\perp} \oplus \gamma_1 C_1^{\perp} \oplus \cdots \oplus \gamma_k C_k^{\perp}$$

elde edilir. $0 \leq i \leq k$ için C_i, F_q üzerinde bir lineer kod olduğundan $C_i^{\perp}$ de F_q üzerinde bir lineer koddur. Böylece $C^{\perp} = \gamma_0 C_0^{\perp} \oplus \gamma_1 C_1^{\perp} \oplus \cdots \oplus \gamma_k C_k^{\perp}$, R üzerinde, uzunluğu n olan bir lineer koddur.

3.2.1. R Üzerindeki Skew Devirli Kodlar

Tanım 3.2.1.1. C, R halkası üzerinde, uzunluğu n olan bir lineer kod ve $\Theta \in Aut(R) \setminus \{\Theta_0\}$ olsun. Eğer

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow \big(\Theta(c_{n-1}), \Theta(c_0), \ldots, \Theta(c_{n-2})\big) \in C$$

koşulu sağlanıyor ise C'ye **skew devirli kod** veya **skew Θ-devirli kod** denir.

$R_n = R[x, \Theta] \big/ (x^n - 1)$ olsun. R^n'deki bir $c = (c_0, c_1 \ldots, c_{n-1})$ kod kelimesi, R_n'deki

$$f(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

polinomu ile eşleştirilebilir. Buradaki

$$c \longleftrightarrow f(x)$$

eşleştirmesi bir R-modül izomorfizmasıdır. $R[x, \Theta]$ skew polinom halkası değişmeli

olmadığından, x^n-1 ideali, $R[x,\Theta]$ skew polinom halkasında her zaman iki yanlı ideal değildir. Bu sebeple, R_n kümesinin bir halka olduğunu garantilemek için x^n-1 idealinin iki yanlı ideal olup olmadığının bilinmesi gerekir. Bu sebeple aşağıdaki sonuç oldukça önemlidir.

Önerme 3.2.1.2. $Z(R[x,\Theta])$, $R[x,\Theta]$ skew polinom halkasının merkezi ve $|\langle\Theta\rangle| = m$ olsun. Bu durumda $x^n-1 \in Z(R[x,\Theta])$ olması için gerek ve yeter koşul $m \mid n$ olmasıdır.

İspat. $m \mid n$ olsun. Bu durumda $n = mk$ olacak şekilde bir $k \in \mathbb{Z}$ vardır. O halde her $a \in R$ için

$$\Theta^n(a) = \Theta^{mk}(a) = a$$

dır. $f(x) = a_0 + a_1x + \cdots + a_rx^r \in R[x,\Theta]$ olsun. Buradan

$$\begin{aligned}
(x^n-1)\,f(x) &= (x^n-1)\,(a_0 + a_1x + \cdots + a_rx^r) \\
&= x^na_0 + x^na_1x + \cdots + x^na_rx^r - (a_0 + a_1x + \cdots + a_rx^r) \\
&= \Theta^n(a_0)x^n + \Theta^n(a_1)x^{n+1} + \cdots + \Theta^n(a_r)x^{n+r} - f(x) \\
&= a_0x^n + a_1x^{n+1} + \cdots + a_rx^{n+r} - f(x) \\
&= (a_0 + a_1x + \cdots + a_rx^r)x^n - f(x) \\
&= f(x)x^n - f(x) \\
&= f(x)(x^n-1)
\end{aligned}$$

elde edilir. Böylece $x^n-1 \in Z(R[x,\Theta])$ sonucuna ulaşılır.

Diğer taraftan $x^n-1 \in Z(R[x,\Theta])$ olsun. Bu durumda her $g(x) \in R[x,\Theta]$ polinomu için $(x^n-1)g(x) = g(x)(x^n-1)$ dir. Özel olarak $a \in R$ olmak üzere

$$(x^n-1)ax^m = ax^m(x^n-1)$$

sağlanır. Bu eşitlikte $R[x,\theta]$ skew polinom halkasındaki çarpma işlemi kullanılarak

$$\begin{aligned}
x^nax^m - ax^m &= ax^{m+n} - ax^m \\
\Theta^n(a)x^{n+m} - ax^m &= ax^{m+n} - ax^m
\end{aligned}$$

elde edilir ki her $a \in R$ için $\Theta^n(a) = a$ olduğunu ifade eder. Buradan

$$m \mid n$$

elde edilir. Böylece ispat bitmiş olur.

Teorem 3.2.1.3. C, R üzerinde, uzunluğu n olan bir lineer kod ve $\Theta \in Aut(R)$ olmak üzere $|\langle\Theta\rangle| = m$ için $m \mid n$ olsun. C'nin bir skew Θ-devirli kod olabilmesi için gerek ve yeter koşul $g(x)$ polinomunun, $R[x,\Theta]$'da $x^n - 1$'in bir sağ böleni olmak üzere $C = \langle g(x)\rangle$ olacak şekilde R_n'in bir sol ideali olmasıdır.

İspat. Hipotez gereği $m \mid n$ olduğundan $x^n - 1 \in Z(R[x,\Theta])$ olup $x^n - 1$'in ürettiği ideal $R[x,\Theta]$'da çift taraflı bir idealdir. Dolayısıyla R_n bir halkadır.

İlk olarak C bir skew Θ-devirli kod olsun. $g(x)$ polinomu C'de sıfırdan farklı derecesi en küçük olan monik polinom ve $a(x) \in C$ keyfi bir eleman olsun. Bölme algoritması ile

$$a(x) = q(x)g(x) + r(x);\ \deg r(x) \leq \deg g(x)$$

olacak şekilde tek türlü belirli $q(x), r(x) \in R[x,\Theta]$ vardır. Böylece $a(x)$, $g(x) \in C$ olduğundan

$$r(x) = a(x) - q(x)g(x) \in C$$

olur ve $g(x)$'in tanımından

$$r(x) = 0$$

elde edilir, dolayısıyla

$$a(x) = q(x)g(x)$$

olup

$$C = \langle g(x)\rangle$$

bulunur. Şimdi $a(x), b(x) \in C$ ve $h(x) = \sum_{i=0}^{n-1} h_i x^i \in R_n$ olsun. C skew, devirli olduğundan dolayı, C bir lineer koddur ve böylece $a(x) + b(x) \in C$ dir. Üstelik C, skew devirli olduğundan

dolayı $x^i a(x) \in C$ dir. Böylece

$$h(x)a(x) = \big(\sum_{i=0}^{n-1} h_i x^i\big)a(x) = \sum_{i=0}^{n-1} h_i x^i a(x) \in C$$

dir, yani C, R_n'in bir sol idealidir. Bölme algoritması ile

$$x^n - 1 = q_1(x)g(x) + r_1(x)\,;\ \deg r_1(x) \leq \deg g(x)$$

olacak şekilde tek türlü belirli $q_1(x), r_1(x) \in R[x,\Theta]$ vardır. $x^n - 1, (R_n, +)$ grubuna göre etkisiz elemandır ve

$$r_1(x) = (x^n - 1) - q_1(x)g(x) \in C$$

olur, üstelik $g(x)$'in tanımından $r_1(x) = 0$ elde edilir, dolayısıyla

$$x^n - 1 = q(x)g(x)$$

olup $g(x)$, $x^n - 1$'in bir sağ bölenidir.

Diğer yandan $C = \langle g(x)\rangle$, R_n'nin bir sol ideali ve $g(x)$, $x^n - 1$'in bir sağ böleni olsun. Bu durumda $(a_0, a_1, \ldots, a_{n-1}) \in C$'nin polinom karşılığı $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ C'de bir ideal olduğundan dolayı $xa(x) \in C$ dir, $x^n \equiv 1 \pmod{x^n - 1}$ olduğundan

$$\begin{aligned} xa(x) &= x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) \\ &= xa_0 + xa_1 x + \cdots + xa_{n-1}x^{n-1} \\ &= \Theta(a_0)x + \Theta(a_1)x^2 + \cdots + \Theta(a_{n-1})x^n \\ &= \Theta(a_{n-1}) + \Theta(a_0)x + \cdots + \Theta(a_{n-2})x^{n-1} \end{aligned}$$

olup $(\Theta(a_{n-1}), \Theta(a_0), \ldots, \Theta(a_{n-2})) \in C$ elde edilir. Böylece C bir skew devirli koddur.

