T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU HALKALAR ÜZERİNDE ÇEŞİTLİ KODLARIN İNŞASI

DOKTORA TEZİ

Fatma Zehra UZEKMEK

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

Haziran 2021

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU HALKALAR ÜZERİNDE ÇEŞİTLİ KODLARIN İNŞASI

DOKTORA TEZİ

Fatma Zehra UZEKMEK

Enstitü Anabilim Dalı : MATEMATİK

Bu tez 16/06/2021 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Prof. Dr. **Mehmet ÖZEN** **Jüri Başkanı**	**Doç. Dr.** **Yalçın YILMAZ** **Üye**	**Prof. Dr.** **Mehmet BEKTAŞOĞLU** **Üye**
Dr. Öğretim Üyesi **Elif Segah ÖZTAŞ** **Üye**		**Dr. Öğretim Üyesi** **Mehmet Emin KÖROĞLU** **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.

Fatma Zehra UZEKMEK

17.05.2021

TEŞEKKÜR

Doktora eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden danışman hocam Prof. Dr. Mehmet ÖZEN'e teşekkürlerimi sunarım.

Çalışmalarımdaki bilgisayar araştırmalarına katkı sağlayan, MAGMA programlama dilindeki bilgilerini ve DNA kodlar ile ilgili bilgilerini benimle paylaşan, bilgi ve desteğini almaktan çekinmediğim değerli hocam Karamanoğlu Mehmetbey Üniversitesi Dr. Öğretim Üyesi Elif Segah ÖZTAŞ'a teşekkür ederim.

Hayatım boyunca her konuda maddi ve manevi desteklerini esirgemeyen, bu süre zarfında da büyük bir anlayış ve titizlikle yanımda olan çok kıymetli anneme, babama ve kardeşlerim Feyza, Rağna, Harun'a teşekkür ederim.

Doktora eğitimim boyunca 2211 Yurt İçi Lisansüstü Burs Programı bünyesinde sağlamış olduğu burs desteğinden dolayı TÜBİTAK - BİDEB'e teşekkürlerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

A	: Adenin
$d_H(c,c')$	: c ile c' arasındaki minimum Hamming uzaklık
$d_L(c,c')$	: c ile c' arasındaki minimum Lee uzaklık
$d_E(c,c')$	: c ile c' arasındaki minimum Öklit uzaklık
CRT	: Çin Kalan Teoremi
DNA	: Deoksiribo Nükleik Asit
$der(f(x))$	: $f(x)$ fonksiyonunun derecesi
G	: Guanin
$T_3[x,\Theta_i]$	: Katsayıları T_3 halkasının elemanları olan Θ_i – otomorfizmaları ile belirli aykırı polinom halkası
C	: Sitozin
$\mathbb{Z}_4$	: Tamsayıların $\bmod 4$ 'e göre kalan sınıflarının kümesi
T	: Timin
u^R	: u dizisinin ters sıralısı
$\overline{u}$	: u dizisinin tamlayanı
$\overline{u^R}$	: u dizisinin ters sıralı tamlayanı
WCC	: Watson Crick Complement
$w_H(\alpha)$	: α kodsözünün Hamming ağırlığı
$w_L(\alpha)$	: α kodsözünün Lee ağırlığı
$w_E(\alpha)$	: α kodsözünün Öklit ağırlığı
$Span\wp$	: $\wp$ kümesinin gerdiği küme
$\lfloor x \rfloor$	: x 'e eşit yada küçük en büyük tamsayı

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Devirli kod, sabit devirli kod, parçalı devirli kod, aykırı devirli kod, aykırı sabit devirli kod, DNA kod, ters sıralı DNA kod, toplamsal kod

Bu çalışma altı bölümden oluşmaktadır. İlk bölümde çeşitli başlıklar altında cebirsel tanım ve teoremlere yer verilmiştir.

İkinci bölümde, $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4+\ldots+u^{k-1}\mathbb{Z}_4$ halkasının yapısı incelenerek Çin Kalan Teoremi yardımıyla halka üzerinde tek uzunluktaki devirli ve sabit devirli kodların yapısı araştırılmıştır. Üreteç polinomları oluşturulmuş, idempotent üretecinin tek türlü olduğu gösterilmiştir. Halkadaki devirli ve sabit devirli kodların $\mathbb{Z}_4$ görüntüleri incelenerek önemli sonuçlara ulaşılmıştır. Elde edilen tüm bu bilgilerden yararlanarak $\mathbb{Z}_4$ üzerinde birçok yeni ve optimal kod elde edilmiştir. Elde edilen kodların bazıları tablolar ile sunulmuştur.

Üçüncü bölümde, $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ halkası üzerinde aşikâr olmayan tüm otomorfizmalar belirlenmiştir. Ayrışım metodu yardımı ile tek uzunluktaki aykırı devirli ve aykırı sabit devirli kodların üreteç polinomu oluşturularak karakteristik yapıları incelenmiştir. Aykırı devirli ve halkadaki tüm birimsel elemanlar için aykırı sabit devirli kodların $\mathbb{Z}_4$ görüntüleri incelenerek birçok yeni ve optimal kod elde edilmiştir. Bulunan kodlar tablo ile sunulmuştur.

Dördüncü bölümde, $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ halkasında ters sıralı DNA kodların varlığına odaklanılmış ve bu kodları bulabilmek için yeni bir polinom tanımlanmıştır. Önceki bölümlerde tanımlanan Gray dönüşüm ile DNA $2-$bazı arasında ilişki kurulmuştur. Halka üzerinde ters sıralı DNA kod inşa edebilmek için yeni bir üretim metodu oluşturulmuştur. Oluşturulan bu metodu daha anlaşılabilir kılabilmek adına örnekler sunulmuştur.

Beşinci bölümde, $\mathbb{Z}_4\mathbb{Z}_4[u]$ halkasının yapısal özellikleri incelenmiş ve $\mathbb{Z}_4R-$devirli ve sabit devirli kodun üreteç polinomları belirlenmiştir. Kodu geren en küçük küme elde edilmiştir. Otomorfizma tanımlanarak aykırı devirli ve aykırı sabit devirli kodların yapısı araştırılmıştır. Devirli, sabit devirli, aykırı devirli ve aykırı sabit devirli kodların $\mathbb{Z}_4-$görüntüleri incelenerek yeni sonuçlar elde edilmiştir.

Altıncı bölümde ise sonuçlara yer verilmiştir.

CONSTRUCTION OF VARIOUS CODES OVER FINITE RINGS

SUMMARY

Keywords: Cyclic code, constacyclic code, quasi cyclic code, skew cyclic code, skew constacyclic code, DNA code, reversible DNA code, addtitive code

This study consists of six sections. In the first section, algebraic definitions and theorems are included under various titles.

In the second section, by examining the structure of the ring $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4+\ldots+u^{k-1}\mathbb{Z}_4$, with the help of the Chinese Remainder Theorem, the structure of cyclic and constacyclic codes with odd length over this ring is investigated. Generator polynomials are constructed and the idempotent generator of the code is shown to be unique. Important results have been obtained by examining the $\mathbb{Z}_4-$images of the cyclic and constacyclic codes over the ring. At the end, many new and optimal linear codes are obtained. Some of these codes are presented in tables.

In the third section, all non-trivial automorphisms over the ring $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ are determined. With the help of the Chinese Remainder Theorem, generator polynomials of skew cyclic and skew constacyclic codes of odd length are constructed and their characteristic structures are analyzed. Many new and optimal linear codes have been obtained by examining $\mathbb{Z}_4-$ images of skew cyclic codes and skew constacyclic codes for all unit elements over the ring. The codes that found are presented with tables.

In the fourth section, the existence of reversible DNA codes over the ring $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ is focused and a new polynomial is defined to find these codes. The relationship is established between DNA $2-$mers and the Gray map in the previous sections. Then, a new construction method is presented to obtain the reversible DNA code over this ring. In order to make this method more understandable, examples are given.

In the fifth section, the structural properties of the ring $\mathbb{Z}_4\mathbb{Z}_4[u]$ are explored and the generator polynomials of the cyclic and constacyclic codes are identified. By defining an automorphism, the structure of skew cyclic and skew constacyclic codes are investigated. New results have been obtained via analyzing $\mathbb{Z}_4-$images of cyclic, constacyclic, skew cyclic and skew constacyclic over this ring.

In the sixth section, the results are given.

BÖLÜM 1. CEBİRSEL TANIMLAR VE TEOREMLER

Bu bölümde, tez boyunca kullanılacak bazı temel cebirsel tanım ve teoremlere yer verilecektir. Bu kavramlar grup, halkalar, modüller, lineer kodlar, hata düzelten kodlar ve DNA kavramına dair temel bilgiler başlıkları altında incelenecektir.

1.1. Grup

Bu kısımda [1] ve [2] numaralı kaynaklar kullanılarak, cebirsel yapı ve grup tanımları verilecektir.

