T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI SONLU HALKALAR ÜZERİNDEKİ DEVİRLİ KOD AİLELERİ

DOKTORA TEZİ

N. Tuğba ÖZZAİM

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR ve SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Prof. Dr. Mehmet ÖZEN**

Kasım 2017

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI SONLU HALKALAR ÜZERİNDEKİ DEVİRLİ KOD AİLELERİ

DOKTORA TEZİ

N. Tuğba ÖZZAİM

Enstitü Anabilim Dalı : MATEMATİK

Bu tez 17 / 11 /2017 tarihinde aşağıdaki jüri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

Prof. Dr.
Fethi ÇALLIALP
Jüri Başkanı

Prof. Dr.
Mehmet ÖZEN
Üye

Prof. Dr.
Ünsal TEKİR
Üye

Doç. Dr.
Mustafa ERÖZ
Üye

Doç. Dr.
Ali Serdar ARIKAN
Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

N. Tuğba ÖZZAİM

17.11.2017

TEŞEKKÜR

Doktora eğitimim boyunca gerekli olan bütün bilgi ve tecrübesini benimle paylaşan, araştırmalarımın her aşamasında yardımlarını esirgemeyen, çalışmalarım konusunda da beni her daim teşvik ve motive eden değerli danışmanım Prof. Dr. Mehmet ÖZEN'e teşekkürlerimi sunarım. MAGMA programlama dilini öğrenmemde yardımcı olan ve bazı çalışmalarımdaki bilgisayar araştırmasına katkı sağlayan değerli arkadaşım Sakarya Üniversitesi Arş. Gör. Halit İNCE'ye teşekkürlerimi iletirim.

Bu uzun süreçte hiçbir zaman desteklerini esirgemeyen, moral ve motivasyonumu her zaman yüksekte tutmamı sağlayan öncelikle aileme sonra arkadaşlarıma çok teşekkür ederim.

Doktora eğitimim boyunca sağlamış olduğu burs desteğinden dolayı TÜBİTAK'a ve bu çalışmadaki Bölüm 2 kısmının desteklenmesine olanak sağlayan Sakarya Üniversitesi Bilimsel Araştırma Projeleri (BAP) Komisyon Başkanlığına (Proje No: 2016-02-00-004) teşekkürlerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$\langle a \rangle_{sol}$	: a elemanının ürettiği sol ideal
$boyC$	: C alt vektör uzayının boyutu
$C^{\perp}$	: C lineer kodunun duali
Çek$f$	: f homomorfizmasının çekirdeği
$d^o f(x)$	: f fonksiyonunun derecesi
$d_H(x,y)$	: x ve y arasındaki minimum Hamming uzaklık
$d_L(x,y)$	: x ve y arasındaki minimum Lee uzaklık
$ebob_{sağ}(a,b)$	: a ile b elemanlarının en büyük sağ ortak bölen
$ebob_{sol}(a,b)$	: a ile b elemanlarının en büyük sol ortak bölen
F_q	: q elemanlı sonlu cisim
Imf	: f fonksiyonunun görüntüsü
$kar(R)$	: R halkasının karakteristiği
$Sp(T)$	: T'nin gerdiği küme
$w_H(x)$	: x'in Hamming ağırlığı
$w_L(x)$	: x'in Lee ağırlığı

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Devirli kodlar, yarı devirli kodlar, skew polinom halkası, en küçük geren kümesi, kuantum kod

Devirli kodların kodlama için zengin bir cebirsel yapıya sahip olması, kodlar arasında en çok çalışılan alan olmasına sebep olmuştur. Bu çalışmada da farklı halkalar üzerindeki devirli kod aileleri incelenmiştir. Bu halkalar üzerindeki devirli kodlar kullanılarak hem yeni hem de optimal kodlar elde edilmiştir.

Bu tez altı bölümden oluşmaktadır ve ilk bölümde cebir ve kodlama teorisi ile ilgili olan temel tanımlar ve teoremler verilmiştir.

İkinci bölümde, $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ halkasının Galois genişlemesi çalışılmıştır. Ayrıca bu halka üzerindeki devirli kodların yapısı incelenmiş ve bu kodların üreteçlerinin genel bir formu ve bu kodlar için en küçük geren küme belirlenmiştir. Elde edilen bu bilgilerden yararlanılarak $\mathbb{Z}_4$ üzerinde yeni lineer kodlar tablo şeklinde bölüm sonunda verilmiştir.

Üçüncü bölümde, $\mathbb{F}_q + v\mathbb{F}_q$ halkası üzerindeki skew yarı devirli kodların cebirsel yapısı incelenmiştir. Skew yarı devirli kodların dualleri tartışılmıştır ve farklı bir bakış açısı ile $\mathbb{F}_q + v\mathbb{F}_q$ üzerindeki skew devirli kodların dualini içermesi için gerek ve yeter şart verilmiştir. Bundan yararlanılarak skew devirli kodlardan kuantum kod inşa edilmiştir.

Dördüncü bölümde, $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$ halkasındaki lineer kodların yapısı incelenip yeni bir Gray dönüşüm verilmiştir. Ayrıca bu halka üzerindeki devirli kodların üreteç polinomları belirlenmiştir. Elde edilen devirli kod sonuçlarından yararlanılarak kuantum kod parametreleri bulunmuştur.

Beşinci bölümde, $\mathbb{F}_2\mathbb{F}_2[u]$-devirli kodu olarak adlandırılacak olan devirli kodların yeni bir sınıfı incelenmiştir. Ayrıca yeni bir Gray dönüşüm tanımlanmış ve bazı $\mathbb{F}_2\mathbb{F}_2[u]$-devirli kodların Gray görüntülerinden elde edilen ikili optimal kod örnekleri tablo halinde sunulmuştur.

Son bölümde ise sonuç ve önerilere yer verilmiştir.

FAMILIES OF CYCLIC CODE OVER SOME FINITE RINGS

SUMMARY

Keywords: Cyclic codes, quasi cyclic codes, skew polynomial ring, minimal spanning set, quantum code

Cyclic codes are the most studied field among the codes because of their rich algebraic structure for coding. In this study, the family of cyclic codes over different rings are investigated. By using cyclic codes over these rings, both new codes and optimal codes are obtained. This thesis consists of six chapters and in the first chapter, some basic definitions and theorems related to algebra and coding theory are given.

In the second chapter, Galois extensions of the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ are studied. Also cyclic codes over this ring are investigated and the general form of the generator and a minimal spanning set of such codes are determined. Using these informations, new linear codes over $\mathbb{Z}_4$ are given in a table at the end of the chapter.

In the third chapter, the algebraic structure of skew quasi cyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$ is investigated. The duals of skew quasi cyclic codes are discussed. Also from a different viewpoint, necessary and suffcient condition for skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$ is given to contain its dual. By using this information, quantum codes are constructed from skew cyclic codes.

In the fourth chapter, the structure of linear codes over $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$ is investigated and a new Gray map is given. Also, generator polynomials of cyclic codes over this ring are determined. Using these results, some parameters of quantum codes are found.

In the fifth chapter, a new class of cyclic codes which is referred to as $\mathbb{F}_2\mathbb{F}_2[u]$-cyclic codes is discussed. Also a new Gray map is defined and some examples of optimal codes which are the binary Gray images of $\mathbb{F}_2\mathbb{F}_2[u]$-cyclic codes are presented in the form a table.

In the last chapter, the conclusion and some recommendations are given.

BÖLÜM 1. GİRİŞ

1.1. Cebirsel Tanımlar ve Teoremler

Bu bölümde, tez boyunca kullanılacak olan temel cebirsel tanımlar ve teoremler verilecektir.

Tanım 1.1.1. A boştan farklı bir küme olsun. $x, y \in A$ olmak üzere her (x, y) sıralı ikilisine A'nın bir ve yalnız bir elemanını karşılık getiren fonksiyona A üzerinde bir ikili işlem denir. A kümesi üzerindeki bir ikili işlem "$*$" ile gösterilecek olursa

$$A \times A \to A$$
$$(x, y) \to x * y$$

ile tanımlanır. Üzerinde en az bir ikili işlem tanımlanmış kümeye de cebirsel yapı denir [1].

Tanım 1.1.2. G boştan farklı bir küme ve "$*$" G kümesi üzerinde tanımlı bir ikili işlem olsun. Aşağıdaki şartları sağlayan $(G, *)$ cebirsel yapısına grup denir.

i. $\forall a, b, c \in G$ için

$$(a * b) * c = a * (b * c)$$

ii. $\forall g \in G$ için

$$e_G * g = g * e_g = g$$

olacak şekilde bir tek $e_G \in G$ elemanı vardır ve bu elemana birim eleman denir.

iii. $\forall g \in G$ için

$$g * g^{-1} = g^{-1} * g = e_G$$

olacak şekilde $g^{-1} \in G$ elemanı vardır ve bu elemana g'nin tersi denir [1].

Tanım 1.1.3. $(G,*)$ grubunda eğer $\forall a,b \in G$ için $a*b=b*a$ şartı sağlanıyor ise $(G,*)$ grubuna değişmeli (abelyen) grup denir [1].

Tanım 1.1.4. *G*'nin boştan farklı bir *H* alt kümesi *G'*deki ikili işlem altında kendi başına bir grup oluyor ise *H* kümesine *G*'nin bir alt grubu denir [1].

Teorem 1.1.1. $(G,*)$ bir grup ve *H* kümesi *G*'nin boştan farklı bir alt kümesi olsun. *H* kümesinin *G*'nin bir alt grubu olması için gerek ve yeter şart $\forall a,b \in H$ için $a*b^{-1} \in H$ olmasıdır [2].

Tanım 1.1.5. Boştan farklı *R* kümesi "$+$" ve "$.$" ikili işlemleri altında aşağıdaki şartları sağlıyor ise *R* kümesine halka denir ve $(R,+,\cdot)$ ile gösterilir. $\forall a,b,c \in R$ için

i. $(R,+)$ değişmeli bir gruptur.

ii. $a.(b.c)=(a.b).c$ dir.

iii. $a.(b+c)=a.b+a.c$ ve $(a+b).c=a.c+b.c$ dir [2].

Kolay gösterim olması adına bundan sonraki bölümlerde $a.b$ yerine ab yazılacaktır.

Tanım 1.1.6. $\forall a,b \in R$ için eğer $ab=ba$ şartı sağlanıyor ise *R* halkasına değişmeli halka denir [2].

Tanım 1.1.7. $\forall a \in R$ için $ae=ea=a$ olacak şekilde tek bir $e \in R$ varsa *R* halkasına birimli halka denir. Genel olarak halkanın birimi 1_R ile gösterilir ve birim eleman veya çarpımsal birim olarak adlandırılır [2].

Tanım 1.1.8. Birimli bir *R* halkasındaki bir $a \in R$ için $ab=ba=1_R$ olacak şekilde bir $b \in R$ varsa *a* elemanına terslenebilen eleman denir [2].

Tanım 1.1.9. Birimli ve değişmeli bir halkada sıfırdan farklı her elemanın tersi var ise bu halkaya cisim denir [2].

Tanım 1.1.10. R bir halka ve $0 \neq a \in R$ olsun. Eğer bir $0 \neq b \in R$ elemanı için $ab = 0$ veya $ba = 0$ oluyor ise a elemanına sıfır bölen denir [2].

Tanım 1.1.11. Birimli, değişmeli ve sıfır bölensiz halkaya tamlık bölgesi denir. [2]

Tanım 1.1.12. R halkasının boştan farklı bir S alt kümesi R'deki ikili işlemler altında kendi başına bir halka oluyor ise S kümesine R halkasının bir alt halkası denir [2].

Teorem 1.1.2. R halkasının boştan farklı bir S alt kümesi

i. $\forall a,b \in S$ için $a-b \in S$ ve

ii. $\forall a,b \in S$ için $ab \in S$

şartlarını sağlıyor ise S kümesine R halkasının bir alt halkası denir [2].

Tanım 1.1.13. R bir halka olmak üzere $\forall a \in R$ için $na = 0$ şartını sağlayan en küçük pozitif n tamsayısına R halkasının karakteristiği denir ve R halkasına da sonlu karakteristiğe sahip denir. Eğer böyle bir en küçük pozitif n tamsayısı bulunamıyor ise R halkasının karakteristiği 0'dır denir. R halkasının karakteristiği $kar(R)$ ile gösterilir [1].

Teorem 1.1.3. Bir tamlık bölgesinin karakteristiği ya sıfırdır ya da asal sayıdır [2].

Tanım 1.1.14. R halkasının boştan farklı bir I alt kümesi

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

ii. $\forall a \in I$ ve $\forall r \in R$ için $ra \in I (ar \in I)$

şartlarını sağlıyor ise I kümesine R halkasının bir sol (sağ) ideali denir. Eğer I ideali hem sağ ideal hem de sol ideal ise I kümesine iki taraflı ideal veya kısaca R halkasının bir ideali denir. Eğer R halkası değişmeli ise sağ ve sol ideal aynı olacaktır [2].

Tanım 1.1.15. Bir R halkasında $I = \{0\}$ ve $I = R$ kümeleri halkanın aşikâr idealleridir. R halkasının aşikâr olmayan ideallerine has (öz) ideal denir [2].

Teorem 1.1.4. *R* birimli bir halka olmak üzere *R* halkasının *I* ideali halkanın birimini içeriyor ise $I = R$ dir [2].

İdealler yardımı ile yeni halkalar yapılandırılabilir. Bu yapılandırma için aşağıdaki şekilde tanımlanan bağıntıya ihtiyaç olacaktır.

Tanım 1.1.16. *R* bir halka olmak üzere *I, R*'nin bir ideali ve $a,b \in R$ olsun.

"$a \equiv b$ olması için gerek ve yeter şart $a-b \in I$ olmasıdır."

şeklinde tanımlanan "$\equiv$" bağıntısı *R* üzerinde bir denklik bağıntısıdır. Bu bağıntıya göre bütün denklik sınıflarının kümesi R/I ile gösterilecek olursa $R/I = \{r+I : r \in R\}$ şeklindedir [1].

Tanım 1.1.17. *R* bir halka ve *I* da *R*'nin bir ideali olsun. $\forall (r+I),(s+I) \in R/I$ için

$$(r+I)+(s+I)=(r+s)+I$$

$$(r+I).(s+I)=rs+I$$

şeklinde tanımlanan toplama ve çarpma işlemleri altında R/I bir halkadır. Bu R/I halkasına *R*'nin *I*'ya göre bölüm halkası denir. Eğer *R* birimli bir halka ise R/I halkasının birimi $1_R + I$ elemanıdır. Eğer *R* değişmeli bir halka ise R/I da değişmeli halkadır [1].

R bir halka ve *I* da *R*'nin bir ideali olduğunda R/I kalan sınıfının bir halka olduğu gösterildi. Bundan sonraki adımda doğal olarak şu soru ortaya çıkar: R/I halkası ne zaman tamlık bölgesi veya cisim yapısını kazanır? Bu sorunun cevabı için aşağıdaki tanımlara ihtiyaç olacaktır.

Tanım 1.1.18. *R* değişmeli halkasındaki $P \neq R$ olacak şekildeki bir *P* ideali

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

şartını sağlıyor ise *P* idealine *R* halkasının asal ideali denir [2].

Tanım 1.1.19. R halkasında $M \neq R$ olacak şekilde bir M ideali olsun. Eğer R halkasında $M \subseteq I \subseteq R$ şartını sağlayan her I ideali için $I = M$ veya $I = R$ oluyor ise M idealine R halkasının maksimal ideali denir [2].

Teorem 1.1.5. R birimli ve değişmeli bir halka ve $P \neq R$ olacak şekilde bir I ideali olsun. R/P halkasının tamlık bölgesi olması için gerek ve yeter şart P idealinin R'nin asal ideali olmasıdır [2].

Teorem 1.1.6. R birimli ve değişmeli bir halka ve $M \neq R$ olacak şekilde bir M ideali olsun. R/M halkasının cisim olması için gerek ve yeter şart M idealinin R'nin maksimal ideali olmasıdır [2].

Teorem 1.1.7. Birimli ve değişmeli bir R halkasında her maksimal ideal asal idealdir. Fakat tersi doğru değildir [2].

Tanım 1.1.20. R birimli ve değişmeli bir halka ve $m_1, m_2, \cdots, m_n \in R$ olmak üzere

$$\langle m_1, m_2, \cdots, m_n \rangle = \{ m_1 r_1 + m_2 r_2 + \cdots + m_n r_n : r_1, r_2, \cdots r_n \in R \}$$

idealine R'nin $m_1, m_2, \cdots, m_n$ tarafından üretilen ideali denir [2].

Özel olarak R halkasının bir I ideali $a \in R$ olmak üzere

$$I = \langle a \rangle = \{ ar : r \in R \}$$

şeklinde tek bir a elemanı tarafından üretiliyor ise I idealine temel ideal denir.
"a" elemanına da I idealinin üreteci denir.

Tanım 1.1.21. Her ideali temel ideal olan R halkasına temel ideal halkası denir. Her ideali temel ideal olan tamlık bölgesine ise temel ideal bölgesi denir [2].

Tanım 1.1.22. Tek bir maksimal ideale sahip olan halkaya lokal halka denir [3].

Tanım 1.1.23. Birimli ve değişmeli bir halkada tüm idealler kapsama işlemi altında bir zincir oluşturuyorsa bu halkaya zincir halkası denir. Yani $i = 0, 2, \cdots, n-1$ için R halkasının tüm I_i idealleri arasında

$$\{0\} = I_0 \subset I_1 \subset \cdots \subseteq I_{n-1} = R$$

şeklinde bir ilişki varsa R halkasına zincir halkası denir [4].

Teorem 1.1.8. Sonlu ve değişmeli bir R halkası için aşağıdaki koşullar denktir.

i. R bir lokal halka ve R'nin M maksimal ideali temel idealdir.

ii. R bir lokal temel ideal halkasıdır.

iii. R bir zincir halkasıdır [4].

Tanım 1.1.24. R ve S iki halka ve $f : R \to S$ fonksiyonu verilmiş olsun. Eğer $\forall a, b \in R$ için

i. $f(a+b) = f(a) + f(b)$

ii. $f(ab) = f(a) f(b)$

şartları sağlanıyor ise f 'ye bir halka homomorfizması denir [1].

Tanım 1.1.25. R ve S iki halka ve $f : R \to S$ bir halka homomorfizması olsun. Eğer f birebir ve örten ise f 'ye bir halka izomorfizması denir. R ve S halkalarına da birbirine izomorf denir ve $R \cong S$ şeklinde ifade edilir. Eğer $R = S$ ise f izomorfizmasına otomorfizma denir [1].

Tanım 1.1.26. R ve S iki halka ve $f : R \to S$ bir halka homomorfizması olsun. Bu durumda

i. Çek $f = \{r \in R : f(r) = 0_S\}$ kümesine f 'nin çekirdeği

ii. Im $f = \{f(r) : r \in R\}$ kümesine f 'nin görüntü kümesi

adı verilir [1].

Teorem 1.1.9. *R* ve *S* iki halka ve $f : R \to S$ bir halka homomorfizması olsun. Bu durumda

i. Çek$f$, *R* halkasının bir idealidir.

ii. Çek$f = \{0_R\}$ ancak ve ancak f birebirdir [1].

Teorem 1.1.10. *R* ve *S* iki halka ve $f : R \to S$ bir halka homomorfizması olsun. Bu durumda

$$R/\text{Çek}f \cong \text{Im } f$$

dir [1].

Tanım 1.1.27. *R* bir halka, *m* pozitif tamsayı ve $0 \le k \le m$ için $a_k \in R$ olmak üzere

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$

ifadesine *R*'den katsayılı bir polinom denir. Bu polinomda $k \ge m+1$ olmak üzere $a_k = 0$ olduğu kabul edilecektir. $0 \le k \le m$ için a_k elemanlarına $f(x)$ polinomunun katsayıları denir. $a_k \neq 0$ olacak şekildeki en büyük *k* tamsayısına $f(x)$ polinomunun derecesi denir ve $d^o f(x)$ şeklinde gösterilir. Bu şartı sağlayan a_k elemanına $f(x)$ polinomunun baş katsayısı, a_0 elemanına ise $f(x)$ polinomunun sabiti denir [1].

Tanım 1.1.28. Katsayıları *R*'den olan *x* belirsizine göre bütün polinomların kümesi *R*[*x*] ile gösterilsin. Bu küme üzerinde polinomların toplamı ve çarpımı

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \in R[x]$$

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n \in R[x]$$

olmak üzere

$$f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$$

$$f(x).g(x) = \sum_{i=0}^{m+n} c_i x^i \quad \text{ve} \quad c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

şeklinde tanımlanır [1].

Tanım 1.1.29. $R[x]$ polinomlar kümesi yukarıda tanımlanan toplama ve çarpma işlemlerine göre bir halkadır [1].

Teorem 1.1.11. R'den katsayılı polinom halkası $R[x]$ olmak üzere

i. Eğer R halkası değişmeli ise $R[x]$ polinom halkası da değişmelidir.

ii. R birimli ise R halkasının birimi aynı zamanda $R[x]$ polinom halkasının da birimidir.

iii. R tamlık bölgesi ise $R[x]$ polinom halkası da tamlık bölgesidir [2].

Teorem 1.1.12. R'den katsayılı polinom halkası R[x] ve

$f(x) = a_0 + a_1x + \cdots + a_mx^m$ ve $g(x) = b_0 + b_1x + \cdots + b_nx^n$ sırası ile *m.* ve *n.* dereceden iki polinom olsun. Bu durumda

$$d^o[f(x) + g(x)] \leq d^0 f(x) + d^o g(x)$$

dir. Eğer R halkası tamlık bölgesi ise

$$d^o[f(x) + g(x)] = d^o f(x) + d^o g(x)$$

dir [2].

Tanım 1.1.30. Baş katsayısı 1 olan polinoma monik polinom denir [2].

Tanım 1.1.31. Sabitten farklı bir $f(x) \in R[x]$ polinomu, derecesi $f(x)$ polinomundan küçük fakat sabit olmayan herhangi iki polinomun çarpımı şeklinde yazılamıyorsa $f(x)$ polinomuna indirgenemez polinom denir [1].

Tanım 1.1.32. $\mathbb{F}_{q^m} = GF(q^m)$ bir cisim ve $\mathbb{F}_{q^m}$ cismi üzerinde tanımlanmış bir $\theta : \alpha \to \alpha^q$ otomorfizması olmak üzere

$$\mathbb{F}_{q^m}[x, \theta] = \{ f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \mid a_i \in \mathbb{F}_{q^m} \text{ ve } i = 0,1,\ldots n-1\}$$

kümesi polinom halkasındaki standart toplama işlemi ve $(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}$ şeklinde tanımlanan çarpma işlemine göre bir halka belirtir. Bu halkaya skew polinom halkası denir [5].

Uyarı 1.1.1. Yukarıdaki tanım $\mathbb{F}_{q^m}$ cismi yerine herhangi bir R halkası alınarakta yapılabilir.

Uyarı 1.1.2. Skew polinom halkası değişmeli olmayan bir halkadır.

Örnek 1.1.1. $\mathbb{F}_4 = GF(2^2)$ için $\theta(0)=0, \theta(1)=1, \theta(w)=w+1, \theta(w+1)=w$ olmak üzere

$$\begin{aligned} wx^2 * (1+w)x^3 &= w\theta^2(1+w)x^5 \\ &= w(1+w)x^5 \\ &= x^5 \\ (1+w)x^3 * wx^2 &= (1+w)\theta^3(w)x^5 \\ &= (1+w)(1+w)x^5 \\ &= wx^5 \end{aligned}$$

eşitliklerinden $\mathbb{F}_4[x,\theta]$ skew polinom halkasının değişmeli olmadığı görülür.

Tanım 1.1.33. Birimli ve değişmeli bir R halkası ve $a,b \in R$ olsun. Eğer $b=ac$ olacak şekilde bir $c \in R$ varsa a elemanı b'yi böler (veya a elemanı b'nin bir çarpanıdır) denir ve $a \mid b$ ile gösterilir [2].

Tanım 1.1.34. Birimli ve değişmeli bir R halkasında $u \in R$ elemanı eğer $u \mid 1_R$ şartını sağlıyor ise yani R de çarpımsal terse sahip ise u elemanına birimsel eleman ya da aritmetik birim denir [2].

Tanım 1.1.35. R bir halka, M bir toplamsal değişmeli grup olmak üzere

$$\begin{aligned} R \times M &\to M \\ (r,m) &\to rm \end{aligned}$$

ile tanımlanan dış işlem $\forall r, r_1, r_2 \in R$ ve $\forall m, m_1, m_2 \in M$ için

i. $r(m_1+m_2) = rm_1 + rm_2$
ii. $(r_1+r_2)m = r_1m + r_2m$
iii. $r_1(r_2m) = (r_1r_2)m$
iv. $1_R m = m$

koşulları sağlanıyor ise *M*'ye bir sol *R*-modül denir. Benzer şekilde sağ *R*-modül de tanımlanabilir. Özel olarak eğer *R* halkası değişmeli ise sağ *R*-modül aynı zamanda sol *R*-modül ve bunun tersi de doğru olacağından kısaca *M*'ye *R*-modül denir [3].

Tanım 1.1.36. *R* bir halka, *M* bir *R*-modül ve *M*'nin boştan farklı bir altkümesi *N* olsun. $\forall n_1, n_2 \in N$ ve $r \in R$ için

i. $0_M \in N$

ii. $n_1 - n_2 \in N$

iii. $rn_1 \in N (n_1 r \in N)$

şartları sağlanıyor ise *N*'ye *M*'nin bir sol (sağ) *R*-alt modülü denir. (0) ve *M*'nin kendisi *M*'nin birer *R*-alt modülleridir. Bu alt modüllere aşikâr alt modüller denir [3].

Örnek 1.1.2. *R* bir halka ve elemanları *R*'den olan sıralı *n*-lilerin kümesi R^n olsun. R^n , *R* üzerinde bir modüldür.

Tanım 1.1.37. *R* bir halka, *M* bir *R*-modül ve *I* indis kümesi olmak üzere $S = \{y_i\}_{i \in I}$ de *M*'nin bir üreteç sistemi olsun. Eğer her $m \in M$ elemanı $r_i \in R$ ve $y_i \in S$ olmak üzere, $m = \sum_{i \in I} r_i y_i$ şeklinde sonlu bir toplam olarak yazılabiliyor ve bu yazılış tek türlü oluyor ise $S = \{y_i\}_{i \in I}$ ye *M*'nin bir tabanı denir. *M* modülüne de serbest modül denir [3].

Tanım1.1.38. *R* bir halka, *M* ve *N* de *R*-modül olsun. Bir $f : M \to N$ fonksiyonu her $m_1, m_2 \in M$ ve her $r \in R$ için

i. $f(m_1 + m_2) = f(m_1) + f(m_2)$

ii. $f(rm) = rf(m)$

koşulları sağlanıyorsa, *f*'ye modül homomorfizması veya *R*-homomorfizması denir [3].

Teorem 1.1.13. (Çin Kalan Teoremi) I ve J idealleri R halkasının $I+J=R$ olacak şekilde iki ideali olsun.

i. Herhangi $a,b\in R$ için

$$x\equiv a(\text{mod}\, I)$$
$$x\equiv b(\text{mod}\, J)$$

sisteminin bir çözümü vardır. Sistemin herhangi iki çözümü $I\cap J$ modülünde kongurüenttir.

ii. $R/_{I\cap J}\cong R/_{I}\times R/_{J}$ halka izomorfizması vardır [6].

Çin Kalan Teoremi aşağıdaki gibi de yorumlanabilir.

Teorem 1.1.14. R birimli ve değişmeli bir halka olmak üzere aşağıdakiler denktir.

i. R'nin bir $(e_i)_{i=1}^{n}$ idempotent ailesi $i\neq j$ için $e_ie_j=0$, $\sum_{i=1}^{n}e_i=1$ ve $R_i=e_iR$ olacak şekilde vardır.

ii. $R=R_1+R_2+\cdots+R_n$ dir [5].

1.2. Kodlama Teorisi ile İlgili Tanımlar ve Teoremler

Kodlama Teorisi, gönderilen bir bilginin bozulma ihtimalinin olduğu (gürültülü) bir iletişim kanalı boyunca bilgiyi iletirken meydana gelebilecek hataları tespit edip düzeltmek amacı ile ortaya çıkmıştır. Bunu yaparken ki temel düşünce, bilgi transferinde veya depolamasında asıl bilgiye eklemeler yaparak onlara bir cebirsel yapı kazandırıp meydana gelebilecek olan bozulmaları en aza indirgemek ve düzeltmektir. Tek amaç hata tespit etmek ya da düzeltmek değildir. Aynı zamanda maliyetinin az ve bilgi transferi ve depolamasının hızlı olması istenmektedir. İşte daha az maliyetli ve en üstün performansa sahip kodları bulmak kodlama teorisinin asıl hedefidir. Dolayısıyla hata kontrolü için kodlamanın kullanılması modern iletişim ve dijital depolama sisteminin tasarımının ayrılmaz bir parçası olmuştur.

Kodlama teorisinde karşılaşılan sorunlar genellikle mühendislik uygulamalardan kaynaklansa da alanın geliştirilmesinde matematiğin oynadığı rol büyüktür. Özellikle cebir ve kombinatöriyel matematiğin önemi kabul gören bir gerçektir. Bu sebepten dolayı kodlama teorisi sadece mühendisler ve bilgisayar teknolojileri ile uğraşan bilim adamlarına değil aynı azmanda matematikçilere de hitap eden bir konu olmuştur.

Bilgi ve kodlama teorisinin başlangıcını simgeleyen "İletişimin Matematiksel Bir Kuramı" başlıklı çalışma 1948'de Claude Shannon tarafından yayınlanmıştır [7]. Bu çalışma ile iletişimin teorik temelleri ortaya konmuştur. Shannon bu makalesinde kanal kapasitesi ($c(p)$) olarak adlandırdığı bir sayı tanımlamış ve gürültülü bir iletişim kanalında bu kapasitenin altındaki bir oranda güvenli iletişimin olabileceğini matematiksel olarak kanıtlamıştır. Örneğin ikili kanal için kanal kapasitesi formülü

$$c(p) = 1 + p.\log_2 p + (1-p).\log_2(1-p)$$

dir. Eğer $p = 0.5$ ise $c(p) = 0$ olur. Bu da gösterir ki hata olasılığı 0.5 olan bir ikili kanal için hiçbir kodlama şeması çalışmaz.

Dikkat edilmelidir ki Shannon'un bu kanıtı yapısal değildir. Yani hatalı kod çözme olasılığını, çok düşük hale getirebilecek kodların varlığını kanıtlamaktadır fakat bu tür kodların nasıl oluşturulacağı hakkında herhangi bir bilgi vermemektedir. Bunun üzerine kodlamanın nasıl yapılacağına dair araştırmalar başlamış ve 1950'de Richard W. Hamming, hata düzelten kodları açıkça tanıtan ilk çalışma olarak gösterilebilecek "Hata Tespit Eden ve Hata Düzelten Kodlar" başlıklı çalışmasını ortaya koymuştur [8].

Kodlama teorisinde kullanılacak olan bazı temel tanımlar ve teoremler aşağıda verilmiştir. Bu kısımda verilen tanımlar ve teoremler için [9] kaynağından yararlanılmıştır.

Tanım 1.2.1. $S=\{s_1,s_2,\cdots,s_q\}$ q elemanlı sonlu bir küme olmak üzere S üzerindeki bütün sıralı n-lilerin kümesi S^n ile gösterilsin. S^n nin boştan farklı herhangi bir C alt kümesine q'lu blok kod ve S kümesine de kod alfabesi denir. C kodunun her bir elemanına kod söz adı verilir. Eğer $C\subset S^n$ kodu M tane eleman içeriyor ise bu koda n uzunluğunda M elemana sahip kod denir ve kısaca (n,M)-kodu olarak gösterilir. (n,M)-kodunun hız oranı ise

$$R=\frac{\log_q M}{n}$$

dir.

Hatanın çözülme olasılığını hesaplamak genelde zor olduğundan kodun kabiliyeti hakkında bilgi edinmek için genelde kombinatoriyel bir ölçüm kullanılır. Bu ölçüm 1950'de Hamming tarafından tanımlanan ve kendi adıyla anılan uzaklık fonksiyonu olup tanımı aşağıda verilmiştir.

Tanım 1.2.2. Aynı alfabe üzerinde iki sıralı n-li $x=(x_1,x_2,\cdots,x_n)$ ve $y=(y_1,y_2,\cdots,y_n)$ olmak üzere x ve y n-lilerinin farklı olan bileşenlerinin sayısına x ve y arasındaki Hamming uzaklık denir ve $d(x,y)$ şeklinde gösterilir. Başka bir ifade ile

$$d_H(x,y)=\left|\{i:x_i\neq y_i,1\leq i\leq n\}\right|$$

olarak tanımlanabilir.

Teorem 1.2.1. $d:S^n\times S^n\to N$ Hamming uzaklık fonksiyonu $x,y,z\in S^n$ olmak üzere aşağıdaki özellikleri sağlıyor ise (S^n,d)-ikilisine bir metrik uzay denir.

i. Pozitif tanımlılık $: d_H(x,y)\geq 0$ ve $d(x,y)=0\Leftrightarrow x=y=0$

ii. Simetri $: d_H(x,y)=d_H(y,x)$

iii. Üçgen Eşitsizliği $: d_H(x,y)\leq d_H(x,z)+d_H(z,y)$

Tanım 1.2.3. *C* kodunun bir kod sözü $x=(x_1,x_2,\cdots,x_n)$ olmak üzere *x* kod sözünün sıfırdan farklı bileşen sayısına *x*'in ağırlığı denir ve $w(x)$ ile gösterilir. Başka bir ifade ile

$$w_H(x)=\left|\{i:x_i\neq 0,1\leq i\leq n\}\right|$$

olarak tanımlanabilir.

Tanım 1.2.4. *C* kodunun minimum ağırlığı

$$w_H(C)=\min_{0\neq x\in C} w(x)$$

olarak tanımlanır.

Tanım 1.2.5. *n* uzunluğunda *M* elemana sahip bir *C* kodunun minimum uzaklığı *C*'deki tüm kod sözler arasındaki en küçük uzaklık olarak tanımlanır. Başka bir ifade ile

$$d_H(C)=\min_{\forall x\neq y\in C} d_H(x,y)$$

olarak tanımlanabilir.

Tanım 1.2.6. *n* uzunluğunda *M* elemanlı *d* minimum uzaklığa sahip bir *C* kodu (n,M,d) -kodu olarak gösterilir. Buradaki *n,M,d* sayılarına da *C* kodunun parametreleri denir.

Bir kodun hata tespit etme ve düzeltme değeri kod sözler arasındaki minimum uzaklık ile daha güzel bir şekilde ifade edilebilir. Aşağıdaki teorem ile minimum uzaklığa dayanarak *u*-hata tespit eden kodun tanımı yapılacaktır.

Teorem 1.2.2. Bir *C* kodunun *u*-hata tespit etmesi için gerek ve yeter şart $d_H(C)\geq u+1$ olmasıdır.

v-hata tespit eden kod tanımı için de benzer bir teorem aşağıdaki gibi verilebilir.

Teorem 1.2.3. Bir C kodunun v-hata tespit etmesi için gerek ve yeter şart $d_H(C) \geq 2v+1$ olmasıdır.

1.2.1. Lineer Kodlar

Eğer kod sözler sonlu vektör uzayındaki vektörler olarak düşünülürse vektör uzayının ilgili cebirsel özellikleri kullanılabilir. Bu da kodlama ve dekodlama şemalarının daha etkili ve elverişli olmasını sağlayacaktır.

Bu bölümde q elemanlı sonlu cisim üzerindeki lineer kodların tanımı ve yapısı hakkında bilgi verilecektir. Kodların özel bir sınıfı olarak bilinen lineer kodlara, diğer kodlardan (lineer olmayan) farklı olarak toplama ve skaler ile çarpa işlemleri ile daha fazla cebirsel özellik kazandırılır. Bu sayede lineer kolar sistematik bir şekilde inşa edilebildiğinden Kodlama Teorisinde önemli bir yer teşkil eder.

Lineer kod tanımına geçmeden önce lineer cebirden gerekli olacak bazı tanımlar [10] kaynağından yararlanılarak verilecektir.