$|\langle\Theta\rangle| = m$ olmak üzere eğer $m \nmid n$ ise $x^n - 1 \notin Z(R[x,\Theta])$ dir, dolayısıyla $x^n - 1$ çift taraflı bir ideal değildir. Bu durumda R_n bir halka değildir ve dolayısıyla R_n'de ideal kavramı anlamsızdır. Bundan dolayı Θ-devirli kodlar ile R_n'deki ideallerin birebir karşılık getirilmesi geçerli değildir. O halde C, R üzerinde, uzunluğu n olan bir lineer kod ve $\Theta \in Aut(R)$ olmak üzere bir C skew Θ-devirli kodundan bahsedebilmemiz için ilk olarak Θ'nın mertebesinin

n'yi bölüp bölmediğinin tespit edilmesi gerekir. Dolayısıyla skew devirli kodlarda uzunluğun otomorfinin mertebesine bağlı olması kısıtlayıcı bir durumdur. Bu kısıtlayıcı durum, Siap vd. [12] tarafından literatüre sunulan çalışma ile ortadan kaldırılmıştır. Siap vd. [12], F sonlu bir cisim olmak üzere $F[x,\theta]/(x^n-1)$ kümesi üzerinde $f(x)+(x^n-1)\in F[x,\theta]/(x^n-1)$ ve $r(x)\in F[x,\theta]$ olmak üzere

$$r(x)\diamond(f(x)+(x^n-1))=r(x)f(x)+(x^n-1) \tag{3.18}$$

şeklinde yeni bir soldan skaler çarpım işlemi tanımlamışlardır. $F[x,\theta]/(x^n-1)$ kümesini

$$\begin{aligned} F[x,\theta]/(x^n-1)=\{a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1} \mid x^n=1 \text{ ve} \\ i=0,1,2,\ldots,n-1 \text{ için } a_i\in F\} \end{aligned} \tag{3.19}$$

şeklinde göz önüne alarak bu skaler çarpıma göre $F[x,\theta]/(x^n-1)$ kümesinin bir sol F-modül ve bir sol $F[x,\theta]$-modül olduğunu göstermişlerdir. Siap vd.[12], $F[x,\theta]/(x^n-1)$'nin sol alt modülleri ile skew devirli kodları karşılık getirmişlerdir. Bu karakterizasyon, sonlu halkalar üzerindeki skew devirli kodlara benzer şekilde genişletilebilir ([1, 5]). $R_n=R[x,\Theta]/(x^n-1)$ olmak üzere $f(x)+(x^n-1)\in R_n$ ve $g(x)\in R[x,\Theta]$ için

$$g(x)\diamond(f(x)+(x^n-1))=g(x)f(x)+(x^n-1)$$

çarpımı ile R_n bir sol $R[x,\Theta]$-modüldür. R_n kümesi

$$\begin{aligned} R_n &= R[x,\Theta]/(x^n-1) \\ &= \{a_0+a_1x+\cdots+a_{n-1}x^{n-1} \mid i=0,1,\ldots,n-1 \text{ için } a_i\in R \text{ ve } x^n=1\} \end{aligned} \tag{3.20}$$

şeklinde de ifade edilebilir. Buradan itibaren "$\diamond$" notasyonu kolaylık için kullanılmayacaktır.

Herhangi bir n için bir skew devirli kodun tanımı aşağıdaki teorem ile verilir.

Teorem 3.2.1.4. R üzerinde, uzunluğu n olan C lineer kodunun bir skew Θ-devirli kod olabilmesi için gerek ve yeter koşul $C=\langle g(x)\rangle$'in sol $R[x,\Theta]$-modül olan R_n'in bir sol $R[x,\Theta]$-alt modülü olmasıdır, burada $g(x)$, C'deki en küçük dereceli bir monik polinomdur. Üstelik C, $\{g(x),\, xg(x),\, \ldots,\, x^{m-1}g(x)\}$ bazına sahip $m=n-\deg g(x)$ boyutlu bir serbest koddur.

İspat. C kodunun R_n'nin bir sol $R[x,\Theta]$-alt modülü olduğu göz önüne alınarak Teorem 3.2.1.3'in ispatına benzer şekilde ispat edilir. Şimdi C kodunun, boyutu $m = n - \deg g(x)$ olan bir serbest alt modül ve $\{g(x), xg(x), \ldots, x^{m-1}g(x)\}$ kümesinin bir baz olduğunu ispat edelim.

$a(x) \in C$ olsun. Bu durumda $a(x) = q(x)g(x)$ olacak şekilde bir $q(x) \in R[x,\Theta]$ vardır. Kod kelimelerinin uzunluğu n olduğundan

$$\begin{aligned} \deg a(x) = \deg q(x) + \deg g(x) < n \;&\Rightarrow\; \deg q(x) < n - \deg g(x) \\ &\Rightarrow \deg q(x) < m \end{aligned}$$

elde edilir. Bu durumda $q(x) = q_0 + q_1 x + \cdots + q_{m-1}x^{m-1} \in R[x,\Theta]$ için

$$\begin{aligned} a(x) &= q(x)g(x) \\ &= (q_0 + q_1 x + \cdots + q_{m-1}x^{m-1})g(x) \\ &= q_0 g(x) + q_1 xg(x) + \cdots + q_{m-1}x^{m-1}g(x) \end{aligned}$$

bulunur. Dolayısıyla $\{g(x), xg(x), \ldots, x^{m-1}g(x)\}$ kümesi C'yi üretir. $R = F_q[u]/(u^{k+1} - u)$ sıfır bölensiz olduğundan dolayı $\{g(x), xg(x), \ldots, x^{m-1}g(x)\}$ lineer bağımsız bir kümedir, yani C, boyutu m olan bir serbest modüldür.

Bu tezin bundan sonraki bölümünde

- Eğer $|\langle\Theta\rangle| = m$ olmak üzere eğer $m \mid n$ ise, Teorem 3.2.1.3'ten, R üzerinde, uzunluğu n olan bir skew devirli kod, R_n'nin bir sol ideali
- Eğer $|\langle\Theta\rangle| = m$ olmak üzere eğer $m \nmid n$ ise, Teorem 3.2.1.4'ten, R üzerinde, uzunluğu n olan bir skew devirli kod, R_n'nin bir sol $R[x,\Theta]$-alt modülü

olarak alınacaktır.

Şimdi, R üzerinde, uzunluğu n olan bir skew Θ-devirli kodun direkt toplam şeklindeki parçalanışı ile ilgili bir inceleme yapılacaktır.

Teorem 3.2.1.5. $C = \gamma_0 C_0 \oplus \gamma_1 C_1 \oplus \cdots \oplus \gamma_k C_k$, R üzerinde, uzunluğu n olan bir lineer kod olsun. Bu durumda C'nin skew Θ-devirli kod olması için gerek ve yeter koşul $0 \leq j \leq k$ için

C_j'lerin, F_q üzerinde, uzunluğu n olan birer skew θ-devirli kod olmalarıdır.

İspat. $0 \leq i \leq n-1$ ve $0 \leq j \leq k$ için $a_{i,j} \in F_q$ ve $x_i = \gamma_0 a_{i,0} + \gamma_1 a_{i,1} + \cdots + \gamma_k a_{i,k} \in R$ olmak üzere $x = (x_0, x_1, \ldots, x_{n-1}) \in C$ olsun. Bu elemanlar

$$\begin{array}{rcccccccc} x_0 & = & \gamma_0 a_{0,0} & + & \gamma_1 a_{0,1} & + & \ldots & + & \gamma_k a_{0,k} \\ x_1 & = & \gamma_0 a_{1,0} & + & \gamma_1 a_{1,1} & + & \ldots & + & \gamma_k a_{1,k} \\ \vdots & & & & & & & & \\ x_{n-1} & = & \gamma_0 a_{n-1,0} & + & \gamma_1 a_{n-1,1} & + & \ldots & + & \gamma_k a_{n-1,k} \end{array}$$

şeklinde açık olarak ifade edilebilir. Bu durumda

$$\begin{aligned} a_0 &= (a_{0,0}, a_{1,0}, \ldots, a_{n-1,0}) \in C_0 \\ a_1 &= (a_{0,1}, a_{1,1}, \ldots, a_{n-1,1}) \in C_1 \\ &\vdots \\ a_k &= (a_{0,k}, a_{1,k}, \ldots, a_{n-1,k}) \in C_k \end{aligned}$$

alalım, genel olarak $0 \leq j \leq k$ için $a_j = (a_{0,j}, a_{1,j}, \ldots, a_{n-1,j}) \in C_j$ şeklinde de yazılabilir. $0 \leq i \leq n-1$ ve $0 \leq j \leq k$ olmak üzere $a_{i,j} \in F_q$ elemanı için

$$\Theta(a_{i,j}) = \theta(a_{i,j})$$

ve

$$\Theta(u) = \Theta(1u) = \theta(1)u = 1u = u$$

olur. Böylece $0 \leq j \leq k$ olmak üzere $\gamma_j = A_j e_j \in F_p[u]$ için

$$\Theta(\gamma_j) = \gamma_j$$

olur. Şimdi C, R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olsun. O halde $\sigma(x) \in C$

dir, yani

$$\begin{aligned}
\sigma(x) &= \sigma((x_0, x_1, \ldots, x_{n-1})) \\
&= \big(\Theta(x_{n-1}), \Theta(x_0), \ldots, \Theta(x_{n-2})\big) \\
&= \big(\Theta(\gamma_0 a_{n-1,0} + \gamma_1 a_{n-1,1} + \cdots + \gamma_k a_{n-1,k}), \Theta(\gamma_0 a_{0,0} + \gamma_1 a_{0,1} + \cdots + \gamma_k a_{0,k}), \ldots, \\
&\qquad\qquad \Theta(\gamma_0 a_{n-2,0} + \gamma_1 a_{n-2,1} + \cdots + \gamma_k a_{n-2,k})\big) \\
&= [\gamma_0\theta(a_{n-1,0}) + \gamma_1\theta(a_{n-1,1}) + \cdots + \gamma_k\theta(a_{n-1,k}),\ \gamma_0\theta(a_{0,0}) + \gamma_1\theta(a_{0,1}) + \ldots \\
&\qquad\qquad + \gamma_k\theta(a_{0,k}),\ \ldots,\ \gamma_0\theta(a_{n-2,0}) + \gamma_1\theta(a_{n-2,1}) + \cdots + \gamma_k\theta(a_{n-2,k})] \\
&= \gamma_0[\theta(a_{n-1,0}),\ \theta(a_{0,0}),\ \ldots,\ \theta(a_{n-2,0})] + \gamma_1[\theta(a_{n-1,1}),\ \theta(a_{0,1}),\ \ldots,\ \theta(a_{n-2,1})] \\
&\qquad\qquad + \cdots + \gamma_k[\theta(a_{n-1,k}),\ \theta(a_{0,k}),\ \ldots,\ \theta(a_{n-2,k})] \\
&= \gamma_0\sigma(a_0) + \gamma_1\sigma(a_1) + \cdots + \gamma_\sigma(a_k) \in C
\end{aligned}$$