Tanım 1.1.1. B boştan farklı bir küme olmak üzere $q, y \in B$ için her (q, y) sıralı ikilisine B kümesinin bir ve yalnız bir elemanını karşılık getiren fonksiyona B üzerinde bir ikili işlem denir. B kümesi üzerindeki bir ikili işlem "$*$" ile gösterilir. Bu durumda fonksiyon

$$B \times B \to B$$
$$(q, y) \to q * y$$

şeklinde tanımlanır. Üzerinde en az bir ikili işlem tanımlanmış kümeye ise cebirsel yapı adı verilir.

Tanım 1.1.2. G boştan farklı bir küme ve "$*$" işlemi G kümesi üzerinde tanımlı bir ikili işlem olmak üzere, $(G, *)$ cebirsel yapısı aşağıdaki aksiyomları sağlıyorsa bu cebirsel yapıya grup adı verilir.

i. "$*$" işlemi G kümesi üzerinde bir ikili işlemdir.

ii. "$*$" işleminin G kümesi üzerinde birleşme özelliği vardır. $\left[\forall q,b,s \in G \ : \ q*(b*s)=(q*b)*s \text{ eşitliği sağlanır.}\right]$

iii. "$*$" işleminin G kümesinde bir birim elemanı vardır. $\left[\forall q \in G \ : \ q*e=e*q=q \text{ olacak şekilde bir } e \in G \text{ vardır.}\right]$

iv. "$*$" işlemine göre G kümesindeki her bir elemanın tersi vardır. $\left[\forall q \in G \ : \ q*q^{-1}=q^{-1}*q=e \text{ olacak şekilde bir } q^{-1} \in G \text{ bulunabilir.}\right]$

Tanım 1.1.3. Grup özelliklerinin yanı sıra her $q,b \in G$ için $q*b=b*q$ eşitliği de sağlanıyorsa $(G,*)$ grubuna değişmeli (abelyen) grup adı verilir.

Teorem 1.1.1. $(G,*)$ bir grup ve K kümesi G kümesinin boştan farklı bir alt kümesi olmak üzere K kümesinin G kümesinin bir alt grubu olması için gerek ve yeter koşul her $q,b \in K$ için $q*b^{-1} \in K$ olmasıdır.

1.2. Halkalar

Bu kısımda [1], [2] ve [3] numaralı kaynaklar kullanılarak, halkalar ile ilgili bazı temel tanım ve teoremler verilecektir.

Tanım 1.2.1. R boştan farklı bir küme ve bu küme üzerinde tanımlı ikili işlem "$+$" ve "$.$" olmak üzere aşağıdaki aksiyomları sağlayan $(R,+,.)$ cebirsel yapısına bir halka denir.

i. $(R,+)$ değişmeli bir gruptur.

ii. "$.$" işleminin R üzerinde birleşme özelliği vardır. $\left[\forall q,b,s \in R \ : \ q(bs)=(qb)s \text{ eşitliği sağlanır.}\right]$

iii. "$.$" işleminin "$+$" işlemi üzerine sağdan ve soldan dağılma özelliği vardır. $\left[\forall q,b,s \in R \ : \ q(b+s)=qb+qs \text{ ve } (q+b)s=qs+bs \text{ eşitlikleri sağlanır.}\right]$

Tanım 1.2.2. Halka özelliklerinin yanı sıra her $q,b \in R$ için $qb = bq$ koşulu da sağlanıyorsa R halkasına değişmeli halka denir.

Tanım 1.2.3. R bir halka ve K kümesi de R halkasının boştan farklı bir alt kümesi olsun. K kümesi R halkasının işlemlerine göre halka koşullarını sağlıyorsa K kümesine R halkasının bir alt halkası denir.

Tanım 1.2.4. Her $q \in R$ için $eq = qe = q$ olacak şekilde tek bir $e \in R$ varsa R halkasına birimli halka denir. Halkanın birimi genel olarak 1_R ile temsil edilir ve birim eleman (çarpımsal birim) olarak adlandırılır.

Tanım 1.2.5. Birimli bir R halkasındaki bir $q \in R$ için $qb = bq = 1_R$ olacak şekilde bir $b \in R$ varsa q elemanına birimli R halkasının terslenebilen elemanı adı verilir.

Tanım 1.2.6. R halkasından alınan sıfırdan farklı bir $q \in R$ için $qb = 0_R$ $\left(\text{veya } bq = 0_R\right)$ olacak şekilde sıfırdan farklı en az bir tane $b \in R$ mevcut ise q elemanına halkanın sıfır böleni adı verilir.

Tanım 1.2.7. Sıfır bölensiz bir halkaya tam halka denir. Birimli, değişmeli ve sıfır bölensiz alt halkaya ise tamlık bölgesi adı verilir.

Tanım 1.2.8. Tamlık bölgesinin tüm elemanlarını bölen R halkasının bir elemanına aritmetik birim veya birimsel eleman denir.

Önerme 1.2.1. R halkasının aritmetik birimleri, halkadaki terslenebilen elemanlardan ibarettir.

Tanım 1.2.9. R bir halka olmak üzere her $a \in R$ için $ma = 0_R$ koşulunu sağlayan en küçük pozitif m tamsayısına halkanın karakteristiği denir. Bu şartı sağlayan m tamsayısının bulunmaması durumunda halkanın karakteristiği sıfırdır denir.

Teorem 1.2.1. Bir tamlık bölgesinin karakteristiği ya sıfırdır ya da asal sayıdır.

Tanım 1.2.10. R bir halka ve L kümesi R halkasının bir alt halkası olsun.

i. Her $b \in R$ ve $q \in L$ için $qb \in L$ ise L bir sağ idealdir.

ii. Her $b \in R$ ve $q \in L$ için $bq \in L$ ise L bir sol idealdir.

iii. L kümesi hem sağ ideal hem de sol ideal ise L kümesine R halkasının bir ideali denir.

Tanım 1.2.11. R halkasında $\{0\}$ ve R kümeleri halkanın aşikar idealleridir. R halkasının aşikar olmayan ideallerine has (öz) ideal adı verilir.

Teorem 1.2.2. Birimli bir halkanın ideali halkanın birimini kapsıyorsa ideal halkanın kendisine eşittir.

Tanım 1.2.12. S kümesi tarafından üretilen ideal (S) ile gösterilir. S kümesinin elemanlarına (S) idealinin üreteçleri denir. $S = \{s_1, \ldots, s_n\}$ ise S ideali sonlu üretilmiştir denir ve $(s_1, \ldots, s_n)$ ile gösterilir. Tek bir s elemanı tarafından üretilen (s) idealine de temel ideal adı verilir. Halkanın tüm idealleri temel ideal ise bu halkaya temel ideal halkası denir.

Teorem 1.2.3. R birimli bir halka ve $q \in R$ olsun. q elemanı tarafından üretilen sağ ideal $qR = \{qr : r \in R\}$ ve sol ideal $Rq = \{rq : r \in R\}$ şeklindedir.

Tanım 1.2.13. R bir halka ve L kümesi R halkasının bir ideali olsun. Her $q, b \in R$ için,

"$q \equiv b \pmod{L}$ olması için gerek ve yeter koşul $q - b \in L$ olmasıdır."

biçiminde tanımlanan "$\equiv$" bağıntısı R halkası üzerinde bir denklik bağıntısı olup bu bağıntıya göre tüm denklik sınıflarının kümesi R/L ile gösterilir. Bu durumda $R/L = \{r + L : r \in R\}$ ile temsil edilir.

Tanım 1.2.14. R bir halka ve L kümesi R halkasının bir ideali olsun. Toplama işleminin $(q+L)+(b+L)=(q+b)L$ biçiminde, çarpma işleminin ise $(q+L)(b+L)$ $=qb+L$ biçiminde tanımlanması durumunda R/L kümesi bir halkadır. Bu halkaya R halkasının L idealine göre bölüm halkası adı verilir. R halkası birimli bir halka ise R/L halkasının birimi 1_R+L şeklindedir. R halkası değişmeli bir halka ise R/L bölüm halkası da değişmeli bir halkadır.

Tanım 1.2.15. R bir halka olmak üzere, R halkasının tüm idealleri tam sıralı ise R halkasına zincir halka denir. Diğer bir ifadeyle, halkanın tüm idealleri kapsama işlemi altında bir zincir oluşturuyorsa R halkası zincir halkadır. Aksi takdirde bu halkaya zincir olmayan halka adı verilir.

Tanım 1.2.16. R birimli ve değişmeli halka ve P de R halkasının (1) idealinden farklı bir ideali olsun. Bu durumda R halkasının P idealini kapsayan P ve R'den başka hiçbir ideali yoksa P idealine R halkasının bir maksimal ideali denir.