Tanım 1.2.1.1. V kümesi, üzerinde vektörel toplam ve $\mathbb{F}_q$ cisminin elemanları ile skaler çarpım işlemlerinin tanımlı olduğu boştan farklı bir küme olsun. Eğer aşağıdaki koşullar sağlanıyor ise V kümesine $\mathbb{F}_q$ cismi üzerinde bir vektör uzayı denir.

i. V kümesi toplama işlemine göre değişmeli bir gruptur.

ii. $\forall \alpha \in \mathbb{F}_q$ ve $\forall u \in V$ için $\alpha c \in V$ dır.

iii. $\forall \alpha \in \mathbb{F}_q$ ve $\forall u, v \in V$ için $\alpha(u+v) = \alpha u + \alpha v$ dır.

iv. $\forall \alpha, \beta \in \mathbb{F}_q$ ve $\forall u \in V$ için $(\alpha+\beta)u = \alpha u + \beta u$ dır.

v $\forall \alpha, \beta \in \mathbb{F}_q$ ve $\forall u \in V$ için $(\alpha\beta)u = \alpha(\beta u)$ dır.

vi. $1_{\mathbb{F}_q}$, $\mathbb{F}_q$ cisminin birim elemanı olmak üzere $\forall u \in V$ için $1_{\mathbb{F}_q} u = u$ dir.

Tanım 1.2.1.2. *V* vektör uzayının herhangi boştan farklı bir *C* alt kümesi *V* üzerinde tanımlı işlemler altında kendi başına bir vektör uzayı ise *C*'ye *V*'nin alt vektör uzayı denir.

Teorem 1.2.1.1. $\mathbb{F}_q$ cismi üzerindeki *V* vektör uzayının boştan farklı bir *C* alt kümesinin *V*'nin alt vektör uzayı olması için gerek ve yeter şart $\forall x, y \in C$ ve $\forall \alpha, \beta \in \mathbb{F}_q$ için

$$\alpha x + \beta y \in C$$

olmasıdır.

Tanım 1.2.1.3. $\mathbb{F}_q$ cismi üzerinde *V* bir vektör uzayı ve $U = \{u_1, u_2, \cdots, u_k\}$ vektörler kümesi *V*'nin boş kümeden farklı bir alt kümesi olsun.

$$\langle U \rangle = \{\alpha_1 u_1 + \alpha_2 u_2 + \cdots \alpha_k u_k : \alpha_i \in \mathbb{F}_q \text{ ve } 1 \le i \le k\}$$

kümesi *V*'nin bir alt uzayıdır ve bu kümeye *U*'nun gerdiği (ürettiği) alt uzay denir.

Verilen bir $C \subseteq V$ alt vektör uzayı ve $U \subseteq C$ alt kümesi için eğer *C*'deki her eleman *U*'daki elemanların bir lineer kombinasyonu şeklinde yazılabiliyorsa yani $\langle U \rangle = C$ oluyor ise *U*'ya *C*'nin üreteç kümesi (geren kümesi) denir.

Tanım 1.2.1.4. $\mathbb{F}_q$ cismi üzerinde *V* bir vektör uzayı ve $\{v_1, v_2, \cdots, v_k\} \subseteq V$ olsun. Eğer

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots \alpha_k v_k = 0$$

eşitliğini sağlayan hepsi aynı anda sıfır olmayan $\alpha_1, \alpha_2, \cdots, \alpha_k$ sabitleri varsa $\{v_1, v_2, \cdots, v_k\}$ kümesine lineer bağımlı küme denir.

Eğer bu eşitlik yalnızca $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$ için sağlanıyor ise $\{v_1, v_2, \cdots, v_k\}$ kümesine lineer bağımsız küme denir.

.

Tanım 1.2.1.5. $\mathbb{F}_q$ cismi üzerinde V bir vektör uzayı $U=\{u_1,u_2,\cdots,u_k\}$ vektörler kümesi V'nin boş kümeden farklı bir alt kümesi olsun. Eğer U kümesi lineer bağımsız ve $\langle U\rangle = V$ ise U'ya V vektör uzayının bir bazı denir.

Uyarı 1.2.1.1. Eğer $U=\{u_1,u_2,\cdots,u_k\}$ kümesi V vektör uzayının bir bazı ise V'deki her vektör U'daki vektörlerin lineer kombinasyonu olarak tek türlü yazılabilir.

Uyarı 1.2.1.2. $\mathbb{F}_q$ cismi üzerindeki V vektör uzayının birden fazla bazı olabilir. Fakat bütün bazlardaki eleman sayıları aynıdır.

Tanım 1.2.1.6. Bir V vektör uzayının herhangi bir bazındaki eleman sayısına V'nin boyutu denir.

Bu tanımlamalardan sonra lineer kod tanımı aşağıdaki şekilde verilebilir.

Tanım 1.2.1.7. $C \subseteq \mathbb{F}_q^n$ kodu eğer $\mathbb{F}_q^n$ vektör uzayının bir k boyutlu bir alt vektör uzayı ise C'ye $\mathbb{F}_q$ üzerinde n uzunluğunda k boyutlu bir lineer kod veya [n,k]-kodu denir Eğer C kodunun minimum uzaklığı $d(C)=d$ ise bu lineer kod [n,k,d]-kodu olarak gösterilir. n,k ve d sayılarına da lineer kodun parametreleri denir [9].

Lineer kodlar sadece cisim üzerinde değil aynı zamanda halka üzerinde de tanımlanabilirler.

Tanım 1.2.1.8. R bir halka olmak üzere R^n nin alt modüllerine R üzerinde n uzunluğunda bir lineer kod denir.

Yukarıdaki tanımlardan da anlaşılacağı gibi lineer kodlara bir cebirsel yapı kazandırılmıştır. Bu ise lineer kodların gerek eleman sayısını ve minimum uzaklığını hesaplamada gerek ise kodu üretmede büyük kolaylık sağlayacaktır. Şimdi bu kolaylıklar hakkında kısa bilgiler verilecektir.

$S = (c_1, c_2, \cdots, c_k)$ kümesi *k* boyutlu bir *C* lineer kod için bir baz olsun. Bu durumda *C* nin her bir *c* elemanı $\alpha_1, \alpha_2, \cdots, \alpha_k \in \mathbb{F}_q$ için

$$c = \alpha_1 c_1 + \alpha_2 c_2 + \cdots \alpha_k c_k$$

olacak şekilde tek türlü yazılabilir. Yani *C*'nin her bir elemanı ile $(\alpha_1, \alpha_2, \cdots, \alpha_k) \in \mathbb{F}_q^k$ elemanları arasında bire bir ilişki vardır. Buradan *C*'nin eleman sayısı $|C| = q^k$ olarak bulunabilir.

M elemana sahip herhangi bir *C* kodunda minimum uzaklığı bulmak için her iki kod söz arasındaki uzaklığa bakılması gerektiğinden $\binom{M}{2}$ hesaplama yapılması gerekmektedir. Lineer kodlarda ise aşağıda verilecek olan teorem ile bu hesaplama sayısı (*M*-1)'e düşmektedir.

Teorem 1.2.1.2. Eğer *C* bir lineer kod ise $d_H(C) = w_H(C)$ dir [9].

Lineer kodların sağladığı bir diğer avantaj ise *C* kodu, q^k tane elemanı tek tek listelemek yerine *C*'deki *k* tane lineer bağımsız kod sözün oluşturduğu baz sayesinde kolayca tanımlanabilir. *n* uzunluğundaki *C* lineer kodu için baz oluşturan *k* kod söz bir matrisin satırları olarak düşünülebilir.

Tanım 1.2.1.9. *C* bir [*n*,*k*]-kodu olsun. Satırları *C* için bir baz oluşturan *k*x*n* boyutundaki bir *G* matrisine *C*'nin üreteç matrisi denir. Başka bir ifade ile

$$C = \left\{ xG : x \in \mathbb{F}_q^k \right\}$$

olarak tanımlanabilir [9].

Bu üreteç matris kaynaktaki bilginin kodlanması için kolay bir metot sağlar. Eğer kaynak *k* uzunluğundaki *q*-lu sözlerin bir kümesi olarak temsil edilirse kaynaktaki $x \in \mathbb{F}_q^n$ sözü *xG* kod sözü olarak kodlanabilir.

Tanım 1.2.1.10. $\mathbb{F}_q^n$ de $x=(x_1,x_2,\cdots,x_n)$ ve $y=(y_1,y_2,\cdots,y_n)$ iki vektör olmak üzere *x* ve *y*'nin iç çarpımı

$$x\cdot y = x_1y_1 + x_2y_2 + \cdots x_ny_n$$

olarak tanımlanır [9].

Tanım 1.2.1.11. *C* bir [*n*,*k*]-kodu olsun. *C* kodunun duali

$$C^{\perp} = \{x \in \mathbb{F}_q^n : x.c = 0,\ \forall c \in C\}$$

kümesi olarak tanımlanır [9].

Teorem 1.2.1.3. *C* bir [*n*,*k*]-kodu olsun.

i. *C* kodunun üreteç matrisi *G* ise

$$C^{\perp} = \{x \in \mathbb{F}_q^n : xG^T = 0\} \text{ dır.}$$

ii. $C^{\perp}$ lineer kodu bir [*n*,*n*-*k*]-koddur [9].

1.2.2. Devirli kodlar

Koddaki her bir kod sözün bir devir kayması ile oluşan elemanın yine *C*'deki bir kod söz olması kodlama ve kod çözümlemede kolaylık sağladığı görülmüştür. Bu şartı sağlayan ve devirli kod olarak adlandırılan bu kodlar lineer kodların belki de en önemli sınıflarından biridir.

Cebirsel yapılarından dolayı lineer kodlar ile çalışmanın kolay olduğu önceki bölümde bahsedilmişti. Fakat kodların kolay uygulanabilmesi ve etkili hata düzelten kodların inşası için lineerliğin yanı sıra daha fazla cebirsel yapı kazandırmak arzu edilmiştir. Devirli kodlar polinom halkaları ile ilişkilendirilerek bu sayede daha güçlü cebirsel yapı kazandırılmıştır. Çok zengin bir matematiksel yapıya sahip olmasının yanında kodlama için cebirsel yapılarının daha elverişli olması kodlar arasında en çok çalışılan alan olmasına sebep olmuştur. İlk olarak Eugene Prange tarafından 1957'de çalışılmıştır [11]. O zamandan itibaren devirli kod üzerindeki çalışmalar oldukça geliştirilmiş ve yıllar içerisinde BCH kodları ve Reed Solomon kodları gibi birçok devirli kod inşa edilmiştir.

Bu kısımda yukarıda bahsedilen devirli kodların tanımı verilecek ve yapısı incelenecektir. Bu yapı cebirsel bir biçime dönüştürülecek ve *n* uzunluğundaki bir devirli kodun, *n*'den daha küçük dereceli bir polinom tarafından tamamen belirlendiğini görülecektir.

Tanım 1.2.2.1. $C \subseteq \mathbb{F}_q^n$ için eğer her $(c_0, c_1, \cdots c_{n-1}) \in C$ iken $(c_{n-1}, c_0, \cdots c_{n-2}) \in C$ oluyor ise *C* kümesine devirli küme denir. Eğer *C* lineer kodu bir devirli küme ise *C* koduna devirli kod denir. Başka bir ifade ile *C* lineer kod ve τ

$$\tau(c_0, c_1, \cdots c_{n-1}) = (c_{n-1}, c_0, \cdots c_{n-2})$$

şeklinde tanımlanan bir permütasyon olmak üzere $\tau(C) = C$ oluyor ise *C* koduna devirli kod denir. Burada ki τ 'ya da devirsel öteleme operatörü denecektir [10].

Devirli kodların bu kombinatoriyel yapısını cebirsel yapıya dönüştürmek için aşağıdaki dönüşüm göz önünde bulundurulacaktır.

C kodu $\mathbb{F}_q$ üzerindeki bir lineer kod olmak üzere *C*'deki her bir $(c_0, c_1, \cdots c_{n-1})$ kod sözü

$$\begin{array}{rccc} \phi: & \mathbb{F}_q^n & \rightarrow & \mathbb{F}_q[x] \Big/ \langle x^n - 1 \rangle \\ & (c_0, c_1, \cdots c_{n-1}) & \rightarrow & (c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \end{array}$$

dönüşümü ile $\mathbb{F}_q[x]$ deki bir polinomla ilişkilendirilebilir. Bu dönüşümün bir izomorfizma olduğunu görmek kolaydır.

Teorem 1.2.2.1. $\mathbb{F}_q^n$ 'nin herhangi *C* bir alt kümesinin devirli kod olması için gerek ve yeter şart $\phi(C)$ 'nin $\mathbb{F}_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının bir ideali olmasıdır [10].

Teorem 1.2.2.2. C , $\mathbb{F}_q[x] \Big/ \langle x^n - 1 \rangle$ halkasının bir ideali olmak üzere, başka bir ifade ile n uzunluğunda bir devirli kod olmak üzere

i. C'de derecesi en küçük olan tek bir monik $g(x)$ polinomu $C = \langle g(x) \rangle$ olacak şekilde mevcuttur. Bu $g(x)$ polinomuna C'nin üreteç polinomu denir.

ii. $g(x)$ üreteç polinomu $x^n - 1$'in bir bölenidir.

iii. Eğer $d^o g(x) = r$ ise $boy(C) = n - r$ dir [9].

Tanım 1.2.2.2. $\mathbb{F}_q$ sonlu cismi üzerinde $n = m\ell$ uzunluğunda lineer blok kodu C olsun. Eğer her $c \in C$ kodsözü ℓ tane devir yaptıktan sonra yine C de bir kod söz oluyor ise C koduna ℓ indeksine sahip yarı devirli kod ya da kısaca ℓ -yarı devirli kod denir. Başka bir deyiş ile

$$c = (c_0, c_1, \cdots c_{n-1}) \in C \Rightarrow c' = (c_{n-\ell}, \cdots, c_0, \cdots, c_{n-\ell-1}) \in C$$

olarak tanımlanabilir. Dikkat edilir ise

$$\tau^{\ell}(c_0, c_1, \cdots c_{n-1}) = (c_{n-l}, \cdots, c_0, \cdots, c_{n-\ell-1})$$

dir. Yani $\tau^{\ell}(C) = C$ oluyor ise C koduna ℓ -yarı devirli kod denir [12].

Tanımda bahsedilen ℓ sayısı kodu sabit bırakan en küçük devir sayısıdır. $\ell = 1$ olarak alınırsa tanım gereği yarı devirli kodların devirli koda dönüşeceği kolayca görülebilir. Yani yarı devirli kodlar, devirli kodların bir genellemesidir.

Devirli kodlardan elde edilen kuantum kodların parametreleri için aşağıdaki teoreme ihitiyaç duyulacaktır.

Teorem 1.2.2.3. C ve $\hat{C}$ kodları $C^{\perp} \subseteq \hat{C}$ olacak şekilde $[n,k,d]$ ve. $[n,\hat{k},\hat{d}]$ parametrelerine sahip iki lineer kod olsun. Bu durumda $[[n, k+\hat{k}, min\{d,\hat{d}\}]]$ parametresine sahip bir kuantum kod vardır. Özel olarak eğer $C^{\perp} \subseteq C$ ise $[[n,2k-n,d]]$ parametresine sahip bir kuantum kod vardır [13].

BÖLÜM 2. $\mathbb{Z}_4[u]/\langle u^3 \rangle$ HALKASI ÜZERİNDE DEVİRLİ KODLAR

Lineer kodların önemli bir sınıfı olan devirli kodlar, polinom halkalarının ideallerine karşılık geldiğinden zengin bir cebirsel yapıya sahiptir. Bu da kodlama teorisinde devirli kodlar üzerinde çok sayıda çalışma yapılmasına sebep olmuştur. Son yıllarda birçok araştırmacının ilgilenmeye başladığı diğer bir konu ise halka üzerindeki kodlardır. Bu sebepten dolayı çeşitli halkalar üzerinde devirli kodların yapısını inceleme fikri doğmuştur [14, 15, 16, 17]. Hem $\mathbb{Z}_4$ halkasının hem de $\mathbb{F}_4$ cisminin birçok özelliği ile benzer özelliğe sahip olduğundan oldukça kullanışlı bir halka olan $\mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerindeki lineer devirli kodlar Bonnecaze ve Udaya tarafından incelenmiştir [18]. Bandi ve Bhaintwal [19] $u^2 = 0$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerindeki devirli kodların cebirsel yapısını incelemişler ve bu kodların üreteçleri hakkında bazı temel gerçekler elde etmişlerdir. Yıldız ve Aydın [20] aynı halka üzerindeki devirli kodları farklı bir yöntem ile incelemiş ve elde edilen sonuçları kullanarak $\mathbb{Z}_4$ üzerinde yeni lineer kodlar bulmuşlardır. Gao ve ark. [21], Yıldız ve Aydın'ın [20] çalışmasını genişleterek q bir asalın kuvveti ve $u^2 = 0$ olmak üzere $\mathbb{Z}_q + u\mathbb{Z}_q$ üzerindeki devirli kodları araştırmışlardır.

Bu bölüm 5 kısımdan oluşmuştur. Bölümün amacı ise $u^3 = 0$ olmak üzere $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ halkası üzerindeki devirli kodların yapısını belirlemek ve bu kodlardan yararlanarak $\mathbb{Z}_4$ üzerinde yeni lineer kodlar bulmaktır. Bunun için halka üzerindeki kodların hangi şartlar altında var olduğunu ve daha verimli olduğunu iyi analiz etmek adına R halkasının cebirsel yapısı ilk bölümde incelenmiştir. İkinci bölümde ise R halkasının Galois genişlemesi ve bu genişlemenin ideal yapısı çalışılmıştır. Bir sonraki bölümde R üzerindeki devirli kodların yapısı, bu kodların üreteçlerinin bir genel formu ve ikinci bölümdeki bazı sonuçlardan yararlanarak devirli

kodlar için en küçük geren küme belirlenmiştir. Dördüncü bölümde *R* üzerindeki devirli kodlar ile $\mathbb{Z}_4$ üzerindeki kodlar arasıdaki geçişi sağlayan Gray dönüşüm tanımlanmış ve bu dönüşüm yardımı ile *R* üzerindeki bir devirli kodun $\mathbb{Z}_4$-görüntüsünün 3-yarı devirli kod olduğu gösterilmiştir. Son olarak *R* üzerindeki devirli kodlardan yararlanarak $\mathbb{Z}_4$ üzerinde bulunan yeni lineer kodlar bir tablo halinde listelenmiştir.

2.1. $\mathbb{Z}_4[u]/\langle u^3\rangle$ Halkasının Cebirsel Yapısı

Bu bölüm boyunca "*R*" harfi $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4 = \{a+ub+u^2c \mid u^3 = 0 \text{ ve } a,b,c \in \mathbb{Z}_4\}$ halkasını temsil edecektir. *R* halkasının $\mathbb{Z}_4[u]/\langle u^3\rangle$ cebirsel yapısına izomorf olduğu kolayca görülür. Yani $R \cong \mathbb{Z}_4[u]/\langle u^3\rangle$ dir. *R* halkası karakteristiği 4 olan 64. mertebeden birimli ve değişmeli bir halkadır. *R* halkasının herhangi bir *x* elemanı $a,b,c \in \mathbb{Z}_4$ olmak üzere $x = a+ub+u^2c$ şeklinde ifade edilebilir. Ayrıca *x* elemanının *R*'nin birimsel elemanı olması için gerek ve yeter şart *a* elemanının $\mathbb{Z}_4$ de birimsel olmasıdır. *R* halkasının aşikâr olmayan ideal sayısı 11 olup aşağıdaki gibi listelenebilir.

$$\langle 2u^2\rangle = \{0, 2u^2\}$$
$$\langle u^2\rangle = \{0, u^2, 2u^2, 3u^2\}$$
$$\langle 2u\rangle = \{0, 2u, 2u^2, 2u+2u^2\}$$
$$\langle 2u+u^2\rangle = \{0, 2u^2, 2u+u^2, 2u+3u^2\}$$
$$\langle 2\rangle = \{0, 2, 2u, 2u^2, 2+2u, 2+2u^2, 2u+2u^2, 2+2u+2u^2\}$$
$$\langle 2+u^2\rangle = \{0, 2u, 2u^2, 2u+2u^2, 2+u^2, 2+3u^2, 2+2u+u^2, 2+2u+3u^2\}$$
$$\langle u\rangle = \left\{\begin{matrix} 0, u, 2u, 3u, u^2, 2u^2, 3u^2, u+u^2, u+2u^2, u+3u^2, 2u+u^2, 2u+2u^2, \\ 2u+3u^2, 3u+u^2, 3u+2u^2, 3u+3u^2 \end{matrix}\right\}$$
$$\langle 2+u\rangle = \left\{\begin{matrix} 0, 2u, u^2, 2u^2, 3u^2, 2+u, 2+3u, 2u+u^2, 2u+2u^2, 2u+3u^2, 2+u+u^2, \\ 2+u+2u^2, 2+u+3u^2, 2+3u+u^2, 2+3u+2u^2, 2+3u+3u^2 \end{matrix}\right\}$$

$$\langle 2u, u^2 \rangle = \{0, u^2, 2u^2, 3u^2, 2u, 2u+u^2, 2u+2u^2, 2u+3u^2\}$$

$$\langle 2, u^2 \rangle = \left\{ \begin{matrix} 0, 2, 2u, u^2, 2u^2, 3u^2, 2+2u, 2+u^2, 2+2u^2, 2+3u^2, 2u+u^2, 2u+2u^2, \\ 2u+3u^2, 2+2u+u^2, 2+2u+2u^2, 2+2u+3u^2 \end{matrix} \right\}$$

$$\langle 2, u \rangle = \left\{ \begin{matrix} 0, 2, u, 2u, 3u, u^2, 2u^2, 3u^2, 2+u, 2+2u, 2+3u, 2+u^2, 2+2u^2, 2+3u^2, \\ u+u^2, u+2u^2, u+3u^2, 2u+u^2, 2u+2u^2, 2u+3u^2 \%, 3u+u^2, 3u+2u^2, \\ 3u+3u^2, 2+u+u^2, 2+u+2u^2, 2+u+3u, 2+2u+u^2, 2+2u+2u^2, \\ 2+2u+3u^2, 2+3u+u^2, 2+3u+2u^2, 2+3u+3u^2 \end{matrix} \right\}$$

$\langle 2, u \rangle$ ideali R halkasının tek maksimal ideali olduğundan R halkası bir lokal Frobenius halkasıdır. $\langle u^2 \rangle$ ve $\langle 2u \rangle$ idealleri kümelerdeki kapsama bağıntısına göre karşılaştırılamadığından R halkası bir zincir halkası değildir. Ayrıca $\langle 2, u \rangle$ ideali gibi tek eleman tarafından üretilemeyen ideallere de sahip olduğundan R halkası temel (esas) ideal halkası değildir.

R'nin kalan cismi $\tilde{R}$ ile gösterilsin. Bu küme

$$\tilde{R} = R \big/ \langle 2, u \rangle = \{0 + \langle 2, u \rangle, 1 + \langle 2, u \rangle\} \cong \mathbb{Z}_2$$

şeklindedir.

Şimdi. $\sim : R \to \tilde{R}$ bir izdüşüm dönüşümü

$$\sim (x) = \begin{cases} 1, & x \text{ birimsel} \\ 0, & \text{Diğer} \end{cases}$$

şeklinde tanımlansın. Bu dönüşüm altında R'nin bir x elemanının görüntüsü $\tilde{x}$ olarak gösterilecektir. R halkası üzerindeki polinom halkası $R[x]$ ile temsil edilmek üzere " $\sim$ " izdüşüm dönüşümü $R[x] \to \tilde{R}[x]$ şeklinde genişletilebilir. Bu durumda da bu dönüşüm altında $R[x]$'in bir $f(x)$ elemanının görüntüsü $\tilde{f}(x)$ olarak gösterilecektir.

Tanım 2.1.1. Eğer $\tilde{f}(x)$ polinomu $\tilde{R}[x]$ polinom halkası üzerinde indirgenemez polinom ise $R[x]$ polinom halkası üzerindeki $f(x)$ polinomuna $R[x]$'de temel indirgenemez polinom denir.

Sonlu cisim üzerindeki indirgenemez polinom ve sonlu lokal halka üzerindeki temel indirgenemez polinom cebirde benzer rol oynarlar.

Tanım 2.1.2. Eğer bir $f(x)$ polinomu $R[x]$'de bir sıfır bölen değil ise $f(x)$ polinomuna regüler polinom denir [5].

Tanım 2.1.3. Eğer $R[x]$ polinom halkasında

$$f(x)a_0(x)+g(x)a_1(x)=1$$

olacak şekilde $a_0(x)$ ve $a_1(x)$ polinomları varsa $f(x)$ ve $g(x)$ polinomları aralarında asaldır denir.

Teorem 2.1.1. (22) (Hensel's Lemma) $f(x)$ polinomu $\mathbb{Z}_4[x]$ de monik polinom olsun. Ayrıca $\tilde{f}_1(x)$, $\tilde{f}_2(x),...,$ $\tilde{f}_r(x)$ polinomları $\mathbb{Z}_2[x]$'de ikişer ikişer aralarında asal ve $\tilde{f}_i(x)\equiv f_i(x)(\bmod 2)$ olmak üzere $\tilde{f}(x)=\tilde{f}_1(x)\tilde{f}_2(x)...\tilde{f}_3(x)$ olsun. Bu durumda aşağıdaki özellikleri sağlayan $h_1(x),h_2(x),\ldots,h_r(x)\in\mathbb{Z}_4[x]$ monik polinomları vardır.

i. $f(x)=h_1(x)h_2(x)...h_r(x).$

ii. $\tilde{h}_i(x)=\tilde{f}_i(x).$

iii. $h_1(x),h_2(x),\ldots,h_r(x)$ polinomları $\mathbb{Z}_4[x]$ de aralarında asaldır [22].

2.2. $\mathbb{Z}_4[u]/\langle u^3\rangle$ Halkasının Galois Genişlemesi

Bu bölümde $R[x]/\langle x^n-1\rangle$ bölüm halkasının ideallerinin belirlenmesinde kullanılacak olan R halkasının Galois genişlemesi incelenecektir. Devirli kodların çalışılmasında önemli bir yere sahip olduğundan dolayı ilk olarak $R[x]$ üzerinde x^n-1 polinomunun çarpanlarına ayrılışı incelenecektir.

Teorem 2.2.1. $h(x)$ polinomu $\mathbb{Z}_2[x]$ de bir indirgenemez polinom ve pozitif bir r tamsayısı için $x^{2^r-1}-1$ polinomunu bölsün. Bu durumda $R[x]$ de $f(x) \mid x^{2^r-1}-1$ ve $\tilde{f}(x)=h(x)$ şartlarını sağlayan bir tek temel indirgenemez $f(x)$ polinomu vardır.

İspat. $h(x) \mid x^{2^r-1}-1$ olduğundan $h(x)\cdot h'(x)=x^{2^r-1}-1$ olacak şekilde bir $h'(x)\in\mathbb{Z}_2[x]$ polinomu vardır. Teorem 2.1.1'den dolayı $f(x)(\bmod 2)=h(x)$ ve $f'(x)(\bmod 2)=h'(x)$ olmak üzere $f(x)\cdot f'(x)=x^{2^r-1}-1$ olacak şekilde $f(x), f'(x) \in\mathbb{Z}_4[x]$ vardır. $\mathbb{Z}_4$ halkası R halkasının bir alt halkası olduğundan $x^{2^r-1}-1$ polinomunun çarpanlara ayrılışı R halkası üzerinde de geçerlidir. Yani $R[x]$ de $f(x) \mid (x^{2^r-1}-1)$ sağlanır. Ayrıca $\tilde{f}(x)\equiv f(x)(\bmod \langle 2,u\rangle)=h(x)$ dir. 2^r-1 tek olduğundan dolayı [5]'deki Teorem XIII.11 kullanılarak $x^{2^r-1}-1$ polinomu R halkası üzerinde ikişer ikişer aralarında asal temel indirgenemez polinomların çarpımı olarak tek türlü yazılabilir. Bu da $f(x)$ polinomunun tek türlü olduğunu ispatlar.

Teorem 2.2.1 deki $f(x)$ polinomu $h(x)$ polinomunun "Hensel Lift"i olarak adlandırılır. R halkasının Galois genişlemelerini çalışabilmek için $\mathbb{Z}_4$ halkasının Galois genişlemesindeki bazı sonuçlara ihtiyaç duyulacaktır. Bu yüzden $\mathbb{Z}_4$ halkasının Galois genişlemesi hakkında bazı temel bilgiler verilecektir. $r(x)$ polinomu $\mathbb{Z}_4[x]$ de derecesi k olan monik temel indirgenemez polinom olsun. Bu durumda $\mathbb{Z}_4$ üzerindeki Galois halkası $\mathbb{Z}_4[x]\big/\langle r(x)\rangle$ kalan sınıf halkası olarak tanımlanır ve $GR(4,k)$ ile gösterilir.

$r(x)$ polinomunun bir kökü ε ve $GR(4,k)$'nın Teichmüller kümesi $T=\{0,1,\varepsilon,\varepsilon^2,\cdots,\varepsilon^{2^k-1}\}$ olsun. Bu durumda $x_0,x_1\in T$ olmak üzere $GR(4,k)$'nın tüm elemanları x_0+2x_1 şeklinde tek türlü ifade edilebilir. Bu gösterime *2-lik* gösterim denir.

Şimdi benzer yöntemle R nin Galois genişlemesi araştırılacaktır. $r(x)$ polinomu $R[x]$ de derecesi k olan monik temel indirgenemez polinom olsun. Bu durumda R üzerindeki Galois halkası $R[x]/\langle r(x)\rangle$ kalan sınıf halkası olarak tanımlanır ve $GR(R,k)$ ile gösterilir. Eğer $r(x)$ polinomunun bir kökü α ise $GR(R,k)$'nın tüm elemanları $i=0,1,\ldots,k-1$ için $r_i \in R$ olmak üzere

$$r_0 + r_1\alpha + \ldots + r_{k-1}\alpha^{k-1}$$

şeklinde ifade edilir ve $GR(R,k)$ Galois halkasının elemanlarının toplamsal gösterimi olarak tanımlanır. $GR(R,k)$ Galois halkası $\{0,1,\alpha,\cdots,\alpha^{k-1}\}$ bazına sahip $|GR(R,k)| = 64^k$ elemanlı bir serbest R-modül olarak düşünülebilir. $\langle 2,u\rangle + \langle r(x)\rangle$ tek maksimal idealine sahip lokal halkadır. F_{2^k} sonlu cismi $GR(R,k)$'nin kalan cismidir. Ayrıca

$$GR(R,k) \cong GR(4,k)[u]/\langle u^3\rangle \cong GR(4,k) + uGR(4,k) + u^2GR(4,k)$$

dır. Bu sebepten dolayı $GR(R,k)$'nın herhangi bir x elemanı $a,b,c \in GR(4,k)$ olmak üzere $x = a + ub + u^2c$ şeklinde yazılabilir. $GR(4,k)$ halkasındaki *2-lik* gösterim kullanılarak $i=1,2$ için $a_i,b_i,c_i \in T$ olmak üzere $a = a_1 + 2a_2, b = b_1 + 2b_2, c = c_1 + 2c_2$ yazılabilir. O halde $GR(R,k)$'nın x elemanı yeniden yazılırsa

$$x = a_1 + 2a_2 + u(b_1 + 2b_2) + u^2(c_1 + 2c_2)$$

elde edilir.

Lemma 2.2.1. $GR(R,k)$'nın sıfırdan farklı $x = a_1 + 2a_2 + u(b_1 + 2b_2) + u^2(c_1 + 2c_2)$ elemanının birimsel olması için gerek ve yeter şart $0 \neq a_1 \in T$ olmasıdır.

İspat. $GR(R,k)$'nın sıfırdan farklı herhangi bir elemanı için $x^4 = a_1^4$ olduğundan istenilen sonuç aşağıdaki gibi elde edilecektir.

$$\begin{aligned} x \text{ birimseldir} &\Leftrightarrow x^4 = a_1^4 \in T \text{ birimseldir} \\ &\Leftrightarrow a_1^4 \neq 0 \\ &\Leftrightarrow a_1 \neq 0 \end{aligned}$$

$GR(R,k)$ halkasının birimsel elemanlarının oluşturduğu grup $GR^*(R,k)$ ile gösterilirse Lemma 2.2.1'den dolayı

$$GR^*(R,k)=\{a_1+2a_2+u(b_1+2b_2)+u^2(c_1+2c_2)\mid a_i,b_i,c_i\in T,(i=1,2);a_1\neq 0\}$$

şeklindedir.

Lemma 2.2.2. $f(x)$ ve $g(x)$, $R[x]$'de iki polinom olsun. $f(x)$ ve $g(x)$ polinomlarının $R[x]$'de aralarında asal olması için gerek ve yeter şart $\tilde{f}(x)$ ve $\tilde{g}(x)$ polinomlarının $\tilde{R}[x]$'de aralarında asal olmasıdır.

İspat. $f(x)$ ve $g(x)$ polinomlarının $R[x]$'de aralarında asal olduğundan

$$f(x)a_0(x)+g(x)a_1(x)=1$$

olacak şekilde $a_0(x),a_1(x)\in R[x]$ polinomları vardır. Buradan da $\tilde{f}(x),\tilde{g}(x),\tilde{a}_0(x),\tilde{a}_1(x)\in\tilde{R}[x]$ polinomları için

$$\tilde{f}(x)\tilde{a}_0(x)+\tilde{g}(x)\tilde{a}_1(x)=1$$

eşitliği sağlanır. Bu sebepten dolayı $\tilde{f}(x)$ ve $\tilde{g}(x)$ polinomlarının $\tilde{R}[x]$'de aralarında asaldır.

Diğer taraftan eğer $\tilde{f}(x)$ ve $\tilde{g}(x)$ polinomlarının $\tilde{R}[x]$'de aralarında asal ise

$$\tilde{f}(x)\tilde{a}_0(x)+\tilde{g}(x)\tilde{a}_1(x)=1$$

olacak şekilde $\tilde{a}_0(x),\tilde{a}_1(x)\in\tilde{R}[x]$ polinomları vardır. Buradan da

$$f(x)a_0(x)+g(x)a_1(x)=1+2s(x)+ut(x)$$

Eşitliği sağlanacak $s(x),t(x)\in R[x]$ polinomları vardır. Eğer

$$\alpha(x)=1-2s(x)$$
$$\beta(x)=1-ut(x)\alpha(x)$$
$$\delta(x)=\beta^2(x)+2ut(x)\alpha(x)$$
$$\Gamma(x)=\alpha(x)\beta(x)\delta(x)$$

polinomları seçilirse

$$\Gamma(x)f(x)a_0(x)+\Gamma(x)g(x)a_1(x)=1$$

elde edilir. Buda $f(x)$ ve $g(x)$ polinomlarının $R[x]$'de aralarında asal olduğunu ispatlar.

Teorem 2.2.2. $f(x)$ polinomu R üzerinde temel indirgenemez polinom olsun. $R[x]/\langle f(x)\rangle$ Galois halkasının idealleri $\{0\}, \langle 1+\langle f(x)\rangle\rangle, \langle 2+\langle f(x)\rangle\rangle, \langle u+\langle f(x)\rangle\rangle,$ $\langle 2u+\langle f(x)\rangle\rangle, \langle u^2+\langle f(x)\rangle\rangle, \langle 2u^2+\langle f(x)\rangle\rangle, \langle 2+u+\langle f(x)\rangle\rangle, \langle 2+u^2+\langle f(x)\rangle\rangle,$ $\langle 2u+u^2+\langle f(x)\rangle\rangle, \langle (2u,u^2)+\langle f(x)\rangle\rangle, \langle (2,u^2)+\langle f(x)\rangle\rangle$ ve $\langle (2,u)+\langle f(x)\rangle\rangle$ dir.