dir. Burada

$$\begin{aligned}
&\sigma(a_0) = (\theta(a_{n-1,0}),\ \theta(a_{0,0}),\ \ldots,\ \theta(a_{n-2,0})) \in C_0 \\
&\sigma(a_1) = (\theta(a_{n-1,1}),\ \theta(a_{0,1}),\ \ldots,\ \theta(a_{n-2,1})) \in C_1 \\
&\qquad\vdots \\
&\sigma(a_k) = (\theta(a_{n-1,k}),\ \theta(a_{0,k}),\ \ldots,\ \theta(a_{n-2,k})) \in C_k
\end{aligned}$$

olup $0 \leq j \leq k$ için $\sigma(a_j) \in C_j$ dir, bu ise C_j'lerin F_q üzerinde, uzunluğu n olan skew θ-devirli kodlar olduğunu gösterir.

Diğer yandan $0 \leq j \leq k$ için C_j'lerin F_q üzerinde, uzunluğu n olan birer skew θ-devirli kod olduğunu varsayalım. Bu durumda $\sigma(a_j) \in C_j$ olur ve

$$\sigma(x) = \gamma_0\sigma(a_0) + \gamma_1\sigma(a_1) + \cdots + \gamma_k\sigma(a_k) \in C$$

elde edilir. Böylece C'nin R üzerinde, uzunluğu n olan skew Θ-devirli kod olduğu elde edilir.

Teorem 3.2.1.5, R üzerinde, uzunluğu n olan bir skew Θ-devirli kodun direk toplam şeklinde nasıl yazıldığını ifade eder. Şimdi $|\langle\Theta\rangle| \mid n$ olmak üzere R üzerinde, uzunluğu n olan bir skew Θ-devirli kodun dualinin de R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olduğunu gösterelim.

Önerme 3.2.1.6. $|\langle\Theta\rangle| \mid n$ olsun. R üzerinde, uzunluğu n olan bir skew Θ-devirli C kodunun dual kodu $C^{\perp}$, R üzerinde, uzunluğu n olan bir skew Θ-devirli koddur.

İspat. C, R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olsun. $x=(x_0,x_1,\ldots,x_{n-1})\in C$ ve $y=(y_0,y_1,\ldots,y_{n-1})\in C^{\perp}$ olsun. $C^{\perp}$'in R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olduğunu göstermek için $\sigma(y)=(\Theta(y_{n-1}),\,\Theta(y_0),\,\ldots,\,\Theta(y_{n-2}))\in C^{\perp}$ olduğunu göstermemiz gerekir. Bunun için x ile $\sigma(y)$'nin

$$\langle x,\,\sigma(y)\rangle = x_0\Theta(y_{n-1})+x_1\Theta(y_0)+\cdots+x_{n-1}\Theta(y_{n-2})$$

iç çarpımını göz önüne alalım. C, bir skew Θ-devirli kod olduğundan $\sigma^{n-1}(x)\in C$ dir, yani

$$\sigma^{n-1}(x)=(\Theta^{n-1}(x_1),\,\Theta^{n-1}(x_2),\,\ldots,\,\Theta^{n-1}(x_{n-1}),\,\Theta^{n-1}(x_0))\in C$$

dir. O halde $\langle\sigma^{n-1}(x),\,y\rangle=0$ dır, yani

$$\langle\sigma^{n-1}(x),\,y\rangle=\Theta^{n-1}(x_1)y_0+\Theta^{n-1}(x_2)y_1+\cdots+\Theta^{n-1}(x_{n-1})y_{n-2}+\Theta^{n-1}(x_0)y_{n-1}=0$$

olur. $|\langle\Theta\rangle| \mid n$ olduğundan Θ^n birim otomorfi olur ve buradan

$$\begin{aligned}
0=\Theta(\langle\sigma^{n-1}(x),\,y\rangle) &= \Theta\big(\Theta^{n-1}(x_1)y_0+\Theta^{n-1}(x_2)y_1+\cdots+\Theta^{n-1}(x_{n-1})y_{n-2}+\Theta^{n-1}(x_0)y_{n-1}\big)\\
&= x_1\Theta(y_0)+x_2\Theta(y_1)+\cdots+x_{n-1}\Theta(y_{n-2})+x_0\Theta(y_{n-1})\\
&= x_0\Theta(y_{n-1})+x_1\Theta(y_0)+\cdots+x_{n-1}\Theta(y_{n-2})\\
&= \langle x,\,\sigma(y)\rangle
\end{aligned}$$

olur. O halde $\sigma(y)\in C^{\perp}$ dir. Böylece $C^{\perp}$, R üzerinde, uzunluğu n olan bir skew Θ-devirli koddur.

Sonuç 3.2.1.7. $|\langle\Theta\rangle| \mid n$ olsun. R üzerinde, uzunluğu n olan bir skew Θ-devirli $C=\gamma_0C_0\oplus\gamma_1C_1\oplus\cdots\oplus\gamma_kC_k$ kodunun

i) $0\le j\le k$ için $C_j^{\perp}$, F_q üzerinde, uzunluğu n olan birer skew θ-devirli koddur,

ii) $C^{\perp}=\gamma_0C_0^{\perp}\oplus\gamma_1C_1^{\perp}\oplus\cdots\oplus\gamma_kC_k^{\perp}$ dual kodu, R üzerinde, uzunluğu n olan bir skew Θ-devirli koddur.

İspat.

i) Teorem 3.2.1.5'in direkt sonucudur.

ii) Önerme 3.2.7 ve Önerme 3.2.1.6'nin direkt sonucudur.

Teorem 3.2.1.8. $C = \gamma_0 C_0 \oplus \gamma_1 C_1 \oplus \cdots \oplus \gamma_k C_k$, R üzerinde, uzunluğu n olan bir skew Θ-devirli kod ve $0 \leq j \leq k$ için $g_j(x)$, F_q üzerinde, uzunluğu n olan skew θ-devirli C_j kodunun monik üreteç polinomu olsun. Bu durumda

i) $C = \langle \gamma_0 g_0(x), \gamma_1 g_1(x), \ldots, \gamma_k g_k(x) \rangle$,

ii) $C = \langle g(x) \rangle$ olacak şekilde bir $g(x) \in R[x, \Theta]$ polinomu vardır, burada $g(x)$, $x^n - 1$'in bir sağ böleni olup $g(x) = \gamma_0 g_0(x) + \gamma_1 g_1(x) + \cdots + \gamma_k g_k(x)$ dır.

İspat. i) C, R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olduğundan Teorem 3.2.1.5'e göre, $0 \leq j \leq k$ için C_j'ler, F_q üzerinde, uzunluğu n olan skew θ-devirli kodlardır. Üstelik $0 \leq j \leq k$ için

$$C_j = \langle g_j(x) \rangle \subseteq F_q[x, \theta] \big/ (x^n - 1)$$

dir. Aynı zamanda $C = \gamma_0 \langle g_0(x) \rangle \oplus \gamma_1 \langle g_1(x) \rangle \oplus \cdots \oplus \gamma_k \langle g_k(x) \rangle$ olduğundan

$$C \subseteq \langle \gamma_0 g_0(x), \gamma_1 g_1(x), \ldots, \gamma_k g_k(x) \rangle \subseteq R[x, \Theta] \big/ (x^n - 1) \tag{3.21}$$

elde edilir. Diğer taraftan

$$\gamma_0 g_0(x) f_0(x) + \gamma_1 g_1(x) f_1(x) + \cdots + \gamma_k g_k(x) f_k(x) \in \langle \gamma_0 g_0(x), \gamma_1 g_1(x), \ldots, \gamma_k g_k(x) \rangle \subseteq R[x, \Theta] \big/ (x^n - 1)$$

olsun, burada $0 \leq j \leq k$ için $f_j(x) \in R[x, \Theta] \big/ (x^n - 1)$ dır. Bu durumda

$$\gamma_j f_j(x) = \gamma_j r_j(x)$$

olacak şekilde $r_j(x) \in F_q[x, \theta] \big/ (x^n - 1)$ vardır. Böylece

$$\gamma_0 g_0(x) f_0(x) + \gamma_1 g_1(x) f_1(x) + \cdots + \gamma_k g_k(x) f_k(k) \in C$$

olur ve

$$\langle \gamma_0 g_0(x), \gamma_1 g_1(x), \ldots, \gamma_k g_k(x) \rangle \subseteq C \tag{3.22}$$

elde edilir. Sonuç olarak

$$C = \langle \gamma_0 g_0(x), \gamma_1 g_1(x), \ldots, \gamma_k g_k(x) \rangle$$

elde edilir.