Önerme 1.2.2. P ideali R halkasının (1) idealinden farklı bir ideali olsun. P idealinin maksimal ideal olması için gerek ve yeter koşul her $x\in R-P$ için $P+(x)=R$ olmasıdır.

Tanım 1.2.17. Tek bir maksimal ideali olan halkaya lokal (yerel) halka, birden fazla maksimal ideali olan halkalara ise yarı lokal halka adı verilir.

Tanım 1.2.18. $(R,+,.)$ ve $(U,+,.)$ iki halka olmak üzere her $r,v\in R$ için,

i. $f(r+v)=f(r)+f(v)$ ve

ii. $f(rv)=f(r)\,f(v)$

şartları sağlanıyorsa $f:R\to U$ fonksiyonuna bir halka homomorfizması denir.

Tanım 1.2.19. $f:R\to U$ halka homomorfizması birebir ve örten ise f fonksiyonuna bir izomorfizma, R ve U halkalarına da izomorf halkalar adı verilir. $R\cong U$ ile temsil edilir. $R=U$ olması durumunda ise f izomorfizması otomorfizma olarak adlandırılır.

Tanım 1.2.20. R bir halka ve $q_0,\ldots,q_t\in R$ olmak üzere, $q_0+q_1x+\ldots+q_tx^t$ ifadesine R halkasından katsayılı bir polinom denir ve bu polinomlar kümesi $R[x]$ ile temsil edilir.

Tanım 1.2.21. R halkasından katsayılı tüm polinomlar kümesi $R[x]$, $f(x)=q_0+q_1x+\ldots+q_px^p\in R[x]$ ve $g(x)=k_0+k_1x+\ldots+k_rx^r\in R[x]$ iki polinom olmak üzere, $R[x]$ kümesi üzerindeki polinomların

i. toplamı; $f(x)+g(x)=\sum_{i=0}^{\max(p,r)}(q_i+k_i)x^i$

ii. çarpımı; $y_i=\sum_{t=0}^{i}q_tk_{i-t}$ iken $f(x).g(x)=\sum_{i=0}^{p+r}y_ix^i$

şeklinde tanımlanır.

Tanım 1.2.22. Yukarıda tanımlanan toplama ve çarpma işlemlerine göre $R[x]$ polinomlar kümesi bir halkadır.

Önerme 1.2.3. R bir halka ise $R[x]$ te bir halkadır.

Tanım 1.2.23. R bir halka olmak üzere aşağıdaki koşullar birbirine denktir.

i. R halkası birimli ise $R[x]$ halkası da birimlidir.

ii. R halkası değişmeli ise $R[x]$ halkası da değişmelidir.

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

Teorem 1.2.4. $R[x]$ polinom halkası, $f(x)=q_0+q_1x+\ldots+q_px^p$ ve $g(x)=k_0+k_1x+\ldots+k_rx^r$ polinomları $R[x]$ halkasında, sırasıyla, $p.$ ve $r.$ dereceden iki polinom olmak üzere, $der[f(x)+g(x)]\le der[f(x)]+der[g(x)]$ eşitsizliği mevcuttur. R halkasının tamlık bölgesi olması durumunda ise $der[f(x)+g(x)]=der[f(x)]+der[g(x)]$ eşitliği sağlanır.

Tanım 1.2.24. $q_t\neq 0$ olmak üzere $f(x)=q_0+q_1x+\ldots+q_tx^t$ polinomunun derecesi t olup $der(f(x))=t$ şeklinde gösterilir. $q_t=1$ olması durumunda bu polinomu özel olarak monik polinomu olarak adlandırılır. $f(x)$ polinomunun ters-sıralı polinomu $x^{der(f(x))}f(x^{-1})$ polinomu olup $f^*(x)$ ile temsil edilir.

Tanım 1.2.25. $\{R_1,R_2,\ldots,R_n\}$ bir takım halkalar kümesi ve $p_i\in R_i$ olmak üzere $(p_1,\ldots,p_n)$ sıralı $n-$lilerden oluşan küme $R_1\times R_2\times\cdots\times R_n$ ile temsil edilsin. Bileşen bileşene toplama ve çarpma işlemi tanımlanması durumunda bu küme bir halka belirtir ve bu halka R_i halkalarının direkt (dış) çarpımı olarak adlandırılır.

Teorem 1.2.5. R bir halka ve bu halkanın bir takım idealleri $L_1,\ldots,L_n$ olsun. Bu durumda,

i. $L_1+L_2+\cdots+L_n=R$ ve

ii. Her $t\in\{1,\ldots,n\}$ için $L_t\cap(L_1+\cdots+L_{t-1}+L_{t+1}+\cdots+L_n)=0$

şartlarının sağlanması durumunda $R\cong L_1\times L_2\times\cdots\times L_n$'dir.

Tanım 1.2.26. R halkasının $L_1,\ldots,L_n$ idealleri Teorem 1.2.5.'teki şartları sağlıyorsa R halkası L_i ideallerinin direkt toplamı (iç çarpımı) olarak adlandırılır. $R=L_1\oplus L_2\oplus\cdots\oplus L_n$ ile temsil edilir.

Teorem 1.2.6. (Çin Kalan Teoremi) R halkasının $L_1,\ldots,L_n$ idealleri için,

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

ii. $\forall i \neq j$ için $L_i + L_j = R$

özelliklerinin sağlanması durumunda herhangi $l_1,\ldots,l_n \in R$ ve $i = 1,\ldots,n$ için $a \equiv a_i \pmod{L_i}$ olacak şekilde bir $a \in R$ elemanı vardır. Ayrıca, a elemanı mod $L_1 \bigcap L_2 \bigcap \ldots \bigcap L_n$'e göre tek türlü olarak belirlidir. R halkasının birimli bir halka olması durumunda $R^2 = R$ eşitliği sağlanır. Böylece R halkasının herhangi bir L ideali için $R^2 + L = R$ eşitliği sağlanır.

Sonuç 1.2.1. R halkasının idealleri $L_1,\ldots,L_n$ olsun. Bu durumda aşağıdaki şekilde bir ϕ halka homomorfizması mevcuttur.

$$\phi : R/L_1 \bigcap L_2 \bigcap \ldots \bigcap L_n \rightarrow R/L_1 \times R/L_2 \times \cdots \times R/L_n$$

Her i için $R^2 + L_i = R$ ve her $i \neq j$ için $L_i + L_j = R$ sağlanıyorsa ϕ bir izomorfizma olur.

Çin Kalan Teoremi aşağıdaki gibi de ifade edilebilir.

Tanım 1.2.27. R birimli ve değişmeli bir halka olmak üzere, her $i \neq j$ için $e_i e_j = 0$ ve $\sum_{i=1}^{n} e_i = 1$ olacak şekilde R halkasının bir $(e_i)_{i=1}^{n}$ idempotent ailesi varsa R halkası $e_i R$ ideallerinin direkt toplamı biçiminde yazılabilir. Diğer bir ifadeyle $R_i = e_i R$ eşitliği mevcuttur. Bu durumda $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ şeklindedir.

1.3. Modüller

Bu kısımda [4] ve [5] numaralı kaynaklar kullanılarak, modüller ile ilgili bazı temel tanım ve teoremler ele alınacaktır.

Tanım 1.3.1. M toplama işlemine göre değişmeli bir grup ve R de bir halka olsun. M grubundaki elemanların, R halkasındaki elemanlarla skaler çarpım fonksiyonu

$$R\times M \to M$$
$$(b,m) \to bm$$

olmak üzere,

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

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

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

iv. Her $m\in M$ için $1_R\, m=m$

koşullarının sağlanması durumunda M 'ye R üzerinde bir sol modül veya kısaca sol $R-$modül denir.

Yukarıdaki işlemler baz alındığında sağ $R-$modül de benzer şekilde tanımlanabilir. R halkasının değişmeli bir halka olması durumunda sağ modül aynı zamanda sol modül de olacağından ve bunun tersi de doğru olacağından M 'ye $R-$modül denir.

Not 1.3.1. Bu çalışmada modüller sol modül olarak nitelendirilecektir.

Önerme 1.3.1. $R-$modül M 'nin boştan farklı bir $K\subseteq M$ alt kümesinin bir alt modül olması için gerek ve yeter koşul $\forall r,r'\in R$ ve $\forall k,k'\in K$ için $rk+r'k'\in K$ olmasıdır.

Tanım 1.3.2. R bir halka, M ve K de $R-$modül olmak üzere $f:M\to K$ fonksiyonu aşağıdaki koşulları sağlıyorsa f fonksiyonuna bir modül homomorfizması veya $R-$homomorfizma denir.

i. Her $m,m'\in M$ için $f(m+m')=f(m)+f(m')$,

ii. Her $b\in R$ için $f(bm)=b\,f(m)$.