İspat. $R[x]/\langle f(x)\rangle$ Galois halkasının sıfırdan farklı bir I ideali ve $g(x)\notin\langle f(x)\rangle$ olacak şekilde $g(x)+\langle f(x)\rangle\in I$ olsun. $f(x)$ polinomu R üzerinde temel indirgenemez polinom olduğundan $\tilde{f}(x)$ polinomu da $\tilde{R}$ üzerinde indirgenemez polinomdur Dolayısıyla $ebob(\tilde{g}(x), \tilde{f}(x))=1$ veya $\tilde{f}(x)$ dir. Kabul edilsin ki $ebob(\tilde{g}(x), \tilde{f}(x))=1$ olsun. Lemma 2.2.2 den dolayı $ebob(g(x), f(x))=1$olduğu söylenebilir. Bu durumda da

$$f(x)a_0(x)+g(x)a_1(x)=1$$

şartını sağlayan $a_0(x), a_1(x)\in R[x]$ polinomları mevcuttur. Yukarıdaki eşitlik aynı zamanda

$$g(x)a_1(x)=1 \mod f(x)$$

olarak da düşünülebilir. Buradan $g(x)$ polinomunun I idealinde terslenebilen eleman olduğu söylenebilir. Bu yüzden $I=\langle 1+(f(x))\rangle$ dir. Diğer taraftan $ebob(\tilde{g}(x), \tilde{f}(x))=\tilde{f}(x)$ olduğu kabul edilsin. O halde $\tilde{g}(x)=\tilde{f}(x)\tilde{h}(x)$ olacak şekilde $\tilde{h}(x)\in\tilde{R}[x]$ polinomu vardır. Böylece $h(x), h_1(x), h_2(x)\in R[x]$ polinomları için

$$g(x)=f(x)h(x)+2h_1(x)+uh_2(x)$$

eşitliği sağlanır ve $ebob(\tilde{f}(x), \tilde{h}_1(x))=1$ veya $ebob(\tilde{f}(x), \tilde{h}_2(x))=1$ dir. Bu da gösterir ki $g(x)+\langle f(x)\rangle\in\langle (2,u)+\langle f(x)\rangle\rangle$ dir. $I\neq\langle 1+\langle f(x)\rangle\rangle$ olduğundan dolayı $I\subset\langle (2,u)+\langle f(x)\rangle\rangle$ olması gerekecektir. $\langle (2,u)+\langle f(x)\rangle\rangle$ elemanı tarafından içerilen

sıfırdan farklı idealler $\langle 2+\langle f(x)\rangle\rangle, \langle u+\langle f(x)\rangle\rangle, \langle 2u+\langle f(x)\rangle\rangle, \langle u^2+\langle f(x)\rangle\rangle,$ $\langle 2u^2+\langle f(x)\rangle\rangle, \langle 2+u+\langle f(x)\rangle\rangle, \langle 2+u^2+\langle f(x)\rangle\rangle, \langle (2,u^2)+\langle f(x)\rangle\rangle$ $\langle (2u,u^2)+\langle f(x)\rangle\rangle$, $\langle 2u+u^2+\langle f(x)\rangle\rangle$ ve $\langle (2,u)+\langle f(x)\rangle\rangle$ idealinin kendisidir.

R halkasının Galois genişlemesinin idealleri ile ilgili olan sonuçlar bir sonraki bölümde *R* üzerindeki *n* uzunluğundaki devirli kodların sayısını belirlemek için kullanılacaktır.

2.3. $\mathbb{Z}_4[u]/\langle u^3\rangle$ Halkası Üzerinde Devirli Kodların Yapısı

Bu bölüm boyunca *n* sayısı tek pozitif tamsayı olarak kabul edilecektir. *R* üzerinde *n* uzunluğundaki lineer kod R^n'nin bir *R*-alt modülüdür. Eğer *C* lineer kodunun her $(c_0, c_1, \ldots, c_{n-1})$ elemanı için $(c_{n-1}, c_0, \ldots, c_{n-2})$ da *C* nin elemanı oluyor ise *C* lineer koduna *R* üzerinde bir devirli kod denir.

$R[x]/\langle x^n-1\rangle$ bölüm halkası R_n ile gösterilsin. R^n cebirsel yapısındaki *n* uzunluğundaki vektörler ile R_n bölüm halkasındaki polinomlar arasında

$$\phi : R^n \to R_n$$
$$c = (c_0, c_1, \ldots, c_{n-1}) \to c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} = c(x)$$

şeklinde bir lineer dönüşüm kurulabilir.

Teorem 2.3.1. R^n boştan farklı bir *C* alt kümesinin devirli kod olması için gerek ve yeter şart *C* kodunun ϕ dönüşümü altındaki görüntüsü olan $\phi(C)$'nin R_n bölüm halkasının ideali olmasıdır.

İspat. Kabul edilsin ki $\phi(C)$, R_n bölüm halkasının bir ideali olsun. İlk olarak R^n boştan farklı *C* alt kümesinin R^n'nin bir *R*-alt modülü olduğu gösterilmelidir. Herhangi bir $\alpha, \beta \in R \subseteq R_n$ ve $a, b \in C$ elemanları için ϕ lineer dönüşüm olduğundan $\alpha\phi(a), \beta\phi(b) \in \phi(C)$ dir. Aynı zamanda $\phi(C)$, R_n bölüm halkasının bir ideali

olduğundan $\alpha\phi(a)-\beta\phi(b)=\phi(\alpha a-\beta b)\in\phi(C)$ dir. Yani $\alpha a-\beta b\in C$ dir. Buradan C kümesinin R^n'nin bir R-alt modülü olduğu sonucuna varılır. Dolayısıyla C lineer koddur. Şimdi devirli olduğu gösterilecektir. $c=(c_0,c_1,\ldots,c_{n-1})\in C$ kodsöz olmak üzere $\phi(c)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}\in\phi(C)$ dir. $\phi(C)$'nin R_n bölüm halkasının ideali olduğundan

$$\begin{aligned} x\phi(c) &= c_0x+c_1x^2+\ldots+c_{n-2}x^{n-1}+c_{n-1}x^n \\ &= c_{n-1}+c_0x+c_1x^2+\ldots c_{n-2}x^{n-1} \end{aligned}$$

elemanı da $\phi(C)$ de bulunacaktır. Yani $(c_{n-1},c_0,\ldots,c_{n-2})\in C$ dir. Bu da gösterir ki C lineer kodu devirli koddur.

Diğer taraftan C devirli kod olsun. $\phi(C)$'nin R_n bölüm halkasının ideali olduğu gösterilecektir.

i. $\phi(c)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$ ve $\phi(d)=d_0+d_1x+\ldots+d_{n-1}x^{n-1}\in\phi(C)$ için $(c_0,c_1,\ldots,c_{n-1}),(d_0,d_1,\ldots,d_{n-1})\in C$ dir. C lineer olduğundan $(c_0-d_0,c_1-d_1,\cdots c_{n-1}-d_{n-1})\in C$ olduğu dikkate alınırsa $\phi(c)-\phi(d)=c_0-d_0+(c_1-d_1)x+\ldots+(c_{n-1}-d_{n-1})x^{n-1}\in\phi(C)$ dir.

ii. Herhangi bir $\phi(c)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}=c(x)$ polinomu için $c=(c_0,c_1,\ldots,c_{n-1})\in C$ dir.

$$xc(x)=c_{n-1}+c_0x+c_1x^2+\ldots c_{n-2}x^{n-1}$$

elemanı da C devirli olduğundan dolayı $\phi(C)$'nin elemanıdır. Benzer mantık ile $x(xc(x))=x^2c(x)$ de yine $\phi(C)$'nin elemanı olacaktır. Bu şekilde devam edilir ise $i\geq 0$ için $x^ic(x)\in\phi(C)$ dir. C lineer kod ve $\phi(C)$ lineer dönüşüm olduğundan dolayı $r(x)\in R_n$ için $r(x)c(x)\in\phi(C)$ sonucuna varılır.Sonuç olarak (i) ve (ii) den dolayı $\phi(C)$, R_n bölüm halkasının idealidir.

Teorem 2.3.1'den de anlaşılacağı gibi R üzerindeki devirli kodların yapısını anlamak için R_n bölüm halkasının yapısını incelemek gerekecektir. Dinh ve Permouth'un [4] çalışmasından biliniyor ki eğer S sonlu bir zincir halkası ve S halkasının karakteristiği

ile n aralarında asal ise S_n bölüm halkası temel ideal halkasıdır. Fakat bu bölümde çalışılan R halkasının karakteristiği ile n tek tamsayısı aralarında asal olmasına rağmen bir zincir halkası olmadığından R_n bölüm halkası temel ideal halkası olmak zorunda değildir. Şimdi R_n bölüm halkasının temel ideal halkası olmadığı aşağıdaki teorem ile ispatlansın.

Teorem 2.3.2. R_n bölüm halkası temel ideal halkası değildir.

İspat. Bu teoremin ispatında Abualrub'un doktora tezinde [23] tanımlamış olduğu grup halkaları kullanılacaktır.

$G = \langle g : g^n = 1 \rangle$ grubu mertebesi n olan devirli bir grup olsun. Herhangi bir RG grup halkası için "arttırma homomorfizması"

$$\xi : RG \to R$$

$$\xi(r_0 + r_1 g + \cdots + r_{n-1} g^{n-1}) = r_0 + r_1 + \cdots + r_{n-1}$$

şeklinde tanımlanır. Bu dönüşüm örten bir halka homomorfizmasıdır. Ayrıca

$$\xi : R_n \to R$$

$$\xi(r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}) = r_0 + r_1 + \cdots + r_{n-1}$$

olarak da tanımlanabilir.

Şimdi R halkasının $I = \langle 2, u \rangle$ ideali göz önünde bulundurulsun ve $J = \xi^{-1}(I)$ olsun. Bir idealin halka homomorfizması altındaki ters görüntüsüde ideal olacağında J , R_n bölüm halkasının bir idealdir. Kabul edilsin ki J ideali temel ideal olsun. I ideali J idealinin homomorf görüntüsü olduğundan I ideali de temel ideal olmak zorundadır. Fakat bu çelişki oluşturur. O halde J ideali R_n bölüm halkasının temel ideal değildir. Bu sebepten dolayı R_n temel ideal halkası olamaz. Böylelikle istenen sağlanır.

Şimdi Çin kalan Teoremi'nden yola çıkarak R_n bölüm halkasının idealleri araştırılacaktır. n pozitif tek tamsayı olduğundan dolayı $x^n - 1$ polinomu R üzerinde

ikişer ikişer aralarında asal temel indirgenemez polinomların çarpımı olarak yazılabilir [5]. Kabul edilsin ki $f_1(x), f_2(x),..., f_s(x)$ ikişer ikişer aralarında asal temel indirgenemez polinomlar ve $x^n-1= f_1(x)f_2(x)\cdots f_s(x)$ olsun. $f_i(x)$ polinomu hariç diğer tüm polinomlarının çarpımı $\hat{f}_i(x)$ ile gösterilsin. O halde $i=1,2,\ldots,s$ için , $\hat{f}_i(x)$ ile $f_i(x)$ aralarında asaldır ve

$$f_i(x)a_i(x)+\hat{f}_i(x)b_i(x)=1$$

olacak şekilde $a_i(x),b_i(x)\in R[x]$ polinomları vardır.

$e_i(x)=\hat{f}_i(x)b_i(x)+\langle x^n-1\rangle$ ve $R_i=e_i(x)R_n$ olsun. Teorem 1.1.14'den dolayı R_n halkası

$$R_n=R_1+R_2+\cdots+R_s$$

şeklinde yazılabilir.

$i=1,2,...,s$ için

$$\begin{aligned}\theta_i:\quad R[x]/\langle f_i(x)\rangle &\to R_i\\ r(x)+\langle f_i(x)\rangle &\to (r(x)+\langle x^n-1\rangle)e_i(x)\end{aligned}$$

şeklinde bir halka izomofizması tanımlanırsa

$$R[x]/\langle x^n-1\rangle \cong R[x]/\langle f_1(x)\rangle + R[x]/\langle f_2(x)\rangle +\cdots+ R[x]/\langle f_s(x)\rangle$$

elde edilir.

Yukarıda bahsedilenleden yola çıkarak aşağıdaki sonuç elde edilebilir.

Sonuç 2.3.1. $i=1,2,\ldots,s$ için R üzerinde ikişer ikişer aralarında asal temel indirgenemez $f_i(x)$ polinomları için x^n-1 in tek türlü çarpanlara ayrılışı $x^n-1=f_1(x)f_2(x)\cdots f_s(x)$ olsun. Bu durumda R_n halkasının herhangi bir ideali $i=1,2,\ldots,s$ olmak üzere $R[x]/\langle f_i(x)\rangle$ 'nin ideallerinin toplamı şeklinde yazılır.

Teorem 2.3.3. $x^n - 1$ polinomunun temel indirgenemez çarpanlarının sayısı s olmak üzere R üzerindeki devirli kod sayısı 13^s dir.

İspat. Sonuç 2.3.1'den dolayı biliniyor ki R_n halkasının herhangi bir ideali $i = 1, 2, \ldots, s$ olmak üzere $R[x] / \langle f_i(x) \rangle$ 'nin ideallerinin toplamı şeklinde yazılabiliyor. Teorem 2.2.2'den dolayı her i değeri için $R[x] / \langle f_i(x) \rangle$ halkası 13 ideale sahiptir. Dolayısıyla i' nin s tane değeri için 13^s tane ideal olacaktır.

Şimdi R üzerindeki devirli kodların üreteçlerinin genel bir formu belirlenecektir. Bunun için ilk olarak R halkasından $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkasına bir homomorfizma tanımlanacaktır. Bu homomorfizma ve $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerindeki devirli kodlar için elde edilmiş bazı sonuçlar kullanılarak R üzerindeki devirli kodların üreteçlerinin genel bir formu belirlenmiş olacaktır.

R halkasından $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkasına

$$\begin{array}{rccc} \Psi: & R & \to & \mathbb{Z}_4 + u\mathbb{Z}_4 \\ & a + ub + u^2 c & \to & a + ub \mod u^2 \end{array}$$

şeklinde bir dönüşüm tanımlansın. $\forall a + ub + u^2 c, x + uy + u^2 z \in R$ için

$$\begin{aligned} \Psi(a + ub + u^2 c + x + uy + u^2 z) &= (a + x) + u(b + y) \mod u^2 \\ &= a + ub + x + uy \mod u^2 \\ &= \Psi(a + ub + u^2 c) + \Psi(x + uy + u^2 z) \\ \Psi((a + ub + u^2 c).(x + uy + u^2 z)) &= \Psi(ax + u(ay + bx) + u^2(az + by + cx)) \\ &= ax + u(ay + bx) \mod u^2 \\ &= (a + ub).(x + uy) \mod u^2 \\ &= \Psi(a + ub + u^2 c).\Psi(x + uy + u^2 z) \end{aligned}$$

koşulları sağlandığından Ψ dönüşümü bir halka homomorfizmasıdır.

Bu homomorfizma polinom halkalarına genişletilirse $a_i \in R$ olmak üzere

$$\Phi : R[x] \Big/ \langle x^n - 1 \rangle \to (\mathbb{Z}_4 + u\mathbb{Z}_4)[x] \Big/ \langle x^n - 1 \rangle$$

$$\Phi(a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}) = \Psi(a_0) + \Psi(a_1)x + \ldots + \Psi(a_{n-1}) x^{n-1}$$

şeklinde bir halka homomorfizması elde edilir.

C lineer kodu R_n halkasında bir devirli kod olsun. Φ fonksiyonu C kümesi üzerine kısıtlanırsa

$$\Phi : C \to (\mathbb{Z}_4 + u\mathbb{Z}_4)[x] \Big/ \langle x^n - 1 \rangle$$

elde edilir.

C devirli kodunun üreteç yapısının belirlenebilmesi için Φ halka homomorfizmasının çekirdeğinden ve görüntüsünden faydalanılacaktır. Bu sebepten dolayı ilk olarak Φ dönüşümünün görüntü ve çekirdek kümeleri sırasıyla aşağıdaki gibi belirlenebilir.

Teorem 2.3.1'den dolayı C devirli kodu aslında R_n bölüm halkasının bir ideali idi. Halka homomorfizmasından dolayı C kodunun Φ homomorfizması altındaki görüntüsü de $(\mathbb{Z}_4 + u\mathbb{Z}_4)[x] \Big/ \langle x^n - 1 \rangle$ bölüm halkasının bir ideali olacaktır. Bu da $\Phi(C)$ 'nin $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkasında devirli kod olacağı anlamına gelir. $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkasındaki devirli kodların yapısı Yıldız ve Aydın [20] tarafından incelendiğinden buradaki bazı sonuçlardan yararlanılarak $\Phi(C)$ devirli kodun üreteç yapısı aşağıdaki gibi belirlenebilir. $i = 1, 2$ için $g_i(x)$ ve $a_i(x)$ polinomları $a_i(x) \mid g_i(x) \mid x^n - 1 \mod 2$ şartını sağlayan $\mathbb{Z}_2$ üzerindeki polinomlar ve $g_i(x) + 2a_i(x)$ $\mathbb{Z}_4$ üzerinde devirli bir kodun üreteç polinomu olmak üzere

$$\Phi(C) = \langle g_1(x) + 2a_1(x) + ug(x), u(g_2(x) + 2a_2(x)) \rangle$$

şeklindedir. Eğer burada ki $g(x)$ polinomu $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerinde alınırsa herhangi bir $a + ub$ katsayısı için $u(a + ub) = ua$ olacağından $g(x)$ polinomunun $\mathbb{Z}_4$ halkası üzerinde alınması yeterli olacaktır.

Şimdi de Φ halka homomorfizmasının çekirdek kümesi belirlensin. $I=\{0,1,...,n-1\}$ indeks kümesi ve $c_i=p_i+uq_i+u^2r_i\in R$ olmak üzere $c\in C$ kod sözünün polinom karşılığı olan $c(x)=c_0+c_1x+...+c_{n-1}x^{n-1}\in R_n$ elemanı alınsın. Çekirdek tanımından dolayı,

$$\begin{aligned}\Phi(c_0+c_1x+\ldots+c_{n-1}x^{n-1}) &= \Psi(c_0)+\ldots+\Psi(c_{n-1})x^{n-1}\\ &= \Psi(p_0+uq_0+u^2r_0)+\ldots+\Psi(p_{n-1}+uq_{n-1}+u^2r_{n-1})x^{n-1}\\ &= (p_0+uq_0)+(p_1+uq_1)x+\ldots+(p_{n-1}+uq_{n-1})x^{n-1}\\ &= 0 \pmod{u^2}\end{aligned}$$

elde edilir. Bu da $\forall i\in I$ için $p_i+uq_i=0\ (\mathrm{mod}\,u^2)$ demektir. Yani $p_i+uq_i\in\langle u^2\rangle$ demektir. $\langle u^2\rangle$ idealindeki elemanlara dikkat edilirse $p_i+uq_i\in u^2\mathbb{Z}_4$ olarak düşünmek yanlış olmayacaktır. Dolayısıyla $c(x)$ polinomu $u^2\,{}^{\mathbb{Z}_4[x]}\!/_{\langle x^n-1\rangle}$ üzerinde bir polinomdur. Buradan Φ halka homomorfizmasının çekirdeği

$$\text{Çek}\Phi=\left\{u^2j(x):\ j(x)\in {}^{\mathbb{Z}_4[x]}\!/_{\langle x^n-1\rangle}\right\}$$

olarak belirlenebilir.

$J=\left\{j(x)\in {}^{\mathbb{Z}_4[x]}\!/_{\langle x^n-1\rangle}:u^2j(x)\in\text{Çek}\Phi\right\}$ kümesi ele alınsın. İddia edilsin ki J kümesi ${}^{\mathbb{Z}_4[x]}\!/_{\langle x^n-1\rangle}$ halkasının idealidir. Şimdi bu iddia ispatlanacaktır.

$\forall j_1(x),j_2(x)\in J$ için $u^2j_1(x),u^2j_2(x)\in\text{Çek}\Phi$ olup halkanın çekirdeği ideal olduğundan

$$u^2(j_1(x)-j_2(x))=u^2j_1(x-u^2j_2(x)\in\text{Çek}\Phi$$

dir. Buradan da $j_1(x)-j_2(x)\in J$ şartı sağlanacaktır. Diğer taraftan $\forall j(x)\in J$ için $u^2j(x)\in\text{Çek}\Phi$ dir. Yine ÇekΦ 'nin halkanın ideali olması gerçeğinden dolayı $\forall r(x)\in Z_4[x]/\langle x^n-1\rangle$ için

$$u^2j(x)r(x)\in\text{Çek}\Phi$$

dir Buradan da $j(x)r(x) \in J$ elde edilir. Sonuç olarak J kümesinin $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ halkasının ideali olduğu görülür.

$\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ halkasının idealleri $\mathbb{Z}_4$ üzerinde n uzunluğunda devirli kodlara karşılık geldiği hatırlatılarak bu aşamada aşağıdaki teoreme ihtiyaç duyulacaktır.

Teorem 2.3.4. C kodu n uzunluğunda $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ halkası üzerinde devirli bir kod olsun. Eğer n tek ise $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ temel ideal halkasıdır ve $g(x), a(x)$ polinomları $a(x) \mid g(x) \mid x^n - 1$ şartını sağlamak üzere

$$C = \langle g(x), 2a(x)\rangle = \langle g(x) + 2a(x)\rangle$$

dir [24].

J kümesi $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ halkasının bir ideali olduğundan devirli kod olarak düşünülebilir. Teorem 2.3.4'den yaralanarak $J = \langle g_3(x) + 2a_3(x)\rangle$ olarak yazılabilir. Yani J kümesinin her elemanı $g_3(x) + 2a_3(x)$ polinomunun bir katı olarak yazılacaktır. Buraya kadar elde edilen sonuçlar altında ÇekΦ'nin $u^2\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ üzerinde devirli kod olarak düşünmek yanlış olmayacaktır. Dolayısıyla Φ halka homomorfizmasının çekirdeği

$$\text{ÇekΦ} = u^2\langle g_3(x) + 2a_3(x)\rangle$$

ile belirlenebilir.

Buraya kadar elde edilen sonuçlar kullanılarak R üzerindeki n uzunluğundaki bir C devirli kodun üreteç yapısı aşağıdaki teorem ile birlikte ortaya konabilir.

Teorem 2.3.5. *C* kodu *R* üzerinde *n* uzunluğundaki bir devirli kod olsun. $i=1,2,3$ için $g_i(x)$ ve $a_i(x)$ polinomları $a_i(x)\,|\,g_i(x)\,|\,x^n-1 \mod 2$ şartını sağlayan $\mathbb{Z}_2$ üzerindeki polinomlar ve $g_i(x)+2a_i(x)$ polinomları da $\mathbb{Z}_4$ üzerinde devirli bir kodun üreteç polinomları olmak üzere *C* kodu

$$C=\langle g_1(x)+2a_1(x)+ug(x)+u^2h(x),u(g_2(x)+2a_2(x))+u^2b(x),u^2(g_3(x)+2a_3(x))\rangle$$

ile belirlenir.

Gösterimde kolaylık sağlaması $i=1,2,3$ için $f_i(x)=g_i(x)+2a_i(x)\in\mathbb{Z}_4[x]$ olarak tanımlansın. Bu durumda *C'*nin üreteci yeniden düzenlenirse

$$C=\langle f_1(x)+ug(x)+u^2h(x),uf_2(x)+u^2b(x),u^2f_3(x)\rangle$$

elde edilir. *C*'nin R_n halkasının bir ideali olduğu göz önünde bulundurulursa

$$u^2(f_1(x)+ug(x)+u^2h(x))=u^2f_1(x)\in C$$

$$u(uf_2(x)+u^2b(x))=u^2f_2(x)\in C$$

elde edilir. Dolayısıyla *C*'deki bu elemanların homomorfizma altındaki görüntüsü $\Phi(u^2f_1(x))=\Phi(u^2f_2(x))=0$ olacaktır. Bu da $u^2f_1(x),u^2f_2(x)\in \text{Çek}\Phi$ anlamına gelir. $\text{Çek}\Phi=u^2\langle f_3(x)\rangle$ olduğundan $f_3(x)\,|\,f_1(x)$ ve $f_3(x)\,|\,f_2(x)$ sonucuna ulaşılır. Benzer şekilde [20] çalışmasındaki homomorfizma kullanılarak $f_2(x)\,|\,f_1(x)$ elde edilebilir. Sonuç olarak $f_3(x)\,|\,f_2(x)\,|\,f_1(x)$ sağlanır.

Lemma 2.3.1. *R* üzerinde $\alpha(x)$ ve $\beta(x)$ iki polinom olsun.. Eğer $\beta(x)$ polinomu regüler polinom ise

$$\alpha(x)=\beta(x)s(x)+t(x)\ ;\ d^o t(x)<d^o\beta(x)$$

olacak şekilde $s(x)$ ve $t(x)$ polinomları vardır.

İspat. Eğer $\beta(x)$ polinomu regüler polinom ise $R[x]$ halkasında $f^*(x)$ monik polinomu ve $q(x)$ birimsel polinomu $\beta(x)=f^*(x)q(x)$ olacak şekilde vardır [5]. $f^*(x)$ monik polinom olduğundan bölme algoritması uygulanırsa

$$\alpha(x) = f^*(x)s(x) + t(x) \ ; \ d^o t(x) < d^o f^*(x)$$

elde edilir. Eşitliğin her iki tarafı $q(x)$ polinomu ile çarpılırsa

$$q(x)\alpha(x) = q(x)f^*(x)s(x) + q(x)t(x)$$

eşitliği sağlanır ki bu da $s(x) = (q(x))^{-1}s'(x)$ olmak üzere $\alpha(x) = \beta(x)s(x) + t(x)$ elde edilmesi anlamına gelir. $f^*(x)$ monik polinom olduğundan

$$d^o\beta(x) = d^o q(x) + d^o f^*(x) \geq d^o f^*(x)$$

eşitsizliği sağlanır. Ayrıca $d^o t(x) < d^o f^*(x)$ olduğu gerçeği de kullanılarak $t(x)$ ve $\beta(x)$ polinomlarının dereceleri arasında $d^o t(x) < d^o \beta(x)$ ilişkisinin olduğu görülür. Böylece istenen sağlanır

Teorem 2.3.6. C kodu R üzerinde n uzunluğundaki bir devirli kod olsun. Eğer $C = \langle f_1(x) + ug(x) + u^2h(x), uf_2(x) + u^2b(x), u^2 f_3(x)\rangle$ ve $f_3(x) = f_1(x)$ ise $C = \langle f_1(x) + ug(x) + u^2h(x)\rangle$ dir. Ayrıca $f_3(x)$ regüler polinom ise $f_1(x) + ug(x) + u^2h(x) \mid (x^n - 1)$ dir.

İspat. Kabul edilsin ki $f_3(x) = f_1(x)$ olsun. $f_3(x) \mid f_2(x) \mid f_1(x)$ koşulundan dolayı $f_3(x) = f_2(x) = f_1(x)$ dir. $\Phi(C) = \langle f_1(x) + ug(x), uf_2(x)\rangle$ kodu $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerinde devirli kod olduğundan ve $u(f_1(x) + ug(x)) = uf_1(x) = uf_2(x)$ eşitliği de göz önünde bulundurularak $\Phi(C) = \langle f_1(x) + ug(x)\rangle$ elde edilir. $f_3(x) = f_1(x)$ eşitliği kullanılarak

$u^2(f_1(x) + ug(x) + u^2h(x)) = u^2 f_1(x) = u^2 f_3(x) \in \langle f_1(x) + ug(x) + u^2h(x)\rangle$

elde edilir. Dolayısıyla $C = \langle f_1(x) + ug(x) + u^2h(x)\rangle$ dir.

Şimdi de $f_3(x) = f_1(x)$ regüler polinom olduğu kabul edilsin. $f_1(x) + ug(x) + u^2h(x) \mid (x^n - 1)$ olduğunun gösterilmesinde bölme algoritmasından yararlanılacaktır. Bölme algoritmasının kullanılabilmesi için de sıfırdan farklı $f_1(x) + ug(x) + u^2h(x)$ polinomunun öncelikle regüler olduğu ispatlanmalıdır.

Aşağıda yapılacak olan işlemlerde yazım kolaylığı olması açısından herhangi bir $a(x)$ polinomu a olarak gösterilecektir.

Herhangi bir $a+ub+u^2c \in R[x]$ polinomu için

$$(f_1+ug+u^2h)(a+ub+u^2c)=0$$

olsun. Yani

$$af_1+u(bf_1+ag)+u^2(cf_1+bg+ah)=0$$

elde edilir. Buradan

$$af_1=0$$
$$bf_1+ag=0$$
$$cf_1+bg+ah=0$$

sonuçlarına varılır. Birinci eşitlikte f_1 polinomu regüler polinom olduğundan $a=0$ olmak zorundadır. O halde ikinci eşitlik yeniden düzenlenirse $bf_1=0$ olur ve yine f_1 polinomu regüler polinom olduğundan $b=0$ olmak zorundadır. Aynı sebeplerden dolayı üçüncü eşitlikten de $c=0$ elde edilir. Dolayısıyla $a+ub+u^2c=0$ elde edilir. Yani $f_1(x)+ug(x)+u^2h(x)$ polinomu regülerdir. O halde Lemma 2.3.1'den dolayı

$$x^n-1=(f_1(x)+ug(x)+u^2h(x))s(x)+t(x)$$

yazılabilir ve $t(x)=0$ veya $d^o t(x)<d^o(f_1(x)+ug(x)+u^2h(x))$ dir. Yukarıdaki eşitlikte $t(x)$ polinomu yalnız bırakılırsa

$$t(x)=(x^n-1)-(f_1(x)+ug(x)+u^2h(x))s(x)=-s(x)(f_1(x)+ug(x)+u^2h(x))\in C$$

elde edilir. Buda $f_1(x)+ug(x)+u^2h(x)$ polinomunun C'nin üreteç polinomu olduğundan en küçük dereceli olması gerçeği ile çelişecektir. Bu sebepten dolayı $t(x)=0$ olmak zorundadır. Buda $f_1(x)+ug(x)+u^2h(x)\,|\,(x^n-1)$ olduğunu ispatlar.

Şimdi R üzerindeki devirli bir kodun en küçük geren kümesi ve eleman sayısı belirlensin. Bunun için ilk olarak aşağıdaki tanıma ihtiyaç olacaktır.

Tanım 2.3.1. *R* halkası tek bir *M* maksimal ideale sahip bir lokal Frobenius halka olsun ve R^n de $r_1,\ldots,r_k$ elemanları alınsın. Bu durumda $r_1,\ldots,r_k$ elemanları modüler bağımsız olması için gerek ve yeter şart her $i=1,\ldots,k$ için $c_i \in M$ olacak şekilde $\sum c_i r_i = 0$ şartının sağlanmasıdır [25] .

Teorem 2.3.7. *n* pozitif tek tamsayı ve *C* kodu *R* üzerinde *n* uzunluğundaki bir devirli kod olsun.

1. $R[x]$ üzerindeki $f_1(x)$ polinomu regüler polinom ve $f(x)=f_1(x)+ug(x)+u^2h(x)$ polinomunun derecesi $d^o f(x)=s$ olmak üzere $C=\langle f(x)\rangle$ ise *C* kodu $n-s$ rankına ve

$$B=\{f(x),xf(x),\ldots,x^{n-s-1}f(x)\}$$

bazına sahip bir serbest koddur.

2. $C=< f_1(x)+ug(x)+u^2h(x),\ uf_2(x)+u^2b(x),\ u^2f_3(x) >$ R üzerinde n uzunluğunda devirli bir kod olsun. $f_1(x)$, $f_2(x)$ ve $f_3(x)$ polinomları $d^o f_1(x)=s_1$, $d^o f_2(x)=s_2$, $d^o f_3(x)=s_3$ derecelerine sahip monik polinomlar olsun. Bu durumda *C* kodu $n-s_3$ rankına sahiptir ve *C*'yi geren en küçük küme;

$$T=\left\{\begin{array}{c} f_1(x)+ug(x)+u^2h(x),x(f_1(x)+ug(x)+u^2h(x)),\ldots,x^{n-s_1-1}(f_1(x)+ug(x)+u^2h(x)),\\ uf_2(x)+u^2b(x),x(uf_2(x)+u^2b(x)),\ldots,x^{s_1-s_2-1}(uf_2(x)+u^2b(x)),\\ u^2f_3(x),x(u^2f_3(x)),\ldots,x^{s_2-s_3-1}(u^2f_3(x)) \end{array}\right\}$$

dir.

İspat.

1. $R[x]$ üzerindeki $f_1(x)$ polinomu regüler polinom ve $f(x)=f_1(x)+ug(x)+u^2h(x)$ polinomunun derecesi $d^o f(x)=s$ olmak üzere $C=\langle f(x)\rangle$ olsun. Teorem 2.3.6'dan dolayı $f(x)\,|\,x^n-1$ olduğu söylenebilir. O halde $x^n-1=f(x)h(x)$ olacak şekilde $d^o h(x)=n-s$ olan bir $h(x)\in R[x]$ polinomu vardır. $c(x)$,*C* kodunun bir elemanı olsun. $C=\langle f(x)\rangle$ olduğundan $c(x)=f(x)k(x)$ olacak şekilde bir $k(x)$ polinomu vardır. Eğer $k(x)$ polinomunun derecesi $n-s-1$ ise istenen sağlanacağından ispat

biter. Aksi halde $k(x)$ polinomunun derecesi $n-s-1$ den büyük ise $h(x)$ polinomu ile bölme algoritması uygulanır ve

$$k(x)=h(x)s(x)+t(x)\ ;\ d^o t(x)\le n-s-1$$

elde edilir.

O halde

$$\begin{aligned} c(x)=f(x)k(x) &= f(x)(h(x)s(x)+t(x)) \\ &= f(x)h(x)s(x)+f(x)t(x) \\ &= f(x)t(x) \end{aligned}$$

sağlanır. Sonuç olarak B kümesi C'nin geren kümesidir. Dikkat edilmelidir ki yukarıdaki işlemler $R[x]\Big/\langle x^n-1\rangle$ halkasında gerçekleştiğinden $f(x)h(x)=x^n-1\equiv 0(\bmod x^n-1)$ dir.

Şimdi de B geren kümesinin baz olduğunu ispatlayabilmek için lineer bağımsız olduğu gösterilmelidir. $a(x)=a_0+a_1x+\cdots+a_{n-s-1}x^{n-s-1}$ polinomu $R[x]$ üzerinde $a(x)f(x)=0$ şartını sağlayan bir polinom olsun. $f(x)$ regüler polinom olduğundan $R[x]$ üzerinde $q(x)$ birimsel polinomu ve f^*_{n-s-1} terslenebilen eleman olmak üzere $f^*(x)=f^*_0+f^*_1x+\cdots+f^*_{n-s-1}x^{n-s-1}$ monik polinomu $f(x)=f^*(x)q(x)$ olacak şekilde vardır. Gösterilmesi gerekilen $a(x)f^*(x)q(x)=0$ eşitliğinin yalnızca $a(x)=0$ olması ile sağlandığıdır. $a(x)$ polinomu açılarak yazılırsa

$$a_0f^*(x)q(x)+a_1f^*(x)q(x)x+\cdots+a_{n-s-1}f^*(x)q(x)x^{n-s-1}=0$$

eşitliği elde edilir. Katsayı karşılaştırması yapıldığında bu eşitliğin sağlanması ancak ve ancak her $i=1,2,\ldots,n-s-1$ için $a_if^*(x)q(x)=0$ olmasıdır. $q(x)$ polinomu birimsel olduğundan $a_if^*(x)=0$ elde edilir. Şimdi de $f^*(x)$ polinomu açılarak yerine yazılırsa her $i=1,2,\ldots,n-s-1.$ için

$$a_if^*_0+a_if^*_1x+\cdots+a_if^*_{n-s-1}x^{n-s-1}=0$$

elde edilir. En büyük dereceli x'in katsayısı karşılaştırılırsa $a_if^*_{n-s-1}=0$ elde edilir ve f^*_{n-s-1} terslenebilen eleman olduğundan her $i=1,2,\ldots,n-s-1$ için $a_i=0$ elde edilir. Dolayısı ile $a(x)=0$ koşulu sağlanır. Sonuç olarak B kümesi C'nin bir bazıdır.

2. $C =< f_1(x)+ug(x)+u^2h(x),\ uf_2(x)+u^2b(x),\ u^2f_3(x) >$ kodu R üzerinde n uzunluğunda devirli bir kod olsun. $f_1(x)$, $f_2(x)$ ve $f_3(x)$ polinomları $d^o f_1(x) = s_1$, $d^o f_2(x) = s_2$, $d^o f_3(x) = s_3$ derecelerine sahip monik polinomlar olsun. $f_3(x) \mid f_2(x) \mid f_1(x)$ ve $f_i(x)$ polinomları monik olduğundan $s_1 > s_2 > s_3$ bağıntısı elde edilebilir. *T* kümesinin *C*'nin en küçük geren kümesi olduğu gösterilecektir. Bunun için gösterilmesi gereken *T* kümesinin

$$X = \left\{ \begin{array}{c} f_1(x)+ug(x)+u^2h(x), x(f_1(x)+ug(x)+u^2h(x)),\ldots, x^{n-s_1-1}(f_1(x)+ug(x)+u^2h(x)), \\ uf_2(x)+u^2b(x), x(uf_2(x)+u^2b(x)),\ldots, x^{n-s_2-1}(uf_2(x))+u^2b(x)), \\ u^2f_3(x), x(u^2f_3(x)),\ldots, x^{n-s_3-1}(u^2f_3(x)) \end{array} \right\}$$

kümesini gerdiği ve *T*'nin modüler bağımsız olduğudur. İlk olarak $x^{s_2-s_3}(u^2f_3(x)) \in Sp(T)$ olduğu gösterilecektir. Kabul edilsin ki $x^{s_2-s_3}f_3(x)$ polinomunun baş katsayısı a_0 ve $f_2(x)+ub(x)$ polinomunun baş katsayısı da b_0 olsun. Bu durumda $a_0 = c_0b_0$ olacak şekilde $c_0 \in \mathbb{Z}_4$ elemanı vardır. $f_2(x)$ monik polinom olduğundan $f_2(x)+ub(x)$ polinomu regüler polinomdur. O halde bölme algoritması uygulanırsa

$$u^2x^{s_2-s_3}f_3(x) = u^2c_0(f_2(x)+ub(x))+u^2t(x)$$

yazılabilir. Burada ki $u^2t(x) = u^2f_3(x)\alpha(x)$ polinomu *C* de derecesi s_2 'den küçük olan bir polinomdur. *C* içerisindeki herhangi bir polinomun derecesi $d^o f_3(x) = s_3$ den büyük ya da eşit olacağından $s_3 \le d^o t(x) < s_2$ elde edilir. O halde

$$u^2t(x) = \alpha_0(u^2f_3(x))+\alpha_1x(u^2f_3(x))+\cdots+\alpha_{s_2-s_3-1}x^{s_2-s_3-1}(u^2f_3(x))$$

yazılabilir. Sonuç olarak $x^{s_2-s_3}(u^2f_3(x)) \in Sp(T)$ dir. Benzer şekilde $x^{s_2-s_3+1}(u^2f_3(x))$, $x^{s_2-s_3+2}(u^2f_3(x)),\ldots,\ x^{n-s_3-1}(u^2f_3(x)) \in Sp(T)$ olduğu gösterilebilir.