ii) $0 \leq j \leq k$ olmak üzere C_j'nin monik üreteci olan $g_j(x)$'ler için, i) kısmından

$$C = \langle \gamma_0 g_0(x), \gamma_1 g_1(x), \ldots, \gamma_k g_k(x) \rangle$$

dır. $g(x) = \gamma_0 g_0(x) + \gamma_1 g_1(x) + \cdots + \gamma_k g_k(x)$ olduğunu varsayıp $C' = \langle g(x) \rangle$ olarak alırsak $g(x) \in C$ olduğundan $C' \subseteq C$ olur. $0 \leq i, j \leq k$ ve $i \neq j$ için $\gamma_j^2 = \gamma_j,\ \gamma_i \gamma_j = 0$ özelliklerinden

$$\begin{aligned} \gamma_j(\gamma_0 g_0(x) + \gamma_1 g_1(x) + \cdots + \gamma_k g_k(x)) &= 0 + \cdots + 0 + \gamma_j^2 g_j(x) + 0 + \cdots + 0 \\ &= \gamma_j g_j(x) \in C' \end{aligned}$$

olup $C \subseteq C'$ bulunur. Böylece $C = C'$ ve $C = \langle g(x) \rangle$ elde edilir, burada $g(x) = \gamma_0 g_0(x) + \gamma_1 g_1(x) + \cdots + \gamma_k g_k(x)$ dır.

Şimdi $g(x)$'in $R[x, \Theta]$'da $x^n - 1$'in bir sağ böleni olduğunu gösterelim. $0 \leq j \leq k$ için $g_j(x)$, C_j'nin monik üreteç polinomu olduğundan $g_j(x)$, $x^n - 1$'i sağdan böler, yani

$$x^n - 1 = h_j(x) g_j(x)$$

olacak şekilde $h_j(x) \in C_j$ vardır. $0 \leq i, j \leq k$ ve $i \neq j$ için $\gamma_j^2 = \gamma_j,\ \gamma_i \gamma_j = 0$ ve $\sum_{i=0}^{k} \gamma_i \equiv 1$

$(\text{mod } u^{k+1}-u)$ olduğundan

$$\begin{aligned} x^n-1 &= (\gamma_0+\gamma_1+\cdots+\gamma_k)(x^n-1) \\ &= \gamma_0(x^n-1)+\gamma_1(x^n-1)+\cdots+\gamma_k(x^n-1) \\ &= \gamma_0 h_0(x)g_0(x)+\gamma_1 h_1(x)g_1(x)+\cdots+\gamma_k h_k(x)g_k(x) \\ &= \big(\gamma_0 h_0(x)+\gamma_1 h_1(x)+\cdots+\gamma_k h_k(x)\big)\big(\gamma_0 g_0(x)+\gamma_1 g_1(x)+\cdots+\gamma_k g_k(x)\big) \\ &= \big(\gamma_0 h_0(x)+\gamma_1 h_1(x)+\cdots+\gamma_k h_k(x)\big)g(x) \end{aligned}$$

bulunur. Böylece $g(x)$, x^n-1'i sağdan böler.

Sonuç 3.2.1.9. $|\langle\Theta\rangle|\,|\,n$ olsun. $C=\gamma_0C_0\oplus\gamma_1C_1\oplus\cdots\oplus\gamma_kC_k$, R üzerinde, uzunluğu n olan bir skew Θ-devirli kod ve $0\le j\le k$ için $g_j(x)$, F_q üzerinde, uzunluğu n olan skew θ-devirli C_j kodunun monik üreteç polinomu olsun. $0\le j\le k$ için $h_j(x)\in F_q[x,\theta]$ olmak üzere $x^n-1=h_j(x)g_j(x)$ olup $h_j(x)=\beta_0+\beta_1x+\cdots+\beta_{n-s}x^{n-s}$ şeklinde ifade edilsin. Bu durumda C_j skew θ-devirli kodunun duali olan $C_j^{\perp}$ için

i) $C^{\perp}=\langle\gamma_0h_0^*(x),\,\gamma_1h_1^*(x),\,\ldots,\,\gamma_kh_k^*(x)\rangle$,

ii) $C^{\perp}=\langle h'(x)\rangle$, olmak üzere $h'(x)=\gamma_0h_0^*(x)+\gamma_1h_1^*(x)+\cdots+\gamma_kh_k^*(x)$

geçerlidir, burada $h_j^*(x)=\beta_{n-s}+\theta(\beta_{n-s-1})x+\cdots+\theta^{n-s}(\beta_0)x^{n-s}$ dir [2].

4. BULGULAR

Bu bölümde R halkası üzerindeki skew Θ-devirli kodların bir uygulaması verilmişti. Bu bölüm iki alt bölümden oluşmaktadır. Birinci alt bölümde, R halkası üzerinde dualini içeren skew Θ-devirli kodlardan kuantum kodların elde edilmesi için gerekli olan teorik çalışma verilmiştir. İkinci alt bölümde ise, ilk alt bölümde yapılan teorik çalışmanın bir uygulaması olarak bazı örnekler sunulmuştur.

4.1. R ÜZERİNDEKİ SKEW DEVİRLİ KODLARDAN ELDE EDİLEN KUANTUM KODLARIN İNŞASI

q bir asal sayının kuvveti olmak üzere F_q sonlu cismi üzerinde, uzunluğu n olan bir kuantum hata düzelten kod, q^n boyutlu $(\mathbb{C}^q)^{\otimes n}$ Hilbert uzayının q^k boyutlu bir alt uzayıdır ve bu kuantum hata düzelten kod $[[n,k,d]]_q$ ile gösterilir, burada $\otimes n$, vektör uzayının tensör çarpımını ve d, kuantum hata düzelten kodun minimum Hamming uzaklığını gösterir. Kuantum hata düzelten kodlar, kuantum hesaplama ve kuantum iletişim üzerinde oldukça önemli bir yere sahiptir. Kuantum hata düzelten kodlar ve klasik hata düzelten kodlar arasında önemli bir bağlantı vardır. İlk kuantum hata düzelten kodlar, birbirinden bağımsız olarak, 1995'de Shor [11] daha sonra 1996'da Steane [13] tarafından elde edilmiştir. 1998'de Calderbank vd. [3], bir halka üzerindeki klasik hata düzelten kodlardan kuantum hata düzelten kodları elde etmek için elverişli bir metod vermiştir. Robert Calderbank, Peter Shor ve Andrew Steane'ye atfen CSS inşa metodu olarak adlandırılan bu metod, sonlu cisimler üzerindeki kuantum hata düzelten kodları elde etmek için verilen önemli bir yöntemdir.

Teorem 4.1.1 ([3], CSS İnşa Metodu)**.** C_1 ve C_2, F_q üzerinde sırasıyla $[n, k_1, d_1]$ ve $[n, k_2, d_2]$ parametrelerine sahip iki lineer kod olsun. $d = \min\{d_1, d_2\}$ olmak üzere eğer $C_2^{\perp} \subseteq C_1$ ise $[[n, k_1 + k_2 - n, d]]_q$ parametreli bir kuantum hata düzelten kod vardır.

Özel olarak eğer $C_1^{\perp} \subseteq C_1$ ise $[[n, 2k_1 - n, d_1]]_q$ parametreli bir kuantum hata düzelten kod vardır.

4.1.1. R Üzerinde Dualini İçeren Skew Devirli Kodlar

Bu bölümde, R halkası üzerindeki skew Θ-devirli kodlardan kuantum kodların elde edilmesi için gerekli olan, bir skew Θ-devirli kodun dualini içermesi için bir gerek ve yeter koşul verilmiştir.

Teorem 4.1.1.1. $|\langle\theta\rangle| \mid n$ olmak üzere $0 \leq j \leq k$ için $C_j = \langle g_j(x)\rangle$, F_q üzerinde, uzunluğu n olan bir skew θ-devirli kod olsun. Bu durumda $C_j^{\perp} \subseteq C_j$ olması için gerek ve yeter koşul $x^n - 1$'in $h_j^*(x)h_j(x)$'i sağdan bölmesidir.

İspat. $0 \leq j \leq k$ için $C_j = \langle g_j(x)\rangle$, F_q üzerinde, uzunluğu n olan, duali içeren skew θ-devirli kod ve $C_j^{\perp} \subseteq C_j$ olsun. Bu durumda $h_j^*(x) \in C_j^{\perp} \subseteq C_j = \langle g_j(x)\rangle$ olduğundan

$$h_j^*(x) = K_j(x)g_j(x)$$

olacak şekilde bir $K_j(x) \in F_q[x,\theta]$ vardır. $|\langle\theta\rangle| \mid n$ olduğundan

$$x^n - 1 = h_j(x)g_j(x) \in Z(F_q[x,\theta])$$

$\Rightarrow h_j(x)$ ve $g_j(x)$ yer değiştirebilir. Böylece

$$\begin{aligned} h_j^*(x)h_j(x) &= (K_j(x)g_j(x))h_j(x) \\ &= K_j(x)(h_j(x)g_j(x)) \\ &= K_j(x)(x^n - 1) \end{aligned}$$

elde edilir. O halde $0 \leq j \leq k$ için $x^n - 1$, $h_j^*(x)h_j(x)$'i sağdan böler.