Tanım 1.3.3. R bir halka, M bir $R-$modül, $S=\{y_i\}_{i\in I}\subseteq M$ ve $r_i\in R$ olmak üzere, her $q\in M$ elemanı için $q=\sum_{i\in I} r_i\, y_i$ şeklinde sonlu bir toplam olarak yazılabiliyorsa ve bu toplam da tek türlü olarak belirlenebiliyorsa $S=\{y_i\}_{i\in I}$ kümesine M modülünün bir bazı (tabanı), M modülüne de serbest modül denir.

Teorem 1.3.1. R sonlu lokal bir halka ve bu halkanın maksimal ideali P, kalan cismi ise K olmak üzere aşağıdaki koşullar birbirine denktir.

i. R bir Frobenius halkadır.
ii. P maksimal idealinin anhilatörünün (sıfırlayıcısı) K kalan cismi üzerindeki boyutu 1'dir.

Teorem 1.3.2. R halkasının değişmeli bir halka olması durumunda,

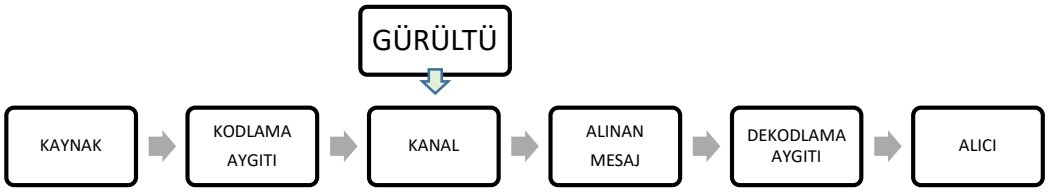
i. R bir Frobenius halkadır.
ii. R bir yarı-Frobenius bir halkadır.
iii. R halkası tek minimal ideale sahip lokal Artinian halkaların sonlu bir direkt toplamıdır.

ifadeleri denk ifadelerdir.

1.4. Hata Düzelten Kodlar

Kodlama teorisi dijital dünyadaki iletişim, veri aktarımı ve veri depolamasını ele alarak, gerçekleşecek veri transferi esnasında alıcı ile kaynak arasında kanal boyunca meydana gelebilecek hataların tespiti ve tespit edilen hataların düzeltilmesi üzerine çalışır. Claude Shannon tarafından 1948 yılında yayınlanan makale, kanal modelinin sistematik yapısına değinerek, iletişimde matematiksel teorinin gelişmesine öncülük etmiştir [6]. Bu makale iki araştırma sahasının ortaya çıkmasını sağlamıştır: Bilgi teorisi ve kodlama teorisi. Kodların varlığını ispatlayan, rollerini tanımlayan ancak bu kodların nasıl bulunacağı ile ilgilenmeyen, bilgi teorisinin öncüsü olan bu çalışmaya göre, veri transferi esnasında kaynaktan çıkan mesajın kanala uygun forma gelebilmesi için öncelikle mesaj kodlama aygıtına girer. Burada kodlandıktan sonra kodsöz adını alan bu mesaj daha sonra kanala aktarılır. Kanaldan çıkıp dekodlama aygıtına girerek

dönüştürülen mesaj alıcıya ulaştırılır. Veri transferinin basit şeması aşağıdaki gibi yapılabilir.



Şekil 1.1. Haberleşme sürecinin aşamaları

Kodsözler kanaldan geçerken gürültü (doğa olayları, manyetik alan vb.) adı verilen hatalara maruz kalması durumunda değişime uğrarlar. Gerçekleşen hata dekodlama kısmında düzeltilerek doğru kodsöz alıcıya iletilir. Bu esnada orijinal mesaja kontrol biti adı verilen eklemeler yapılarak bu mesaja cebirsel bir yapı kazandırılır. Kodlama teorisinin en temel hedefi mesajın mümkün olan en doğru formunun alıcıya ulaştırılması, verimin düşmeden minimum maliyet ve maksimum hız ile en üstün performanslara sahip kodları elde etmektir. Uygun kodlamanın nasıl yapılacağı konusu üzerine ilk adımı atan, hata düzelten kodların en temel yapıtaşlarından biri olan Hamming'in 1950 yılındaki [7] makalesi olmuştur. Sonrasında ise hızla büyüyerek mühendisler, bilgisayar bilimciler ve matematikçiler tarafından birçok çalışmanın konusu haline getirilmiştir. Bu kısımda [8-21] numaralı kaynaklar kullanılarak, kodlama teorisi, lineer kodlar, devirli kodlar ve aykırı devirli kodlar ile ilgili bazı temel tanım ve teoremler ele alınacaktır.

Tanım 1.4.1. $B=\{b_1,b_2,\ldots,b_q\}$ kümesi eleman sayısı q olan sonlu elemanlı bir küme olmak üzere B kümesi üzerindeki tüm sıralı $n-$liler kümesi B^n ile temsil edilsin. Bu durumda,

i. B kümesine kod alfabesi denir.

ii. $w_i \in B$ olmak üzere, $w=w_1w_2\ldots w_n$ dizisine B alfabesi üzerinde n uzunluğunda $q-$lu söz adı verilir. Aynı zamanda w sözü, $(w_1,\ldots,w_n)$ şeklinde bir vektör olarak ta ifade edilebilir.

iii. B kümesinin elemanlarından oluşan n uzunluğundaki vektörlerin oluşturduğu boştan farklı $C \subseteq B^n$ kümesine kod, bu C kodunun her bir elemanına da C kodunun kodsözleri adı verilir.

iv. B kümesi $\mathbb{Z}_2 = \{0,1\}$ kümesinin elemanlarından oluşuyorsa C koduna ikili kod adı verilir.

Tanım 1.4.2. $u = (u_1, \ldots, u_n)$ ve $v = (v_1, \ldots, v_n)$ sözleri aynı alfabe üzerinde tanımlanmış n uzunluğunda birer söz olmak üzere, bu iki söz arasındaki Hamming uzaklık $d_H(u,v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|$ ile tanımlanır.

Örnek 1.4.1. $B = \{0,1,2,3\}$ iken B^6 kümesinden seçilen $u = 123032$ ve $v = 220131$ kodsözleri arasındaki Hamming uzaklık $d_H(u,v) = 4$ olur.

Tanım 1.4.3. C kodunun farklı kodsözleri arasındaki uzaklıkların en küçüğüne C kodunun minimum Hamming uzaklığı denir ve $d_H(C)$ ile temsil edilir.

Tanım 1.4.4. q elemanlı bir alfabede tanımlı olan C kodu n uzunluğunda M eleman sayısına sahip ve minimum uzaklığı da d olan bir kod olsun. Bu durumda n, M, ve d sayılarına C kodunun parametreleri denir ve bu kod kısaca $(n, M, d)_q$ – kod olarak adlandırılır.

Örnek 1.4.2. $C = \{00000, 11001, 11011, 00010\}$ ikili kod olmak üzere C kodunun kodsözleri arasındaki Hamming uzaklıklar $d_H(11001, 11011) = 1$, $d_H(11001, 00010) = 4$ ve $d_H(11011, 00010) = 3$ olduğundan $d_H(C) = 1$ elde edilir. C koduna da $(5,4,1)_2$ – kod adı verilir.

Teorem 1.4.1. Hamming uzaklık fonksiyonu $d_H : B^n \times B^n \to \mathbb{N}$ aşağıdaki özellikleri sağlıyor ise (B^n, d_H) – ikilisine metrik uzay adı verilir.

Her $q,b,s \in B^n$ için,

i. (Pozitif tanımlılık) $d_H(q,b) \geq 0$ ve $d(q,b)=0 \Leftrightarrow q=b$,

ii. (Simetri) $d_H(q,b)=d_H(b,q)$,

iii. (Üçgen eşitsizliği) $d_H(q,b) \leq d_H(q,s)+d_H(s,b)$.

Tanım 1.4.5. $x=(x_1,\ldots,x_n)$ vektörü C kodunun bir kodsözü olmak üzere x kodsözünün sıfırdan farklı bileşen sayısına x vektörünün Hamming ağırlığı adı verilir ve $w_H(x)$ ile temsil edilir. Diğer yandan $w_H(x)=\left|\{i: x_i \neq 0\ , 1 \leq i \leq n\}\right|$ şeklinde de tanımlanabilir.

Tanım 1.4.6. C kodunun minimum ağırlığı, C kodundaki sıfırdan farklı kodsözlerin ağırlıklarının en küçüğü olarak tanımlanır.

Kodun tespit edebileceği ve düzeltebileceği hata sayısı hakkındaki bilgiyi kodsözler arasındaki en küçük uzaklık verir. Buradan hareketle aşağıdaki teoremler verilebilir.

Teorem 1.2.2. C kodunun $u-$hata tespit edebilmesi için gerek ve yeter koşul $d(C) \geq u+1$ olmasıdır.

Bu teorem diğer bir ifade ile,

Teorem 1.4.3. En küçük uzaklığı d olan C kodu tam olarak $d-1$ hata tespit eder.