Şimdi de $x^{s_1-s_2}(uf_2(x)+u^2b(x)) \in Sp(T)$ olduğu gösterilmelidir. Kabul edilsin ki $x^{s_1-s_2}(f_2(x)+ub(x))$ polinomunun baş katsayısı a_1 ve $f_1(x)+ug(x)+u^2h(x)$ polinomunun baş katsayısı da b_1 olsun. Bu durumda $a_1 = c_1b_1$ olacak şekilde $c_1 \in \mathbb{Z}_4$

elemanı vardır. $f_1(x)+ug(x)+u^2h(x)$ polinomu regüler polinom olduğundan Lemma 2.3.1'den dolayı

$$x^{s_1-s_2}(uf_2(x)+u^2b(x)=c_1u(f_1(x)+ug(x)+u^2h(x))+ur(x)$$

elde edilir ve $d^o ur(x)<s_1$ dir. $ur(x)\in C$ olduğundan dolayı

$$ur(x)=A(x)(uf_2(x)+u^2b(x))+B(x)(u^2f_3(x))$$

olarak ifade edilebilir. Burada $d^oB(x)=s_2-s_3-1$ ve $d^oA(x)=k$ dir. $d^our(x)<s_1$ olduğundan k sayısı s_1-s_2'den küçük olmak zorundadır. Bu da $x^{s_1-s_2}(uf_2(x)+u^2b(x))\in Sp(T)$ olmasını gerektirir. Aynı yöntem ile $x^{s_1-s_2+1}(uf_2(x)+u^2b(x)),\ldots,x^{n-s_2-1}(uf_2(x)+u^2b(x))\in Sp(T)$ olduğu da gösterilebilir.

Şimdi T'nin modüler bağımsız olduğu gösterilsin.

$f_1(x)+ug(x)+u^2h(x)=g_0+g_1x+\cdots+g_{s_1}x^{s_1}$, $f_2(x)+ub(x)=b_0+b_1x+\cdots+b_{s_2}x^{s_2}$ ve $f_3(x)=f_0+f_1x+\cdots+f_{s_3}x^{s_3}$ monik polinomlar olsun. Yani g_{s_1}, b_{s_2}, ve f_{s_3} terslenebilen elemanlar olsun. Kabul edilsin ki $k(x)=\sum_{i=0}^{n-s_1-1}k_ix^i\in R[x]$, $l(x)=\sum_{i=0}^{s_1-s_2-1}l_ix^i\in R[x]$ ve $m(x)=\sum_{i=0}^{s_2-s_3-1}m_ix^i\in\mathbb{Z}_4[x]$ polinomları

$$k(x)(f_1(x)+ug(x)+u^2h(x))+l(x)(uf_2(x)+u^2b(x))+m(x)(u^2f_3(x))=0$$

olacak şekilde var olsun. Yukarıdaki eşitliğin her iki tarafındaki x^{n-1}'in katsayıları karşılaştırılırsa $k_{n-s_1-1}g_{s_1}=0$ olduğu görülür. g_{s_1} elemanı terslenebilir olduğundan $k_{n-s_1-1}=0$ elde edilir. Eğer x^{n-2}'nin katsayıları karşılaştırılırsa $k_{n-s_1-2}g_{s_1}+k_{n-s_1-1}g_{s_1-1}=0$ olduğu görülür. g_{s_1} elemanı terslenebilir ve $k_{n-s_1-1}=0$ olduğundan $k_{n-s_1-2}=0$ elde edilir. Bu şekilde devam edilirse her $i=0,1,...,n-s_1-1$ için $k_i=0$ elde edilir. Ayrıca u sıfır bölen olduğundan her $i=0,1,\ldots,s_1-s_2-1$ için herhangi bir l_i elemanını içeren x'in katsayılarının *0* olması için gerek koşul $l_i\in<2,u>$ olmasıdır. Aynı sebepten dolayı $j=0,1,\ldots,s_2-s_3-1$ için de $l_i\in<2,u>$ dır. Tanım 2.3.1'den dolayı T'nin modüler bağımsız olduğu görülür.

Bu bölüm R üzerindeki n uzunluğundaki devirli kodların minimum Hamming ağırlıkları hakkındaki bir teorem ile bitirilsin.

Teorem 2.3.8. $C = \langle f_1(x) + ug(x) + u^2h(x), uf_2(x) + u^2b(x), u^2 f_3(x)\rangle$ kodu n uzunluğunda R üzerinde devirli kod olsun. Bu durumda w_H Hamming ağırlığı göstermek üzere $w_H(C) = w_H(\text{ÇekΦ})$ dir.

İspat. Kabul edilsin ki $r_0(x), r_1(x), r_2(x) \in \mathbb{Z}_4[x]$ olmak üzere $r(x) = r_0(x) + u\, r_1(x) + u^2\, r_2(x) \in C$ olsun. $u^2 r(x) = u^2 r_0(x) \in C$ olduğundan $w_H(u^2 r(x)) \le w_H(r(x))$ dir. Yani $w_H(u^2 C) \le w_H(C)$ dir. Diğer taraftan u^2C kodu C'nin bir alt kodu olduğundan $w_H(C) \le w_H(u^2C)$ elde edilir. Bu yüzden $w_H(C) = w_H(u^2C)$ dir.

2.4. $\mathbb{Z}_4[u]/\langle u^3\rangle$ Halkası Üzerindeki Devirli Kodların $\mathbb{Z}_4$ Görüntüleri

$\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ halkasından $\mathbb{Z}_4^3$ halkasına

$$\begin{aligned} \varphi:\ \mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4 &\to \mathbb{Z}_4^3 \\ a + ub + u^2c &\to (a, a+b+c, b) \end{aligned}$$

şeklinde bir Gray dönüşüm tanımlansın. Bu dönüşüm R^n cebirsel yapısından $\mathbb{Z}_4^{3n}$ cebirsel yapısına

$\varphi(a_0 + ub_0 + u^2c_0, \cdots, a_{n-1} + ub_{n-1} + u^2c_{n-1}) = (a_0, a_0 + b_0 + c_0, b_0, \cdots, a_{n-1}, a_{n-1} + b_{n-1} + c_{n-1}, b_{n-1})$

şeklinde genişletilebilir.

Teorem 2.4.1. φ Gray dönüşümü $\mathbb{Z}_4$-lineer dönüşümdür.

İspat. $\forall a + ub + u^2c, x + uy + u^2z \in R$ ve $\alpha, \beta \in \mathbb{Z}_4$ için

$$\begin{aligned}\varphi(\alpha(a+ub+u^2c)+\beta(x+uy+u^2z)) &= \varphi((\alpha a+\beta x)+(\alpha b+\beta y)u+(\alpha c+\beta z)u^2)\\ &= (\alpha a+\beta x, \alpha(a+b+c)+\beta(x+y+z), \alpha b+\beta y)\\ &= \alpha(a, a+b+c, b)+\beta(x, x+y+z, z)\\ &= \alpha\varphi(a+ub+u^2c)+\beta\varphi(x+uy+u^2z)\end{aligned}$$

olduğundan $\mathbb{Z}_4$-lineerdir.

Teorem 2.4.1'den ve Gray dönüşümün tanımından dolayı $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ üzerinde *n* uzunluğunda lineer bir kodun görüntüsünün $\mathbb{Z}_4$ üzerinde *3n* uzunluğunda lineer koda denk geleceği görülür.

Şimdi aşağıda verilecek olan teorem ile $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ üzerindeki *n* uzunluğundaki bir devirli kodun φ altındaki $\mathbb{Z}_4$-görüntüsünün 3*n* uzunluğunda 3-yarı devirli kod olduğu ortaya konabilir.

Teorem 2.4.2. φ Gray dönüşüm ve τ devirsel öteleme operatörü olmak üzere $\varphi\tau=\tau^3\varphi$ dir.

İspat. φ Gray dönüşüm ve τ devirselsel öteleme operatörü olsun. $v_i=a_i+ub_i+u^2c_i$ olmak üzere $\vec{v}=(v_1,v_2,\ldots,v_n)\in R^n$ olsun. Bu durumda

$$\tau(\vec{v})=(v_n,v_1,\ldots,v_{n-1})$$

ve

$$\varphi(\tau(\vec{v}))=(a_n,a_n+b_n+c_n,b_n,a_1,a_1+b_1+c_1,b_1,\ldots,a_{n-1},a_{n-1}+b_{n-1}+c_{n-1},b_{n-1}) \quad \ldots\ldots(1)$$

elde edilir. Diğer taraftan

$$\varphi(\vec{v})=(a_1,a_1+b_1+c_1,b_1,\ldots,a_n,a_n+b_n+c_n,b_n)$$

ve

$$\tau^3(\varphi(\vec{v}))=(a_n,a_n+b_n+c_n,b_n,a_1,a_1+b_n+c_1,b_1,\ldots,a_{n-1},a_{n-1}+b_{n-1}+c_{n-1},b_{n-1}) \quad \ldots\ldots(2)$$

dir. (1) ve (2)'den dolayı $\varphi\tau=\tau^3\varphi$ dir.

Teorem 2.4.3. *C* kodu *R* üzerinde *n* uzunluğunda bir devirli kod olsun. Bu durumda $\varphi(C)$ de $\mathbb{Z}_4$ üzerinde 3*n* uzunluğunda 3-yarı devirli koddur.

İspat. *C* kodu *R* üzerinde *n* uzunluğunda bir devirli kod ise $\tau(C)=C$ dir. Teorem 2.4.2'den dolayı $\tau^3(\varphi(C))=\varphi(\tau(C))=\varphi(C)$ elde edilir. Yani $\varphi(C)$ kodu $\mathbb{Z}_4$ üzerinde 3*n* uzunluğunda 3-yarı devirli koddur.

2.5. Hesaplama Sonuçları

Şimdiye kadar elde edilen sonuçlardan yararlanarak $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ üzerindeki devirli kodlar için bilgisayar çalışması yapılmıştır. Teorem 2.3.6 'da verilen özel duruma göre $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ halkası üzerinde n tek uzunluktaki devirli kodlar göz önünde bulundurulmuştur. Yani *f* polinomu $\mathbb{Z}_4$ üzerinde *n* uzunluğunda devirli kodun üreteç polinomu ve *g,h* polinomları da $\mathbb{Z}_4$ üzerinde herhangi iki polinom olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ üzerindeki üreteç polinomlar $\langle f(x)+ug(x)+u^2h(x)\rangle$ formunda olacaktır. Ayrıca $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ üzerindeki devirli kodların yukarıda tanımlanan dönüşüm altındaki $\mathbb{Z}_4$-görüntüleri de incelenmiştir. Yapılan araştırmada $\mathbb{Z}_4$ üzerinde yeni lineer kodlar bulunmuştur. Aşağıdaki tablolar *n = 7* uzunluğundaki bazı kodların parametresini göstermektedir. Bu sebeple kodların $\mathbb{Z}_4$- görüntülerinin uzunluğu 21 dir. Her bir üreteç $\mathbb{Z}_4$ üzerindeki 3 polinom tarafından belirlidir. Yazım kolaylığı olması açısından *x* in en büyük derecesinden başlayarak azalan bir şekilde sadece katsayılar yazılmıştır. Yani $2x^4+3x+1$ polinomu 20031 olarak gösterilmiştir. Ayrıca arka arkaya *n* defa tekrar eden bir *d* katsayısı varsa buda d^n şeklinde kısaltılmıştır. Yani $3x^3+3x^2+3x+3$ polinomu 3^4 olarak yazılmıştır. Aşağıdaki tablolarda $\mathbb{Z}_4$ üzerindeki kodlar için önemli olan Lee ve Öklit ağırlıkları $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ üzerindeki devirli kodların $\mathbb{Z}_4$- görüntüleri için bakılmıştır. $x\in\mathbb{Z}_4$ olmak üzere *x* elemanının Lee ağırlığı $w_L(x)=\min\{|x|,|4-x|\}$ olarak tanımlanmıştır. Bu yüzden 0,1,2,3 elemanlarının Lee ağırlıkları sırası ile 0,1,2,1 dir. *x* elemanının Öklit ağırlığı

ise $w_E(x) = \min\{x^2, (4-x)^2\}$ olarak tanımlanmıştır. $\mathbb{Z}_4^n$'deki bir vektörün Lee ağırlığı bileşenlerinin Lee ağırlıklarının toplamına eşittir. $\mathbb{Z}_4^n$'deki bir vektörün Öklit ağırlığıda benzer şekilde tanımlanır. İlk tabloda kodlar Lee ağırlıklarına göre ikinci tabloda ise Öklit ağırlıklarına göre ayrılmıştır. $\mathbb{Z}_4$ üzerindeki lineer kodlar [26] makalesinde ve online olarak da $\mathbb{Z}_4$ Codes.info adresinde listelenmiştir. Bu çalışmada elde edilen yeni lineer kodlarda bu listeye eklenmiştir.

Tablo 2.1. 7 uzunluğundaki bazı devirli kodların $\mathbb{Z}_4$ - görüntüleri ve Lee ağırlıkları

$f(x)$	$g(x)$	$h(x)$	$\mathbb{Z}_4$**-görüntülerinin parametreleri**
1113313	2000222	110300	$[21, 4^2 2^{15}, 4]$
22	3131333	221212	$[21, 4^2 2^{18}, 2]$
22202	1130120	2120111	$[21, 4^3 2^{12}, 4]$
2	1302030	3220121	$[21, 4^4 2^{14}, 4]$
$1^6 3$	3223011	2202002	$[21, 4^5 2^{15}, 4]$
11323	202	2031110	$[21, 4^6 2^{14}, 4]$
$1^6 3$	230110	3212323	$[21, 4^6 2^{15}, 2]$
1113133	3210231	101213	$[21, 4^8 2^6, 4]$
$1^6 3$	3011032	21322	$[21, 4^8 2^{13}, 2]$
11303	3132322	3122031	$[21, 4^9 2^9, 4]$
3231	22020	3313312	$[21, 4^{11} 2^1, 6]$
1211	1021310	1223110	$[21, 4^{11} 2^9, 4]$
1321	2133	301302	$[21, 4^{12} 2^6, 4]$
10113	110023	1033223	$[21, 4^{13} 2^2, 4]$
3121	3122301	1101123	$[21, 4^{14} 2^0, 4]$
31	1320101	3212112	$[21, 4^{15} 2^3, 4]$
11	2120113	3200330	$[21, 4^{15} 2^6, 2]$
31	3211101	1330033	$[21, 4^{16} 2^0, 4]$

Tablo 2.2. 7 uzunluğundaki bazı devirli kodların $\mathbb{Z}_4$ - görüntüleri ve Öklit ağırlıkları

$f(x)$	$g(x)$	$h(x)$	$\mathbb{Z}_4$ **-görüntülerinin parametreleri**
1113313	2000222	110300	$[21, 4^2 2^{15}, 8]$
2	3313313	313312	$[21, 4^1 2^{20}, 4]$
20222	2002	233202	$[21, 4^3 2^9, 8]$
$1^6 3$	3113111	3113132	$[21, 4^3 2^{18}, 4]$
2	23213	2303332	$[21, 4^4 2^{17}, 3]$
$1^6 3$	1123003	2101301	$[21, 4^5 2^{16}, 4]$
11323	2200202	2223112	$[21, 4^6 2^{12}, 7]$
11323	220	2031110	$[21, 4^6 2^{14}, 6]$
11323	$1^6 3$	1122132	$[21, 4^7 2^{14}, 4]$
12333	1313113	1123320	$[21, 4^8 2^{12}, 4]$
3^7	120213	3011120	$[21, 4^9 2^6, 3]$
12313	233301	202121	$[21, 4^9 2^8, 6]$
1211	3311113	3232310	$[21, 4^9 2^{12}, 4]$
11303	101332	2001210	$[21, 4^{10} 2^9, 4]$
11323	2312102	3212330	$[21, 4^{10} 2^{11}, 3]$
3231	22020	3313312	$[21, 4^{11} 2^1, 6]$
1211	1303201	3020223	$[21, 4^{11} 2^{10}, 4]$
11	200	23002	$[21, 4^{12} 2^9, 4]$
10113	110023	1033223	$[21, 4^{13} 2^2, 4]$
10113	2210110	2031121	$[21, 4^{13} 2^5, 3]$
3231	102133	3133202	$[21, 4^{14} 2^1, 4]$
1211	3322310	3332300	$[21, 4^{14} 2^7, 2]$
31	3103003	203120	$[21, 4^{15} 2^5, 4]$
11	3100121	203120	$[21, 4^{15} 2^6, 3]$
31	3312122	321201	$[21, 4^{16} 2^3, 3]$

BÖLÜM 3. $\mathbb{F}_q + v\mathbb{F}_q$ ÜZERİNDE SKEW YARI DEVİRLİ KODLAR

Literatürde devirli kodlar üzerinde yapılmış birçok çalışma görmek mümkündür. Fakat bu çalışmaların çoğu değişmeli halkalar üzerindedir. Son zamanlarda yapılan çalışmalar da devirli ve yarı devirli kodlar, değişmeli olmayan halkalar üzerinde skew devirli ve skew yarı devirli olarak incelenmiştir.

Değişmeli olmayan halkalar üzerindeki devirli kodların yapısı ilk olarak 2007 yılında Boucher ve arkadaşları tarafından incelendi. Bu çalışmada $\mathbb{F}_q$ sonlu bir cisim ve θ, $\mathbb{F}_q$ üzerinde bir otomorfizma olmak üzere $\mathbb{F}_q[x,\theta]$ ile gösterilen skew polinom halkası üzerindeki devirli kodları çalışmışlardır. Skew polinom halkası üzerinde kod çalışmanın en önemli sebeplerinden biri bu halka üzerindeki polinomların birden fazla çarpanlara ayrılmasıdır. Bu sebepten dolayı skew polinom halkaları ideal sayısı bakımından değişmeli olan halkalardan daha fazla avantaj sağlamaktadır. Bu yüzden skew polinom halkası üzerindeki çalışmalara bakıldığında literatürde en iyi bilinen lineer kodlardan daha iyi Hamming uzaklığa sahip yeni kodlar görmek mümkündür [27, 28]. Abualrub ve ark. [27] sonlu cisim üzerinde skew yarı devirli kodları çalışmıştır. Bhaintwal [29] Galois halkası üzerinde skew yarı devirli kodları çalışmıştır. Ayrıca bu çalışmada Galois halkası üzerindeki skew devirli kodların serbest olması için bir şart verilmiştir. Boucher ve ark. [30] sonlu cisim üzerindeki θ devirli kodların dualleri hakkında bazı sonuçlar ortaya koymuştur. Tüm bu çalışmalar da skew devirli kodlar kodun uzunluğunun otomorfizmanın mertebesini böldüğü koşulu altında incelenmiştir. Şiap ve ark. [31] hiçbir koşul olmadan herhangi bir uzunluktaki kod için sonlu cisim üzerinde skew devirli kodların yapısını incelemişlerdir. Abualrub ve ark. [32] $\mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerindeki skew devirli kodları çalışmışlardır ve bu halka üzerinde tanımlanan skew devirli kodların üreteç

polinomlarını vermişlerdir. $\mathbb{F}_3+v\mathbb{F}_3$ ve $\mathbb{F}_p+v\mathbb{F}_p$ üzerindeki skew devirli kodlar sırasıyla [33] ve [34] makalelerinde incelenmiştir.

Bu bölümde ilk olarak kullanılacak olan temel tanımlar ve teoremler ele alınmıştır. Daha sonra $\mathbb{F}_q+v\mathbb{F}_q$ üzerindeki skew yarı devirli kodların cebirsel yapısı incelenmiştir. Bir üreteçli serbest skew yarı devirli kodlar için bir baz verimiş ve bu kodların minimum uzaklığı için sınır verilmiştir. Skew yarı devirli kodların dualleri tartışılmıştır ve farklı bir bakış açısı ile *R* üzerindeki skew devirli kodların dualini içermesi için gerek ve yeter şart verilmiştir. Bundan yararlanarak skew devirli kodlardan quantum kod inşa edilmiştir. MAGMA cebirsel programlama sistemi [35] kullanılarak bazı quantum kod parametreleri listelenmiştir.

3.1. Temel Tanımlar ve Teoremler

$\mathbb{F}_q$, q elemanlı sonlu cisim ve *m* pozitif tam sayı olmak üzere $q=p^m$ olsun. Bu bölüm boyunca "*R*" harfi $\mathbb{F}_q+v\mathbb{F}_q=\{a+vb \mid v^2=v \text{ ve } a,b\in\mathbb{F}_q\}$ halkasını temsil edecektir. *R* halkası $<v>$ ve $<1-v>$ olmak üzere iki maksimal ideale sahiptir. *R* üzerindeki halka otomorfizması

$$\begin{aligned}\sigma_s:\ \mathbb{F}_q+v\mathbb{F}_q &\rightarrow \mathbb{F}_q+v\mathbb{F}_q\\ x+vy &\rightarrow x^{p^s}+vy^{p^s}\end{aligned}$$

şeklinde tanımlansın. $s=1$ için σ_1 otomorfizması Frobenius otomorfizması olarak adlandırılır. σ_1 ve σ_s otomorfizmalarının tanımından dolayı $\sigma_s=\sigma_1^s$ olduğu görülür. *R* üzerindeki polinomlar kümesi

$$R[x,\sigma_s]=\{f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1} \mid a_i\in R \text{ ve } i=0,1,\ldots n-1\}$$

ile temsil edilsin. Bu küme polinomlarda bilinen toplama işlemi ve $\alpha,\beta\in R$ olmak üzere $(\alpha x^i)(\beta x^j)=\alpha\cdot\sigma_s^i(\beta)x^{i+j}$ ile tanımlanan çarpma işlemi altında bir halkadır. Bu $R[x,\sigma_s]$ halkasına skew polinom halkası denir. Bu halka değişmeli olmayan bir halkadır.

Tanım 3.1.1. R^n 'nin bir alt kümesi C olsun. Eğer C kümesi aşağıdaki şartları sağlıyor C'ye n uzunluğunda skew devirli kod denir.

i. C kümesi R^n 'nin bir R-alt modülüdür.

ii. τ skew devir öteleme operatörü olmak üzere $c=(c_0,c_1,\ldots,c_{n-1})\in C$ iken $\tau(c)=(\sigma_s(c_{n-1}),\sigma_s(c_0),\ldots,\sigma_s(c_{n-2}))\in C$ dir [36].

Tanım 3.1.2. $f(x),g(x)\in R[x,\sigma_s]$ polinomları için $f(x)=p(x)g(x)$ olacak şekilde bir $p(x)\in R[x,\sigma_s]$ polinomu varsa $g(x)$ polinomu $f(x)$ in bir sağ böleni olarak tanımlanır. Sol bölen tanımı da benzer şekilde yapılabilir.

Tanım 3.1.3. $p(x),q(x)\in R[x,\sigma_s]$ iki polinom olsun. Eğer bir $r(x)$ polinomu için

i. $r(x)$ polinomu $p(x)$ ve $q(x)$ polinomlarının bir sağ böleni ve.

ii. Eğer $s(x)$ polinomu $p(x)$ ve $q(x)$ polinomlarının başka bir sağ böleni ise $s(x)$ polinomu $r(x)$ polinomunun da bir sağ böleni

oluyor ise $r(x)$ polinomuna $p(x)$ ve $q(x)$ polinomlarının en büyük sağ ortak böleni denir ve $ebob_{sağ}(p(x),q(x))=r(x)$ ile gösterilir. En büyük ortak sol bölen de aynı şekilde tanımlanabilir ve $ebob_{sol}(p(x),q(x))=r(x)$ ile gösterilir.

Skew devirli kodlar skew yarı devirli kodların araştırmasında önemli bir rol oynadığı için $\mathbb{F}_q+v\mathbb{F}_q$ üzerindeki skew devirli kodların yapısına ihtiyacımız olacaktır. Gürsoy ve ark [36]'da Teorem 1.1.14 kullanarak $\mathbb{F}_q+v\mathbb{F}_q$ üzerindeki skew devirli kodların yapısını incelemiştir ve $\mathbb{F}_q+v\mathbb{F}_q$ üzerindeki skew devirli kodların tek bir eleman tarafından üretildiğini aşağıdaki teorem ile ortaya koymuşlardır.

Teorem 3.1.1. $C=(1-v)C_1+vC_2$ kodu R halkası üzerinde n uzunluğunda bir skew devirli kod olsun. $\mathbb{F}_q$ üzerindeki $u_1(x)$ ve $u_2(x)$ polinomları sırası ile C_1 ve C_2 skew devirli kodların üreteç polinomları olmak üzere $C=\langle u(x)\rangle=\langle(1-v)u_1(x)+vu_2(x)\rangle$ şeklinde üretilir. Ayrıca $u(x)$ polinomu tek ve x^n-1'in bir sağ bölenidir.

Dikkat edilmelidir ki $u(x)$ üreteç polinomunun monik olması gerekmiyor. Bu koşul kodun serbest olup olmayacağını belirleyecektir. Bunu ispatlamadan önce aşağıdaki Teorem'e ihtiyaç olacaktır.

Teorem 3.1.2. [Sağ Bölme Algoritması]: $f(x)$ ve $g(x)$ polinomları $R[x,\sigma_s]$ skew halkasında sıfırdan farklı iki polinom ve $g(x)$ polinomunun baş katsayısı birimsel eleman olsun. Bu durumda $q(x)$ ve $r(x)$ polinomları

$$f(x)=q(x)g(x)+r(x) \quad ; \quad d^o r(x)<d^o g(x)$$

olacak şekilde tek türlü vardır.

İspat. $f(x)=a_0+a_1x+\ldots+a_nx^n$, $g(x)=b_0+b_1x+\ldots+b_mx^m \in R[x,\sigma_s]$ polinomları ve $b_m^{-1}\in R$ olsun. Tümevarım yöntemi ile derecesi n'den küçük olan her polinom için hipotezin doğru olduğu kabul edilsin $a_n\cdot\sigma_s^{n-m}(b_m^{-1})x^{n-m}g(x)$ polinomunun derecesi. n'den küçük ve baş katsayısı a_n dir. Buradan görülür ki

$$f_1(x)=f(x)-a_n\cdot\sigma_s^{n-m}(b_m^{-1})x^{n-m}g(x)$$

polinomunun derecesi de n'den küçüktür. Kabulümüzden dolayı $q_1(x)$ ve $r(x)$ polinomları

$$f_1(x)=f(x)-a_n\cdot\sigma_s^{n-m}(b_m^{-1})x^{n-m}g(x)=q_1(x)g(x)+r(x)$$

ve $d^o r(x)<d^o g(x)$ olacak şekilde mevcuttur. Dolayısıyla

$$q(x)=q_1(x)+a_n\sigma_s^{n-m}(b_m^{-1})x^{n-m}$$

olarak alınırsa

$$f(x)=a_n\cdot\sigma_s^{n-m}(b_m^{-1})x^{n-m}g(x)+q_1(x)g(x)+r(x)=q(x)g(x)+r(x)$$

elde edilir.

Şimdi $q(x)$ ve $r(x)$ polinomlarının tek türlü olduğunu gösterilsin. Kabul edilsin ki $d^o r_1(x)<d^o g(x)$ ve $d^o r_2(x)<d^o g(x)$ .olacak şekilde

$$f(x)=q_1(x)g(x)+r_1(x) \text{ ve } f(x)=q_2(x)g(x)+r_2(x)$$

olsun. Buradan

$$q_1(x)g(x)+r_1(x)=q_2(x)g(x)+r_2(x)\Leftrightarrow(q_1(x)-q_2(x))g(x)=r_2(x)-r_1(x)$$

elde edilir. Baş katsayı birimsel eleman olduğundan

$$d^o(q_1(x)-q_2(x))+d^o g(x)=d^o(r_2(x)-r_1(x))$$

yazılabilir. Ayrıca $d^o(r_2(x)-r_1(x))=\max\{d^o r_1(x),d^o r_2(x)\}<d^o g(x)$ olduğundan yukarıdaki eşitliğin doğru olması $q_1(x)=q_2(x)$ ve $r_1(x)=r_2(x)$ olmasını gerektirir. Buradan tek türlü olması gerektiği anlaşılır.

Şimdi skew devirli kodların serbest olması için gerekli olan şart aşağıdaki teorem ile verilebilir.

Teorem 3.1.3. $\mathbb{F}_q+v\mathbb{F}_q$ üzerindeki derecesi k olan $u(x)$ polinomu x^n-1'in bir sağ böleni olmak üzere $C=\ <u(x)>$ kodu n uzunluğunda skew devirli kod olsun. Eğer $u(x)$ bir monik polinom ise C kodu $S=\{u(x),xu(x),\ldots,x^{n-k-1}u(x)\}$ bazına sahip bir serbest koddur ve $boyC=n-k$ dır.

İspat. $C=<u(x)>$ skew devirli kod ve $x^n-1=\upsilon(x)u(x)$ olsun. $u(x)$ ve x^n-1 polinomları monik olduğundan $\upsilon(x)$ polinomu da derecesi $n-k$ olan monik polinom olmak zorundadır. C kodunun herhangi bir $c(x)$ elemanı için $c(x)=k(x)u(x)$ olacak şekilde bir $k(x)\in R[x,\sigma_s]$ elemanı vardır. Eğer $d^o k(x)\le n-k-1$ ise S kümesi C'yi gerer. Aksi taktirde Teorem 3.1.2'den dolayı $q(x)$ ve $r(x)$ polinomları

$$k(x)=q(x)\upsilon(x)+r(x)\quad;\quad d^o r(x)<d^o\upsilon(x)\quad veya\quad r(x)=0$$

olacak şekilde mevcuttur. Yukarıdaki eşitliğin her iki tarafı $u(x)$ ile sağdan çarpılırsa $k(x)u(x)=q(x)h(x)u(x)+r(x)u(x)c(x)=k(x)u(x)=r(x)u(x)$ elde edilir. Buradan da S kümesinin C'yi gerdiği görülür.

Şimdi S'nin lineer bağımsız olduğu gösterilmelidir. $a(x)$ polinomu $a(x)u(x)=0$ şartını sağlayan $n-k-1$ derecesine sahip bir polinom olsun. Buda gösterir ki x^n-1 polinomu $a(x)u(x)$'in bir bölenidir. x^n-1 polinomu monik ve $d^o(a(x)u(x))<n$

olduğundan $a(x)$ polinomu sıfır olmak zorundadır. Bu da S'nin lineer bağımsız olduğunu ve C için bir baz olduğunu gösterir.

Tanım 3.1.4. Eğer $a(x), b(x) \in R[x, \sigma_s]$ polinomları

$$a(x)p_1(x) + b(x)p_2(x) = 1$$

olacak şekilde mevcut ise $p_1(x), p_2(x) \in R[x, \sigma_s]$ polinomlarına sağdan aralarında asaldır denir. Soldan aralarında asal tanımı da benzer şekilde yapılabilir.

Lemma 3.1.1. C kodu $x^n - 1 = \upsilon(x)u(x)$ olacak şekilde $u(x)$ üreteç polinomuna sahip skew devirli kod olsun. C nin herhangi bir üreteç polinomu $< p(x)u(x) >$ biçimindedir ve $\upsilon(x)$ ve $p(x)$ sağdan aralarında asaldır.

İspat. Kabul edilsin ki $\upsilon(x)$ ve $p(x)$ sağdan aralarında asal olsun ve $k(x)$ polinomu $p(x)u(x)$ elemanını temsil etsin yani $k(x) = p(x)u(x)$ olsun. $\upsilon(x)$ ve $p(x)$ sağdan aralarında asal olduklarından tanım gereği

$$a_1(x)p(x) + a_2(x)\upsilon(x) = 1$$

olacak şekilde $a_1(x), a_2(x) \in R[x, \sigma_s]$ polinomları vardır. Yukarıdaki eşitliğin her iki tarafı sağdan $u(x)$ polinomu ile çarpılırsa

$$a_1(x)p(x)u(x) + a_2(x)\upsilon(x)u(x) = u(x)$$

elde edilir. Başka bir ifade ile

$$a_1(x)p(x)u(x) = a_1(x)k(x) = u(x) \bmod (x^n - 1)$$

dir. Buradan $u(x) \in \langle k(x) \rangle_{sol}$ olduğu görülür. Dolayısıyla $\langle u(x) \rangle_{sol} \subseteq \langle k(x) \rangle_{sol}$ dir. Diğer taraftan $k(x) = p(x)u(x)$ olduğundan $\langle k(x) \rangle_{sol} \subseteq \langle u(x) \rangle_{sol}$ dir. Sonuç olarak $\langle k(x) \rangle_{sol} = \langle u(x) \rangle_{sol} = C$ dir. Yani $k(x) = p(x)u(x)$ polinomu C için bir üreteç olur.

3.2. $\mathbb{F}_q + v\mathbb{F}_q$ Halkası Üzerindeki Skew Yarı-Devirli Kodların Cebirsel Yapısı

Tanım 3.2.1. $\sigma_s, \mathbb{F}_q + v\mathbb{F}_q$ nin bir otomorfizması ve $|\sigma_s| = m$ olsun. $m|n$ olacak şekilde $N = n\ell$ pozitif tamsayı olsun. Eğer C aşağıdaki şartları sağlıyor ise C koduna N uzunluğunda indeksi ℓ olan skew yarı devirli kod denir.

i. C, $R^{n\ell}$ nin bir R-alt modülüdür.

ii. $c = \left(c_{0,0}, \ldots, c_{0,\ell-1}, c_{1,0}, \ldots, c_{1,\ell-1}, \ldots, c_{n-1,0}, \ldots, c_{n-1,\ell-1}\right) \in C$ iken

$$\tau_\ell(c) = \left(\sigma_s(c_{n-1,0}), \ldots, \sigma_s(c_{n-1,\ell-1}), \ldots, \sigma_s(c_{n-2,0}), \ldots, \sigma_s(c_{n-2,\ell-1})\right) \in C$$

dir. Diğer bir deyiş ile $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde ℓ indeksli N uzunluğunda skew yarı devirli kod τ_ℓ dönüşümü altında sabit kalan bir lineer koddur. $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde skew yarı devirli kod, eğer $\ell = 1$ olarak alınırsa skew devirli koda, eğer σ_s otomorfizması birim otomorfizma olarak alınırsa bilinen yarı-devirli koda dönüşür.

Teorem 3.2.1. $|\sigma_s| = m$ olmak üzere eğer $m|n$ ise $x^n - 1$ elemanı $R[x, \sigma_s]$ halkasının merkezindedir.

İspat: $a(x) = a_0 + a_1 x + \cdots + a_r x^r \in R[x, \sigma_s]$ olsun. $m|n$ olduğundan dolayı herhangi bir $a \in R$ için $\sigma_s^n(a) = a$ dır.

$$\begin{aligned}
(x^n - 1)a(x) &= (x^n - 1)(a_0 + a_1 x + \cdots + a_r x^r) \\
&= x^n a_0 + x^n(a_1 x) + \cdots + x^n(a_r x^r) - a(x) \\
&= \sigma_s^n(a_0)x^n + \sigma_s^n(a_1)x^{n+1} + \cdots + \sigma_s^n(a_r)x^{n+r} - a(x) \\
&= a_0 x^n + a_1 x^{n+1} + \cdots + a_r x^{n+r} - a(x) \\
&= (a_0 + a_1 x + \cdots + a_r x^r)x^n - a(x) \\
&= a(x)(x^n - 1)
\end{aligned}$$

olduğundan $x^n - 1$ elemanı $R[x, \sigma_s]$ halkasının merkezindedir.