Diğer taraftan, $0 \leq j \leq k$ için $x^n - 1$, $h_j^*(x)h_j(x)$'i sağdan bölsün. Bu durumda

$$h_j^*(x)h_j(x) = l(x)(x^n - 1)$$

olacak şeklide bir $l(x) \in F_q[x,\theta]$ vardır. Şimdi bir $a(x) \in C_j^{\perp} = \langle h_j^*(x)\rangle$ alalım. Buradan

$$a(x) = c(x)h_j^*(x)$$

olacak şekilde bir $c(x) \in F_q[x,\theta]$ vardır. Bu eşitliğin her iki tarafı $h_j(x)$ ile çarpılırsa

$$\begin{aligned} a(x)h_j(x) &= (c(x)h_j^*(x))h_j(x) \\ &= c(x)(h_j^*(x)h_j(x)) \\ &= c(x)l(x)(x^n-1) \\ &= c(x)l(x)(h_j(x)g_j(x)) \\ &= c(x)l(x)g_j(x)h_j(x) \end{aligned}$$

elde edilir. Buradan

$$\begin{aligned} a(x)h_j(x) - c(x)l(x)g_j(x)h_j(x) &= 0 \\ \big(a(x) - c(x)l(x)g_j(x)\big)h_j(x) &= 0 \end{aligned}$$

bulunur. $h_j(x) \neq 0$ olduğundan $\big(a(x) - c(x)l(x)g_j(x)\big) = 0$ olur. Böylece

$$a(x) = c(x)l(x)g_j(x)$$

elde edilir. Dolayısıyla $a(x) \in \langle g_j(x)\rangle = C_j$ ve buradan $C_j^{\perp} \subseteq C_j$ sonucuna varılır. Böylece ispat bitmiş olur.

Not: $x^n - 1 = h_j(x)g_j(x)$ olacak şekildeki $h_j(x) \in F_q[x,\theta]$ polinomunun hesaplanması durumunda x^n-1'in herhangi bir sırada $g_j(x)$'den farklı bir çarpanı alınamaz. Örneğin x^8-1 polinomu F_{25} üzerinde çarpanlarına ayrılırsa

$$x^8 - 1 = (w+x)(w^3+x)^2(w^4+x)(w^8+x)(w^{10}+x)(w^{14}+x)(w^{17}+x) \in F_{25}[x,\theta]$$

elde edilir. $j = 0,1,2$ için $g_j(x) = w^3 + x$ olsun. Bu durumda $j = 0,1,2$ için $C_j = \langle g_j(x)\rangle$'ler, F_{25} üzerinde birer skew devirli kod olur. Şimdi

$$\begin{aligned} h_1(x) &= (w+x)(w^3+x)(w^4+x)(w^8+x)(w^{10}+x)(w^{14}+x)(w^{17}+x) \\ h_2(x) &= (w^4+x)(w^8+x)(w^{10}+x)(w^{14}+x)(w^{17}+x)(w+x)(w^3+x) \end{aligned}$$

polinomlarını göz önüne alalım. Buradan

$$\begin{aligned}(w^3+x)h_1(x) &= (w^3+x)(w+x)(w^3+x)(w^4+x)(w^8+x)(w^{10}+x)(w^{14}+x)(w^{17}+x)\\ &= 4+w^7x+w^{11}x^2+w^3x^3+w^{19}x^5+w^{23}x^6+w^{15}x^7+x^8\\ &\neq x^8-1\end{aligned}$$

elde edilir. Diğer taraftan

$$\begin{aligned}(w^3+x)h_2(x) &= (w^3+x)(w^4+x)(w^8+x)(w^{10}+x)(w^{14}+x)(w^{17}+x)(w+x)(w^3+x)\\ &= x^8-1\end{aligned}$$

elde edilir. Yani $h_j(x)$'in hesaplanmasında dikkatli olunmalıdır.

Teorem 4.1.1.2. $|\langle\Theta\rangle|\ n$ olmak üzere $C=\gamma_0C_0\oplus\gamma_1C_1\oplus\cdots\oplus\gamma_kC_k$, R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olsun. Bu durumda $0\leq j\leq k$ için $C^{\perp}\subseteq C$ olması için gerek ve yeter koşul x^n-1'in $h_j^*(x)h_j(x)$'i sağdan bölmesidir.

İspat. $|\langle\Theta\rangle|\ n$ olmak üzere R üzerinde, uzunluğu n olan bir skew Θ-devirli C kodu için $C^{\perp}\subseteq C$ olsun. Bu durumda

$$\gamma_0C_0^{\perp}\oplus\gamma_1C_1^{\perp}\oplus\cdots\oplus\gamma_kC_k^{\perp}\subseteq\gamma_0C_0\oplus\gamma_1C_1\oplus\cdots\oplus\gamma_kC_k$$

yazılır. Her iki tarafı modülo γ_j'ye göre göz önüne alırsak $0\leq j\leq k$ için

$$C_j^{\perp}\subseteq C_j$$

elde edilir. Böylece Teorem 4.1.1.1'e göre $0\leq j\leq k$ için x^n-1, $h_j^*(x)h_j(x)$'i sağdan böler.

Diğer taraftan $0\leq j\leq k$ için x^n-1, $h_j^*(x)h_j(x)$'i sağdan bölsün. Bu durumda Teorem 4.1.1.1'göre $C_j^{\perp}\subseteq C_j$ dir. Bu

$$\gamma_0C_0^{\perp}\oplus\gamma_1C_1^{\perp}+\oplus\cdots\oplus\gamma_kC_k^{\perp}\subseteq\gamma_0C_0\oplus\gamma_1C_1\oplus\cdots\oplus\gamma_kC_k$$

olduğunu ifade eder. Böylece

$$C^{\perp}\subseteq C$$

elde edilir ve böylece ispat bitmiş olur.

Sonuç 4.1.1.3. $|\langle\Theta\rangle| \, n$ olmak üzere $C = \langle g(x)\rangle$, R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olsun. Bu takdirde $0 \leq j \leq k$ için $C^{\perp} \subseteq C$ olması için gerek ve yeter koşul $C_j^{\perp} \subseteq C_j$ olmasıdır.

İspat. İspat, Teorem 4.1.1.1 ve Teorem 4.1.1.2'nin bir sonucu olarak elde edilir.

4.1.2. Kuantum Kodların İnşası

Teorem 4.1.2.1. $|\langle\Theta\rangle| \, | \, n$ olmak üzere $C = \gamma_0 C_0 \oplus \gamma_1 C_1 \oplus \cdots \oplus \gamma_k C_k$ R üzerinde, uzunluğu n olan bir skew Θ-devirli kod olsun. Eğer $0 \leq j \leq k$ için $C_j^{\perp} \subseteq C_j$ ise bu durumda $C^{\perp} \subseteq C$ ve $[[(k+1)n,\, 2k' - (k+1)n,\, d_H]]_q$ parametrelerine sahip bir kuantum hata düzelten kod vardır, burada d_H, $\phi(C)$ kodunun Hamming uzaklığını ve k', $\phi(C)$ kodunun boyutunu göstermektedir.

İspat. $C = \gamma_0 C_0 \oplus \gamma_1 C_1 \oplus \cdots \oplus \gamma_k C_k$ R üzerinde, uzunluğu n olan bir skew Θ-devirli kod ve $0 \leq j \leq k$ için $C_j^{\perp} \subseteq C_j$ olsun. Bu durumda Sonuç 4.1.1.3'e göre $C^{\perp} \subseteq C$ dir. Şimdi $\phi(C^{\perp}) \subseteq \phi(C)^{\perp}$ olduğunu ispat edelim. Bunun için $x_1 = \gamma_0 a_0 + \gamma_1 a_1 + \cdots + \gamma_k a_k \in C$ ve $x_2 = \gamma_0 b_0 + \gamma_1 b_1 + \cdots + \gamma_k b_k \in C^{\perp}$ alalım. O halde x_1 ile x_2'nin iç çarpımı 0'dır, yani

$$\langle x_1, x_2\rangle = \gamma_0 a_0 b_0 + \gamma_1 a_1 b_1 + \cdots + \gamma_k a_k b_k = 0$$

olur. $R = F_q + uF_q + \cdots + u^k F_q$, F_q üzerinde, boyutu $k+1$ olan bir vektör uzayı olduğu için R'deki her eleman $\{\gamma_0, \gamma_1, \ldots, \gamma_k\}$ kümesinin bir lineer kombinasyonu olarak yazılır. $\{\gamma_0, \gamma_1, \ldots, \gamma_k\}$ kümesinin elemanları sıfırdan farklı olup bu elemanlar idempotenttir ve ikişer ikişer ortogonaldir, üstelik R'yi üretir. Bu küme lineer bağımsızdır, çünkü eğer

$$d_0\gamma_0 + d_1\gamma_1 + \cdots + d_k\gamma_k = 0$$

ise $0 \leq i \leq k$ için her iki tarafı γ_i ile çarparsak $d_i\gamma_i^2 = 0$ ve böylece

$$d_i = 0$$

elde edilir. Dolayısıyla $\{\gamma_0, \gamma_1, \ldots, \gamma_k\}$ lineer bağımsızdır ve R için bir bazdır. Bundan dolayı