Teorem 1.4.4. C kodunun $u-$hata düzeltebilmesi için gerek ve yeter koşul ise $d(C) \geq 2u+1$ olmasıdır.

Bu teorem diğer bir ifade ile;

Teorem 1.4.5. En küçük uzaklığı d olan C kodu tam olarak $\left\lfloor \frac{d-1}{2} \right\rfloor$ hata tespit eder.

1.4.1. Lineer kodlar

Kodsözlerin sonlu vektör uzayındaki vektörler olarak düşünülmesi durumunda vektör uzayının cebirsel özellikleri kullanılacağından kodlama teorisi baz alınarak yapılan çalışmaların çoğunluğu lineer kodlar üzerinedir. Ayrıca lineer kodların sistematik bir şekilde inşa edilebilmesi, kodlama ve dekodlamasının daha kolay yapılabilmesinin de lineer kodların önem kazanmasında büyük rol oynadığı söylenebilir. Bu kısımda [8-15] numaralı kaynaklar kullanılarak, öncelikle lineer cebir daha sonra ise lineer kodlar ile ilgili bazı temel tanım ve teoremler verilecektir.

Tanım 1.4.1.1. $\mathbb{F}$ cismi üzerinde tanımlı, elemanları vektörler olan $\mathbf{V}$ kümesi,

i. $\mathbf{V}$ kümesi toplama işlemine göre değişmeli bir gruptur.
ii. Her $q \in \mathbb{F}$ ve her $u \in \mathbf{V}$ için $qu \in \mathbf{V}$,
iii. Her $q \in \mathbb{F}$ ve her $u, v \in \mathbf{V}$ için $q(u+v) = qu + qv$,
iv. Her $q, b \in \mathbb{F}$ ve her $u \in \mathbf{V}$ için $(q+b)u = qu + bu$,
v. $1_{\mathbb{F}}$ elemanı $\mathbb{F}$ cisminin birimsel elemanı olmak üzere her $u \in \mathbf{V}$ için $1_{\mathbb{F}} u = u$

aksiyomlarını sağlıyorsa $\mathbf{V}$ kümesine vektör uzayı adı verilir.

Tanım 1.4.1.2. $\mathbf{V}$ vektör uzayının boştan farklı bir $\mathbf{W}$ alt kümesi $\mathbf{V}$ vektör uzayının bütün aksiyomlarını sağlıyorsa $\mathbf{W}$'ya $\mathbf{V}$ vektör uzayının bir alt vektör uzayı denir.

Teorem 1.4.1.1. $\mathbf{V}$ vektör uzayının boştan farklı bir $\mathbf{W}$ alt kümesi,

i. Her $x, y \in \mathbf{V}$ için $x + y \in \mathbf{W}$ ve
ii. Her $q \in \mathbb{F}$ için $qx \in \mathbf{W}$

aksiyomlarını sağlıyorsa $\mathbf{W}$ kümesi $\mathbf{V}$ vektör uzayının bir alt vektör uzayıdır.

Tanım 1.4.1.3. $\mathbb{F}$ cismi üzerinde $\mathbf{V}$ bir vektör uzayı, $U = \{u_1, \ldots, u_k\}$ vektörler kümesi ise $\mathbf{V}$ vektör uzayının boştan farklı bir alt kümesi olmak üzere,

$$\langle U \rangle = \{\alpha_1 u_1 + \ldots + \alpha_k u_k \mid \alpha_i \in F \ , 1 \le i \le k\}$$

kümesi $\mathbf{V}$ vektör uzayının bir alt uzayıdır ve $\langle U \rangle$ kümesine U vektörünün ürettiği alt uzay adı verilir. $\mathbf{V}$ vektör uzayının bir $C \subseteq \mathbf{V}$ alt vektör uzayı ve C alt vektör uzayının bir $U \subseteq C$ alt kümesi için C kodundaki her bir eleman U alt kümesindeki elemanların lineer kombinasyonu olarak yazılabiliyorsa U kümesine C kodunun üreteç kümesi adı verilir.

Tanım 1.4.1.4. $\mathbb{F}$ cismi üzerinde $\mathbf{V}$ vektör uzayı ve $\{v_1,\ldots,v_k\} \subseteq \mathbf{V}$ verilsin. $\alpha_1 v_1 + \ldots + \alpha_k v_k = 0$ olacak şekilde,

i. En az biri sıfırdan farklı olan $\alpha_1,\ldots,\alpha_k$ sabitleri mevcut ise $\{v_1,\ldots,v_k\}$ vektörler kümesi lineer bağımlıdır,

ii. $\alpha_1 = \ldots = \alpha_k = 0$ eşitliği mevcut ise $\{v_1,\ldots,v_k\}$ vektörler kümesi lineer bağımsızdır,

denir.

Tanım 1.4.1.5. $\mathbf{V}$ bir vektör uzayı olmak üzere $U = \{v_1,\ldots,v_k\}$ kümesinin lineer bağımsız bir küme ve $\mathbf{V}$ vektör uzayını geren bir küme olması durumunda U kümesine $\mathbf{V}$ vektör uzayının bir tabanı (bazı) denir.

Not 1.4.1.1. U kümesinin $\mathbf{V}$ vektör uzayının bir bazı olması durumunda $\mathbf{V}$ vektör uzayındaki her bir vektör U kümesindeki vektörlerin lineer kombinasyonu olarak tek türlü yazılır.

Not 1.4.1.2. $\mathbf{V}$ vektör uzayının herhangi bir tabanındaki eleman sayısı $\mathbf{V}$ vektör uzayının boyutu olarak adlandırılır.

Tüm bu tanımlamalar ışığında lineer kod tanımı aşağıdaki gibidir.

Tanım 1.4.1.6. $C \subseteq \mathbb{F}_q^n$ kodunun $\mathbb{F}_q^n$ vektör uzayının k boyutlu bir alt vektör uzayı olması durumunda C koduna $\mathbb{F}_q$ üzerinde n uzunluğunda, boyutu k olan lineer kod,

diğer bir ifadeyle, $[n,k]-$kodu adı verilir. C kodunun en küçük uzaklığının d olması durumunda ise bu lineer koda $[n,k,d]-$kodu adı verilir. n, k ve d sabitlerine de lineer kodun parametreleri adı verilir.

Tanım 1.4.1.7. C kodu n uzunluğunda lineer bir kod, $u=(u_1,\ldots,u_n)\in C$ ve $v=(v_1,\ldots,v_n)\in C$ de C kodunun kodsözleri olsun.

i. u kodsözü için Hamming ağırlık $w_H(u)=|\{i:u_i\neq 0\}|$ şeklinde tanımlıdır.

ii. u ve v kodsözleri arasındaki Hamming uzaklık ise $d_H(u,v)=w_H(u-v)$ eşitliği ile tanımlıdır.

iii. C kodunun sıfırdan farklı kodsözlerinin en küçük Hamming ağırlığına C kodunun en küçük ağırlığı denir ve $w_H(C)$ ile temsil edilir.

Teorem 1.4.1.2. C bir lineer kod ise $d_H(C)=w_H(C)$ eşitliği sağlanır.

Tanım 1.4.1.8. q elemanlı bir alfabe üzerinde tanımlı, n uzunluğunda, k boyutlu ve en küçük Hamming ağırlığı d olan, diğer bir ifade ile parametreler cinsinden ifade edilecek olursa, $[n,k,d]_q-$kod olan C lineer kodu için baz $S=\{c_1,\ldots,c_k\}$ olsun. $\alpha_1,\ldots,\alpha_k\in\mathbb{F}_q$ için, C kodunun her bir c elemanı $c=\alpha_1 c_1+\ldots+\alpha_k c_k$ şeklinde tek türlü olarak yazılır. Bu da C kodunun her bir elemanı ile $(\alpha_1,\ldots,\alpha_k)\in\mathbb{F}_q^k$ arasında birebir bir eşleme mevcut olduğu anlamına gelir. Böylece C kodunun eleman sayısının $|C|=q^k$ olduğu söylenir.

Not 1.4.1.3. Boyutun sıfır olması durumunda C koduna aşikâr kod adı verilir ve bu kod sadece sıfır vektörünü içerir.

Örnek 1.4.1.2. $C=\{000000,111010,110010,001000\}$ ikili lineer kodun kodsözlerinin ağırlıkları $w_H(000000)=0$, $w_H(111010)=4$, $w_H(110010)=3$ ve

$w_H(001000)=1$ olup C lineer kodun uzunluğu 6, minimum Hamming uzaklığı 1, boyutu da 2 olduğundan bu kod $[6,2,1]_2$ −kod olarak isimlendirilir.