Tanım 3.2.2. $R_n = R[x,\sigma_s] \Big/ \langle x^n - 1 \rangle$ ve $a = \left(a_{1,1}, a_{1,2} \ldots, a_{1,\ell}; \ldots; a_{n,1}, \ldots, a_{n,\ell}\right) \in R^{n\ell}$ olsun.

$a_i(x) = \sum_{j=1}^{n} a_{ji} x^{j-1}$ olmak üzere

$$\begin{array}{rccc} \phi: & R^{n\ell} & \to & R_n^{\ell} \\ & \left(a_{1,1}, a_{1,2} \ldots, a_{1,\ell}; \ldots; a_{n,1}, \ldots, a_{n,\ell}\right) & \to & (a_1(x), a_2(x), \cdots, a_\ell(x)) = a(x) \end{array}$$

birebir dönüşümü verilsin. Bu dönşüm yardımı ile *C*'deki herbir kod söz bir polinom olarak temsil edilebilir.

Teorem 3.2.2. $R_n^{\ell} = \left(R[x,\sigma_s] \Big/ \langle x^n - 1 \rangle \right)^{\ell}$ bölüm halkası

$$\alpha(x)(q_1(x), q_2(x), \cdots, q_\ell(x)) = (\alpha(x)q_1(x), \alpha(x)q_2(x), \cdots, \alpha(x)q_\ell(x))$$

şeklinde tanımlanan çarpma işlemi altında sol $R_n = R[x,\sigma_s] \Big/ \langle x^n - 1 \rangle$-modüldür.

İspat: Bu ispatta herhangi bir $f(x)$ polinomu kısaca *f* olarak gösterilecektir.

$\forall \alpha, \beta \in R_n$ ve $\forall q = (q_1, q_2, \cdots, q_\ell),\ p = (p_1, p_2, \cdots, p_\ell) \in R_n^{\ell}$ için

i. $$\begin{aligned} \alpha(p+q) &= \alpha(q_1 + p_1, q_2 + p_2, \cdots, q_\ell + p_\ell) \\ &= (\alpha q_1 + \alpha p_1, \alpha q_2 + \alpha p_2, \cdots, \alpha q_\ell + \alpha p_\ell) \\ &= \alpha(q_1, q_2, \cdots, q_\ell) + \alpha(p_1, p_2, \cdots, p_\ell) \\ &= \alpha p + \alpha q \end{aligned}$$

ii. $$\begin{aligned} (\alpha+\beta)p &= (\alpha p_1 + \beta p_1, \alpha p_2 + \beta p_2, \cdots, \alpha p_\ell + \beta p_\ell) \\ &= (\alpha p_1, \alpha p_2, \cdots, \alpha p_\ell) + (\beta p_1, \beta p_2, \cdots, \beta p_\ell) \\ &= \alpha p + \beta p \end{aligned}$$

iii. $$\begin{aligned} \alpha(\beta p) &= \alpha(\beta p_1, \beta p_2, \cdots, \beta p_\ell) \\ &= (\alpha\beta p_1, \alpha\beta p_2, \cdots, \alpha\beta p_\ell) \\ &= \alpha\beta(p_1, p_2, \cdots, p_\ell) \\ &= (\alpha\beta)p \end{aligned}$$

iv. $1_{R_n}\, p = p$

şartları sağlandığından R_n^{ℓ} bir sol R_n -modüldür.

Tanım 3.2.2 ve Teorem 3.2.2 den R üzerinde $N = n\ell$ uzunluğundaki skew yarı devirli kod R_n^ℓ'nin bir R_n- sol alt modülüdür. Eğer R üzerindeki C skew yarı devirli kodu $u_1(x), u_2(x), \ldots, u_k(x) \in R_n^\ell$ gibi k tane eleman tarafından üretiliyorsa C'ye k-üreteçli skew yarı devirli kod denir. Bundan sonraki bölümlerde bir üreteçli skew yarı devirli kodların yapısı incelenecektir.

3.3. $\mathbb{F}_q + v\mathbb{F}_q$ Halkası Üzerindeki Bir Üreteçli Skew Yarı-Devirli Kodlar

C skew yarı devirli kodu k tane $u_1(x), u_2(x), \ldots, u_k(x) \in R_n^\ell$ elemanları tarafından üretilir ise C'ye k-üreteçli skew yarı kod deniyordu. Eğer $k = 1$ olarak alınırsa C skew yarı devirli kodu $u(x) = (u_1(x), u_2(x), \ldots, u_\ell(x))$ gibi tek bir eleman tarafından üretilir ve bu C kodu

$$C = \{g(x)u(x) = g(x)u_1(x), g(x)u_2(x), \ldots, g(x)u_\ell(x)) \mid g(x) \in R_n\}$$

şeklindedir.

C kodu $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde $N = n\ell$ uzunluğunda $u(x) = (u_1(x), u_2(x), \ldots, u_\ell(x))$ tarafından üretilen 1- üreteçli skew yarı devirli kod olsun. R_n^ℓ halkasından R_n halkasına

$$\begin{array}{rccc} \phi_i : & R_n^\ell & \to & R_n \\ & (f_1(x), f_2(x), ..., f_\ell(x)) & \to & f_i(x) \end{array}$$

şeklinde bir dönüşüm tanımlansın. Hem R_n^ℓ hem de R_n'nin bir R_n modül olduğu göz önünde bulundurularak

$\forall f(x) = (f_1(x), f_2(x), ..., f_\ell(x)), g(x) = (g_1(x), g_2(x), ..., g_\ell(x)) \in R_n^\ell$ ve $r(x) \in R_n$ için

$$\begin{aligned} \phi_i(f(x) + g(x)) &= \phi_i(f_1(x) + g_1(x), ..., f_\ell(x) + g_\ell(x)) \\ &= f_i(x) + g_i(x) \\ &= \phi_i(f(x)) + \phi_i(g(x)) \\ \phi_i(r(x) f(x)) &= \phi_i(r(x) f_1(x), ..., r(x) f_\ell(x)) \\ &= r(x) f_i(x) \\ &= r(x)\phi_i(f(x)) \end{aligned}$$

şartları sağlandığından bir modül homomorfizmasıdır.

$\phi_i(C) = C_i$ olsun. C kodu $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde 1- üreteçli skew yarı devirli kod olduğundan R_n^ℓ nin bir R_n -sol alt modülüdür. Homomorfizmadan dolayı $\phi_i(C) = C_i$ de R_n'nin bir R_n - sol alt modülüdür. Başka bir deyiş ile $\phi_i(C) = C_i$ kodu $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde *n* uzunluğunda skew devirli koddur. Teorem 3.1.1 den biliyoruz ki $x^n - 1$'in bir sağ böleni olan $u_i(x)$ tarafından üretilir yani $C_i = \langle u_i(x) \rangle$ ve $x^n - 1 = \upsilon_i(x) u_i(x)$ dir. Bu durumda $\upsilon_i(x)$ ve $p_i(x)$ aralarında sağdan asal olmak üzere *C*'nin herhangi bir üreteci $\langle p_i(x) u_i(x) \rangle$ formundadır. Bu durum aşağıdaki teorem ile özetlenebilir.

Teorem 3.3.1. *C* kodu $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde $N = n\ell$ uzunluğunda 1- üreteçli skew yarı devirli kod olsun. $u_i(x)$ polinomu $x^n - 1$'in bir sağ böleni ve $ebob_{sağ}\left(p_i(x), \dfrac{x^n - 1}{u_i(x)} \right) = 1$ olmak üzere *C*'nin herhangi bir üreteci olarak $\mathbf{u}(\mathbf{x}) = (p_1(x)u_1(x), p_2(x)u_2(x), \ldots, p_\ell(x)u_\ell(x))$ seçilebilir.

C kodu $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde indeksi ℓ olan $N = n\ell$ uzunluğunda 1- üreteçli skew yarı devirli kod olmak üzere

$$u(x) = ebob_{sol}(\mathbf{u}(\mathbf{x}), x^n - 1) = ebob_{sol}\left(f_1(x)u_1(x),\ f_2(x)u_2(x), \cdots,\ f_\ell(x)u_\ell(x), x^n - 1 \right)$$

olacak şekilde tek bir monik polinomu vardır.

Teorem 3.3.2. *C* kodu $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde $N = n\ell$ uzunluğunda Teorem 3.3.1'deki gibi üretilen skew yarı devirli kod ve $u(x) = ebob_{sol}(\mathbf{u}(\mathbf{x}), x^n - 1)$ olsun. Bu durumda *C* kodu $S = \{\mathbf{u}(\mathbf{x}), x\mathbf{u}(\mathbf{x}), \ldots, x^{n - d^o u(x) - 1}\mathbf{u}(\mathbf{x})\}$ kümesi tarafından üretilir.

İspat. $x^n - 1$ polinomu monik $u(x)$ polinomu tarafından bölünebilmektedir. Dolayısıyla $x^n - 1 = u(x)\upsilon(x)$ olacak şekilde monik bir $\upsilon(x)$ polinomu vardır. Kabul edilsin ki $d^o u(x) = t$ olsun. O halde $d^o \upsilon(x) = n - t$ elde edilir. *C*'nin herhangi bir $c(x)$

elemanı $k(x) \in R_n$ olmak üzere $c(x) = k(x)\mathbf{u}(\mathbf{x})$ olarak ifade edilebilir. Sağ bölme algoritmasından dolayı $q(x), r(x) \in R[x, \sigma_s]$ polinomları

$$k(x) = q(x)\upsilon(x) + r(x) \quad \text{ve} \quad 0 \le d^o r(x) < n - t$$

olacak şekilde vardır. $u(x) = ebob_{sol}(\mathbf{u}(\mathbf{x}), x^n - 1)$ olduğu göz önünde tutulursa $s(x) \in R_n$ polinomu $\mathbf{u}(\mathbf{x}) = u(x)s(x)$ olacak şekilde mevcuttur. Ayrıca $x^n - 1$, Teorem 3.2.1'den dolayı $R[x, \sigma_s]$ halkasının merkezinde bulunduğu için $x^n - 1 = u(x)\upsilon(x) = \upsilon(x)u(x)$ durumu geçerlidir. Buradan

$$\upsilon(x)\mathbf{u}(\mathbf{x}) = \upsilon(x)u(x)s(x) = u(x)\upsilon(x)s(x) \equiv 0 \bmod(x^n - 1)$$

elde edilir. Bu yüzden

$$\begin{aligned} c(x) &= (q(x)\upsilon(x) + r(x))\mathbf{u}(\mathbf{x}) \\ &= q(x)\upsilon(x)\mathbf{u}(\mathbf{x}) + r(x)\mathbf{u}(\mathbf{x}) \\ &\equiv r(x)\mathbf{u}(\mathbf{x}) \bmod(x^n - 1) \end{aligned}$$

dir.Dikkat edilmelidir ki $d^o r(x) < n - t$ olduğundan $c(x)$ elemanı $\{\mathbf{u}(\mathbf{x}), x\mathbf{u}(\mathbf{x}), \ldots, x^{n-d^o u(x)-1}\mathbf{u}(\mathbf{x})\}$ elemanları tarafından ifade edilebilir demektir. Bu sebepten dolayı *S* kümesi *C*'yi gerer.

Teorem 3.3.2'deki *S* kümesi lineer bağımsız değildir. Başka bir deyişle R_n'nin herhangi bir elemanı $S = \{\mathbf{u}(\mathbf{x}), x\mathbf{u}(\mathbf{x}), \ldots, x^{n-d^o u(x)-1}\mathbf{u}(\mathbf{x})\}$ elemanlarının farklı lineer kombinasyonları ile temsil edilebiliyor. Şimdi *C* kodunun serbest olması için gerekli şart aşağıdaki Teorem ile verilecektir. Teorem 3.1.3'den biliniyor ki eğer üreteç polinom bir monik polinom ise *C* kodu $S = \{u(x), xu(x), \ldots, x^{n-k-1}u(x)\}$ bazına sahip bir serbest koddur ve $boyC = n - k$ dır. Bir sonraki teoremde 1- üreteçli skew yarı devirli kodların serbest olması için gerekli olan şart verilmiştir.

Teorem 3.3.3. $u_i(x)$ polinomu $x^n - 1$'in bir monik sağ böleni ve $ebob_{sağ}\left(p_i(x), \dfrac{x^n - 1}{u_i(x)}\right) = 1$ olmak üzere *C* kodu

$$\mathbf{u}(\mathbf{x}) = (p_1(x)u_1(x), p_2(x)u_2(x), \ldots, p_\ell(x)u_\ell(x))$$

tarafından üretilen $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde $N = n\ell$ uzunluğunda skew yarı devirli kod olsun. C kodu rankı $n - d^o u(x)$ ve bazı $S = \{\mathbf{u}(\mathbf{x}), x\mathbf{u}(\mathbf{x}), \ldots, x^{n-d^o u(x)-1}\mathbf{u}(\mathbf{x})\}$ olan bir serbest R-modüldür.

İspat. Bir önceki teoremde S kümesinin C'yi gerdiği gösterilmişti. Şimdi S kümesinin lineer bağımsız olduğu gösterilmesi gerekecektir. Kabul edilsin ki $a(x)\mathbf{u}(\mathbf{x}) = 0$ şartını sağlayan bir $a(x) = a_0 + a_1(x)x + \ldots + a_{n-t-1}x^{n-t-1}$ polinomu olsun. Her $i = 1, 2, \ldots \ell$ için $a(x)p_i(x)u_i(x) = 0$ dır. Yani $x^n - 1$ polinomu $a(x)p_i(x)u_i(x)$'in bir bölenidir. Ayrıca $x^n - 1$ polinomu $a(x)(x^n - 1)$'inde bir böleni olduğundan

$$x^n - 1 \mid ebob_{sol}(a(x)p_1(x)u_1(x), \ldots, a(x)p_\ell(x)u_\ell(x), a(x)(x^n - 1)) = a(x)u(x)$$

elde edilir. $x^n - 1$ polinomu n. dereceden monik bir polinom ve $d^o(a(x)u(x)) = n - 1 < n$ olduğundan $a(x) = 0$ olmak zorundadır. Bu sebepten her $i = 1, 2, \ldots, n - t - 1$ için $a_i = 0$ dır. Dolayısıyla S kümesi lineer bağımsızdır ve C için bir baz olur.

$\mathbb{F}_q + v\mathbb{F}_q$ üzerinde skew yarı devirli kodun minimum uzaklığı için bir sınır verilecektir. Bundan önce $\mathbb{F}_q + v\mathbb{F}_q$ üzerindeki skew devirli kodlardaki minimum uzaklık için sınırın verildiği aşağıdaki teoreme ihtiyaç olacaktır.

Teorem 3.3.4. $\mathbb{F}_q$ üzerindeki $u_1(x)$ ve $u_2(x)$ polinomları sırası ile C_1 ve C_2 skew devirli kodların üreteç polinomları olmak üzere $C = \langle u(x) \rangle = \langle (1-v)u_1(x) + vu_2(x) \rangle$ kodu n uzunluğunda $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde skew devirli kod olsun. Eğer C_1 ve C_2 kodlarının minimum uzaklıkları sırasıyla en az δ_1 ve δ_2 olmak üzere $d(C) \geq min\{\delta_1, \delta_2\}$ dir [36].

Şimdi Teorem 3.3.4 kullanılarak $\mathbb{F}_q + v\mathbb{F}_q$ üzerindeki skew devirli kodların minimum uzaklığı için bir sınır verilebilir.

Teorem 3.3.5. $u(x)$ polinomu x^n-1'in bir monik sağ böleni ve $ebob_{sağ}\left(f_i(x),\frac{x^n-1}{u(x)}\right)=1$ olmak üzere C kodu

$$U(x)=(f_1(x)u(x),\, f_2(x)u(x),\ldots,\, f_\ell(x)u(x))$$

tarafından üretilen $\mathbb{F}_q+v\mathbb{F}_q$ üzerinde $N=n\ell$ uzunluğunda skew yarı devirli kod olsun. Bu durumda $d(C)\geq \ell min\{\delta_1,\delta_2\}$ dir.

İspat. $u(x)$ polinomu x^n-1'in bir monik sağ böleni olduğundan $x^n-1=\upsilon(x)u(x)$ olsun. Lemma 3.1.1'den dolayı her $i=1,2,\ldots,\ell$ için $<f_i(x)u(x)>=<u(x)>$ elde edilir. Yani $U(x)$'in her bir bileşeni $u(x)$ tarafından üretilen bir skew devirli koddur. $c(x)\in C$ kod sözü için

$$c(x)=k(x)U(x)=(k(x)f_1(x)u(x),\ldots,k(x)f_\ell(x)u(x))$$

ve bazı $i=1,2,\ldots,\ell$ için $k(x)f_i(x)u(x)=0$ olsun. O halde

$$k(x)f_i(x)u(x)=0 \Leftrightarrow x^n-1 \mid k(x)f_i(x)u(x)$$
$$\Leftrightarrow \frac{x^n-1}{u(x)} \mid k(x)f_i(x)$$

dir ve $f_i(x)$ ve $\frac{x^n-1}{u(x)}$ sağdan aralarında asal olduklarından dolayı $\frac{x^n-1}{u(x)} \mid k(x)$ dir. Yani $\upsilon(x) \mid k(x)$ dir. Bu da $k(x)=0$ anlamına gelir. Sonuç olarak tek bir i değeri için $k(x)f_i(x)u(x)=0$ olmasının gerek ve yeter şartı $c(x)=0$ olmasıdır. Diğer bir değiş ile $c(x)\neq 0$ olması için gerek ve yeter şart tüm $i=1,2,\ldots,\ell$ değerleri için $k(x)f_i(x)u(x)\neq 0$ olmasıdır. Bu sebepten $c(x)$'in her bir bileşeni $u(x)$ tarafından üretilen sıfırdan farklı bir skew devirli koddur. Teorem 3.3.4'den dolayı bir skew devirli kodun minimum uzaklığı $\geq min\{\delta_1,\delta_2\}$ şeklindedir. Bu yüzden $d(C)\geq \ell min\{\delta_1,\delta_2\}$ dir.

Örnek 3.3.1. $\mathbb{F}_4+v\mathbb{F}_4$ üzerinde $n=6$ uzunluğunda $u(x)=x^3+(v+w)x^2+(v+w^2)x+v+w^2$ (ve $u_1=x^3+wx^2+w^2x+w^2, u_2=x^3+w^2x^2+wx+w$ $u_2=x^3+w^2x^2+wx+w$) üreteç polinomuna sahip skew devirli kod 4^6 elemana ve 3 Lee uzaklığına sahiptir. Bu kodun Gray görüntüsü $\mathbb{F}_4$. üzerinde [12,6,3]-kodudur. Teorem 3.3.5'den dolayı $\langle u,uf\rangle$ (f teoremdeki şartları sağlayan bir polinom) formundaki üretece sahip 2-yarı devirli kod $\mathbb{F}_4+v\mathbb{F}_4$ üzerinde $[12,6,\geq 6]$ parametresine sahiptir. Örneğin $f=x$ ve $uf=x^4+(v+w^2)x^3+(v+w)x^2+(v+w)x$ olmak üzere üretilen kod 8 minimum uzaklığa sahiptir. Bu sebepten $\mathbb{F}_4$ üzerinde [24,6,8] kodu elde edilir.

3.4. $\mathbb{F}_q+v\mathbb{F}_q$ Halkası Üzerindeki Skew Yarı Devirli Kodların Duali

İlk olarak $\mathbb{F}_q+v\mathbb{F}_q$ üzerindeki $n\ell$ uzunluğuna ve ℓ indeksine sahip skew yarı devirli kodların dualinin de yine aynı uzunluğa ve indekse sahip skew yarı devirli kod olduğu gösterilecektir. Bunun için aşağıda birkaç tanım verilecektir.

Tanım 3.4.1. $1\leq i\leq n-1$ için $a_i=(a_{i0},a_{i1},\ldots,a_{i(\ell-1)}), b_i=(a_{i0},a_{i1},\ldots,a_{i(\ell-1)})\in R^\ell$ olmak üzere $a=(a_0,a_1,\ldots,a_{n-1})$ ve $b=(b_0,b_1,\ldots,b_{n-1})$ elemanlarının Öklid iç çarpımı

$$a\cdot b=\sum_{i=0}^{n-1}a_i\cdot b_i=\sum_{i=0}^{n-1}\sum_{j=0}^{\ell-1}a_{ij}b_{ij}$$

şeklinde tanımlanır.

Tanım 3.4.2. Öklid iç çarpımına göre *C* kodunun duali de

$$C^\perp=\{b\in R^{n\ell}\mid a\cdot b=0,\forall a\in C\}$$

olarak tanımlanır.

Tanım 3.4.3. $\sigma_s(a_i)=(\sigma_s(a_{i0}),\sigma_s(a_{i1}),\ldots,\sigma_s(a_{i(\ell-1)}))$ olmak üzere $a=(a_0,a_1,\ldots,a_{n-1})\in R^{n\ell}$ elemanı için

$$\tau_\ell(a_0,a_1,\ldots,a_{n-1})=(\sigma_s(a_{n-1}),\sigma_s(a_0),\ldots,\sigma_s(a_{n-2}))$$

şeklinde tanımlanan τ_ℓ operatörüne skew yarı devirli kodu öteleme operatörü denir.

Teorem 3.4.1. Skew yarı devirli kodun duali de skew yarı devirli koddur.

İspat. C kodu $n\ell$ uzunluğuna ve ℓ indeksine sahip skew yarı devirli kod olsun. $a\in C$ ve $b\in C^\perp$ olmak üzere iki eleman olsun. σ_s^n dönüşümünün $\mathbb{F}_q+v\mathbb{F}_q$ üzerinde birim dönüşüm olduğu göz önünde tutulursa

$$\begin{aligned}a\cdot\tau_\ell(b)&=\sum_{i=0}^{n-1}a_i\cdot\sigma_s(b_{i+n-1})=\sum_{i=0}^{n-1}\sigma_s(\sigma_s^{n-1}(a_i)b_{i+n-1})\\&=\sigma_s(\tau_\ell^{n-1}(a)\cdot b)\\&=\sigma_s(0)\\&=0\end{aligned}$$

elde edilir. Burada $i+n-1$ indisleri $\bmod n$ olarak düşünülecektir. Sonuç olarak $\tau_\ell(b)\in C^\perp$ olduğu elde edilir. Bu da $C^\perp$'nin $n\ell$ uzunluğuna ve ℓ indeksine sahip skew yarı devirli kod olduğunu gösterir.

Tanım 3.2.2'de bahsedilen ϕ dönüşümü R üzerinde $n\ell$ uzunluğuna ve ℓ indeksine sahip skew yarı devirli kodlar ile R_n üzerinde ℓ uzunluğunda lineer kodlar arasında birebir bir ilişki kurar. Bu dönüşüm skew yarı devirli kodların bir polinom gösterimi olarak düşünülürse Hermityen iç çarpımı daha uygun olacaktır.

Tanım 3.4.4. R_n üzerinde bir φ eşlenik dönüşümü $0\le i\le n-1$ için $\varphi(cx^i)=\sigma_s^{-i}(c)x^{n-i}$ olarak tanımlansın. R_n^ℓ'nin $u(x)=(u_0(x),u_1(x),\ldots,u_{\ell-1}(x))$ ve $\upsilon(x)=(\upsilon_0(x),\upsilon_1(x),\ldots,\upsilon_{\ell-1}(x))$ iki elemanının Hermityen iç çarpımı

$$u(x)*\upsilon(x)=\sum_{i=0}^{\ell-1}u_i(x)\varphi(\upsilon_i(x))$$

olarak tanımlanır.

Teorem 3.4.2. $a,b \in R^{n\ell}$ ve $a(x)$, $b(x)$ de bu elemanların polinom gösterimi olsun. $0 \le m \le n-1$ için $\tau_\ell^m(a)\cdot b = 0$ olması için gerek ve yeter şart $a(x)*b(x) = 0$ olmasıdır.

İspat. $a(x)*b(x) = 0$ olsun.

$$\begin{aligned} 0 = \sum_{j=0}^{\ell-1} a_j(x)\varphi(b_j(x)) &= \sum_{j=0}^{\ell-1}\left(\sum_{i=0}^{n-1} a_{ij}x^i\right)\varphi\left(\sum_{m=0}^{n-1} b_{mj}x^m\right) \\ &= \sum_{j=0}^{\ell-1}\left(\sum_{i=0}^{n-1} a_{ij}x^i\right)\left(\sum_{m=0}^{n-1} \sigma_s^{-i}(b_{mj})x^{n-m}\right) \\ &= \sum_{t=0}^{n-1}\left(\sum_{j=0}^{\ell-1}\sum_{i=0}^{n-1} a_{i+t,j}\sigma_s^t(b_{ij})\right)x^t \end{aligned}$$

elde edilir. Burada $i+t$ indisleri $\bmod n$ olarak alınacaktır. Her iki tarafın x^t katsayıları karşılaştırılırsa her bir $0 \le t \le n-1$ için

$$0 = \sum_{j=0}^{\ell-1}\sum_{i=0}^{n-1} a_{i+t,j}\sigma_s^t(b_{ij}) = \sigma_s^t(\tau_\ell^{n-t}(a)\cdot b)$$

elde edilir. Bu da gösterir ki her $0 \le t \le n-1$ için $\tau_\ell^{n-t}(a)\cdot b = 0$ elde edilir. Bu da $0 \le m \le n-1$ için $\tau_\ell^m(a)\cdot b = 0$ demektir.

Sonuç 3.4.1. C kodu $F_q + vF_q$ üzerinde $N = n\ell$ uzunluğunda skew yarı devirli kod olsun. Bu durumda

$$C^\perp = \{b(x) \in R_n^\ell \mid a(x)*b(x) = 0, \forall a(x) \in C\}$$

dir.

Teorem 3.4.3. C kodu R üzerinde $n\ell$ uzunluğuna ve ℓ indeksine sahip skew yarı devirli kod olsun. $R^{n\ell}$ üzerinde Öklit iç çarpım ve R_n^ℓ R_n^ℓ üzerinde Hermityen iç çarpım tanımlı olmak üzere $\phi(C)^\perp = \phi(C^\perp)$ dir.

İspat. C kodu skew yarı devirli kod ve $a \in C$ olsun. O halde $\tau_\ell^m(a) \in C$ dir. Teorem 3.4.2'den $\tau_\ell^m(a) \cdot b = 0$ elde edilir. Bu da gösterir ki $b \in C^\perp$ dir. Yani $\phi(b) \in \phi(C^\perp)$ dir. Tekrar Teorem 3.4.2'den $\tau_\ell^m(a) \cdot b = 0$ ise $a(x) * b(x) = 0$ dır. Yani $\phi(a) * \phi(b) = 0$ dır. Dolayısıyla $\phi(C^\perp) \subseteq \phi(C)^\perp$ dir.

Tersine; $b(x) = \phi(b) \in \phi(C)^\perp$ olsun. O halde $a(x) * b(x) = \phi(a) * \phi(b) = 0$ olacak şekilde $\phi(C)$ da $a(x) = \phi(a)$ elemanı vardır. Teorem 3.4.2'den $\tau_\ell^m(a) \cdot b = 0$ dir. $a \in C$ ve C skew yarı devirli kod olduğundan $\tau_\ell^m(a) \in C$ dir. Buda $b \in C^\perp$ yani $\phi(b) \in \phi(C^\perp)$ olduğunu gösterir. Dolayısıyla $\phi(C)^\perp \subseteq \phi(C^\perp)$ dir. Sonuç olarak, $\phi(C)^\perp = \phi(C^\perp)$ elde edilir.

Sonuç 3.4.2. C kodu R üzerinde $n\ell$ uzunluğuna ve ℓ indeksine sahip skew yarı devirli kod olsun. C kodu R üzerinde Öklit iç çarpımına göre self dual olmas çin gerek ve yeter şart $\phi(C)$ kodu R_n üzerinde Hermityen iç çarpımına göre self dual olmasıdır.

3.5. $\mathbb{F}_q + v\mathbb{F}_q$ Üzerindeki Skew Devirli Kodlardan Kuantum Kodlar Elde Etme

Bu bölümde $\mathbb{F}_q + v\mathbb{F}_q$ üzerindeki skew devirli kodlardan kuantum kod inşa edilecektir. Bunun için $\mathbb{F}_q + v\mathbb{F}_q$ üzerindeki skew devirli kodların dualini içermesi için gerek ve yeter şart verilecektir.

R'nin herhangi elemanı $a, b \in \mathbb{F}_q$ olmak üzere $a + vb \in R$ şeklinde ifade edilebilir. R halkasından $\mathbb{F}_q^2$ halkasına

$$\begin{array}{rccc} \psi: & R & \to & \mathbb{F}_q^2 \\ & a+vb & \to & (a, a+b) \end{array}$$

şeklinde bir Gray dönüşüm tanımlanabilir [36].

Tanımlanan bu dönüşüm R^n cebirsel yapısından $\mathbb{F}_q^{2n}$ cebirsel yapısına

$$(a_0 + vb_0, \cdots, a_{n-1} + vb_{n-1}) \to (a_0, a_0 + b_0, \cdots, a_{n-1}, a_{n-1} + b_{n-1})$$

olarak genişletilebilir. Herhangi bir $x \in R$ elemanının Lee ağırlığı $w_L(x) = w_H(\psi(x))$ olarak tanımlanır. Herhangi iki $x, y \in R$ elemanları için Lee uzaklık $d_L(x, y) = w_L(x - y)$ ile hesaplanabilir. $x = a + vb$ ve $y = c + vd$ olmak üzere

$$\begin{aligned}
\psi(\alpha x + \beta y) &= \psi(\alpha a + \beta c + v(\alpha b + \beta d)) \\
&= (\alpha a + \beta c, \alpha(a + b) + \beta(c + d)) \\
&= \alpha(a, a + b) + \beta(c, c + d) \\
&= \alpha\psi(a + vb) + \beta\psi(c + vd) \\
&= \alpha\psi(x) + \beta\psi(y)
\end{aligned}$$

ve

$$\begin{aligned}
d_L(x, y) &= w_L(x - y) = w_L((a - c) + v(b - d)) \\
&= w_H(\psi((a - c) + v(b - d))) \\
&= w_H(a - c, a + b - (c + d)) \\
&= w_H((a, a + b) - (c, c + d)) \\
&= w_H(\psi(a + vb) - \psi(c + vd)) \\
&= w_H(\psi(x) - \psi(y)) \\
&= d_H(\psi(x), \psi(y))
\end{aligned}$$

olduğundan tanımlanan Gray dönüşüm (R^n, Lee uzaklık)'tan ($\mathbb{F}_q^{2n}$, Hamming uzaklık)'a tanımlanan bir lineer izometri olduğu görülür. Ayrıca *C* kodu *R* üzerinde kendi üzerine ortogonal bir kod iken yani $x = a + vb \in C$ ve $y = c + vd \in C^{\perp}$ olmak üzere

$$x \cdot y = ac + v(ad + bc + bd) = 0 \Rightarrow ac = ad + bc + bd = 0$$

iken

$$\psi(x) \cdot \psi(y) = (a, a + b) \cdot (c, c + d) = ac + ac + ad + bc + bd = 0$$

olduğundan ortogonalliği koruyan bir dönüşümdür. Yani *C* kodu *R* üzerinde kendi üzerine ortogonal bir kod ise $\psi(C)$'de $\mathbb{F}_q$ üzerinde kendi üzerinde ortogonaldir.

Teorem 3.5.1. C_1 ve C_2 lineer kodları F_q üzerinde sırasıyla k_1 ve k_2 boyutlarına ayrıca $d(C_1)$ ve $d(C_2)$ Hamming uzaklıklarına sahip olmak üzere $C = (1-v)C_1 + vC_2$ kodu $F_q + vF_q$ üzerinde n uzunluğunda bir lineer kod olsun. Bu durumda $\psi(C)$ de $GF(q)$. üzerinde $[2n, k_1 + k_2, min\{d(C_1), d(C_2)\}]$ parametresine sahip koddur [36].

Tanım 3.5.1. $\mathbb{F}_q[x,\sigma_s] \Big/ \langle x^n - 1 \rangle$ halkasında $u(x) = u_0 + u_1 x + \ldots + u_r x^r$ ve $\upsilon(x) = \upsilon_0 + \upsilon_1 x + \ldots + \upsilon_{n-r} x^{n-r}$ iki polinom ve $x^n - 1 = \upsilon(x)u(x)$ olmak üzere C kodu $u(x)$ tarafında üretilen skew devirli kod olsun. Bu durumda C skew devirli kodun duali $\upsilon^R(x) = \upsilon_{n-r} + \sigma_s(\upsilon_{n-r-1})x + \ldots + \sigma_s^{n-r}(\upsilon_0)x^{n-r}$ ile üretilir [30] .

Teorem 3.5.2. $\mathbb{F}_q$ üzerinde C_1 ve C_2 skew devirli kodları sırasıyla $x^n - 1 = \upsilon_1(x)u_1(x)$ ve $x^n - 1 = \nu_2(x)u_2(x)$ şartlarını sağlayan $u_1(x)$ ve $u_2(x)$ üreteç polinomlarına sahip olsun. Eğer $C = (1-v)C_1 + vC_2$ ise $i = 1, 2$ için $\nu_i^R(x)$ polinomu is $\nu_i(x)$ polinomunun resiprosıl polinomu olmak üzere $C^{\perp} = \langle (1-v)\upsilon_1^R(x) + v\upsilon_2^R(x) \rangle$ dir [36].

R üzerindeki skew devirli kodların duallerini içermesi için gerek ve yeter koşulu vermeden önce aşağıdaki teoreme ihtiyaç olacaktır. Bu teorem ile $\mathbb{F}_q$ üzerindeki skew devirli kodların kendi üzerine ortogonal olması için gerekli şart verilecektir.

Teorem 3.5.3. $\mathbb{F}_q$ üzerinde $C = \langle u(x) \rangle$ kodu n uzunluğunda skew devirli kod olsun. C kodunun kendi üzerinde ortogonal olması için gerek ve yeter şart $\upsilon^R(x)$ polinomu $u(x)$ polinomunun bir sağ bölenidir.

İspat. C kodu $\mathbb{F}_q$ üzerinde kendi üzerine ortogonal olan skew devirli kod olsun. $u(x) \in C \subset C^{\perp}$ olduğundan $u(x) = b(x)\upsilon^R(x)$ olacak şekilde bir $b(x)$ polinomu vardır. Buradan görülür ki $\upsilon^R(x)$ polinomu $u(x)$ polinomunun bir sağ bölenidir.

Tersine herhangi bir $c(x) \in C$ elemanı için $c(x) = a(x)u(x)$ olacak şekilde bir $a(x)$ polinomu vardır. $u(x)$ polinomu $\upsilon^R(x)$ tarafından sağdan bölündüğünden $u(x) = b(x)\upsilon^R(x)$ yazılabilir. Bu eşitliğin her iki tarafı $a(x)$ ile çarpılırsa

$$\begin{aligned} c(x) = a(x)u(x) &= a(x)[b(x)\upsilon^R(x)] \\ &= [a(x)b(x)]\upsilon^R(x) \end{aligned}$$

elde edilir. Bu da $c(x) \in C^{\perp}$ olduğu anlamına gelir. Yani C kendi üzerine ortogonaldir.

Teorem 3.5.4. $\mathbb{F}_q$ üzerinde $C = <u(x)>$ kodu n uzunluğunda skew devirli kod ve otomorfizmanın mertebesi n sayısını bölüyor olsun. C'nin kendi üzerine ortogonal olması için gerek ve yeter şart $\upsilon^R(x)\upsilon(x)$ 'nin $x^n - 1$'nin bir sağ böleni olmasıdır.

İspat. $\mathbb{F}_q$ üzerinde C kodu n uzunluğu çift tamsayı olan kendi üzerine ortogonal bir skew devirli kod olsun. Teorem 3.5.3'den $\upsilon^R(x)$ polinomu $u(x)$ polinomunun bir sağ bölenidir. Dolayısıyla $u(x) = b(x)\upsilon^R(x)$ olacak şekilde bir $b(x)$ polinomu vardır. Eşitliğin her iki tarafı sağdan $\nu(x)$ polinomu ile çarpılırsa

$$\begin{aligned} x^n - 1 = u(x)\nu(x) &= [b(x)\upsilon^R(x)]\upsilon(x) \\ &= b(x)[\upsilon^R(x)\upsilon(x)] \end{aligned}$$

elde edilir. Buradan görülür ki $\upsilon^R(x)\upsilon(x)$ 'nin $x^n - 1$'nin bir sağ bölenidir.