$$\gamma_0 a_0 b_0 + \gamma_1 a_1 b_1 + \cdots + \gamma_k a_k b_k = 0$$

denkleminden

$$a_0b_0 = a_1b_1 = \ldots = a_kb_k = 0$$

elde edilir. Böylece, $MM^T = \lambda I_{k+1}$ olduğundan, $\phi(x_1)$ ile $\phi(x_2)$'nin iç çarpımından

$$\begin{aligned}\langle \phi(x_1), \phi(x_2) \rangle &= \langle (a_0, a_1, \ldots, a_k)M, (b_0, b_1, \ldots, b_k)M \rangle \\ &= \lambda^2(a_0b_0 + a_1b_1 + \cdots + a_kb_k) \\ &= 0\end{aligned}$$

elde edilir. $x_1 \in C$ olduğundan $\phi(x_1) \in \phi(C)$ olur. Dolayısıyla, yukarıdaki sonuçtan $\phi(x_2) \in \phi(C)^\perp$ dir. $x_2 \in C^\perp$ olduğundan $\phi(x_2) \in \phi(C^\perp)$ olup böylece $\phi(C^\perp) \subseteq \phi(C)^\perp$ elde edilir. Şimdi $x \in \phi(C^\perp)$ olsun. $\phi(C^\perp) \subseteq \phi(C)^\perp$ olduğundan $x \in \phi(C)^\perp$ olur. Ayrıca $x \in \phi(C^\perp)$ olduğundan $x = \phi(y)$ olacak şekilde bir $y \in C^\perp$ vardır. $C^\perp \subseteq C$ olduğundan $y \in C$ elde edilir. Böylece $x = \phi(y) \in \phi(C)$ dir. Dolayısıyla $\phi(C)^\perp \subseteq \phi(C)$ olur. O halde $\phi(C)$, F_q üzerinde, $[(k+1)n, k', d_H]$ parametrelerine sahip olan bir lineer kod olduğundan Teorem 4.1.1'de verilen CSS inşa metodu ile, $[[(k+1)n, 2k' - (k+1)n, d_H]]_q$ parametrelerine sahip bir kuantum hata düzelten kod vardır, böylece ispat bitmiş olur.

4.2. ÖRNEKLER

Bu kısımda önceki bölümlerde yapılan teorik çalışmanın bir uygulaması olarak bazı örnekler verilecektir. Bu örnekler [5] çalışmasından alınmıştır. Aşağıdaki örneklerde $F_{p^m}^*$ notasyonu $F_{p^m}^* = F_{p^m} \backslash \{0\} = \langle w \rangle$ şeklinde ifade edilen w tarafından üretilen devirli gruptur.

Örnek 4.2.1. Eleman sayısı 9 olan sonlu cismi ele alalım. F_9 ile gösterilen bu cisim F_3 üzerinde, boyutu 2 olan bir vektör uzayıdır ve

$$\begin{aligned}F_9 = F_3[\alpha]/\langle \alpha^2 + 1 \rangle &= \{a_0 + a_1\alpha \mid a_0, a_1 \in F_3\} \\ &= \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}\end{aligned}$$

şeklinde ifade edilir. F_9 cisminin işlem tabloları aşağıdaki gibidir:

$+ \pmod 3$	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
0	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
1	1	2	0	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	$2+2\alpha$	2α
2	2	0	1	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2α	$1+2\alpha$
α	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$	0	1	2
$1+\alpha$	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	$2+2\alpha$	2α	1	2	0
$2+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2α	$1+2\alpha$	2	0	1
2α	2α	$1+2\alpha$	$2+2\alpha$	0	1	2	α	$1+\alpha$	$2+\alpha$
$1+2\alpha$	$1+2\alpha$	$2+2\alpha$	2α	1	2	0	$1+\alpha$	$2+\alpha$	α
$2+2\alpha$	$2+2\alpha$	2α	$1+2\alpha$	2	0	1	$2+\alpha$	α	$1+\alpha$

Tablo 4.1: F_9'un toplam tablosu

$\cdot \pmod 3$	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2	0	2	1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α	0	α	2α	2	$2+\alpha$	$2+2\alpha$	1	$1+\alpha$	$1+2\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	2α	1	$1+2\alpha$	2	α
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	1	α	$1+\alpha$	2α	2
2α	0	2α	α	1	$1+2\alpha$	$1+\alpha$	2	$2+2\alpha$	$2+\alpha$
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	2	2α	$2+2\alpha$	α	1
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	α	2	$2+\alpha$	1	2α

Tablo 4.2: F_9'un çarpım tablosu

$F_9^* = F_9 \backslash \{0\}$ kümesi çarpma işlemine göre mertebesi 8 olan bir devirli gruptur. $w := x+1$ elemanı bu devirli grubun bir üreteci olup

$$F_9^* = F_9 \backslash \{0\} = \langle w \rangle = \{w^0, w, w^2, w^3, w^4, w^5, w^6, w^7\}$$

şeklinde yazılır, burada

$$w^0 = w^8 = (1+\alpha)(2+\alpha) = w^{8n} = 1$$
$$w^1 = 1+\alpha$$
$$w^2 = (1+\alpha)(1+\alpha) = 2\alpha$$
$$w^3 = (1+\alpha)(2\alpha) = 1+2\alpha$$
$$w^4 = (1+\alpha)(1+2\alpha) = 2$$

$$w^5 = (1+\alpha)2 = 2+2\alpha$$
$$w^6 = (1+\alpha)(2+2\alpha) = \alpha$$
$$w^7 = (1+\alpha)\alpha = 2+\alpha$$

dır. Şimdi F_9'un işlem tablolarını ve her $a \in F_9$ için $\theta(a) = a^3$ şeklinde tanımlı F_9'un Frobenius otomorfisini göz önüne alarak $F_9[x,\theta]$ üzerinde x^8-1 polinomunun

$$x^8-1 = (w^2+x)^2(w^3+x)(w^5+x)(1+w^3x+x^2)(1+w^7x+x^2)$$

şeklinde verilen çarpanlara ayrılışı sağladığını gösterelim.

$$\begin{aligned}*(w^2+x)^2 &= (w^2+x)(w^2+x)\\ &= w^4+w^2x+xw^2+x^2\\ &= w^4+w^2x+\theta(w^2)x+x^2\\ &= w^4+w^2x+w^6x+x^2\\ &= w^4+(w^2+w^6)x+x^2\\ &= w^4+(2\alpha+\alpha)x+x^2\\ &= w^4+x^2\end{aligned}$$

olur. Benzer şekilde

$$\begin{aligned}*(w^2+x)^2(w^3+x) &= (w^4+x^2)(w^3+x)\\ &= w^7+w^4x+w^3x^2+x^3,\end{aligned}$$

$$\begin{aligned}*(w^2+x)^2(w^3+x)(w^5+x) &= (w^7+w^4x+w^3x^2+x^3)(w^5+x)\\ &= w^4+x^4,\end{aligned}$$

$$\begin{aligned}*(w^2+x)^2(w^3+x)(w^5+x)(1+w^3x+x^2) &= (w^4+x^4)(1+w^3x+x^2)\\ &= w^4+w^7x+w^4x^2+x^4+w^3x^5+x^6\end{aligned}$$

ve son olarak

$$\begin{aligned}
&*(w^2+x)^2(w^3+x)(w^5+x)(1+w^3x+x^2)(1+w^7x+x^2)\\
&\qquad=(w^4+w^7x+w^4x^2+x^4+w^3x^5+x^6)(1+w^7x+x^2)\\
&\qquad=w^4+(w^7+w^3)x+(w^4+w^7w^5+w^4)x^2+(w^4w^7+w^7)x^3+(1+w^4)x^4\\
&\qquad\qquad+(w^3+w^7)x^5+(1+w^3w^5+1)x^6+(w^7+w^3)x^7+x^8\\
&\qquad=2+0x+0x^2+0x^3+0x^4+0x^5+0x^6+0x^7+x^8\\
&\qquad=2+x^8\\
&\qquad=x^8-1
\end{aligned}$$

elde edilir.

Örnek 4.2.2. Örnek 3.2.3'te verilen $R = F_9[u]/(u^2-u)$ halkasını ve bu halka üzerinde tanımlı Gray dönüşümü göz önüne alalım. R halkası için $k=1$ ve $p=3$ olur. $0 \leq i \leq 1$ için $\theta(a_i) = a_i^3$ şeklinde verilen $\theta \in Aut(F_9)$ Frobenius otomorfisinin

$$\Theta : R \longmapsto R$$

olmak üzere

$$\Theta(a_0+ua_1) = \theta(a_0)+u\theta(a_1) = a_0^3+ua_1^3$$

şeklinde verilen genişlemesini ele alalım. $n=8$ ve $|\langle\theta\rangle| = 2$ olduğundan $|\langle\theta\rangle| \mid n$ dir. Örnek 4.2.1'den x^8-1 polinomu $F_9[x,\theta]$ üzerinde

$$x^8-1 = (w^2+x)^2(w^3+x)(w^5+x)(1+w^3x+x^2)(1+w^7x+x^2)$$

şeklinde çarpanlarına ayrılır. O halde $g_0(x) = w^2+x$ ve $g_1(x) = (1+w^7x+x^2)(w^2+x)$ polinomları için $C_0 = \langle g_0(x)\rangle$ ve $C_1 = \langle g_1(x)\rangle$, F_9 üzerinde skew devirli kodlardır. Böylece

$$C = \langle \gamma_0 C_0, \gamma_1 C_1\rangle = \langle \gamma_0 g_0(x), \gamma_1 g_1(x)\rangle$$