Tanım 1.4.1.9. C bir lineer kod, $u=(u_1,\ldots,u_n)\in \mathbb{F}_q^n$ ve $v=(v_1,\ldots,v_n)\in \mathbb{F}_q^n$ vektörleri ise $\mathbb{F}_q^n$ vektör uzayında tanımlı iki vektör olmak üzere, işlemler $\mathbb{F}_q$ üzerinde olacak şekilde, u ve v vektörlerinin Öklit iç çarpımı $\langle u,v\rangle = u_1v_1+\ldots+u_nv_n$ ile hesaplanır.

Tanım 1.4.1.10. n,k,d parametrelerinden n ve k aynı iken d parametresinin, n ve d aynı iken k parametresinin en iyi olduğu kodlara optimal kod adı verilir.

Tanım 1.4.1.11. $\beta\in\mathbb{Z}_4$ için, Öklit ağırlık $w_E(\beta)=\min\left\{\beta^2,(4-\beta)^2\right\}$ ile, Lee ağırlık ise $w_L(\beta)=\min\{|\beta|,|4-\beta|\}$ şeklinde tanımlanır.

Tanım 1.4.1.12. Her $c,c'\in C$ kodsöz çifti arasındaki Lee uzaklık $d_L(c,c')$, Öklit uzaklık ise $d_E(c,c')$ olmak üzere,

i. $d_L=\min d_L(c,c')$ ifadesine C kodunun en küçük Lee uzaklığı,

ii. $d_E=\min d_E(c,c')$ ifadesine ise C kodunun en küçük Öklit uzaklığı

denir.

1.4.2. Devirli kodlar

Lineer kodların özel bir ailesi olan devirli kodlar ilk olarak Eugene Prange tarafından 1957 yılında [16] çalışması ile keşfedilmiştir. Daha sonra bu kodlar üzerindeki çalışmalar ciddi derecede önem kazanmış, Hamming kodlar, BCH kodlar ve Golay kodlar gibi birçok devirli kod aileleri inşa edilmiştir.

Koddaki her bir kodsözün bir devir döndürülmesi (kaydırılması) durumunda yine bir kodsöz elde edilebiliyorsa bu kodlara devirli kod adı verilecektir. Devirli kodlar kodlama ve dekodlamada avantaj sağladığından lineer kodların en önemli sınıflarından biri olduğu söylenebilir. Bu kodların yapısı incelendiğinde uzunluğu n olan devirli bir kodun derecesi $n-k$ olan bir polinom tarafından belirlenebildiği görülmüştür. Bu kısımda [8] ve [17] numaralı kaynaklar kullanılarak, devirli kodlar ile ilgili bazı temel tanım ve teoremlere yer verilecektir.

Tanım 1.4.2.1. C, uzunluğu n olan lineer bir kod olsun. Her $(c_0, c_1, \ldots, c_{n-1}) \in C$ için $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ sağlanıyor ise C koduna devirli kod adı verilir. Diğer bir ifadeyle, $\sigma(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ şeklinde tanımlanan bir permütasyon için $\sigma(C) = C$ eşitliği sağlanıyorsa C koduna devirli kod denir. Burada devirsel hareketi sağlayan σ dönüşümüne ise devirsel öteleme operatörü adı verilir.

Devirli kodların kombinatoriyel yapısını cebirsel yapıya dönüştürmek için polinomlardan yardım alınır.

C, $\mathbb{F}_q^n$ üzerinde lineer bir kod olmak üzere, lineer $\Gamma : \mathbb{F}_q^n \to \mathbb{F}_q[x] \Big/ \langle x^n - 1 \rangle$ dönüşümü ile $c = (c_0, \ldots c_{n-1})$ kodsözü $\mathbb{F}_q[x]$ polinom halkasındaki $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ polinomu ile birebir ve örten bir şekilde eşleştirilir. Bu durumda c elemanının devirsel ötelemesi $\mathbb{F}_q[x]$ polinom halkasında $x\,c(x)$ polinomuna karşılık gelir. Daha açık bir şekilde ifade edilecek olursa, herhangi bir $(c_0, c_1, \ldots, c_{n-1}) \in C$ kodsözü için $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ ifadesi artık $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \in C$ iken $x(c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}) \in C$ şeklinde ifade edilebilir. Bu da C kodunun tanımlanan birebir ve örten Γ lineer dönüşümü altındaki görüntüsünün yine C kodunun içine düştüğü anlamına gelir. Ayrıca bu dönüşümün bir izomorfizma olduğunu görmek te oldukça kolaydır. Tanımlanan Γ lineer dönüşümü aracılığıyla devirli kodlar ideallerle izah edilebilir.

Teorem 1.4.2.1. $C \subseteq \mathbb{F}_q^n$ lineer kodunun devirli bir kod olması için gerek ve yeter şart $\Gamma(C)$ kümesinin $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ bölüm halkasının bir ideali olmasıdır.

Teorem 1.4.2.2. L ideali $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ bölüm halkasının sıfırdan farklı bir ideali, $g(x)$ polinomu da L idealindeki sıfırdan farklı başkatsayısı 1 olan en küçük dereceli bir polinom olsun. Bu takdirde $g(x)$ polinomu L idealinin bir üretecidir ve $x^n - 1$ polinomunu böler.

Not 1.4.2.1. $C \subseteq \mathbb{F}_q^n$ kodu devirli bir kod olmak üzere $\Gamma(C) = \langle g(x) \rangle$ eşitliği sağlanıyorsa $g(x)$ polinomuna C devirli kodunun üreteç polinomu denir ve $C = \langle g(x) \rangle$ ile temsil edilir.

Teorem 1.4.2.3. $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ bölüm halkasının sıfırdan farklı herhangi bir L idealinin sıfırdan farklı en küçük dereceli monik polinomu tektir.

Tanım 1.4.2.2. $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ bölüm halkasının sıfırdan farklı L idealinin sıfırdan farklı en küçük dereceli monik polinomu L idealinin üreteç polinomu olarak adlandırılır. Devirli C kodu için $\Gamma(C)$'nin üreteç polinomu ile C kodunun üreteç polinomu aynıdır.

Teorem 1.4.2.4. $\mathbb{F}_q[x]$ halkasının bir elemanı olan ve $x^n - 1$ polinomunu bölen $g(x)$ polinomunun derecesi k olmak üzere bu polinom tarafından üretilen ideale tekabül eden kod uzunluğu n, boyutu ise $n-k$ olan devirli koddur.

Tanım 1.4.2.3. $f(x)=a_0+a_1x+\ldots+a_tx^t$ polinomu $\mathbb{F}_q[x]$ halkasında derecesi t olan polinomun ters sıralı polinomu $f^*(x)=x^t f\left(\frac{1}{x}\right)=\sum_{i=0}^{t}a_{t-i}x^i$ ile tanımlıdır.

Teorem 1.4.2.5. C kodu $g(x)$ polinomu tarafından üretilen $\mathbb{F}_q$ üzerinde n uzunluğunda devirli kod ve $x^n-1=g(x)h(x)$ olsun.

i. Derecesi $n-t$ olan $g(x)=g_0+g_1x+\ldots+g_{n-t}x^{n-t}$ polinomu dikkate alınarak C kodunun üreteç matrisi

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

ile tanımlanır.

ii. Derecesi t olan $h(x)=h_0+h_1x+\ldots+h_tx^t$ polinomu ele alınarak C kodunun kontrol matrisi

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

ile tanımlanır.

Tanım 1.4.2.4. C kodu, $\mathbb{F}_q$ üzerinde uzunluğu $n=ml$ olan bir lineer blok kod olsun. Her $c\in C$ kodsözü l devir yaptıktan sonra da C kodunda bir kodsöz, yani $c=(c_0,\ldots,c_{n-1})\in C$ iken $(c_{n-l},\ldots,c_0,\ldots,c_{n-l-1})\in C$, olmak üzere $\upsilon_l(c)=\left(\sigma(c_0)\,\middle|\,\sigma(c_1)\,\middle|\,\ldots\,\middle|\,\sigma(c_{n-1})\right)\in C$ oluyorsa C koduna $l-$parçalı devirli (quasi cyclic) kod denir. Burada l sayısı kodu sabit bırakan en küçük devir sayısını, υ_l dönüşümü $l-$

parçalı devirli kod operatörünü, σ dönüşümü devirsel öteleme operatörünü temsil etmektedir.

Tanım 1.4.2.5. C kodu uzunluğu n olan lineer bir kod olsun. R halkasındaki birimsel elemanlar λ ile temsil edilmek üzere C kodundan alınan $c=(c_0,\ldots,c_{n-1})\in C$ kodsözü için $(\lambda c_{n-1},c_0,\ldots,c_{n-2})\in C$ sağlanıyorsa, diğer bir ifade ile, $\rho_\lambda(c_0,c_1,\ldots,c_{n-1})=(\lambda c_{n-1},c_0,\ldots,c_{n-2})$ ile tanımlanan permütasyon için $\rho_\lambda(C)=C$ eşitliği sağlanıyorsa C koduna $\lambda-$sabit devirli ($\lambda-$constacyclic) kod denir. Burada λ devirsel hareketi sağlayan ρ_λ dönüşümüne ise $\lambda-$sabit devirli öteleme operatörü adı verilir.