Tersine $\upsilon^R(x)\upsilon(x)$ 'nin $x^n - 1$'nin bir sağ böleni olduğundan

$$\begin{aligned} x^n - 1 &= a(x)[\upsilon^R(x)\upsilon(x)] \\ u(x)\nu(x) &= a(x)[\upsilon^R(x)\upsilon(x)] \end{aligned}$$

elde edilir. Bu da $(u(x) - a(x)\upsilon^R(x))\upsilon(x) = 0$ olduğu anlamına gelir. $\upsilon(x)$ sıfırdan farklı bir polinom olduğundan $u(x) - a(x)\upsilon^R(x) = 0$ elde edilir. Yani $u(x) = a(x)\upsilon^R(x)$ dir.Teorem 3.5.3'den C'nin kendi üzerine ortogonal olduğu söylenebilir.

Sonuç 3.5.1. $\mathbb{F}_q$ üzerinde $C =< u(x) >$ kodu n uzunluğunda skew devirli kod ve otomorfizmanın mertebesi n sayısını bölüyor olsun. C'nin duali içermesi için gerek ve yeter şart $x^n - 1$'in $\upsilon^R(x)\upsilon(x)$ tarafından sağdan bölünebilir olmasıdır.

Şimdi R üzerindeki skew devirli kodların dualini içermesi için gerek ve yeter şart aşağıdaki teorem ile verilebilir.

Teorem 3.5.5. R üzerinde $C = \langle u(x) \rangle = \langle (1-v)u_1(x) + vu_2(x) \rangle$ kodu n uzunluğunda skew devirli kod ve otomorfizmanın mertebesi n sayısını bölüyor olsun. $C^{\perp} \subset C$ olması için gerek ve yeter şart $x^n - 1$'in $\upsilon_1^R(x)\upsilon_1(x)$ tarafından sağdan bölünebilir olmasıdır.

İspat. $x^n - 1$ polinomu $\upsilon_1^R(x)\upsilon_1(x)$ ve $\upsilon_2^R(x)\upsilon_2(x)$ tarafından sağdan bölünebilir olsun. Sonuç 3.5.1'den $C_1^{\perp} \subseteq C_1$ ve $C_2^{\perp} \subseteq C_2$ elde edilir. Buradan da

$$(1-v)C_1^{\perp} \subseteq (1-v)C_1 \text{ ve } vC_2^{\perp} \subseteq vC_2$$

sağlanır. Bu sebepten dolayı

$$\langle (1-v)\upsilon_1^R(x) + v\upsilon_2^R(x) \rangle \subseteq \langle (1-v)u_1(x) + vu_2(x) \rangle >$$

yazılabilir. Dolayısıyla $C^{\perp} \subseteq C$ dir.

Tersine eğer $C^{\perp} \subseteq C$ ise $(1-v)C_1^{\perp} + vC_2^{\perp} \subseteq (1-v)C_1 + vC_2$ dir. Ayrıca

$$(1-v)C^{\perp} = (1-v)C_1^{\perp} \subseteq (1-v)C_1 = (1-v)C$$

ve

$$vC^{\perp} = vC_2^{\perp} \subseteq vC_2 = vC$$

olduğu görülür. Bu sebepten dolayı $C_1^{\perp} \subseteq C_1$ ve $C_2^{\perp} \subseteq C_2$ dir.Sonuç 3.5.1'den $x^n - 1$ polinomu $\upsilon_1^R(x)\upsilon_1(x)$ ve $\upsilon_2^R(x)\upsilon_2(x)$ tarafından sağdan bölünebilir.

Teorem 3.5.6. $C_1 = \langle u_1(x) \rangle$, $C_2 = \langle u_2(x) \rangle$ ve $u(x) = (1-v)u_1(x) + vu_2(x)$ olmak üzere $C = \langle u(x) \rangle$ kodu *R* üzerinde *n* uzunluğunda bir skew devirli kod olsun.

$$C^{\perp} \subset C \;\Leftrightarrow\; C_1^{\perp} \subset C_1 \text{ ve } C_2^{\perp} \subset C_2$$

dir.

Teorem 1.2.2.3 ve Teorem 3.5.5 kullanılarak kuantum kod elde edilebilir.

Teorem 3.5.7. $\mathbb{F}_q + v\mathbb{F}_q$ üzerinde *n* uzunluğunda p^k elemana sahip $C = (1-v)C_1 + vC_2$ skew devirli kodu olsun. Eğer $C^{\perp} \subseteq C$ ise $[[2n, 2k-2n, min\{d(C_1), d(C_2)\}]]$ parametrelerine sahip bir kuantum kod vardır.

3.6. Hesaplama Sonuçları

Örnek 3.6.1. $n = 14$ için $x^{14} - 1$ polinomu $\mathbb{F}_4$ üzerinde aşağıdaki gibi çarpanlarına ayrılır:

$$(x+w^2)(x+w)(x^3+x^2+x+w^2)(x^3+wx^2+w^2x+w)(x^3+w^2x^2+w^2x+w^2)(x^3+x^2+x+w).$$

[14,11,3] parametrelerine sahip C_1 ve C_2 skew devirli kodların üreteç polinomları sırası ile $u_1(x) = x^3 + x^2 + x + w$ ve $u_2(x) = x^3 + wx^2 + w^2x + w$ olsun. Bu durumda *C* kodu uzunluğu 14, Lee uzaklığı 3 ve eleman sayısın 4^{22} olan bir koddur. Ayrıca bu kodu $\mathbb{F}_4$ üzerindeki Gray görüntüsü bir [28,22,3] koddur.

$$\upsilon_1(x) = x^{11} + x^{10} + wx^8 + wx^6 + x^5 + w^2x^4 + x^3 + x^2 + x + w^2,$$

$$\upsilon_1^R(x) = wx^{11} + x^{10} + x^9 + x^8 + wx^7 + x^6 + w^2x^5 + w^2x^3 + x + 1$$

ve

$$\upsilon_2(x) = x^{11} + w^2x^{10} + w^2x^9 + w^2x^8 + x^7 + w^2x^6 + wx^5 + wx^3 + w^2x + w^2,$$

$$\upsilon_2^R(x) = wx^{11} + w^2x^{10} + wx^8 + wx^6 + wx^5 + x^4 + wx^3 + w^2x^2 + wx + 1.$$

olsun. Burada $\upsilon_1^R(x)\upsilon_1(x)$ ve $\upsilon_2^R(x)\upsilon_2(x)$ polinomlarının $x^{14} - 1$'i sağdan böldüğü kolayca görülebilir. Sonuç 3.5.1'den dolayı $C_1^{\perp} \subseteq C_1$ ve $C_2^{\perp} \subseteq C_2$ dir.

Teorem 3.5.7'den dolayı $C^{\perp} \subseteq C$ dir. Dolayısıyla [[28, 16, 3]] parametreli kuantum kod inşa edilebilir.

Örnek 3.6.2. $n = 6$ için $x^6 - 1$ polinomu $\mathbb{F}_9$ üzerinde aşağıdaki gibi çarpanlarına ayrılır:

$$x^6 - 1 = (x + w^6)^2 (x + w^2)^2 (x + 1)(x + 2).$$

[6,5,2] parametrelerine sahip C_1 ve C_2 skew devirli kodların üreteç polinomları sırası ile $u_1(x) = x$ ve $u_2(x) = x + w^6$ olsun. Bu durumda *C* kodu uzunluğu 6, Lee uzaklığı 2 ve eleman sayısın 9^{10} olan bir koddur. Ayrıca bu kodu $\mathbb{F}_9$ üzerindeki Gray görüntüsü bir [12,10,2] koddur.

$$\upsilon_1(x) = x^5 + 2x^4 + x^3 + 2x^2 + x + 2,$$

$$\upsilon_1^R(x) = 2x^5 + x^4 + 2x^3 + x^2 + 2x + 1,$$

ve

$$\upsilon_2(x) = x^5 + w^6 x^4 + x^3 + w^6 x^2 + x + w^6,$$

$$\upsilon_2^R(x) = w^2 x^5 + x^4 + w^2 x^3 + x^2 + w^2 x + 1.$$

olsun. Burada $\upsilon_1^R(x)\upsilon_1(x)$ ve $\upsilon_2^R(x)\upsilon_2(x)$ polinomlarının $x^6 - 1$'i sağdan böldüğü kolayca görülebilir. Sonuç 3.5.1'den dolayı $C_1^{\perp} \subseteq C_1$ ve $C_2^{\perp} \subseteq C_2$ dir. Teorem 3.5.7'den dolayı $C^{\perp} \subseteq C$ dir. Dolayısıyla [[12, 8, 2]]. parametreli kuantum kod inşa edilebilir.

$\mathbb{F}_4 + v\mathbb{F}_4$ ve $\mathbb{F}_9 + v\mathbb{F}_9$ üzerindeki skew devirli kodlardan elde edilen kuantum kod parametreleri sırası ile Tablo 1 ve Tablo 2 de verilmiştir. Tablodaki sonuçlar hesaplanırken $a \in \mathbb{F}_4$ ve $b \in \mathbb{F}_9$ olmak üzere $\mathbb{F}_4$ ve $\mathbb{F}_9$ üzerindeki σ otomorfizması sırası ile $\sigma(a) = a^2$ ve $\sigma(b) = b^3$ olarak tanımlanmıştır. Kolaylık olması açısından üreteç polinomların sadece katsayılar *x*'in azalan derecesine göre yazılmıştır. Örneğin; $u_1(x) = x^3 + x^2 + x + w$ polinomu $111w$ olarak gösterilecektir.

Tablo 3.1. $\mathbb{F}_4$ üzerindeki kuantum kod parametreleri

n	**Üreteç polinom**	**[[*n,k,d*]]**
12	$g_1 = 1w0www$ $g_2 = 1w^2 0w^2 w^2 w^2$	[[24, 4, 4]]
16	$g_1 = 1w0w01$ $g_2 = 10w0w1$	[[32, 12, 4]]
24	$g_1 = 10w^2 0w1w^2 01w$ $g_2 = 10wwww^2 w0ww^2$	[[48, 12, 6]]
28	$g_1 = 11w^2 00w^2 0001w^2$ $g_2 = 10www^2 1w01ww$	[[56, 16, 6]]
30	$g_1 = g_2 = 1www^2 w10w^2 ww^2 w$	[[60, 20, 6]]
30	$g_1 = g_2 = 1ww^2 ww^2 1w^2 1w^2 ww011w$	[[60, 4, 7]]
40	$g_1 = 1w^2 + w^2 www^2 10ww00w^2$ $g_2 = 1ww1w111w^2 ww11$	[[80, 32, 4]]
60	$g_1 = g_2 = 1w^2 www01w^2 w^2 001w^2 0w10w0w$	[[120, 44, 8]]
60	$g_1 = g_2 = 1w^2 w0w^2 www1ww1ww^2 w^2$	[[120, 64, 6]]
70	$g_1 = 10w^2 1ww^2 ww$ $g_2 = 1w^2 ww10ww^2$	[[140,112, 4]]

Tablo 3.2. $\mathbb{F}_9$ üzerindeki kuantum kod parametreleri

n	**Üreteç polinom**	**[[*n,k,d*]]**
18	$g_1 = 1w21w^2 w^2 w^3 w^6$ $g_2 = 1ww^2 w^5 1w^3 w^6 w^7 1$	[[36, 6, 4]]
18	$g_1 = 12w^5 10w^2 w^5 w^6 w^6$ $g_2 = 1ww^2 w^5 1w^3 w^6 w^7 1$	[[36, 4, 6]]
24	$g_1 = 121w^3 w^6 2w^7 2w$ $g_2 = 1w^3 w^2 w^5 ww^7 w^2 0w^7$	[[48, 16, 6]]
26	$g_1 = g_2 = 1w^3 w^7 111211w^2 w22w^2 w^6 2w^3 w^6$	[[52, 16, 7]]
30	$g_1 = 1ww^2 w^7 w^6 1w^7 w^6$ $g_2 = 1w^5 w^2 2w1w^3 w^6$	[[60, 32, 4]]
32	$g_1 = 1w^7 0w^2 ww^5 w^3 1$ $g_2 = 122w21w^5 w^6$	[[64, 36, 5]]
40	$g_1 = 1w^7 20ww^7 0w^2 ww^6$ $g_2 = 1w^7 0w^2 w^7 w^6 w^3 0w^2 w^2$	[[80, 44, 4]]

BÖLÜM 4. $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3$ ÜZERİNDEKİ DEVİRLİ KODLARDAN KUANTUM KODLARIN ELDE EDİLMESİ

Kuantum hata düzeltme, kuantum bileşenleri arasındaki uyumun kaybolmasından dolayı meydana gelen hataları düzeltmek için kullanıldığından kuantum hesaplamalarında önemli bir rol oynar. İlk olarak kuantum hata düzelten kodların varlığı Shor [37] ve ondan bağımsız olarak Steane [38] tarafından gösterilmiştir. 1998 de Calderbank ve ark klasik hata düzelten kodları kullanarak kuantum kodların inşası için bir teori geliştirdikleri çalışma yayınlamışlardır [13]. Son yıllarda literatürde kuantum hata düzelten kodlar ile ilgili yapılan çalışmaların sayısında artış görülmüştür. Örneğin Qian tarafından $v^2=v$ olmak üzere $\mathbb{F}_2+v\mathbb{F}_2$ üzerindeki devirli kodlardan kuantum kod elde ettiği yeni bir metot geliştirmiştir [39]. Bunun yanısıra Kai ve Zhu Gray görüntüleri $\mathbb{F}_4$ üzerinde Hermityen metrik uzayına göre kendi üzerine ortogonal olan $\mathbb{F}_4+u\mathbb{F}_4$ üzerindeki devirli kodlardan kuantum kod inşa etmişlerdir [40]. Yin ve Ma $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ üzerindeki devirli kodlardan elde edilen kuantum kodların varlığı için gerekli olan şartı vermişlerdir [41]. Özen ve Güzeltepe tarafından Gauss tamsayıları üzerindeki klasik kodlar kullanılarak bazı kuantum kodlar elde edilmiştir [42]. Guenda ve ark. CSS inşa yapısını sonlu değişmeli Frobenius halkasına genişletmişlerdir [43]. Ayrıca Dertli ve ark. $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ üzerindeki devirli kodlardan kuantum kod elde etmişlerdir [44]. Ashraf ve Mohammad $\mathbb{F}_3+v\mathbb{F}_3$ üzerindeki devirli kodlardan kuantum kod inşa etmek için bir yapı ortaya koymuşlardır. Bu halka ise bu bölümde çalışılacak olan yeni $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3$ halkasını incelemek için motive kaynağı olmuştur. Bu halkanın bir avantajı $\mathbb{F}_3$ üzerinde daha çok kuantum parametresi elde etmeye olanak sağlayacaktır.

Bu bölümde konu ile alakalı temel tanım ve teoremler verildikten sonra uzaklığı koruyan Gray dönüşümü tanımlanmış ve $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3$ halkası üzerindeki lineer kodların Gray görüntüleri incelenmiştir. Ayrıca herhangi bir *n* uzunluğundaki devirli kodların yapısı araştırılmıştır. Teorem 1.1.14 kullanılarak $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3$ halkasındaki devirli kodların üreteç polinomları bulunmuş ve devirli kodların temel olarak üretildiği gösterilmiştir. Elde edilen bu sonuçlar kullanılarak, devirli kodun dualini içerme şartı verilmiş ve $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3$ halkası üzerindeki devirli kodlardan inşa edilen kuantum kod parametreleri belirlenmiştir. Son olarak elde edilen bu teorik sonuçlar kullanılarak, MAGMA cebirsel programlama sistemi [35] ile yazılan bilgisayar programı ile örneklendirilmiştir.

4.1. Temel Tanımlar ve Teoremler

$\mathbb{F}_3=\{0,1,2\}$ kümesi 3 elemanlı sonlu cisim ve *R*'de $u^2=1, v^2=1$ ve $uv=vu$ olmak üzere $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3=\{a+vb+uc+uvd : a,b,c,d\in\mathbb{F}_3\}$ halkasını temsil etsin. Bu halkanın özellikleri aşağıdaki gibidir.

i. 81 elemanlı karakteristiği 3 olan birimli ve değişmeli bir halkadır.

ii. Birimsel eleman sayısı 16 dır.

iii. 14 tane aşikar olmayan ideali vardır.

iv. Maksimal idealleri:

$<2+u+2v>,<2+v+uv>,<u+v+2uv>,<2u+2v+2uv>$ dir.

v. Temel ideal halkasıdır fakat zincir halkası değildir.

R^n'nin boştan farklı bir alt kümesi *C* olmak üzere eğer *C* kümesi R^n'nin bir *R*-alt modülü ise *C*'ye *R* üzerinde *n* uzunluğundaki lineer kod denir. τ bir devir öteleme operatörü olmak üzere eğer *C* lineer kodunun her $c=(c_0,c_1,\ldots,c_{n-1})$ elemanı için $\tau(c)=(c_{n-1},c_0,\ldots,c_{n-2})$ da *C* nin elemanı oluyor ise *C* lineer koduna *R* üzerinde bir devirli kod denir. Bu bölümde de kodun her bir elemanı polinom halkasının bir elemanı ile eşleştirilecektir.

$R[x]/\langle x^n-1\rangle$ bölüm halkası R_n olmak üzere

$$\phi: R^n \to R_n$$
$$c=(c_0,c_1,\ldots,c_{n-1}) \to c_0+c_1x+\ldots+c_{n-1}x^{n-1}=c(x)$$

şeklinde bir dönüşüm ile bu gerçekleştirilebilir.

4.2. $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3$ Üzerindeki Lineer Kodlar

R'deki herhangi bir eleman $a,b,c,d\in\mathbb{F}_3$ olmak üzere $a+vb+uc+uvd\in R$ olarak yazılabilir. R halkasından $\mathbb{F}_3^4$ yapısına

$$\psi: R \to \mathbb{F}_3^4$$
$$a+vb+uc+uvd \to (a+b+c+d, a-b+c-d, a+b-c-d, a-b-c+d)$$

şeklinde bir Gray dönüşüm tanımlansın.

Bu dönüşüm R^n'den $\mathbb{F}_3^{4n}$'yapısına $i=1,\cdots,n$ için $r_i=a_i+vb_i+uc_i+uvd_i\in R$ ve $\alpha_{1i}=a_i+b_i+c_i+d_i, \alpha_{2i}=a_i-b_i+c_i-d_i, \alpha_{3i}=a_i+b_i-c_i-d_i, \alpha_{4i}=a_i-b_i-c_i+d_i$ olmak üzere

$$(r_1,r_2,\cdots r_n)\to(\alpha_{11},\alpha_{21},\alpha_{31},\alpha_{41},\cdots,\alpha_{1n},\alpha_{2n},\alpha_{3n},\alpha_{4n})$$

şeklinde genişletilebilir. $x\in R$ elemanı için Lee ağırlık $w_L(x)=w_H(\psi(x))$ olarak tanımlanır. Ayrıca $x,y\in R$ için Lee uzaklıkta $d_L(x,y)=w_L(x-y)$ ile tanımlıdır.

Teorem 4.2.1. Gray dönüşüm (R^n, Lee uzaklık)'tan ($\mathbb{F}_3^{4n}$, Hamming uzaklık)'a uzaklık koruyan lineer bir dönüşümdür.

İspat. $x_1,x_2\in R$ve $\lambda\in\mathbb{F}_3$ için $\psi(x_1+x_2)=\psi(x_1)+\psi(x_2)$ ve $\psi(\lambda x_1)=\lambda\psi(x_1)$ olduğundan ψ lineerdir. Şimdi de ψ'nin uzaklığı koruduğu gösterilsin. Tanımdan dolayı aşağıdaki eşitlik elde edilir.

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

Teorem 4.2.2. Eğer C , R üzerinde $|C|=3^k$ elemana sahip n uzunluğunda bir lineer kod ise $\psi(C)$ de $\mathbb{F}_3$ üzerinde $[4n,k,d_H]$ parametrelerine sahip bir üçlü lineer koddur.

İspat. Gray dönüşüm tanımından ve Teorem 4.2.1'den dolayı R üzerindeki n uzunluğundaki lineer bir kodun görüntüsü $\mathbb{F}_3$ üzerinde $4n$ uzunluğunda lineer kod olacaktır. Ayrıca bu dönüşüm birebir olacağından $|\psi(C)|=3^k$ olup $\mathbb{F}_3$ üzerinde k boyuta sahiptir.

Teorem 4.2.3. C kodu kendi üzerine ortogonal ise $\psi(C)$ de kendi üzerine ortogonaldir.

İspat. C kodu kendi üzerine ortogonal ve $\alpha=a+vb+uc+uvd$, $\beta=x+vy+uz+uvt\in C$ olsun. C kodu kendi üzerine ortogonal olduğundan

$$\alpha.\beta=ax+by+cz+dt+v(ay+bx+ct+dz)+u(az+bt+cx+dy)+uv(at+bz+cy+dx)=0$$

dır. Yani

$$ax+by+cz+dt=(ay+bx+ct+dz)=(az+bt+cx+dy)=(at+bz+cy+dx)=0$$

elde edilir. Diğer taraftan

$$\psi(\alpha).\psi(\beta)=(a+b+c+d,a-b+c-d,a+b-c-d,a-b-c+d)(x+y+z+t,x-y+z-t,x+y-z-t,x-y-z+t)=0$$

dır. Dolayısıyla $\psi(C)$ de kendi üzerine ortogonaldir.

Şimdi R halkasındaki lineer kodların yapısı incelenecektir. Bunun için aşağıdaki tanımlara ihtiyaç olacaktır.

A_1,A_2,A_3,A_4 lineer kodlar olmak üzere

$$A_1\oplus A_2\oplus A_3\oplus A_4=\{a_1+a_2+a_3+a_4:a_i\in A_i;1\le i\le 4\}$$

$$A_1\otimes A_2\otimes A_3\otimes A_4=\{(a_1,a_2,a_3,a_4):a_i\in A_i;1\le i\le 4\}$$

kümeler tanımlansın.

Tanım 4.2.1. *R* üzerindeki bir *C* lineer kodu için

$$C_1 = \{x + y + z + t \in \mathbb{F}_3 \mid x + vy + uz + uvt \in C\}$$
$$C_2 = \{x - y + z - t \in \mathbb{F}_3 \mid x + vy + uz + uvt \in C\}$$
$$C_3 = \{x + y - z - t \in \mathbb{F}_3 \mid x + vy + uz + uvt \in C\}$$
$$C_4 = \{x - y - z + t \in \mathbb{F}_3 \mid x + vy + uz + uvt \in C\}$$

kümeleri tanımlanır.

Teorem 4.2.4. *C* kodu *R* üzerinde *n* uzunluğunda bir lineer kod olsun. Bu durumda $\psi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ ve $|C| = |C_1|.|C_2|.|C_3|.|C_4|$ dir.

İspat. Herhangi bir $(x_1,\ldots,x_n,y_1,\ldots,y_n,z_1,\ldots,z_n,t_1,\ldots,t_n) \in \psi(C)$ için $1 \le i \le n$ olmak üzere $c_i = x_i + y_i + z_i + t_i + v(x_i - y_i + z_i - t_i) + u(x_i + y_i - z_i - t_i) + uv(x_i - y_i - z_i + t_i)$ olsun. ψ birebir ve örten olduğundan $c = (c_1, c_2, \ldots, c_n) \in C$ dir. C_1, C_2, C_3, C_4 tanımından dolayı

$$(x_1, x_2 \ldots, x_n) \in C_1, (y_1, y_2, \ldots, y_n) \in C_2, (z_1, z_2, \ldots, z_n) \in C_3, (t_1, t_2, \ldots, t_n) \in C_4$$

elde edilir. Buradan görülür ki $(x_1,\ldots,x_n,y_1,\ldots,y_n,z_1,\ldots,z_n,t_1,\ldots,t_n) \in C_1 \otimes C_2 \otimes C_3 \otimes C_4$ dir. Dolayısıyla $\psi(C) \subseteq C_1 \otimes C_2 \otimes C_3 \otimes C_4$ sonucuna varılır.

Diğer taraftan $x = (x_1, x_2 \ldots, x_n) \in C_1, y = (y_1, y_2, \ldots, y_n) \in C_2$, $z = (z_1, z_2, \ldots, z_n) \in C_3$, $t = (t_1, t_2, \ldots, t_n) \in C_4$ olmak üzere

$$(x_1,\ldots,x_n,y_1,\ldots,y_n,z_1,\ldots,z_n,t_1,\ldots,t_n) \in C_1 \otimes C_2 \otimes C_3 \otimes C_4$$

olsun. $p_i, q_i, r_i, s_i \in F_3$ olmak üzere $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n)$ $c = (c_1, c_2, \ldots, c_n)$, $d = (d_1, d_2, \ldots, d_n) \in C$ elemanları

$$a_i = x_i + (1 + 2v + u + 2uv)\, p_i$$
$$b_i = y_i + (1 + v + u + uv) q_i$$
$$c_i = z_i + (1 + 2v + 2u + uv) r_i$$
$$d_i = t_i + (1 + v + 2u + 2uv) s_i$$

olacak şekilde vardır.

C lineer olduğundan

$$c = (1+v+u+uv)a + (1+2v+u+2uv)b + (1+v+2u+2uv)c + (1+2v+2u+uv)d$$
$$= x+y+z+t+(x-y+z-t)v+(x+y-z-t)u+(x-y-z+t)uv$$

eşitliği sağlanır. Buradan da görülür ki $\psi(C) = (x,y,z,t) \in \psi(C)$ dir. Dolayısıyla $C_1 \otimes C_2 \otimes C_3 \otimes C_4 \subseteq \psi(C)$ dir. Sonuç olarak $\psi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ elde edilir. $\psi(C)$ birebir ve örten olduğundan

$$|C| = |\psi(C)| = |C_1 \otimes C_2 \otimes C_3 \otimes C_4| = |C_1|.|C_2|.|C_3|.|C_4|$$

sonucuna da varılır.

İlerleyen bölümlerde λ_1, λ_2, λ_3, λ_4 sembolleri sırasıyla $(1+v+u+uv)$, $(1+2v+u+2uv)$, $(1+v+2u+2uv)$, $(1+2v+2u+uv)$ elemanlarını temsil edecektir.

Teorem 1.1.14'den dolayı aşağıdaki sonuç elde edilebilir.

Sonuç 4.2.1. Eğer $\psi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$, ise $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4$.

Lemma 4.2.1. $i = 1,2,3,4$ için $\mathbb{F}_3$ üzerindeki C_i lineer kodların üreteç matrisler G_i olmak üzere R üzerindeki C lineer kodunun üreteç matrisi

$$\begin{pmatrix} \lambda_1 G_1 \\ \lambda_2 G_2 \\ \lambda_3 G_3 \\ \lambda_4 G_4 \end{pmatrix}$$

dir.

İspat. $\mathbb{F}_3$ üzerindeki C_i lineer kodların üreteç matrisler G_i ise $\psi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ lineer kodunun üreteç matrisi

$$\begin{pmatrix} G_1 & 0 & 0 & 0 \\ 0 & G_2 & 0 & 0 \\ 0 & 0 & G_3 & 0 \\ 0 & 0 & 0 & G_4 \end{pmatrix}$$

Teorem 4.2.4'den dolayı C nin üreteç matrisi

$$\begin{pmatrix} \lambda_1 G_1 \\ \lambda_2 G_2 \\ \lambda_3 G_3 \\ \lambda_4 G_4 \end{pmatrix}$$

olduğu görülür.

Lemma 4.2.2. C kodu R üzerinde lineer kod olmak üzere

$$d_H(C) = d_L(C) = min\{d(C_1), d(C_2), d(C_3), d(C_4)\}$$

dir.

İspat. ψ uzaklık koruyan bir dönüşüm olduğundan

$$d_L(C) = d_H(\psi(C)) = d_H(C_1 \otimes C_2 \otimes C_3 \otimes C_4) = min\{d(C_1), d(C_2), d(C_3), d(C_4)\}$$

dir.

4.3. $\mathbb{F}_3 + v\mathbb{F}_3 + u\mathbb{F}_3 + uv\mathbb{F}_3$ Üzerindeki Devirli Kodlar

Bu bölümde R halkası üzerindeki devirli kodların yapısı ve üreteç polinomları belirlenecektir.

Teorem 4.3.1. $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4$ kodu R üzerinde n uzunluğunda bir lineer kod olsun. C'nin R üzerinde n uzunluğunda devirli kod olması için gerek ve yeter şart $i = 1,2,3,4$ için C_i kodlarının $\mathbb{F}_3$ üzerinde n uzunluğunda devirli kod olmasıdır.

İspat. $j = 1,\ldots,n$ için $c_j = \lambda_1 x_j + \lambda_2 y_j + \lambda_3 z_j + \lambda_4 t_i$ olmak üzere $c = (c_1, c_2, \ldots, c_n) \in C$ ve $x = (x_1, \ldots, x_n) \in C_1, y = (y_1, \ldots, y_n) \in C_2, z = (z_1, \ldots, z_n) \in C_3, t = (t_1, \ldots, t_n) \in C_4$ .olsun. $i = 1,2,3,4$ için C_i kodları $\mathbb{F}_3$ üzerinde n uzunluğunda devirli kod olduğundan $\tau(x) = (x_n, x_1, \ldots, x_{n-1}) \in C_1$, $\tau(y) = (y_n, y_1, \ldots, y_{n-1}) \in C_2$, $\tau(z) = (z_n, z_1, \ldots, z_{n-1}) \in C_3$, $\tau(t) = (t_n, t_1, \ldots, t_{n-1}) \in C_4$ dir.

Buradan dikkat edilmelidir ki

$$\tau(c) = (c_n, c_1, \ldots, c_{n-1}) = \lambda_1\tau(x) + \lambda_2\tau(y) + \lambda_3\tau(z) + \lambda_4\tau(t) \in C$$

elde edilir. Yani bu da *C*'nin *R* üzerinde *n* uzunluğunda devirli kod olduğu anlamına gelir.

Şimdi ise *R* üzerinde *n* uzunluğunda devirli kodun üreteç polinomu araştırılacaktır. Bunun için, $i = 1,2,3,4$ olmak üzere C_i kodları $\mathbb{F}_3$ üzerinde *n* uzunluğunda devirli kod olduğundan bu kodların üreteç yapısından yararlanılacaktır.

Teorem 4.3.2. $\mathrm{C} = \lambda_1\mathrm{C}_1 \oplus \lambda_2\mathrm{C}_2 \oplus \lambda_3\mathrm{C}_3 \oplus \lambda_4\mathrm{C}_4$ kodu R halkası üzerinde *n* uzunluğunda bir devirli kod olsun. $\mathbb{F}_3[x]$ üzerindeki $g_i(x)$ polinomları C_i devirli kodlarının üreteç polinomları olmak üzere $\mathrm{C} = \langle \lambda_1 g_1(x), \lambda_2 g_2(x), \lambda_3 g_3(x), \lambda_4 g_4(x) \rangle$ şeklinde üretilir. Ayrıca $|C| = 3^{4n - \sum_{i=1}^{4} d^o(g_i(x))}$ dır.

İspat. $C_i = \langle g_i(x) \rangle$ ve $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4$ olsun.

$$C = \{c(x) = \lambda_1 g_1 s_1 + \lambda_2 g_2 s_2 + \lambda_3 g_3 s_3 + \lambda_4 g_4 s_4 \mid s_i \in \mathbb{F}_3[x]\}$$

kümesi tanımlansın. Açıkça görülür ki

$$C \subseteq \langle \lambda_1 g_1(x), \lambda_2 g_2(x), \lambda_3 g_3(x), \lambda_4 g_4(x) \rangle \qquad \ldots\ldots\ldots\ldots\ldots(1)$$

dir. Diğer taraftan $d(x) \in \langle \lambda_1 g_1(x), \lambda_2 g_2(x), \lambda_3 g_3(x), \lambda_4 g_4(x) \rangle$ olsun. $1 \le i \le 4$ için $k_i(x) \in R[x]$ elemanları

$$d(x) = \lambda_1 g_1(x) k_1(x) + \lambda_2 g_2(x) k_2(x) + \lambda_3 g_3(x) k_3(x) + \lambda_4 g_4(x) k_4(x)$$

olacak şekilde vardır. Ayrıca $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ elemanlarının oluşturdukları idealler incelenirse $\lambda_1 s_1(x) = \lambda_1 k_1(x)$, $\lambda_2 s_2(x) = \lambda_2 k_2(x)$, $\lambda_3 s_3(x) = \lambda_3 k_3(x)$, $\lambda_4 s_4(x) = \lambda_4 k_4(x)$ olacak şekilde $s_i(x) \in F_3[x]$ elemanları bulunabileceği görülür. Buradan da

$$\langle \lambda_1 g_1(x), \lambda_2 g_2(x), \lambda_3 g_3(x), \lambda_4 g_4(x) \rangle \subseteq C \qquad \ldots\ldots\ldots\ldots\ldots(2)$$

elde edilir. (1) ve (2)'den $C = \langle \lambda_1 g_1(x), \lambda_2 g_2(x), \lambda_3 g_3(x), \lambda_4 g_4(x) \rangle$ sonucuna varılır. Teorem 4.2.4'den $|C| = |C_1| . |C_2| . |C_3| . |C_4|$ olduğu bilindiğine göre $|C| = 3^{4n - \sum_{i=1}^{4} d^o(g_i(x))}$ olduğu söylenebilir.

Teorem 4.3.3. *C* kodu R halkası üzerinde *n* uzunluğunda bir devirli kod olsun. $g(x) = \lambda_1 g_1(x) + \lambda_2 g_2(x) + \lambda_3 g_3(x) + \lambda_4 g_4(x)$ olmak üzere C = $\langle g(x) \rangle$ olacak şekilde bir $g(x)$ polinomu vardır ve $g(x) | x^n - 1$ dir.

İspat. $g(x) = \lambda_1 g_1(x) + \lambda_2 g_2(x) + \lambda_3 g_3(x) + \lambda_4 g_4(x)$ olsun ve Teorem 4.3.2'den dolayı C = $\langle \lambda_1 g_1(x), \lambda_2 g_2(x), \lambda_3 g_3(x), \lambda_4 g_4(x) \rangle$ olduğu bilinmektedir. Buradan açıkça görülür ki $\langle g(x) \rangle \subseteq C$ .dir. Diğer taraftan $\lambda_1 g(x) = \lambda_1 g_1(x)$, $\lambda_2 g(x) = \lambda_2 g_2(x)$, $\lambda_3 g(x) = \lambda_3 g_3(x)$, $\lambda_4 g(x) = \lambda_4 g_4(x)$ olduğundan $C \subseteq \langle g(x) \rangle$ .elde edilir ve $C = \langle g(x) \rangle$ sonucuna varılır. $1 \le i \le 4$ için $g_i(x) | x^n - 1$ olduğundan $r_i(x) \in R[x] / \langle x^n - 1 \rangle$ polinomları

$$x^n - 1 = g_1(x) r_1(x) = g_2(x) r_2(x) = g_3(x) r_3(x) = g_4(x) r_4(x)$$

olacak şekilde vardır. Bu eşitlikleri kullanarak

$$\begin{aligned} & g(x)[\lambda_1 r_1(x) + \lambda_2 r_2(x) + \lambda_3 r_3(x) + \lambda_4 r_4(x)] \\ &= \lambda_1 g(x) r_1(x) + \lambda_2 g(x) r_2(x) + \lambda_3 g(x) r_3(x) + \lambda_4 g(x) r_4(x) \\ &= \lambda_1 g_1(x) r_1(x) + \lambda_2 g_2(x) r_2(x) + \lambda_3 g_3(x) r_3(x) + \lambda_4 g_4(x) r_4(x) \\ &= (x^n - 1)(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4) \\ &= x^n - 1 \end{aligned}$$

elde edilir ki buradan da $g(x) | x^n - 1$ olduğu görülür.

Sonuç 4.3.1. $R[x] / \langle x^n - 1 \rangle$ in her ideli temel idealdir.

Teorem 4.3.4. ψ Gray dönüşüm τ devirsel öteleme operatörü olmak üzere $\psi\tau = \tau^4\psi$ .dir.

İspat. $i = 1, \cdots, n$ için $r_i = a_i + vb_i + uc_i + uvd_i \in R$ ve $\alpha_{1i} = a_i + b_i + c_i + d_i$, $\alpha_{2i} = a_i - b_i + c_i - d_i$, $\alpha_{3i} = a_i + b_i - c_i - d_i$, $\alpha_{4i} = a_i - b_i - c_i + d_i$ olsun.

$$\tau(r_1, r_2, \cdots r_n) = (r_n, r_1, \cdots r_{n-1})$$

olup

$$\psi(\tau(r_1, r_2, \cdots r_n)) = \psi((r_n, r_1, \cdots r_{n-1})) = (\alpha_{1n}, \alpha_{2n}, \alpha_{3n}, \alpha_{4n}, \cdots, \alpha_{1n-1}, \alpha_{2n-1}, \alpha_{3n-1}, \alpha_{4n-1})$$

elde edilir.