R üzerinde bir skew devirli kod olur. $g_0(x)$ ve $g_1(x)$ polinomları için

- $h_0(x) = w^2+x+w^2x^2+x^3+w^2x^4+x^5+w^2x^6+x^7$

- $h_1(x) = w^2 + w^3x + 2x^2 + w^6x^3 + w^3x^4 + x^5$

dır. $h_0(x)$ ve $h_1(x)$ polinomları için

- $h_0^*(x) = 1 + w^6x + x^2 + w^6x^3 + x^4 + w^6x^5 + x^6 + w^6x^7$
- $h_1^*(x) = 1 + wx + w^6x^2 + 2x^3 + w^3x^4 + w^6x^5$

olup

- $h_0^*(x)h_0(x) = (w^6 + w^6x^2 + w^6x^4 + w^6x^6)(x^8 - 1)$
- $h_1^*(x)h_1(x) = (w^6 + w^6x^2)(x^8 - 1)$

elde edilir. Dolayısıyla $x^8 - 1$ polinomu $h_0^*(x)h_0(x)$ ve $h_1^*(x)h_1(x)$ polinomlarını sağdan böler. Böylece Teorem 4.1.1.2'ye göre $C^{\perp} \subseteq C$ elde edilir. $\phi(C)$, F_9 üzerinde bir $[16, 12, 4]$ lineer kod olur ve Teorem 4.1.2.1'e göre $[[16, 8, 4]]_9$ parametrelerine sahip bir kuantum hata düzelten kod vardır.

Örnek 4.2.3. Örnek 3.2.4'de verilen $R = F_{25}[u]/(u^3 - u)$ halkasını ve bu halka üzerinde tanımlı Gray dönüşümü göz önüne alalım. R halkası için $k = 2$ ve $p = 5$ olur. $0 \leq i \leq 2$ için $\theta(a_i) = a_i^5$ şeklinde verilen $\theta \in Aut(F_{25})$ Frobenius otomorfisinin

$$\Theta : R \longmapsto R$$

olmak üzere

$$a_0 + ua_1 + u^2a_2 \longmapsto \theta(a_0) + u\theta(a_1) + u^2\theta(a_2) = a_0^5 + ua_1^5 + u^2a_2^5$$

şeklindeki verilen genişlemesini ele alalım. $n = 16$ ve $|\langle\theta\rangle| = 2$ olduğundan $|\langle\theta\rangle| \mid n$ dir. $x^{16} - 1$ polinomu $F_{25}[x, \theta]$ üzerinde

$$\begin{aligned} x^{16} - 1 =& (1 + x)(4 + x)(w^2 + x)(w^5 + x)(w^{11} + x)(w^{13} + x)(w^{19} + x)(w^{22} + x) \\ & (w + w^8x + x^2)(w^5 + w^{20}x + x^2)(w^7 + w^{17}x + x^2)(w^{11} + w^5x + x^2) \in F_{25}[x, \theta] \end{aligned}$$

şeklinde çarpanlarına ayrılır. O halde $g_0(x) = w^5 + x$, $g_1(x) = w^5 + x$ ve $g_2(x) = (w^{22} + x)(w + w^8x + x^2)$ polinomları için $C_0 = \langle g_0(x) \rangle$, $C_1 = \langle g_1(x) \rangle$ ve $C_2 = \langle g_2(x) \rangle$, F_{25} üzerinde skew devirli kod olurlar. Bu durumda

$$\begin{aligned} C =& \langle \gamma_0 g_0(x),\, \gamma_1 g_1(x),\, \gamma_2 g_2(x) \rangle \\ =& \langle \gamma_0 C_0,\, \gamma_1 C_1,\, \gamma_2 C_2 \rangle \end{aligned}$$

R üzerinde bir skew devirli kod olur. $g_0(x)$, $g_1(x)$ ve $g_2(x)$ polinomları için

- $h_0(x) = h_1(x) = w^7 + 3x + wx^2 + 4x^3 + w^{19}x^4 + 2x^5 + w^{13}x^6 + x^7 + w^7x^8 + 3x^9 + wx^{10} + 4x^{11} + w^{19}x^{12} + 2x^{13} + w^{13}x^{14} + x^{15}$
- $h_2(x) = w^{13} + w^9x + w^{10}x^2 + w^8x^3 + w^5x^4 + w^5x^5 + w^4x^6 + w^2x^7 + w^3x^8 + w^{22}x^9 + w^{16}x^{10} + w^{14}x^{11} + w^{14}x^{12} + x^{13}$

dır. $h_0(x), h_1(x)$ ve $h_2(x)$ polinomları için

- $h_0^*(x) = h_1^*(x) = 1 + w^{17}x + 2x^2 + w^{23}x^3 + 4x^4 + w^5x^5 + 3x^6 + w^{11}x^7 + x^8 + w^{17}x^9 + 2x^{10} + w^{23}x^{11} + 4x^{12} + w^5x^{13} + 3x^{14} + w^{11}x^{15}$
- $h_2^*(x) = 1 + w^{22}x + w^{14}x^2 + w^8x^3 + w^{22}x^4 + w^{15}x^5 + w^2x^6 + w^{20}x^7 + w^5x^8 + wx^9 + w^8x^{10} + w^2x^{11} + w^9x^{12} + w^{17}x^{13}$

olup

- $h_i^*(x)h_i(x) = (w^{19} + w^{19}x + w^{23}x^2 + w^7x^4 + w^7x^5 + w^{11}x^6 + w^{19}x^8 + w^{19}x^9 + w^{23}x^{10} + w^7x^{12} + w^7x^{13} + w^{11}x^{14})(x^{16} - 1)$; $i = 0, 1$
- $h_2^*(x)h_2(x) = (w + w^{15}x + w^3x^2 + 3x^4 + 2x^6 + w^3x^8 + w^3x^9 + w^{17}x^{10})(x^{16} - 1)$

elde edilir. Dolayısıyla $k = 0, 1, 2$ için $x^{16} - 1$ polinomu $h_k^*(x)h_k(x)$ polinomunu sağdan böler. Teorem 4.1.1.2'ye göre $C^{\perp} \subseteq C$ elde edilir. $\phi(C)$, F_{25} üzerinde bir $[48, 43, 4]$ lineer kod olur ve Teorem 4.1.2.1'e göre $[[48, 38, 4]]_{25}$ parametrelerine sahip bir kuantum hata düzelten kod vardır.

Örnek 4.2.4. Örnek 3.2.5'te verilen $R = F_{49}[u]/(u^4 - u)$ halkasını ve bu halka üzerinde tanımlı Gray dönüşümü göz önüne alalım. R halkası için $k = 3$ ve $p = 7$ olur. $0 \leq i \leq 3$ için $\theta(a_i) = a_i^7$ şeklinde verilen $\theta \in Aut(F_{49})$ Frobenius otomorfisinin

$$\Theta : R \longmapsto R$$

olmak üzere

$$a_0 + ua_1 + u^2a_2 + u^3a_3 \longmapsto \theta(a_0) + u\theta(a_1) + u^2\theta(a_2) + u^3\theta(a_3) = a_0^7 + ua_1^7 + u^2a_2^7 + u^3a_3^7$$

şeklinde verilen genişlemesini ele alalım. $n = 18$ ve $|\langle\theta\rangle| = 2$ olduğundan $|\langle\theta\rangle| \mid n$ dır. $x^{18} - 1$ polinomu $F_{49}[x, \theta]$ üzerinde

$$\begin{aligned} x^{18} - 1 =& (1+x)(3+x)(4+x)(6+x)(w^{22}+x)(w^{34}+x)(w^{10} + w^7x + w^{18}x^2 + x^3) \\ & (w^{14} + w^{22}x + w^{27}x^2 + x^3)(w^{26} + w^{22}x + w^{21}x^2 + x^3) \\ & (w^{46} + w^7x + w^6x^2 + x^3) \in F_{49}[x, \theta] \end{aligned}$$

şeklinde çarpanlarına ayrılır. O halde

$$\begin{aligned} g_0(x) &= (w^{26} + w^{22}x + w^{21}x^2 + x^3)(w^{34} + x)(w^{22} + x) \\ g_1(x) &= w^{22} + x \\ g_2(x) &= w^{46} + w^7x + w^6x^2 + x^3 \\ g_3(x) &= 4 + x \end{aligned}$$

polinomları için $k = 0, 1, 2, 3$ olmak üzere $C_k = \langle g_k(x)\rangle$, F_{49} üzerinde bir skew devirli kod olur. Bu durumda

$$\begin{aligned} C =& \langle \gamma_0 g_0(x),\, \gamma_1 g_1(x),\, \gamma_2 g_2(x),\, \gamma_3 g_3(x)\rangle \\ =& \langle \gamma_0 C_0,\, \gamma_1 C_1,\, \gamma_2 C_2,\, \gamma_3 C_3\rangle \end{aligned}$$