Not 1.4.2.3. Tanım 1.4.2.4.'te $l=1$ olması durumunda parçalı devirli kodların aynı zamanda bir devirli kod, Tanım 1.4.2.5.'te ise $\lambda=1$ olması durumunda $\lambda-$sabit devirli kodların aynı zamanda bir devirli kod olacağı aşikardır. Bu bağlamda parçalı devirli ve $\lambda-$sabit devirli kodlar için devirli kodların birer genellemesi olduğu rahatlıkla söylenebilir.

1.4.3. Aykırı devirli kodlar

İlk olarak Boucher ve ark. tarafından 2007 yılında [18] makalesiyle tanımlanan ve aynı zamanda devirli kodların önemli bir genellemesi olan aykırı devirli kodlar, devirli kodlardaki gibi polinom halkaları ile çalışılmış ve bu kod ailesinin zengin bir cebirsel yapı kazanması sağlanmıştır. Ancak bu kod ailesinde işlem yaparken kullanılan toplama işlemi bilinen toplama işlemi olmasına rağmen çarpma işleminin bilinen çarpma işleminden farklı olduğuna dikkat edilmelidir. Tanımlanan bu çarpma işlemi, aykırı polinom halkasının değişmeli olmayan bir yapıda olmasının en temel sebebidir. Aykırı devirli kodlar optimal kod bulma açısından devirli kodlara göre çok daha avantajlı yapılardır. Aykırı devirli kodlar, bazı çalışmalarda $\Theta-$devirli kod olarak ta adlandırılmaktadır. Bu kısımda aykırı devirli kodlar ile ilgili bazı temel tanım ve teoremler ele alınırken, [13, 19, 20, 21] numaralı kaynaklardan yararlanılmıştır.

Tanım 1.4.3.1. $\mathbb{F}_{q^m}$ bir cisim ve bu cisim üzerinde tanımlanmış bir otomorfizma Θ olmak üzere,

$$\mathbb{F}_{q^m}[x,\Theta]=\left\{ f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1} \;\middle|\; a_i\in\mathbb{F}_{q^m},\ 0\le i\le n-1\right\}$$

kümesi polinom halkalarında tanımlı olan standart toplama işlemi ve $\left(ax^i\right)*\left(bx^j\right)=a\,\Theta^i(b)\,x^{i+j}$ ile tanımlanan farklı bir çarpma işlemine göre bir halka belirtir. Bu halkaya da aykırı polinom halkası adı verilir.

Not 1.4.3.1. Bu tanım $\mathbb{F}_{q^m}$ cismi yerine bir R halkası alınarak ta ifade edilebilir.

Tanım 1.4.3.2. C kodu $\mathbb{F}_q$ cismi üzerinde uzunluğu n olan lineer bir kod, Θ ise $\mathbb{F}_q$ cismi üzerinde tanımlı bir otomorfizma olmak üzere her $c=\left(c_0,\ldots,c_{n-1}\right)\in C$ kodsözü için $\sigma_\Theta(c)=\left(\Theta(c_{n-1}),\Theta(c_0),\ldots,\Theta(c_{n-2})\right)\in C$ ifadesi sağlanıyorsa C koduna uzunluğu n olan aykırı devirli kod denir. Buradaki σ_Θ dönüşümü aykırı devirsel öteleme operatörünü temsil etmektedir.

Sonuç 1.4.3.1. Θ otomorfizmasının birim otomorfizma olması durumunda C kodu devirli kod olur. Bu da aykırı devirli kodların devirli kodları kapsadığını gösterir.

C kodunun kodsözleri polinomlar cinsinden ifade edilmek istenirse, birebir ve örten olan

$$\psi: C\to \mathbb{F}_q[x,\Theta]\Big/ x^n-1$$
$$\left(c_0,\ldots,c_{n-1}\right)\to c(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$$

dönüşümü ile tanımlanır. Buradaki ψ dönüşümü bir izomorfizmadır. $c\in C$ kodsözünün aykırı devirsel ötelenmiş formu $\sigma_\Theta(c)$ polinomu yazımı olarak

$xc(x)=\Theta(c_{n-1})+\ \Theta(c_0)x+\ldots+\Theta(c_{n-2})x^{n-1}$ ifadesine tekabül eder. Yukarıdaki dönüşüm altında C kodunun görüntüsü de C ile gösterilsin.

Teorem 1.4.3.1. $\mathbb{F}_q$ cismi üzerinde tanımlı uzunluğu n olan C kodu bir lineer kod olsun. C kodunun aykırı devirli kod olması için gerek ve yeter koşul C kodunun $\mathbb{F}_q[x,\Theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $\mathbb{F}_q[x,\Theta]-$alt modülü olmasıdır.

Önerme 1.4.3.1. C kodu $\mathbb{F}_q[x,\Theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $\mathbb{F}_q[x,\Theta]-$alt modülü olsun. Bu takdirde C kodu devirli alt modüldür ve C kodundaki sıfırdan farklı en küçük dereceye sahip monik bir polinom tarafından üretilir.

Teorem 1.4.3.2. C kodu $\mathbb{F}_q[x,\Theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $\mathbb{F}_q[x,\Theta]-$alt modülü ve $f(x)$ polinomu da C kodunda sıfırdan farklı en küçük dereceye sahip monik bir polinom olmak üzere $f(x)$ polinomu x^n-1 polinomunun bir sağ bölenidir.

Tanım 1.4.3.3. $\mathbb{F}_q[x,\Theta]$ halkasında $x^n-1=g(x)h(x)$, C kodunu üreten $g(x)$ polinomunun derecesi de r olsun. C kodu $\mathbb{F}_q[x,\Theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $\mathbb{F}_q[x,\Theta]-$alt modülü olmak üzere C kodu serbest bir sol $\mathbb{F}_q-$alt modülüdür. Bu takdirde C kodunun bir tabanı $\varsigma=\{g(x),xg(x),\ldots,x^{n-r-1}g(x)\}$ formundadır. $\alpha_i\in\mathbb{F}_q$ olmak üzere C kodundaki her bir $c\in C$ elemanı $c=\alpha_0 g(x)+\alpha_1 x g(x)+\ldots$ $+\alpha_{n-r-1}x^{n-r-1}g(x)$ şeklinde yazılabilir ve bu yazılış tek türlüdür.

Not 1.4.3.3. x^n-1 polinomunun sağ bölenleri $\mathbb{F}_q[x,\Theta]\Big/\langle x^n-1\rangle$ modülünde birer sol $\mathbb{F}_q[x,\Theta]-$alt modül üretir ve bu modüller de aykırı devirli koda tekabül eder. x^n-1 polinomunun derecesi $n-t$ olan her bir sağ böleni, uzunluğu n boyutu t olan aykırı devirli bir kod üretir.

Teorem 1.4.3.3. $\mathbb{F}_q[x,\Theta]$ halkasında x^n-1 polinomunun bir sağ böleni ve derecesi $n-t$ olan $g(x)=g_0+g_1x+\ldots+g_{n-t}x^{n-t}$ polinomu tarafından üretilen n uzunluğundaki aykırı devirli C kodunun üreteç matrisi

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{t-1}g(x) \end{pmatrix}=\begin{pmatrix} g_0 & g_1 & \cdots & \cdots & g_{n-t} & 0 & 0 & \cdots & 0 \\ 0 & \Theta(g_0) & \Theta(g_1) & \cdots & \cdots & \Theta(g_{n-t}) & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \ddots & & & \vdots \\ 0 & 0 & \cdots & 0 & \Theta^t(g_0) & \Theta^t(g_1) & \cdots & \cdots & \Theta^t(g_{n-t}) \end{pmatrix}$$

şeklinde tanımlanır.

Teorem 1.4.3.3. $\mathbb{F}_q$ üzerinde tanımlı uzunluğu n olan C kodu aykırı devirli bir kod, Θ otomorfizmasının mertebesi de m olsun. m ile n sayılarının aralarında asal olması durumunda C kodu devirli bir koddur.

Teorem 1.4.3.4. $t\le n$ olmak üzere derecesi t olan $h(x)$ polinomu ve derecesi $n-t$ olan $g(x)$ polinomu $\mathbb{F}_q[x,\Theta]$ halkasında tanımlı iki polinom ve $\Theta^n(g(x))=\Theta^n(g_0)+\Theta^n(g_1)x+\ldots+\Theta^n(g_{n-t})x^{n-t}$ olmak üzere $x^n-1=h(x)g(x)$ olması için gerek ve yeter koşul $x^n-1=\Theta^n(g(x))h(x)$ olmasıdır.