Diğer taraftan

$$\psi((r_1, r_2, \cdots r_n)) = (\alpha_{11}, \alpha_{21}, \alpha_{31}, \alpha_{41}, \cdots, \alpha_{1n}, \alpha_{2n}, \alpha_{3n}, \alpha_{4n})$$

olup

$$\begin{aligned}\tau^4(\psi((r_1, r_2, \cdots r_n))) &= \tau^4(\alpha_{11}, \alpha_{21}, \alpha_{31}, \alpha_{41}, \cdots, \alpha_{1n}, \alpha_{2n}, \alpha_{3n}, \alpha_{4n}) \\ &= (\alpha_{1n}, \alpha_{2n}, \alpha_{3n}, \alpha_{4n}, \cdots, \alpha_{1n-1}, \alpha_{2n-1}, \alpha_{3n-1}, \alpha_{4n-1})\end{aligned}$$

elde edilir. Dolayısıyla $\psi\tau = \tau^4\psi$ dir.

Teorem 4.3.5. *C* kodu R halkası üzerinde *n* uzunluğunda bir devirli koddur ancak ve ancak $\psi(C)$, $\mathbb{F}_3$ üzerinde 4*n* uzunluğunda 4-yarı devirli koddur.

İspat. *C* kodu R halkası üzerinde *n* uzunluğunda bir devirli kod olsun yani $\tau(C) = C$ olsun. Teorem 4.3.4 kullanılarak $\tau^4(\psi(C)) = \varphi(\tau(C)) = \psi(C)$ elde edilir. Buradan da görülür ki $\psi(C)$ indeksi 4 olan F_3 üzerinde yarı devirli koddur.

Diğer taraftan $\psi(C)$ indeksi 4 olan $\mathbb{F}_3$ üzerinde yarı devirli kod olsun yani $\tau^4(\psi(C)) = \psi(C)$ olsun. Teorem 4.3.4 kullanılarak $\psi(\tau(C)) = \tau^4(\psi(C)) = \psi(C)$ elde edilir. ψ dönüşümü birebir olduğundan dolayı $\tau(C) = C$ olup *C*'nin devirli kod olduğu görülür.

4.4. $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+uv\mathbb{F}_3$ Halkası Üzerindeki Devirli Kodlardan Kuantum Kod Elde Etme

Teorem 4.4.1. $C=\lambda_1C_1\oplus\lambda_2C_2\oplus\lambda_3C_3\oplus\lambda_4C_4$ kodu R halkası üzerinde n uzunluğunda bir devirli kod olsun. Bu durumda $h_i(x)=x^n-1/g_i(x)$ ve $h_i^*(x)=x^{\deg(h_i(x))}h_i(x^{-1})$ olmak üzere

$$C^{\perp}=\left\langle \lambda_1h_1^*(x)+\lambda_2h_2^*(x)+\lambda_3h_3^*(x)+\lambda_4h_4^*(x)\right\rangle$$

şeklindedir. Ayrıca $|C^{\perp}|=3^{d^og_1(x)+d^og_2(x)+d^og_3(x)+d^og_4(x)}$ dir.

Aşağıdaki Lemma ile C devirli kodunun dikini içermesi için gerek ve yeter şartı verilmiştir.

Lemma 4.4.1. $g(x)$ üreteç polinomuna sahip C devirli kodunun dikini içermesi için gerek ve yeter şart

$$x^n-1\equiv 0(\mathrm{mod}\, g(x)g^*(x))$$

olmasıdır [13].

Teorem 4.4.2. $C=\left\langle \lambda_1g_1(x),\lambda_2g_2(x),\lambda_3g_3(x),\lambda_4g_4(x)\right\rangle$ kodu R halkası üzerinde n uzunluğunda bir devirli kod olsun. $C^{\perp}\subset C$ koşulunun sağlanması için gerek ve yeter şart $i=1,2,3,4$ olmak üzere $x^n-1\equiv 0(\mathrm{mod}\, g_i(x)g_i^*(x))$ olmasıdır.

İspat. $C=\left\langle \lambda_1g_1(x),\lambda_2g_2(x),\lambda_3g_3(x),\lambda_4g_4(x)\right\rangle$ kodu R halkası üzerinde n uzunluğunda bir devirli kod olsun. Lemma 4.4.1'den dolayı $C_i^{\perp}\subseteq C_i$ dir. Buradan da $\lambda_iC_i^{\perp}\subseteq\lambda_iC_i$ elde edilir. Dolayısıyla

$$\left\langle \lambda_1h_1^*(x)+\lambda_2h_2^*(x)+\lambda_3h_3^*(x)+\lambda_4h_4^*(x)\right\rangle\subseteq\left\langle \lambda_1g_1(x),\lambda_2g_2(x),\lambda_3g_3(x),\lambda_4g_4(x)\right\rangle$$

olup $C^{\perp}\subseteq C$ sağlanır.

Tersine, eğer $C^{\perp} \subseteq C$ ise

$$\lambda_1 C_1^{\perp} \oplus \lambda_2 C_2^{\perp} \oplus \lambda_3 C_3^{\perp} \oplus \lambda_4 C_4^{\perp} \subseteq \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4$$

$\lambda_i C_i = C \bmod \lambda_i$ olduğundan $C_i^{\perp} \subseteq C_i$ dir ve $i = 1,2,3,4$ .için $x^n - 1 \equiv 0 (\bmod g_i g_i^*)$ dir.

Sonuç 4.4.1. $\mathrm{C} = \lambda_1 \mathrm{C}_1 \oplus \lambda_2 \mathrm{C}_2 \oplus \lambda_3 \mathrm{C}_3 \oplus \lambda_4 \mathrm{C}_4$ R halkası üzerinde n uzunluğunda bir devirli kod olsun. $C^{\perp} \subset C$ koşulunun sağlanması için gerek ve yeter şart $i = 1,2,3,4$ olmak üzere $C_i^{\perp} \subset C_i$ olmasıdır.

Teorem 1.2.2.3 ve Sonuç 4.4.1'den aşağıdaki Teorem ortaya konabilir.

Teorem 4.4.3. $\mathrm{C} = \lambda_1 \mathrm{C}_1 \oplus \lambda_2 \mathrm{C}_2 \oplus \lambda_3 \mathrm{C}_3 \oplus \lambda_4 \mathrm{C}_4$ R halkası üzerinde n uzunluğunda 3^k elemanına ve d_L minimum uzaklığına sahip bir devirli kod olsun. Eğer $C^{\perp} \subset C$ ise $[[4n, 2k - 4n, d_L]]$ parametresine sahip quantum kod vardır.

Örnek 4.4.1. $n = 24$ olmak üzere $x^n - 1$'in $\mathbb{F}_3$ üzerinde çarpanlara ayrılışı

$$x^{24} - 1 = (x+1)^3 (x+2)^3 (x^2+1)^3 (x^2+x+2)^3 (x^2+2x+2)^3$$

şeklindedir.

$$g_1(x) = g_2(x) = g_3(x) = g_4(x) = x^8 + x^6 + 2x^5 + 2x^3 + 2x^2 + 2$$

polinomları için

$$g(x) = \lambda_1 g_1(x) + \lambda_2 g_2(x) + \lambda_3 g_3(x) + \lambda_4 g_4(x)$$

olmak üzere $C = \langle g(x) \rangle$ kodu R üzerinde n uzunluğunda bir devirli kod olsun. $i = 1,2,3,4$ için $g_i(x)$ polinomları $\mathbb{F}_3$ üzerinde [24,16,4] parametresine sahip devirli kod üretir. Lemma 4.2.2'den $d_L(C) = 4$ ve Teorem 4.3.2'den $|C| = 3^{64}$ dir. Ayrıca

$$g_1^*(x) = g_2^*(x) = g_3^*(x) = g_4^*(x) = 2x^8 + 2x^6 + 2x^5 + 2x^3 + x^2 + 1$$

olmak üzere $x^{24} - 1$ polinomu $i = 1,2,3,4$ için $g_i g_i^*$ ile bölünebilir. Bu yüzden Teorem 4.4.2'den dolayı $C^{\perp} \subseteq C$ dir. Teorem 4.4.3'den dolayı [[96,32,4]] kuantum kod parametresi elde edilebilir.

Tablo 4.1 $\mathbb{F}_3$ üzerinde kuantum kod parametreleri

n	Üreteç polinomlar	$[[n,k,d_L]]$
6	$g_1 = g_2 = x+1$ $g_3 = g_4 = x+2$	[[24,16,2]]
9	$g_1 = g_2 = g_3 = g_4 = x+2$	[[36,28,2]]
11	$g_1 = g_2 = x^5 + x^4 + 2x^3 + x^2 + 2$ $g_3 = g_4 = x^5 + 2x^3 + x^2 + 2x + 2$	[[44,4,5]]
15	$g_1 = g_2 = g_3 = g_4 = x+2$	[[60,52,2]]
18	$g_1 = g_2 = g_3 = g_4 = x+2$	[[72,64,2]]
21	$g_1 = g_2 = g_3 = x+2$ $g_4 = x+1$	[[84,76,2]]
22	$g_1 = g_2 = g_3 = g_4$ $= x^{10} + x^9 + x^8 + 2x^7 + 2x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + x + 2$	[[88,8,7]]
23	$g_1 = g_2 = g_3 = g_4$ $= x^{11} + x^{10} + x^9 + 2x^8 + 2x^7 + x^5 + x^3 + 2$	[[92,4,8]]
24	$g_1 = g_2 = g_3 = g_4 = x^5 + x^3 + 2x + 2$	[[96,56,3]]
30	$g_1 = g_2 = g_3 = x+2$ $g_4 = x^2 + 2$	[[120,110,2]]
35	$g_1 = g_2 = g_3 = g_4$ $= x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + x^7 + x^5 + 2x^4 + x^2 + 1$	[[140,44,5]]

BÖLÜM 5. $\mathbb{F}_2(\mathbb{F}_2+u\mathbb{F}_2)$ -DEVİRLİ KOD

Kodlama teorisindeki başlangıç çalışmaların genel olarak cisimler üzerinde olduğu, son yıllarda ise çalışmaların çeşitli halkalar üzerine genişletildiği daha önceki bölümlerde bahsedilmişti. Bu çalışmalarda lineer kodlar elemanları cisim ya da halkalardan olan tek bir alfabe kullanılarak elde edilmiştir. İlk olarak Brouwer ve ark. farklı iki alfabe üzerindeki kodları incelemiş ve bazı sınırlar vermişlerdir (45) [45]. Daha sonrasında ise bileşenleri ikili ve dörtlü alfabeden olan $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kod olarak adlandırılan yeni bir hata düzelten kod sınıfı Borges ve ark. tarafından incelenmiştir (46) [46]. Bu toplamsal kod hem ikili lineer kodun hem de dörtlü lineer kodun bir genelleştirilmesi olup son yıllarda birçok araştırmacı tarafından üzerinde çalışılan ve ilgi çeken bir konu haline gelmiştir (47), (48) [47, 48]. $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodları Aydoğdu ve ark. tarafından $\mathbb{Z}_2\mathbb{Z}_{2^s}$-toplamsal kodlarına genişletilmiştir (49) [49]. Ayrıca $\mathbb{Z}_2\mathbb{Z}_2[u]$-toplamsal kodları da Aydoğdu ve ark. tarafından çalışılmıştır [50]. Bu çalışmaların yanı sıra $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal devirli kodlar ve onların dualleri çalışılmıştır [51, 52].

Bu bölümde ise $\mathbb{F}_2\mathbb{F}_2[u]$-devirli kodu olarak adlandıracağımız devirli kodların yeni bir sınıfı incelenmiştir. Yeni bir Gray dönüşüm tanımlanmış ve bazı $\mathbb{F}_2\mathbb{F}_2[u]$-devirli kodların Gray görüntülerinden elde edilen ikili lineer optimal kod örnekleri verilmiştir.

5.1. Temel Tanımlar ve Teoremler

$\mathbb{F}_2 + u\mathbb{F}_2 = \{x+uy : x, y \in \mathbb{F}_2 \text{ ve } u^2 = 1\} = \{0,1,u,1+u\}$ halkası R ile gösterilsin. r ve s pozitif tamsayılar olmak üzere $r+s$ uzunluğundaki C kodun ilk r bileşeni $\mathbb{F}_2$ alfabesinden, son s bileşeni ise R alfabesinden olacak şekilde parçalanabiliyor ise buna $\mathbb{F}_2 R$-kodu denecektir. Şimdi bu şekilde tanımlanan kodun aslında $\mathbb{F}_2^r \times R^s$ 'nin bir R-alt modülü olarak tanımlanabildiği gösterilsin. İlk olarak $\mathbb{F}_2 R$ halkası

$$\mathbb{F}_2 R = \{(a,b) : a \in \mathbb{F}_2 \text{ ve } b \in R\}$$

olarak tanımlansın. bu halka bilinen toplama işlemine göre kapalı olmasına rağmen $u \in R$ skaleri ile çarpma işlemine göre kapalı değildir. Yani $\mathbb{F}_2 R$ halkası standart skaler ile çarpma işlemine göre R-modül olamaz. Bu halkayı R-modül yapmak ve cebirsel yapısını zenginleştirmek adına aşağıdaki gibi yeni bir skaler ile çarpma işlemi tanımlanabilir. Bunun için

$$\mu : R \to \mathbb{F}_2$$
$$x + uy \to x + y$$

dönüşümü tanımlansın. Yani $\mu(0) = \mu(1+u) = 0$ ve $\mu(1) = \mu(u) = 1$ dir. $\forall a+ub, c+ud \in R$ için

$$\begin{aligned}
\mu((a+ub)+(x+uy)) &= \mu((a+x+u(b+y)) \\
&= a+x+b+y \\
&= (a+b)+(x+y) \\
&= \mu(a+ub)+\mu(x+uy) \\
\mu((a+ub)(x+uy)) &= \mu(ax+by+u(ay+bx)) \\
&= ax+by+ay+bx \\
&= (a+b)(x+y) \\
&= \mu(a+ub)\mu(x+uy)
\end{aligned}$$

olduğundan μ dönüşümü bir halka homomorfizmasıdır. Şimdi bu homomorfizma yardımı ile herhangi bir $(a,b) \in \mathbb{F}_2 R$ ve $d \in R$ için skaler çarpım

$$d * (a,b) = (\mu(d).a, d.b)$$

şeklinde tanımlanabilir.

Bu çarpım $d \in R$ ve $c = (a_0, a_1, \cdots, a_{r-1} \mid b_0, b_1, \cdots, b_{s-1}) \in \mathbb{F}_2^r \times R^s$ olmak üzere

$$\begin{aligned} d * c &= d * (a_0, a_1, \cdots, a_{r-1} \mid b_0, b_1, \cdots, b_{s-1}) \\ &= (\mu(d).a_0, \mu(d).a_1, \cdots, \mu(d).a_{r-1} \mid d.b_0, d.b_1, \cdots, d.b_{s-1}) \end{aligned}$$

şeklinde genişletilebilir.

Lemma 5.1.1. $\mathbb{F}_2^r \times R^s$ yukarıda tanımlanan skaler ile çarpma işlemine göre bir R-modüldür.

İspat. $\forall \alpha, \beta \in R$ ve $\forall (a \mid b), (c \mid d) \in \mathbb{F}_2^r \times R^s$ için

i. $$\begin{aligned} \alpha * [(a \mid b) + (c \mid d)] &= \alpha * (a + c \mid b + d) \\ &= (\mu(\alpha)(a + c) \mid \alpha(b + d)) \\ &= (\mu(\alpha)a \mid \alpha b) + (\mu(\alpha)c \mid \alpha d) \\ &= \alpha * (a \mid b) + \alpha * (c \mid d) \end{aligned}$$

ii. $$\begin{aligned} (\alpha + \beta) * (a \mid b) &= (\mu(\alpha + \beta)a \mid (\alpha + \beta)b) \\ &= (\mu(\alpha)a + \mu(\beta)a \mid \alpha b + \beta b) \\ &= (\mu(\alpha)a \mid \alpha b) + (\mu(\beta)a \mid \beta b) \\ &= \alpha * (a \mid b) + \beta * (a \mid b) \end{aligned}$$

iii. $$\begin{aligned} \alpha * [\beta * (a \mid b)] &= \alpha * [\mu(\beta)a \mid \beta b)] \\ &= (\mu(\alpha)\mu(\beta)a \mid \alpha\beta b) \\ &= (\mu(\alpha\beta)a \mid \alpha\beta b) \\ &= (\alpha\beta) * (a \mid b) \end{aligned}$$

iv. $1_R * (a \mid b) = (\mu(1_R)a \mid b) = (a \mid b)$

şartları sağlandığından Tanım 1.1.35'den dolayı $\mathbb{F}_2^r \times R^s$ tanımlanan skaler ile çarpma işlemine göre bir *R*-modüldür.

Tanım 5.1.1. Eğer $\mathbb{F}_2^r \times R^s$ 'nin herhangi bir *C* alt kümesi $\mathbb{F}_2^r \times R^s$ 'nin bir *R*-alt modülü ise *C*'ye $\mathbb{F}_2 R$-lineer kod denir.

Not. Kolayca görülür ki $r=0$ ise R üzerinde bir lineer kod, $s=0$ ise F_2 üzerinde bir lineer koddur.

Tanım 5.1.2. Herhangi bir $c=(a_0,a_1,\cdots,a_{r-1}\,|\,b_0,b_1,\cdots,b_{s-1})\in\mathbb{F}_2^r\times R^s$ elemanı için τ devirsel öteleme operatörü

$$\tau(c)=(a_{r-1},a_0,\cdots,a_{r-2}\,|\,b_{s-1},b_0,\cdots,b_{s-2})$$

olarak tanımlansın. Eğer C, $\mathbb{F}_2R$-lineer kodu τ devir operatörü altında sabit kalıyor ise yani $\tau(C)=C$ oluyor ise C'ye $\mathbb{F}_2R$-devirli kod denir.

Devirli kod çalışmalarında, kod sözleri polinomlar ile temsil ederek koda daha fazla cebirsel özellik kazandırmak en genel ve temel yöntemdir. Burada da $\mathbb{F}_2^r\times R^s$ halkasının elemanları ile $R_{r,s}=\mathbb{F}_2[x]/\langle x^r-1\rangle\times R[x]/\langle x^s-1\rangle$ halkasının elemanları arasında yapılacak olan 1-1 eşleme

$$(a_0,\cdots,a_{r-1}\,|\,b_0,\cdots,b_{s-1})\to(a_0+a_1x+\cdots+a_{r-1}x^{r-1}\,|\,b_0+b_1x+\cdots+b_{s-1}x^{s-1})=(a(x)\,|\,b(x))$$

şeklinde verilebilir.

Tanım 5.1.3. $d(x)=d_0+d_1x+\cdots d_tx^t\in R[x]$ ve $(a(x)\,|\,b(x))\in R_{r,s}$ elemanları için

$$\mu(d(x))=\mu(d_0)+\mu(d_1)x+\cdots\mu(d_t)x^t\in R[x]$$

olmak üzere

$$d(x)*(a(x)\,|\,b(x))=(\mu(d(x).a(x)\,|\,d(x).b(x))$$

çarpımı tanımlanabilir.

Teorem 5.1.1 $R_{r,s}=\mathbb{F}_2[x]/\langle x^r-1\rangle\times R[x]/\langle x^s-1\rangle$ halkası yukarıda tanımlanan çarpma işlemine göre $R[x]$ -modüldür.

İspat. $\forall\alpha(x),\beta(x)\in R[x]$ ve $\forall(a(x)\,|\,b(x)),(c(x)\,|\,d(x))\in R_{r,s}$ için

i. $\alpha*[(a\,|\,b)+(c\,|\,d)]=\alpha*(a+c\,|\,b+d)$
$=(\mu(\alpha)(a+c)\,|\,\alpha(b+d))$
$=(\mu(\alpha)a\,|\,\alpha b)+(\mu(\alpha)c\,|\,\alpha d)$
$=\alpha*(a\,|\,b)+\alpha*(c\,|\,d)$

ii. $(\alpha+\beta)*(a\,|\,b)=(\mu(\alpha+\beta)a\,|\,(\alpha+\beta)b)$
$=(\mu(\alpha)a+\mu(\beta)a\,|\,\alpha b+\beta b)$
$=(\mu(\alpha)a\,|\,\alpha b)+(\mu(\beta)a\,|\,\beta b)$
$=\alpha*(a\,|\,b)+\beta*(a\,|\,b)$

iii. $\alpha*[\beta*(a\,|\,b)]=\alpha*[\mu(\beta)a\,|\,\beta b)]$
$=(\mu(\alpha)\mu(\beta)a\,|\,\alpha\beta b)$
$=(\mu(\alpha\beta)a\,|\,\alpha\beta b)$
$=(\alpha\beta)*(a\,|\,b)$

iv. $1_{R[x]}*(a\,|\,b)=(\mu(1_{R[x]})a\,|\,b)=(a\,|\,b)$

şartları sağlandığından Tanım 1.1.35'den dolayı $R_{r,s}$ tanımlanan skaler ile çarpma işlemine göre bir $R[x]$ -modüldür. İspat yapılırken yazımda kolaylık olması açısından herhangi bir $f(x)$ polinomu f olarak gösterilmiştir.

Şimdi $\mathbb{F}_2R$-devirli kodun polinom olarak tanımı verilsin.

Tanım 5.1.4. $R_{r,s}$ 'nin boştan farklı bir alt kümesi C olmak üzere eğer C kümesi $R_{r,s}$ 'nin bir alt grubu ve herhangi bir $\alpha\in R$ ve her $c(x)=(a_0+a_1x+\cdots+a_{r-1}x^{r-1}\,|\,b_0+b_1x+\cdots+b_{s-1}x^{s-1})\in C$ için

$\alpha x*(a(x)\,|\,b(x))=\alpha x*(a_0+a_1x+\cdots+a_{r-1}x^{r-1}\,|\,b_0+b_1x+\cdots+b_{s-1}x^{s-1})$
$=(\mu(\alpha)(a_{r-1}+a_0x+\cdots+a_{r-2}x^{r-1})\,|\,\alpha(b_{s-1}+b_0x+\cdots+b_{s-2}x^{s-1}))$

yine C'nin bir elemanı oluyor ise C'ye $\mathbb{F}_2R$-devirli kod denir.

Teorem 5.1.2. $C\subseteq R_{r,s}$ kodunun $\mathbb{F}_2R$-devirli kod olması için gerek ve yeter şart C'nin $R_{r,s}$ 'nin bir $R[x]$ - alt modülü olmasıdır.

İspat. $C, \mathbb{F}_2R$-devirli kod ve $c(x)=(a(x)\,|\,b(x))\in C$ olsun. C, $R_{r,s}$'nin bir alt grubu olduğundan $c_1(x), c_2(x)\in C$ için $c_1(x)-c_2(x)\in C$ olduğu açıktır. C, $\mathbb{F}_2R$-devirli kod olduğundan $x*c(x)\in C$ dir. Aynı sebepten dolayı $x*(x*c(x))=x^2*c(x)\in C$ dir. Bu şekilde devam edilirse $i\geq 0$ için $x^i*c(x)\in C$ olacağı açıktır. C kodunun lineerliğinden dolayı $\forall r(x)\in R[x]$ için de $r(x)*c(x)\in C$ elde edilir. Dolayısıyla C kodu $R_{r,s}$'nin bir $R[x]$ - alt modülüdür. Tersine C kodu $R_{r,s}$'nin bir $R[x]$ - alt modülü olsun. Alt modül şartlarından dolayı C, $R_{r,s}$'nin bir alt grubudur ve $c(x)\in C$ ve $x\in R[x]$ için $x*c(x)\in C$ olacağından C kodu $\mathbb{F}_2R$-devirli koddur.

5.2. $\mathbb{F}_2(\mathbb{F}_2+u\mathbb{F}_2)$- Devirli Kodun Üreteç Polinomu ve En Küçük Geren Kümesi

Bu bölümde $\mathbb{F}_2R$-devirli kodun üreteçleri hakkında bilgi verilecektir. Bölüm boyunca C kodu $\mathbb{F}_2R$-devirli kodu olarak düşünülecektir. $\mathbb{F}_2R$-devirli kodun üreteç polinomu bulunurken aşağıdaki teoreme ihtiyaç duyulacaktır.

Teorem 5.2.1. C kodu $R_n=\mathbb{F}_2[u][x]\Big/\langle x^n-1\rangle$ de n uzunluğunda devirli bir kod olsun.

i. Eğer n tek ise R_n temel ideal halkası ve $g(x), a(x)$ polinomları $a(x)\,|\,g(x)\,|\,x^n-1$ şartını sağlayan ikili alfabe üzerindeki polinomlar olmak üzere $C=\langle g(x)+(1+u)a(x)\rangle$ dir.

ii. Eğer n çift ise

a. Eğer $g(x)=a(x)$ ise $g(x), p(x)$ polinomları $g(x)\,|\,x^n-1 \bmod 2$ ve $g(x)+(1+u)p(x)\,|\,x^n-1$ şartını sağlayan ikili alfabe üzerindeki polinomlar olmak üzere $C=\langle g(x)+(1+u)p(x)\rangle$ dir.

b. $g(x), a(x), p(x)$ polinomları $a(x)\,|\,g(x)\,|\,x^n-1 \bmod 2$, $a(x)\,|\,p(x)\dfrac{x^n-1}{g(x)}$ ve $d^o g(x)>d^o a(x)>d^o p(x)$ şartını sağlayan ikili alfabe üzerindeki polinomlar olmak üzere $C=\langle g(x)+(1+u)p(x),(1+u)a(x)\rangle$ dir [53].

Hem C kodu hem de $R[x]/\langle x^s-1\rangle$ halkası $R_{r,s}$ 'nin bir $R[x]$ - alt modülü olduğundan

$$\begin{aligned}\pi: \quad C \quad &\to \quad R[x]/\langle x^s-1\rangle \\ (f(x)\,|\,g(x)) &\to \quad g(x)\end{aligned}$$

şeklinde bir $R[x]$-modül homomorfizması tanımlanabilir. Burada π homomorfizmasının çekirdek kümesi

$$\text{Çek}\pi = \left\{ (f(x)\,|\,0) \in C : f(x) \in \mathbb{F}_2[x]/\langle x^r-1\rangle \right\}$$

olup C'nin bir alt modülüdür.

$$I = \left\{ f(x) \in \mathbb{F}_2[x]/\langle x^r-1\rangle : (f(x)\,|\,0) \in \text{Çek}\pi \right\}$$

şeklinde tanımlanan I kümesi $\mathbb{F}_2[x]/\langle x^r-1\rangle$ halkasının bir idealidir. Başka bir deyiş ile $\mathbb{F}_2[x]/\langle x^r-1\rangle$ halkasında devirli kod olup Teorem 1.2.2.2'den dolayı $f(x)\,|\,\langle x^r-1\rangle$ olacak şekilde $I=\langle f(x)\rangle$ dir. Yani herhangi bir $(k(x)\,|\,0)\in \text{Çek}\pi$ elemanı için $k(x)\in I$ olduğundan $k(x)=m(x)f(x)$ olacak şekilde $m(x)\in \mathbb{F}_2[x]/\langle x^r-1\rangle$ polinomu vardır. Dolayısıyla

$$(k(x)\,|\,0) = (m(x)f(x)\,|\,0) = m(x)*(f(x)\,|\,0)$$

olup $\text{Çek}\pi = \langle (f(x)\,|\,0)\rangle$ elde edilir.

Diğer taraftan $\text{Im}\,\pi$ de $R[x]/\langle x^s-1\rangle$ 'nin bir alt modülü olduğundan $\mathbb{F}_2+u\mathbb{F}_2$ üzerinde devirli koddur ve Teorem 5.2.1 dikkate alınarak s'nin tek ya da çift olmasına göre $\mathbb{F}_2R$ -devirli kodun üreteç polinomları belirlenecektir.

Uyarı 5.2.1. Yazımda kolaylık olması açısından herhangi bir $f(x)$ polinomu kısaca f olarak gösterilecektir.

Durum 1: s tek ve $a \mid g \mid x^s - 1$ olmak üzere $\mathrm{Im}\,\pi = \langle g + (1+u)a \rangle$ ve $\text{Çek}\pi = \langle (f \mid 0) \rangle$ olsun.

Teorem 5.2.2. C kodu $\mathbb{F}_2 R$-devirli kod olmak üzere $C = \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ dır.

İspat. Kabul edilsin ki C kodu $\mathbb{F}_2 R$-devirli kod ve $\mathrm{Im}\,\pi = \langle g + (1+u)a \rangle$ olsun. Yani $\pi((l \mid g + (1+u)a)) = g + (1+u)a$ olacak şekilde bir $(l \mid g + (1+u)a) \in C$ elemanı vardır. Şimdi herhangi bir $(a(x) \mid b(x)) = (a \mid b) \in C$ elemanının $(f \mid 0)$ ve $(l \mid g + (1+u)a)$ elemanları tarafından üretildiği gösterilsin.

$$\pi((a \mid b)) = b = d_1(g + (1+u)a)$$

olacak şekilde $d_1 \in R[x] \Big/ \langle x^s - 1 \rangle$ vardır.

$$(a \mid b) - d_1 * (l \mid g + (1+u)a) = (a - \mu(d_1)l \mid 0) \in \text{Çek}\pi$$

olduğundan $(a - \mu(d_1)l \mid 0) = d_2(f \mid 0)$ olacak şekilde $d_1 \in \mathbb{F}_2[x] \Big/ \langle x^r - 1 \rangle$ vardır. Yukarıdaki eşitlik kullanılarak

$$\begin{aligned}(a \mid b) &= d_1 * (l \mid g + (1+u)a) + (a - \mu(d_1)l \mid 0) \\ &= d_1 * (l \mid g + (1+u)a) + d_2(f \mid 0)\end{aligned}$$

olup $C \subseteq \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ elde edilir. Tersine $C \supseteq \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ de olduğundan $C = \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ sonucuna varılır.

Lemma 5.2.1. Eğer $C = \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod ise $d^o l < d^0 f$ olarak kabul edilebilir.

İspat. Kabul edilsin ki $d^o l) \geq d^0 f$ olsun. f ve l polinomları cisim üzerinde olduklarından bölme algoritması uygulanabilir. Dolayısıyla

$$l = f.q + r \quad ; \quad 0 \leq d^0 r < d^o f$$

olacak şekilde $q, r \in \mathbb{F}_2[x] \Big/ \langle x^r - 1 \rangle$ polinomları vardır. Buradan üreteç polinom yeniden yazılırsa,

$$\begin{aligned} \langle (f \mid 0), (l \mid g + (1+u)a) \rangle &= \langle (f \mid 0), (fq + r \mid g + (1+u)a) \rangle \\ &= \langle (f \mid 0), (r \mid g + (1+u)a) \rangle \end{aligned}$$

olduğu görülür. Yani $d^o l < d^0 f$ olarak kabul edilebilir.

Lemma 5.2.2. Eğer $C = \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod ise $f \mid \frac{x^s - 1}{a} l \mod(1+u)$ dır.

İspat. $\frac{x^s - 1}{a} * (l \mid g + (1+u)a) = \left(\mu\left(\frac{x^s - 1}{a} \right) l \mid \frac{x^s - 1}{a} (g + (1+u)a) \right) = \left(\mu\left(\frac{x^s - 1}{a} \right) l \mid 0 \right)$

olduğu göz önünde bulundurulursa

$$\pi\left(\left(\mu\left(\frac{x^s - 1}{a} \right) l \mid 0 \right) \right) = 0$$

elde edilir ve $\left(\mu\left(\frac{x^s - 1}{a} \right) l \mid 0 \right) \in \text{Çek}\pi \subseteq C$ olduğundan $f \mid \frac{x^s - 1}{a} l \mod(1+u)$ sonucuna varılır.

Teorem 5.2.3. $C = \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod olsun. Bu durumda

$$S_1 = \bigcup_{i=0}^{r - d^o f - 1} \left\{ x^i * (f \mid 0) \right\}$$

$$S_2 = \bigcup_{i=0}^{s - d^o g - 1} \left\{ x^i * (l \mid g + (1+u)a) \right\}$$

$$S_3 = \bigcup_{i=0}^{d^o g - d^o a - 1} \left\{ x^i * (\mu(h) l \mid (1+u)ah) \right\}$$

olsun. Bu durumda $S = S_1 \cup S_2 \cup S_3$ kümesi C kodunu geren en küçük kümedir. Ayrıca C kodu $2^{r - d^o f} 4^{s - d^o g} 2^{d^o g - d^o a}$ tane kod söze sahiptir.

İspat. $C = \langle (f \mid 0), (l \mid g + (1+u)a) \rangle$ ve $c(x) \in C$ herhangi bir kod söz olsun. Bu durumda $d_1 \in \mathbb{F}_2[x]$ ve $d_2 \in R[x]$ polinomları

$$c(x) = d_1(f \mid 0) + d_2 * (l \mid g + (1+u)a)$$

olacak şekilde mevcuttur. Eğer $d^o d_1 \le r - d^o f - 1$ ise $d_1(f \mid 0) \in Span(S_1)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_1, r_1 \in \mathbb{F}_2[x]$ polinomları

$$d_1 = \frac{x^r - 1}{f} q_1 + r_1 \quad ; \quad 0 \le d^o r_1 \le r - d^o f - 1$$

olacak şekilde vardır. d_1 yerine yazılırsa

$$\begin{aligned} d_1(f \mid 0) &= \left(\frac{x^r - 1}{f} q_1 + r_1 \right)(f \mid 0) \\ &= q_1 \left(\frac{x^r - 1}{f} f \mid 0 \right) + r_1(f \mid 0) \\ &= r_1(f \mid 0) \end{aligned}$$

elde edilir. Yani $d_1(f \mid 0) \in Span(S_1)$ olduğu görülür.

Eğer $d^o d_2 \le s - d^o g - 1$ ise $d_2 * (l \mid g + (1+u)a) \in Span(S_2)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_2, r_2 \in \mathbb{F}_2[x]$ polinomları

$$d_2 = \frac{x^s - 1}{g} q_2 + r_2 = hq_2 + r_2 \quad ; \quad 0 \le d^o r_2 \le s - d^o g - 1$$

olacak şekilde vardır. d_2 yerine yazılırsa

$$\begin{aligned} d_2 * (l \mid g + (1+u)a) &= (hq_2 + r_2) * (l \mid g + (1+u)a) \\ &= q_2(\mu(h)l \mid hg + (1+u)ha) + r_2(l \mid g + (1+u)a) \\ &= q_2(\mu(h)l \mid (1+u)ha) + r_2(l \mid g + (1+u)a) \end{aligned}$$

elde edilir. $0 \le d^o r_2 \le s - d^o g - 1$ olduğundan $r_2(l \mid g + (1+u)a) \in Span(S_2)$ dir.

Şimdi $q_2(\mu(h)l \mid (1+u)ha) \in Span(S)$ olduğu gösterilsin. Dikkat edilmelidir ki $a \mid g \mid x^n - 1$ olduğundan $g = a.k$ olacak şekilde $k \in R[x]$ vardır ve $x^s - 1 = gh = akh$ dir. Eğer $d^o q_2 \le d^o g - d^o a - 1$ ise $q_2(\mu(h)l \mid (1+u)ha) \in Span(S_3)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_3, r_3 \in \mathbb{F}_2[x]$ polinomları

$$q_2 = \frac{x^s - 1}{ha} q_3 + r_3 \quad ; \quad 0 \le d^o r_3 \le d^o g - d^o a - 1$$

olacak şekilde vardır. q_2 yerine yazılırsa

$$\begin{aligned} q_2(\mu(h)l \mid (1+u)ha) &= \left(\frac{x^s - 1}{ha} q_3 + r_3 \right)(\mu(h)l \mid (1+u)ha) \\ &= q_3 \left(\frac{x^s - 1}{ha} \mu(h)l \mid \frac{x^s - 1}{ha}(1+u)ha \right) + r_3(\mu(h)l \mid (1+u)ha) \\ &= q_3 \left(\frac{x^s - 1}{ha} \mu(h)l \mid 0 \right) + r_3(\mu(h)l \mid (1+u)ha) \end{aligned}$$

elde edilir. $0 \le d^o r_3 \le d^o g - d^o a - 1$ olduğundan $r_3(\mu(h)l \mid (1+u)ha) \in Span(S_3)$ dir. Ayrıca Lemma 5.2.2 den dolayı $\frac{x^s - 1}{a} l = fm$ olduğu göz önünde bulundurulursa $q_3 \left(\frac{x^s - 1}{ha} \mu(h)l \mid 0 \right) \in Span(S_1)$ dir. Sonuç olarak $S = S_1 \cup S_2 \cup S_3$ kümesi C kodu için geren kümedir. Ayrıca S kümesindeki diğer elemanlar ile lineer bağımlı olacak şekilde bir eleman olmadığından S'ye C için en küçük geren kümesi denilebilir. Bu sebepten dolayı C'de $2^{r-d^o f} 4^{s-d^o g} 2^{d^o g - d^o a}$ tane kod söz vardır.