R üzerinde bir skew devirli kod olur. $g_0(x)$, $g_1(x)$, $g_2(x)$ ve $g_3(x)$ polinomları için

$$h_k^*(x)h_k(x) = f_k(x)(x^{16} - 1)\,,\ 0 \leq k \leq 3$$

- $f_0(x) = w^{14} + w^{29}x + w^{44}x^2 + w^{34}x^3 + w^{44}x^4 + w^{10}x^5 + w^{44}x^6 + w^5x^7 + w^{26}x^8$
- $f_1(x) = w^{26} + w^5x + w^4x^2 + w^{29}x^3 + w^{14}x^4 + w^{26}x^6 + w^5x^7 + w^4x^8 + w^{29}x^9 + w^{14}x^{10} + w^{26}x^{12} + w^5x^{13} + w^4x^{14} + w^{29}x^{15} + w^{26}x^{14}$
- $f_2(x) = w^2 + w^{41}x + w^{33}x^2 + w^3x^3 + w^{39}x^4 + w^{41}x^5 + w^{28}x^6 + w^{17}x^7 + w^9x^8 + w^{27}x^9 + w^{15}x^{10} + w^{17}x^{11} + w^{38}x^{12}$
- $f_3(x) = 2 + 2x + 5x^3 + 5x^4 + 2x^6 + 2x^7 + 5x^9 + 5x^{10} + 2x^{12} + 2x^{13} + 5x^{15} + 5x^{16}$

elde edilir. Dolayısıyla $k = 0, 1, 2, 3$ için $x^{18} - 1$ polinomu $h_k^*(x)h_k(x)$ polinomunu sağdan böler. Teorem 4.1.1.2'ye göre $C^{\perp} \subseteq C$ elde edilir. $\phi(C)$, F_{49} üzerinde bir $[72, 62, 4]$ lineer kod olur ve Teorem 4.1.2.1'e göre $[[72, 52, 4]]_{49}$ parametrelerine sahip bir kuantum hata düzelten kod vardır.

5. TARTIŞMA VE SONUÇ

Cebirsel kodlama teorisinde akla gelen ilk alfabe iki elemanlı $F_2 = \{0,1\}$ cismidir. Bu alfabenin bir genelleştirilmesi p bir asal sayı olmak üzere p elemanlı $\mathbb{F}_p$ sonlu cismidir. Günümüzde cebirsel kodlama teorisi alanında farklı cebirsel yapıların göz önüne alınması büyük ilgi görmektedir. Son zamanlarda farklı tipteki cisim ve halkaların göz önüne alınmasıyla tanımlanan halkalar üzerinde cebirsel kodlama teorisi çalışılmaya başlanmıştır.

Literatürde lineer kodlardan kuantum hata düzelten kodların elde edilmesi için genellikle devirli kodlar kullanılmıştır. Son yıllarda ise skew devirli kodlardan kuantum hata düzelten kodların elde edilmesi büyük ivme kazanan bir çalışma alanıdır.

Bu tez kapsamında, cebirsel kodlama teorisi alanında yeni çalışılmaya başlanan bir halka üzerindeki skew devirli kodların özellikleri ve bu halka üzerindeki skew devirli kodlardan kuantum hata düzelten kodların elde edilmesi incelenmiştir. Daha açık bir ifade ile p tek bir asal sayı ve m bir doğal sayısı olsun. Bu tez çalışmasında $k \mid p-1$ ve $q = p^m$ olacak şekilde bir k ve q tam sayıları için $F_q[u]/(u^{k+1}-u)$ şeklinde tanımlanan halka üzerinde skew devirli kodların özellikleri araştırılmıştır. Hem skew devirli kodlar için hem de skew devirli kodların duali için üreteç polinomlarının sağlaması gereken koşullar araştırılmıştır. Teorik çalışmanın bir uygulaması olarak $F_q[u]/(u^{k+1}-u)$ halkası üzerinde dualini içeren skew devirli kodlardan, CSS inşa metodu kullanılarak kuantum hata düzelten kodların elde edildiği ispatlanmıştır.

Tez kapsamında ilk olarak $F_q[u]/(u^{k+1}-u)$ halkasının birimden farklı bir otomorfisi göz önüne alınarak karşılık gelen skew polinom halkası tanımlanıp bu halka üzerinde tanımlı skew polinom halkasının özellikleri ve ideal kavramı incelenmiştir. Ayrıca $F_q[u]/(u^{k+1}-u)$ halkası üzerindeki bir skew devirli kodun, elde edilen skew polinom halkasında karşılık geldiği polinom belirlenmiştir. İkinci adım olarak $F_q[u]/(u^{k+1}-u)$ halkası üzerindeki skew devirli kodların üreteç polinomları ile ilgili bir inceleme yapılmıştır. Daha sonra

$F_q[u]/(u^{k+1}-u)$ halkası üzerindeki skew devirli kodların Öklid dual kodları çalışılmıştır. Elde edilen bilgiler yardımıyla $F_q[u]/(u^{k+1}-u)$ halkası üzerindeki bir skew devirli kodun dualini içermesi için bir gerek ve yeter koşul verilmiştir. Son olarak CSS inşa metodu kullanılarak, $F_q[u]/(u^{k+1}-u)$ halkası üzerinde dualini içeren skew devirli kodlardan kuantum hata düzelten kodların elde edildiği ispatlanmıştır.

Bu çalışmanın bir sonraki aşamasında, teorik çalışmanın bir uygulaması olarak uygun bilgisayar algoritmaları yazılarak $F_q[u]/(u^{k+1}-u)$ halkası üzerinde iyi parametrelere sahip skew devirli kodların ve daha iyi parametrelere sahip kuantum hata düzelten kodların elde edilmesi araştırılabilir. Diğer bir çalışma konusu olarak lineer kodlardan kuantum hata düzelten kodların elde edilme yöntemleri araştırılarak bu tezde göz önüne alınan $F_q[u]/(u^{k+1}-u)$ halkası üzerindeki lineer kodlardan kuantum kodların elde edilme yolları çalışılabilir. Farklı bir çalışma konusu olarak, $F_q[u]/(u^{k+1}-u)$ halkası üzerindeki farklı kod aileleri çalışılarak iyi parametrelere sahip kodlar elde edilebilir. Diğer yandan bu tez kapsamındaki metot ve yöntem, literatürde çalışılmayan farklı halka tiplerine uygulanabilir. Daha açık bir ifade ile bu tezde incelenen problemlerin çözümü için sunulan fikirler farklı cebirsel yapılar göz önüne alınarak da çalışılabilir ve elde edilen sonuçlar yorumlanabilir. Örneğin farklı cisim veya halka tiplerinin kartezyen çarpımları ile oluşturulan cebirsel yapılar üzerinde skew devirli kodlar çalışılabilir.

KAYNAKLAR

[1]. T. ABUALRUB, N. AYDIN, AND P. SENEVIRATNE, *On θ-cyclic codes over $F_2 + vF_2$*, Australas. J. Combin, 54 (2012), pp. 115–126.

[2]. D. BOUCHER AND F. ULMER, *Coding with skew polynomial rings*, Journal of Symbolic Computation, 44 (2009), pp. 1644–1656.

[3]. A. R. CALDERBANK, E. M. RAINS, P. SHOR, AND N. J. SLOANE, *Quantum error correction via codes over $GF(4)$*, IEEE Transactions on Information Theory, 44 (1998), pp. 1369–1387.

[4]. Y. CAO, Y. CAO, H. Q. DINH, F.-W. FU, J. GAO, AND S. SRIBOONCHITTA, *Constacyclic codes of length np^s over $F_p^m + uF_p^m$*, Advances in Mathematics of Communications, 12 (2018).

[5]. H. Q. DINH, T. BAG, A. K. UPADHYAY, R. BANDI, AND R. TANSUCHAT, *A class of skew cyclic codes and application in quantum codes construction*, Discrete Mathematics, 344 (2021), p. 112189.

[6]. R. HILL, *A first course in coding theory*, Oxford University Press, 1986.

[7]. P. KAYE, R. LAFLAMME, AND M. MOSCA, *An introduction to quantum computing*, OUP Oxford, 2006.

[8]. S. LING AND C. XING, *Coding theory: a first course*, Cambridge University Press, 2004.

[9]. B. R. MCDONALD, *Finite rings with identity / Bernard R. McDonald*, M. Dekker New York, 1974.

[10]. O. ORE, *Theory of non-commutative polynomials*, Annals of Mathematics, 34 (1933), pp. 480–508.

[11]. P. W. SHOR, *Scheme for reducing decoherence in quantum computer memory*, Physical review A, 52 (1995), p. R2493.

[12]. I. SIAP, T. ABUALRUB, N. AYDIN, AND P. SENEVIRATNE, *Skew cyclic codes of arbitrary length*, Int. J. Inf. Coding Theory, 2 (2011), pp. 10–20.

[13]. A. M. STEANE, *Simple quantum error-correcting codes*, Physical Review A, 54 (1996), p. 4741.

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Mohammad Kamal MKHALLALATI
Doğum Yeri	
Doğum Tarihi	
Uyruğu	[ ] T.C. [X] Diğer: Suriye
E-Posta Adresi	

Eğitim Bilgileri	
Lisans	
Üniversite	Halep Üniversitesi
Fakülte	Fen Fakültesi
Bölümü	Matematik, Cebir
Mezuniyet Yılı	2016

Yüksek Lisans	
Üniversite	İstanbul Üniversitesi
Enstitü Adı	Fen Bilimleri
Anabilim Dalı	Matematik Anabilim Dalı
Programı	Matematik Programı
Mezuniyet Tarihi	2022