Durum 2: s çift ve $g \mid x^s - 1 \bmod 2$, $g + (1+u)p \mid x^s - 1$ olmak üzere $\mathrm{Im}\,\pi = \langle g + (1+u)p \rangle$ ve $\text{Çek}\pi = \langle (f \mid 0) \rangle$ olsun.

Teorem 5.2.4. C kodu $\mathbb{F}_2 R$-devirli kod olmak üzere $C = \langle (f \mid 0), (l \mid g + (1+u)p) \rangle$ dır.

İspat. Teorem 5.2.2 deki ispatta $a = p$ alınarak istenen sağlanır.

Lemma 5.2.3. Eğer $C = \langle (f \mid 0), (l \mid g + (1+u)p) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod ise $d^o l < d^o f$ olarak kabul edilebilir.

İspat. Lemma 5.2.1 deki ispat aynen sağlanır.

Lemma 5.2.4 Eğer $C = \langle (f \mid 0), (l \mid g + (1+u)p) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod ise $f \mid \frac{x^s - 1}{g + (1+u)p} l \mod(1+u)$ dır.

İspat.

$$\frac{x^s - 1}{g + (1+u)p} * (l \mid g + (1+u)p) = \left(\frac{x^s - 1}{g + (1+u)p} l \mid \frac{x^s - 1}{g + (1+u)p} (g + (1+u)a) \right)$$
$$= \left(\frac{x^s - 1}{g + (1+u)p} l \mid 0 \right)$$

olduğu göz önünde bulundurulursa

$$\pi\left(\left(\frac{x^s - 1}{g + (1+u)p} l \mid 0 \right) \right) = 0$$

elde edilir ve $\left(\frac{x^s - 1}{g + (1+u)p} l \mid 0 \right) \in \text{Çek}\pi \subseteq C$ olduğundan $f \mid \frac{x^s - 1}{g + (1+u)p} l \mod(1+u)$ sonucuna varılır.

Teorem 5.2.5 $C = \langle (f \mid 0), (l \mid g + (1+u)p) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod olsun. Bu durumda

$$S_1 = \bigcup_{i=0}^{r - d^o f - 1} \{ x^i * (f \mid 0) \}$$
$$S_2 = \bigcup_{i=0}^{s - d^o (g + (1+u)p) - 1} \{ x^i * (l \mid g + (1+u)p) \}$$

olsun. Bu durumda $S = S_1 \cup S_2$ kümesi C kodunu geren en küçük kümedir.

İspat. $C = \langle (f \mid 0), (l \mid g + (1+u)p) \rangle$ ve $c(x) \in C$ herhangi bir kod söz olsun. Bu durumda $d_1 \in \mathbb{F}_2[x]$ ve $d_2 \in R[x]$ polinomları

$$c(x) = d_1 (f \mid 0) + d_2 * (l \mid g + (1+u)p)$$

olacak şekilde mevcuttur. Eğer $d^o d_1 \le r - d^o f - 1$ ise $d_1 (f \mid 0) \in Span(S_1)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_1, r_1 \in \mathbb{F}_2[x]$ polinomları

$$d_1 = \frac{x^r - 1}{f} q_1 + r_1 \quad ; \quad 0 \le d^o r_1 \le r - d^o f - 1$$

olacak şekilde vardır. d_1 yerine yazılırsa

$$\begin{aligned} d_1(f \mid 0) &= \left(\frac{x^r - 1}{f} q_1 + r_1 \right)(f \mid 0) \\ &= q_1 \left(\frac{x^r - 1}{f} f \mid 0 \right) + r_1(f \mid 0) \\ &= r_1(f \mid 0) \end{aligned}$$

elde edilir. Yani $d_1(f \mid 0) \in Span(S_1)$ olduğu görülür.

Eğer $d^o d_2 \le s - d^o(g + (1+u)p) - 1$ ise $d_2 * (l \mid g + (1+u)p) \in Span(S_2)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_2, r_2 \in \mathbb{F}_2[x]$ polinomları

$$d_2 = \frac{x^s - 1}{g + (1+u)p} q_2 + r_2 = hq_2 + r_2 \quad ; \quad 0 \le d^o r_2 \le s - d^o(g + (1+u)p) - 1$$

olacak şekilde vardır. d_2 yerine yazılırsa

$$\begin{aligned} d_2 * (l \mid g + (1+u)p) &= (hq_2 + r_2) * (l \mid g + (1+u)p) \\ &= q_2(\mu(h)l \mid h(g + (1+u)p)) + r_2(l \mid g + (1+u)p) \\ &= q_2(\mu(h)l \mid 0) + r_2(l \mid g + (1+u)p) \\ &= q_2\left(\mu\left(\frac{x^s - 1}{g + (1+u)p} \right) l \mid 0 \right) + r_2(l \mid g + (1+u)p) \end{aligned}$$

elde edilir. $0 \le d^o r_2 \le s - d^o(g + (1+u)p) - 1$ olduğundan $r_2(l \mid g + (1+u)p) \in Span(S_2)$ dir. Ayrıca Lemma 5.2.4'den dolayı $\frac{x^s - 1}{g + (1+u)p} l \mod(1+u) = f.k$ olduğundan $q_2\left(\mu\left(\frac{x^s - 1}{g + (1+u)p} \right) l \mid 0 \right) \in Span(S_1)$ olup $S = S_1 \cup S_2$ kümesi *C* kodu için geren kümedir. Ayrıca *S* kümesindeki diğer elemanlar ile lineer bağımlı olacak şekilde bir eleman olmadığından *S*'ye *C* için en küçük geren kümesi denilebilir.

Durum 3: n çift ve $a \mid g \mid x^n - 1 \bmod 2$, $a \mid p\dfrac{x^n-1}{g}$ ve olmak üzere $\mathrm{Im}\,\pi = \langle g + (1+u)p, (1+u)a \rangle$ ve $\text{Çek}\pi = \langle (f \mid 0) \rangle$ olsun.

Teorem 5.2.6. C kodu $\mathbb{F}_2 R$-devirli kod olmak üzere $C = \langle (f \mid 0), (l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \rangle$ dır.

İspat. Kabul edilsin ki C kodu $\mathbb{F}_2 R$-devirli kod ve $\mathrm{Im}\,\pi = \langle g + (1+u)p, (1+u)a \rangle$ olsun. Yani $g + (1+u)p, (1+u)a \in \mathrm{Im}\,\pi$ olduğundan $\pi((l_1 \mid g + (1+u)p)) = g + (1+u)p$ ve $\pi((l_2 \mid (1+u)a)) = (1+u)a$ olacak şekilde $(l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \in C$ elemanları vardır. Şimdi herhangi bir $(a(x) \mid b(x)) = (a \mid b) \in C$ elemanının $(f \mid 0)$ ve $(l_1 \mid g + (1+u)p)$ ve $(l_2 \mid (1+u)a)$ elemanları tarafından üretildiği gösterilsin.

$$\pi((a \mid b)) = b = k_1(g + (1+u)p) + k_2((1+u)a)$$

olacak şekilde $k_1, k_2 \in R[x] \Big/ \langle x^s - 1 \rangle$ vardır.

$$(a \mid b) - (k_1 * (l_1 \mid g + (1+u)p) + k_2 * (l_2 \mid (1+u)a)) = (a - (\mu(k_1)l_1 + \mu(k_2)l_2) \mid 0) \in \text{Çek}\pi$$

olduğundan $(a - (\mu(k_1)l_1 + \mu(k_2)l_2 \mid 0) = k_3(f \mid 0)$ olacak şekilde $k_3 \in \mathbb{F}_2[x] \Big/ \langle x^r - 1 \rangle$ vardır. Yukarıdaki eşitlik kullanılarak

$$\begin{aligned}(a \mid b) &= k_1 * (l_1 \mid g + (1+u)p) + k_2 * (l_2 \mid (1+u)a) + (a - (\mu(k_1)l_1 + \mu(k_2)l_2) \mid 0) \\ &= k_1 * (l_1 \mid g + (1+u)p) + k_2 * (l_2 \mid (1+u)a) + k_3(f \mid 0)\end{aligned}$$

olup $C \subseteq \langle (f \mid 0), (l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \rangle$ elde edilir.

Tersine $C \supseteq \langle (f \mid 0), (l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \rangle$ de olduğundan $C = \langle (f \mid 0), (l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \rangle$ sonucuna ulaşılır.

Lemma 5.2.5. Eğer $C = \langle (f \mid 0), (l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod ise $d^o l_1 < d^o f$ ve $d^o l_2 < d^o f$ olarak kabul edilebilir.

İspat. Lemma 5.2.1 deki ispat aynen sağlanır.

Lemma 5.2.6. Eğer $C = \langle (f \mid 0), (l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod ise

i. $f \mid \dfrac{x^s - 1}{a} l_1 \mod(1+u)$ dır.

ii. $x^s - 1 = gh$ ve $ebob(hp, x^s - 1) = m_1$ olmak üzere $m_1 m_2 = x^s - 1$ ise $f \mid h l_1 m_2 \mod(1+u)$ dir.

İspat.

1. Lemma 5.2.2 deki ispat aynen sağlanır.

2. $ebob(hp, x^s - 1) = m_1$ ise $m_1 m_3 = hp$ olacak şekilde $m_3 \in R[x]$ vardır. Dolayısıyla $hpm_2 = m_1 m_3 m_2 = x^s - 1$ dir. $R[x] \Big/ \langle x^s - 1 \rangle$ halkasında $hpm_2 = hg = x^s - 1 = 0$ olduğu dikkate alınırsa

$$\begin{aligned} m_2 h * (l_1 \mid g + (1+u)p) &= (\mu(m_2 h) l_1 \mid m_2 hg + (1+u) m_2 hp) \\ &= (\mu(m_2 h) l_1 \mid 0) \end{aligned}$$

elde edilir. Bu eşitlik göz önünde bulundurularak

$$\pi\big((\mu(m_2 h l_1) \mid 0)\big) = 0$$

elde edilir ve $(\mu(m_2 h l_1) \mid 0) \in \text{Çek}\pi \subseteq C$ olduğundan $f \mid h l_1 m_2 \mod(1+u)$ sonucuna varılır.

Teorem 5.2.7. $C = \langle (f \mid 0), (l_1 \mid g + (1+u)p), (l_2 \mid (1+u)a) \rangle$ kodu $\mathbb{F}_2 R$-devirli kod olsun. Bu durumda

$$S_1 = \bigcup_{i=0}^{r - d^o f - 1} \{ x^i * (f \mid 0) \}$$

$$S_2 = \bigcup_{i=0}^{s - d^o g - 1} \{ x^i * (l_1 \mid g + (1+u)p) \}$$

$$S_3 = \bigcup_{i=0}^{s-d^o m_1 - 1} \left\{ x^i * (\mu(h) l_1 \mid (1+u)\, ph) \right\}$$

$$S_4 = \bigcup_{i=0}^{s-d^o a - 1} \left\{ x^i * (l_2 \mid (1+u) a) \right\}$$

olsun. Bu durumda $S = S_1 \cup S_2 \cup S_3 \cup S_4$ kümesi C kodunu geren en küçük kümedir.

İspat. $C = \langle (f \mid 0), (l_1 \mid g + (1+u)\, p), (l_2 \mid g + (1+u) a) \rangle$ ve $c(x) \in C$ herhangi bir kod söz olsun. Bu durumda $d_1 \in \mathbb{F}_2[x]$ ve $d_2, d_3 \in R[x]$ polinomları

$$c(x) = d_1 (f \mid 0) + d_2 * (l \mid g + (1+u) a) + d_3 * (l_2 \mid (1+u) a)$$

olacak şekilde mevcuttur. Eğer $d^o d_1 \le r - d^o f - 1$ ise $d_1 (f \mid 0) \in Span(S_1)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_1, r_1 \in \mathbb{F}_2[x]$ polinomları

$$d_1 = \frac{x^r - 1}{f} q_1 + r_1 \quad ; \quad 0 \le d^o r_1 \le r - d^o f - 1$$

olacak şekilde vardır. d_1 yerine yazılırsa

$$\begin{aligned} d_1 (f \mid 0) &= \left(\frac{x^r - 1}{f} q_1 + r_1 \right) (f \mid 0) \\ &= q_1 \left(\frac{x^r - 1}{f} f \mid 0 \right) + r_1 (f \mid 0) \\ &= r_1 (f \mid 0) \end{aligned}$$

elde edilir. Yani $d_1 (f \mid 0) \in Span(S_1)$ olduğu görülür.

Eğer $d^o d_2 \le s - d^o g - 1$ ise $d_2 * (l_1 \mid g + (1+u)\, p) \in Span(S_2)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_2, r_2 \in \mathbb{F}_2[x]$ polinomları

$$d_2 = \frac{x^s - 1}{g} q_2 + r_2 = h q_2 + r_2 \quad ; \quad 0 \le d^o r_2 \le s - d^o g - 1$$

olacak şekilde vardır. d_2 yerine yazılırsa

$$\begin{aligned} d_2 * (l_1 \mid g + (1+u)\, p) &= (h q_2 + r_2) * (l_1 \mid g + (1+u)\, p) \\ &= q_2 (\mu(h) l_1 \mid hg + (1+u) hp) + r_2 (l_1 \mid g + (1+u)\, p) \\ &= q_2 (\mu(h) l_1 \mid (1+u) hp) + r_2 (l_1 \mid g + (1+u)\, p) \end{aligned}$$

elde edilir. $0 \le d^o r_2 \le s - d^o g - 1$ olduğundan $r_2 (l_1 \mid g + (1+u)\, p) \in Span(S_2)$ dir.

Şimdi $q_2(\mu(h)l_1 \mid (1+u)hp) \in Span(S)$ olduğu gösterilsin. Dikkat edilmelidir ki $a \mid g \mid x^n - 1$ olduğundan $g = a.k$ olacak şekilde $k \in R[x]$ vardır ve $x^s - 1 = gh = akh$ dir. Eğer $d^o q_2 \le d^o g - d^o a - 1$ ise $q_2(\mu(h)l_1 \mid (1+u)hp) \in Span(S_3)$ dir. Aksi taktirde $hpm_2 = m_1 m_3 m_2 = x^s - 1$ olduğundan m_2 ile bölme algoritması uygulanırsa $q_3, r_3 \in \mathbb{F}_2[x]$ polinomları

$$q_2 = m_2 q_3 + r_3 \quad ; \quad 0 \le d^o r_3 \le d^o m_2 - 1 = s - d^o m_1 - 1$$

olacak şekilde vardır. q_2 yerine yazılırsa

$$\begin{aligned} q_2(\mu(h)l_1 \mid (1+u)hp) &= \left(m_2 q_3 + r_3\right)(\mu(h)l_1 \mid (1+u)hp) \\ &= q_3\left(m_2\mu(h)l_1 \mid (1+u)m_2 hp\right) + r_3(\mu(h)l_1 \mid (1+u)hp) \\ &= q_3\left(m_2\mu(h)l_1 \mid 0\right) + r_3(\mu(h)l_1 \mid (1+u)hp) \end{aligned}$$

elde edilir. $0 \le d^o r_3 \le s - d^o m_1 - 1$ olduğundan $r_3(\mu(h)l_1 \mid (1+u)hp) \in Span(S_3)$ dir. Ayrıca Lemma 5.2.6 (*ii*) den dolayı $fm = hm_2 l_1 \bmod(1+u)$ olduğu göz önünde bulundurulursa $q_3\left(m_2\mu(h)l \mid 0\right) \in Span(S_1)$ dir. Yani $d_2 * (l_1 \mid g + (1+u)p) \in Span(S_1 \cup S_2 \cup S_3)$ dir.

Son olarak $d_3 * (l_2 \mid (1+u)a) \in Span(S_4)$ olduğu gösterilsin. Eğer $d^o d_3 \le s - d^o a - 1$ ise $d_3 * (l_2 \mid (1+u)a) \in Span(S_4)$ dir. Aksi taktirde bölme algoritması uygulanırsa $q_4, r_4 \in \mathbb{F}_2[x]$ polinomları

$$d_3 = \frac{x^s - 1}{a} q_4 + r_4 \quad ; \quad 0 \le d^o r_4 \le s - d^o a - 1$$

olacak şekilde vardır. d_3 yerine yazılırsa

$$\begin{aligned} d_3 * (l_2 \mid (1+u)a) &= \left(\frac{x^s - 1}{a} q_4 + r_4\right) * (l_2 \mid (1+u)a) \\ &= q_4\left(\mu\left(\frac{x^s - 1}{a}\right) l_2 \mid \frac{x^s - 1}{a} a(1+u)\right) + r_4 * (l_2 \mid (1+u)a) \\ &= q_4\left(\mu\left(\frac{x^s - 1}{a}\right) l_2 \mid 0\right) + r_4 * (l_2 \mid (1+u)a) \end{aligned}$$

elde edilir. $0 \le d^o r_4 \le s - d^o a - 1$ olduğundan $r_4 * (l_2 \mid (1+u)a) \in Span(S_4)$ dir. Ayrıca Lemma 5.2.6. (i)'den dolayı $fk = \frac{x^s - 1}{a} l_1 \mod(1+u)$ olduğu göz önünde bulundurulursa $q_4\left(\mu\left(\frac{x^s-1}{a}\right)l_2 \mid 0\right) \in Span(S_1)$ dir. Yani $d_3 * (l_2 \mid (1+u)a) \in Span(S_1 \cup S_4)$ dir. Sonuç olarak $S = S_1 \cup S_2 \cup S_3$ kümesi C kodu için geren kümedir. Ayrıca S kümesindeki diğer elemanlar ile lineer bağımlı olacak şekilde bir eleman olmadığından S'ye C için en küçük geren kümesi denilebilir.

5.3. $\mathbb{F}_2(\mathbb{F}_2 + u\mathbb{F}_2)$ - Devirli Kodun Gray Görüntüsü

Bu bölümde $\mathbb{F}_2 R$ yapısından $\mathbb{F}_2^3$ yapısına bir Gray dönüşüm tanımlanacaktır. Bunun öncesinde aşağıdaki Gray dönüşümüne ihtiyaç olacaktır.

R yapısından $\mathbb{F}_2^2$ yapısına tanımlanan Gray dönüşüm

$$\begin{array}{rccc} \phi: & R & \to & \mathbb{F}_2^2 \\ & a+ub & \to & (a,b) \end{array}$$

şeklindedir. Tanımlanan bu dönüşüm R^n'den $\mathbb{F}_2^{2n}$'e

$$(a_1 + ub_1, \cdots, a_n + ub_n) \to (a_1, b_1, \cdots, a_n, b_n)$$

şeklinde genişletilebilir. Herhangi bir $\alpha \in R$ elemanı için Lee ağırlık $w_L(\alpha) = w_H(\phi(\alpha))$ olarak tanımlanır. Ayrıca $\alpha, \beta \in R$ için Lee uzaklıkta $d_L(\alpha, \beta) = w_L(\alpha - \beta)$ ile tanımlıdır. $x = a + ub$ ve $y = c + ud$ olmak üzere

$$\begin{aligned} \psi(\alpha x + \beta y) &= \psi(\alpha a + \beta c + u(\alpha b + \beta d)) \\ &= (\alpha a + \beta c, \alpha b + \beta d) \\ &= \alpha(a,b) + \beta(c,d) \\ &= \alpha\psi(a+ub) + \beta\psi(c+ud) \\ &= \alpha\psi(x) + \beta\psi(y) \end{aligned}$$

ve

$$\begin{aligned} d_L(x,y) &= w_L(x-y) = w_L((a-c)+u(b-d)) \\ &= w_H(\psi((a-c)+u(b-d))) \\ &= w_H(a-c,b-d) \\ &= w_H((a,b)-(c,d)) \\ &= w_H(\psi(a+ub)-\psi(c+ud)) \\ &= w_H(\psi(x)-\psi(y)) \\ &= d_H(\psi(x),\psi(y)) \end{aligned}$$

şartları sağlandığından tanımlanan bu Gray dönüşüm (R^n ,Lee uzaklık)'tan ($\mathbb{F}_2^{2n}$,Hamming uzaklık)'a tanımlanan uzaklığı koruyan lineer bir dönüşümdür.

Bu tanım yardımı ile $\mathbb{F}_2R$ yapısından $\mathbb{F}_2^3$ yapısına tanımlanacak olan Gray dönüşüm

$$\begin{array}{rccc} \varphi: & \mathbb{F}_2R & \to & \mathbb{F}_2^3 \\ & (a\,|\,b) & \to & (a\,|\,\phi(b)) \end{array}$$

şeklindedir. Bu dönüşüm de

$$\varphi((a_0,a_1,\cdots,a_{r-1}\,|\,b_0,b_1,\cdots,b_{s-1})) = (a_0,a_1,\cdots,a_{r-1}\,|\,\phi(b_0),\phi(b_1),\cdots,\phi(b_{s-1}))$$

olarak $\mathbb{F}_2^r R^s$ 'den $\mathbb{F}_2^{r+2s}$ 'e genişletilebilir. Herhangi bir $(a\,|\,b)\in\mathbb{F}_2^r R^s$ elemanının Lee ağırlığı

$$\begin{aligned} w_L((a\,|\,b)) &= w_H(a)+w_L(b) \\ &= w_H(a)+w_H(\phi(b)) \end{aligned}$$

olarak tanımlanabilir.

Örnek 5.3.1. $R_{3,3} = \mathbb{F}_2[x]\Big/\langle x^3-1\rangle \times R[x]\Big/\langle x^3-1\rangle$ üzerinde *C*, $\mathbb{F}_2R$-devirli kodu olsun. $f=0$ $l=x^2$, $g=x^2+x+1$ ve $a=1$ olmak üzere *C* kodu

$$C = \langle (x^2\,|\,x^2+x+u)\rangle$$

formunda olsun. Tablo 5.1'de C koduna ait kod sözler ve bu kod sözlerin ağırlıkları verilmişti. Bu kodun Gray görüntüsü $\mathbb{F}_2$ üzerinde [9, 4, 4] parametresine sahip optimal lineer koddur. Kodun optimalliği [54]'de verilen veri tabanından kontrol edilebilir.

Tablo 5.1. $R_{3,3}$ üzerindeki $C = \langle (x^2 \mid x^2 + x + u) \rangle$ koduna ait kod sözler ve ağırlıkları

Kod söz	**Kod sözün Ağırlığı**	**Kod söz**	**Kod sözün Ağırlığı**
$(0,0)$	0	$\left(x^2 + x, (u+1)x\right)$	4
$\left(x^2, ux^2 + ux + 1\right)$	4	$\left(x^2, x^2 + x + u\right)$	5
$\left(x^2 + 1, (u+1)x^2\right)$	4	$\left(x^2 + x + 1, ux^2 + ux + u\right)$	6
$(x + 1,\ u + 1)$	4	$\left(x^2 + x + 1, x^2 + x + 1\right)$	6
$\left(x, ux^2 + x + 1\right)$	4	$\left(0, (u+1)x^2 + (u+1)x + u + 1\right)$	6
$\left(1, x^2 + ux + 1\right)$	4	$\left(x^2 + 1, (u+1)x + u + 1\right)$	6
$\left(x, x^2 + ux + u\right)$	4	$\left(x + 1, (u+1)x^2 + (u+1)x\right)$	6
$\left(1, ux^2 + x + u\right)$	4	$\left(x^2 + x, (u+1)x^2 + u + 1\right)$	6

Polinom gösterimi olan bu kodsözler vektörlere dönüştürülür ise her bir $(a_1, a_2, a_3 \mid b_1, b_2, b_3) \in C$ kod sözü için $(a_3, a_1, a_2 \mid b_3, b_1, b_2) \in C$ olduğu görülecektir.

Tablo 5.2'de listelenmiş olan parametreler $\mathbb{F}_2 R$-devirli kodların Gray görüntülerinden elde edilen $\mathbb{F}_2$ üzerindeki optimal kodların parametreleridir. Bu tablo oluşturulurken Teorem 5.2.3'den yararlanılmıştır.

Tablo 5.2. $\mathbb{F}_2 R$-devirli kodların gray görüntülerinden elde edilen optimal kodlar

r ve s uzunlukları	Üreteç polinomları	Gray görüntüleri
$r = 5$ ve $s = 3$	$l = x^4 + x^3 + x + 1$ $f = x^4 + x^3 + x^2 + x + 1$ $g = x^2 + x + 1,\ a = 1$	[11, 5, 4]
$r = 3$ ve $s = 5$	$l = x^2 + x + 1$ $g = a = x^4 + x^3 + x^2 + x + 1$	[13, 2, 8]
$r = 7$ ve $s = 3$	$l = x^6 + x^3 + x + 1$ $g = x^2 + x + 1 \quad a = 1$	[13, 4, 6]
$r = 5$ ve $s = 5$	$l = x^4 + x^3$ $f = x^4 + x^3 + x^2 + x + 1$ $g = a = x + 1$	[15, 9, 4]
$r = 3$ ve $s = 7$	$l = x^2 + x + 1$ $g = x^4 + x^2 + x + 1 \quad a = 1$	[17, 10, 4]
$r = 5$ ve $s = 7$	$l = x^4 + x$ $g = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ $a = x^3 + x^2 + 1$	[19, 5, 8]
$r = 5$ ve $s = 7$	$l = x^4 + x^2 + 1$ $g = x^4 + x^2 + x + 1$ $a = x + 1$	[19, 9, 6]
$r = 7$ ve $s = 7$	$l = x^3 + x + 1$ $g = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ $a = x^3 + x + 1$	[21, 5, 10]
$r = 7$ ve $s = 7$	$l = x^6 + x^5 + x^4 + x$ $g = a = x^4 + x^2 + x + 1$	[21, 6, 8]

BÖLÜM 6. SONUÇ VE ÖNERİLER

Cebirsel yapısından dolayı kodlama teorisinde önemli bir yere sahip olan devirli kod aileleri hem değişmeli olan hem de değişmeli olmayan skew polinom halkaları üzerinde çalışılmıştır.

$\mathbb{Z}_4[u]/\langle u^3 \rangle$ halkası üzerindeki devirli kodların Gray görüntülerinin $\mathbb{Z}_4$ üzerinde lineer kod olduğu bulunmuştur. Bu halka üzerindeki devirli kodların Gray görüntüleri alınıp hem Lee hem de Öklit minimum uzaklık kullanılarak literatüre yeni $\mathbb{Z}_4$-lineer kodlar kazandırılmıştır. Elde edilen bu kodlar online veri tabanına eklenmiştir.

Devirli kodların bir genellemesi olan yarı devirli kodlar, uzunluğu büyük olan kodlar için elverişli olup genelde değişmeli olan halkalar üzerinde bakılmıştır. Bu çalışma da ise değişmeli olmayan $\mathbb{F}_q + v\mathbb{F}_q$'dan katsayılı skew polinom halkası üzerinde incelenmiştir. Ayrıca bu halkadaki skew devirli kodlardan kuantum kod elde edilmesi için gerekli şart verilmiştir.

$\mathbb{F}_3 + u\mathbb{F}_3$ halkası genelleştirilerek yeni bir $\mathbb{F}_3 + v\mathbb{F}_3 + u\mathbb{F}_3 + uv\mathbb{F}_3$ halkası ortaya konmuştur. Bu halkanın cebirsel yapısı incelenmiş ve üzerinde lineer kod, devirli kod ve kuantum kod bakılmıştır.

Aynı uzunluğa ve boyuta sahip kodlar arasından en yüksek minimum uzaklığa sahip kod optimal olarak adlandırılır. Bu çalışmada da devirli kodların yeni bir sınıfı olan ve $\mathbb{F}_2\mathbb{F}_2[u]$-devirli kod olarak adlandırılan yapılardan yararlanarak optimal kodlar bulunmuştur.

KAYNAKLAR

[1] Fraleigh, J. B., A first course in abstract algebra. Pearson Education, Boston, 2003.

[2] Çallıalp, F., Örneklerle soyut cebir. Birsen Yayınevi, İstanbul, 2013.

[3] Çallıalp, F., Tekir Ü., Değişmeli halkalar ve modüller. Birsen Yayınevi, İstanbul, 2009.

[4] Dinh, H. Q., Permouth, S. R., Cyclic and negacyclic codes over finite chain rings. IEEE T Inform Theory, 50(8), 1728-1744, 2004.

[5] MacDonald, B. R., Finite rings with identity. Marcel Deccer, New York, 1974.

[6] Hungerford, T. W., Abstract algebra an introduction. Saunders College publishing.

[7] Shannon, C.E., A Mathematical Theory of Communication. The Bell System Technical Journal, 27, 379-423, 1948.

[8] Hamming, R.W., Error Detecting and Error Correcting Codes. The Bell System Technical Journal, 29, 147-160, 1950.

[9] Roman, S., Coding and Information Theory. Springer Verlag, 1992.

[10] Ling, S., Xing C., Coding Theory A First Course. Cambridge University, 2004.

[11] Prange, E., Cyclic Error Correcting Codes in Two Symbols. Air Force Cambridge Research Center, Cambridge Mass., AFCRC-TN-57, 103, 1957.

[12] Skjærbæk, T. H., Quasi Cycli Code Represented by Gröbner Bases. Aalborg University Department of Mathematical Sciences, 2010.

[13] Calderbank, A. R., Rains, E. M., Shor, P. M., Sloane, N. J. A., Quantum error correction via codes over $GF(4)$. IEEE Trans. Inf. Theory, 44(4), 1369-1387, 1998.

[14] Abualrub, T., Şiap, İ., Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. Des Code Crypt., 42, 271-287, 2007.

[15] Al-Ashker, M., Chen, J. Cyclic codes of arbitrary length over $\mathbb{F}_q + u\mathbb{F}_q + \cdots u^{k-1}\mathbb{F}_q$. Plastine J Math., 2(1), 72-80, 2013.

[16] Yıldız, B., Karadeniz, S., Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Des Code Crypt., 58, 221-234, 2011.

[17] Singh, A. K., Kewat, P. K., On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k \rangle$. Des Code Crypt., 74, 1-13, 2015.

[18] Bonnecaze, A., Udaya, P., Cyclic codes and self dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE T Inform Theory, 45(4), 1250-1255, 1999.

[19] Bandi, R. K., Bhaintwal, M., A note on cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. Discrete Mathematics, Algorithms and Applications, 8(1), 1650017 (17 pages), 2016.

[20] Yıldız, B., Aydın, N., On cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and $\mathbb{Z}_4$ images. Int J Inf Coding Theory, 2(4), 226-237, 2014.

[21] Gao, J., Fu, F. W., Xiao, L., Bandi, R. K., Some results on cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$. Discrete Math Algorithms Appl., 7(4), 1550058 (9 pages), 2015.

[22] Wan, Z. X., Finite Fields and Galois Rings. World Scientific, Singapore, 2003.

[23] Abualrub, T., Cyclic codes over the ring of integers mod m. University of Iowa, Doktora Tezi. 1988.

[24] Abualrub, T., Şiap, İ., Reversible Cyclic Codes Over $\mathbb{Z}_4$. Austral J Combinat., 38, 195-205, 2007.

[25] Dougherty, S. T., Liu, H. Independence of vectors in codes over rings. Des Code Crypt., 51(1), 55-68, 2009.

[26] Aydın, N., Asamov, T., A Database of $\mathbb{Z}_4$-codes. J Comb Inf Syst Sci., 34, 1-12, 2009.

[27] Abualrub, T., Ghrayeb, A., Aydın, N., Şiap, İ., On the Construction of Skew Quasi Cyclic Codes. IEEE Trans. Inf. Theory, 56, 2081-2090, 2010.

[28] Boucher, D., Geiselmann, W., Ulmer, F., Skew cyclic codes. AAECC, 18(4), 379-389, 2007.

[29] Bhaintwal, M., Skew quasi cyclic codes over Galois rings. Des. Codes. and Crypt., 62, 85-101, 2012.

[30] Boucher, D., Ulmer, F., Coding with skew polynomial ring. Journal of Symbolic, 44, 1644-1656, 2009.

[31] Şiap, İ., Abualrub, T., Aydın, N., Seneviratne, P., Skew cyclic codes of arbitrary length. Int. J. Inf. and Coding Theory, 2(1), 10-20, 2011.

[32] Abualrub, T., Aydın, N., Seneviratne, P., Theta-Cyclic Codes Over $\mathbb{F}_2 + v\mathbb{F}_2$. Australasian J. Combinatorics, 54, 115-126, 2012.

[33] Ashraf, M., Mohammad, G., On skew cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$. Int. J. Inf. and Coding Theory, 2(4), 218-225, 2014.

[34] Gao J., Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. Journal of Applied Mathematics and Informatics, 31(3-4), 337-342, 2013.

[35] Bosma, W., Cannon, J., Playoust, C. The Magma algebra system I: The user language. J. Symbolic Comput., 24, 235-265, 1997.

[36] Gürsoy, F., Şiap, İ., Yıldız, B., Construction of Skew Cyclic Codes over $\mathbb{F}_q + v\mathbb{F}_q$. Advanced in Math. of Communication, 8, 313-322, 2014.

[37] Shor, P. W., Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A., 52(4), 2493- 2496, 1995.

[38] Steane, A. M., Simple quantum error correcting codes. Phys. Rev. Lett., 77, 793 – 797, 1996.

[39] Qian, J., Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Journal of Inform Computational Science, 10(6), 1715 – 1722, 2013.

[40] Kai, X., Zhu S., Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Int. J. Quantum Inform., 9(2), s. 689 – 700, 2011.

[41] Yin, X., Ma W., Gray Map And Quantum Codes Over The Ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. International Joint Conferences of IEEE TrustCom, 11, 2011.

[42] Özen, M., Güzeltepe M., Quantum Codes From Codes over Gaussian Integers with Respect to The Mannheim Metric. Quantum Information and Computation, 12, 813 – 819, 2012.

[43] Guenda, K., Gulliver T. A., Quantum codes over rings. Int. J. Quantum Inform., 12(4), 1450020(11 pages), 2014.

[44] Dertli, A., Çengellenmiş, Y., Eren Ş., On quantum codes obtained from cyclic codes over A_2. Int. J. Quantum Inform., 3(5), 2015.

[45] Brouwer, A. E., Hamalainen, H. O., Ostergard, P. R. J., Sloane,.N. J. A., Bounds on mixed binary/ternary codes. IEEE Trans. Inform. Theory, 44(1), 140-161, 1998.

[46] Borges, J., Fernández-Córdoba, C., Pujol, J., Ri´fa, J., Villanueva M., $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: Generator matrices and duality. Des Codes Crypt., 54, 167–179, 2010.

[47] Fernández-Córdoba, C., Pujol, J., Villanueva, M., $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: rank and kernel. Des Codes Crypt., 56, 43-59, 2010.

[48] Bilal, M., Borges, J., Dougherty, S. T., Fernández-Córdoba, C., Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. Des Codes Crypt. 61, 31–40, 2011.

[49] Aydoğdu, İ., Şiap, İ.,. The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$ -additive codes: Bounds on the minimum distance. Appl. Math. Inform. Sci., 7(6), 2271–2278, 2013.

[50] Aydoğdu, İ., Abualrub, T., Şiap, İ., On $\mathbb{Z}_2\mathbb{Z}_2[u]-$Additive Codes. International Journal of Computer Mathematics, 92(9), 1806-1814, 2015.

[51] Borges, J., Fernández-Córdoba, C., Ten-Valls R., $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, generator polynomials and dual codes. IEEE Trans. Inf. Theory, 62(11), 6348–6354, 2016.

[52] Abualrub, T., Şiap, İ., Aydın, N., $\mathbb{Z}_2\mathbb{Z}_4$ -additive Cyclic Codes. IEEE Trans. Inf. Theory, 60(3), 1508-1514, 2014.

[53] Şiap, İ., Abualrub, T., Ghrayeb, A., Cyclic DNA codes over the ring $\mathbb{F}_2[u]/\langle u^2-1\rangle$ based on the deletion distance. Journal of Franklin Institue, 346, 731-740, 2009.

[54] Grassl., M., Table of Bounds on Linear Codes [Online]. http://www.codetables.de, Erişim Tarihi: 12.08.2017, 1995.

ÖZGEÇMİŞ

N.Tuğba ÖZZAİM, 30.05.1988 de Ankara' da doğdu. İlk, orta ve lise eğitimini Ankara'da tamamladı. 2006 yılında Ankara Keçiören Kanuni Süper Lisesi'nden okul birincisi olarak mezun oldu. 2006 yılında başladığı Sakarya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nü 2010 yılında bölüm ikincisi olarak bitirdi. 2010-2012 yılları arasında Sakarya Üniversitesi Matematik Anabilim Dalında Cebir ve Sayılar Teorisi Bilim Dalında yüksek lisans eğitimini tamamladıktan sonra Hata Düzelten Kodlar Teorisi üzerine doktora eğitimine başlamıştır.