Teorem 1.4.3.5. Θ otomorfizmasının mertebesi m ve $\mathbb{F}_q$ cisminin otomorfizma tarafından sabit bırakılan alt cismi K olsun. m ile n sayılarının aralarında asal olması

durumunda $x^n - 1$ polinomunun $\mathbb{F}_q[x, \Theta]$ halkasındaki çarpanlara ayrılışı $K[x]$ değişmeli halkasındaki çarpanlara ayrılıştan ibarettir.

1.5. DNA ile İlgili Bazı Temel Bilgiler ve DNA Kodlar

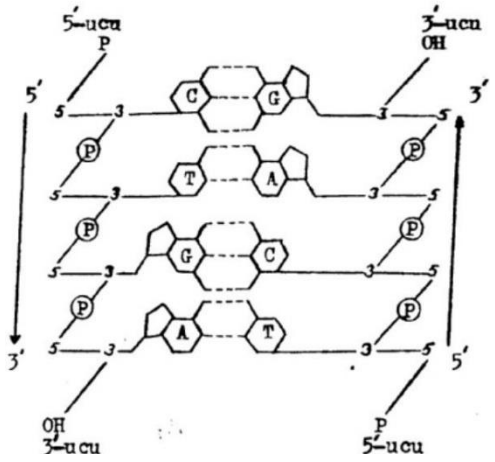
DNA, hücrelerin canlılık işlevlerinin gerçekleşebilmesi için gerekli olan genetik bilgiyi taşıyan moleküldür. Burkulmuş merdiven görüntüsünde olan DNA yapısının asıl iskeleti şeker ve fosfat kombinasyonundan oluşur.

Şekil 1.2. DNA çift sarmal görüntüsü [22]

Bilginin genetik şekilde depolandığı yer olan adeta merdiven basamaklarını andıran yapı ise Adenin (A), Timin (T), Guanin (G), Sitozin (C) adı verilen dört temel bazın birbiri ardına dizilmesinden oluşur ve DNA molekülünün bir iplikçiğini oluştururlar. İki DNA iplikçiği Watson Crick Complement (WCC) özelliği ile birbirine tutunur ve böylece DNA'yı kalıtımın temelini oluşturmaya uygun molekül yapan çift sarmal yapıyı oluşturur. Watson Crick Complement özelliği gereğince Adenin ile Timin, Guanin ile Sitozin birbirinin tamamlayanı olup Adenin ile Timin arasında ikili hidrojen bağı, Guanin ile Sitozin arasında ise üçlü hidrojen bağı mevcuttur. Bu yapının oluşması hibridizasyon olarak adlandırılır.

DNA dizisinin uç noktaları $3'-$ucu ve $5'-$ucu olarak isimlendirilir ve hem DNA hem de RNA dizileri yazılırken $5'-$ucundan $3'-$ucuna doğru yazılır. Çift sarmal yapı oluşurken birbirinin tamlayanı olan uygun DNA bazlarının bir araya gelme esnasında

$3'-$ucu ve $5'-$ucu birbirini tamamlar. Bu anlatıma göre, DNA dizisi ile bu DNA dizisinin ters sıralı tamlayanının DNA çift sarmalını oluşturacağı aşikârdır.



Şekil 1.3. DNA ipliğinin bir parçası [23]

Örnek 1.5.1. $5'-ATGACGTTACGAT-3'$ ile $5'-ATCGTAACGTCAT-3'$ DNA dizileri Watson Crick Complement (WCC) özelliğine göre birbirine bağlanarak DNA çift sarmal yapısını oluştururlar.

Tanım 1.5.1. Uzunluğu n olan vektörlerden oluşan D kodunun $\{f_1,\ldots,f_n\}$ kodsözlerinin bileşenleri $\{A,T,G,C\}$ kümesinin elemanları ise koduna DNA kod adı verilir.

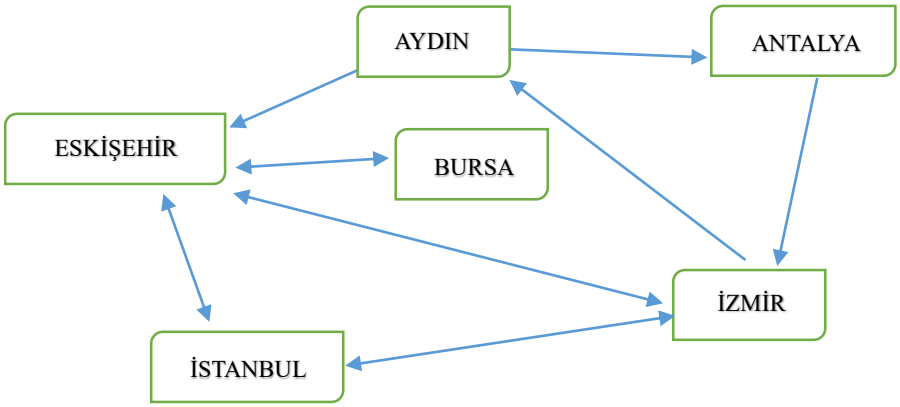
Tanım 1.5.2. D bir DNA kod, u da bir kodsöz olmak üzere u kodsözünün ters sıralısı u^R, tamlayanı $\bar{u}$, ters sıralı tamlayanı ise $\overline{u^R}$ ile temsil edilir.

Örnek 1.5.2. $u=ATCAGGCTAACT$ DNA kodsözünün ters sıralısı $u^R=TCAATCGGACTA$, tamlayanı $\bar{u}=TAGTCCGATTGA$, ters sıralı tamlayanı ise $\overline{u^R}=AGTTAGCCTGAT$ şeklindedir.

1.5.1. DNA kodlar ve DNA hesaplama

7 düğüm için Hamilton yolu problemi Adleman [24] numaralı makalesinde, sentetik DNA dizilerinin deney tüplerinde WCC özelliğine göre dizilerin karşılıklı etkileşimlerinden faydalanarak manipüle edilmesi ile çözmüştür. Ayrıca bu çalışma matematiksel problemlerin çözümü için DNA dizilerinin bir hesaplama aracı olması bakımından öncü olmaktadır. Hamilton yolu problemine kısaca değinmek gerekirse; yönlü yahut yönsüz bir graf verilmesi durumunda her bir düğümden yalnız bir defa geçilmek suretiyle tüm düğümlere uğrayarak geçen bir yol olup olmadığının araştırıldığı bir problemdir. [25] makalesinden yararlanarak bu problem deneyinin 6 düğüm için modellendiği örnek aşağıda verilmiştir.

Örnek 1.5.1.1. Şekil 1.4.'te şehirlerarasındaki uçuşlar yönlü graf ile gösterilmiştir. Bu grafa göre Aydın'dan Eskişehir'e, Aydın'dan Antalya'ya, İzmir'den Aydın'a ve Antalya'dan İzmir'e uçuş varken Eskişehir'den Aydın'a, Antalya'dan Aydın'a, Aydın'dan İzmir'e ve İzmir'den de Antalya'ya uçuş yoktur.



Şekil 1.4. Şehirlerarası uçuşlar

Aydın'dan başlayıp her bir şehire birer kez uğramak koşuluyla Bursa'ya giden bir Hamilton yol arandığı varsayılsın. Bu yolu bulabilmek için öncelikle her bir şehir 6 uzunluğundaki sentetik DNA dizileri ile kodlansın.

Tablo 1.1. Şehirler ve DNA karşılıkları

Şehirler	**DNA dizisi**
Aydın	*AGCTAC*
Antalya	*CATTGC*
İzmir	*CCTAGC*
İstanbul	*AATCTA*
Eskişehir	*GCATTC*
Bursa	*AAGCTA*

Şehirlerarasındaki olası tüm uçuşların hesaplaması, var olan şehirler için yapılan sentetik DNA kodlamaları göz önünde bulundurularak bu kodların tamamlayıcı bazları ile temsil edilecektir. Bu uçuşlar arasındaki hesaplamalar yapılırken kalkış şehrini simgeleyen DNA dizisinin son $3-$bazının tamlayanı ile varış şehrini simgeleyen DNA dizisinin ilk $3-$bazının tamlayanı şeklinde kodlanacaktır.

Tablo 1.2. Uçuşların DNA hesaplanması

Uçuşlar	**DNA karşılıkları**	**Yolun DNA kodlaması**
Aydın -- Antalya	*AGCTAC – CATTGC*	*ATGGTA*
Antalya -- İzmir	*CATTGC – CCTAGC*	*ACGGGA*
İzmir – İstanbul	*CCTAGC – AATCTA*	*TCGTTA*
İstanbul – Eskişehir	*AATCTA – GCATTC*	*GATCGT*
Eskişehir – Bursa	*GCATTC – AAGCTA*	*AAGTTC*

Hamilton yolu probleminin çözümü için her bir şehre karşılık gelen sentetik DNA dizileri bir deney tüpüne, yollara karşılık gelen DNA dizileri ise çoğaltılarak diğer bir deney tüpüne koyulur ve bu iki tüp ortak bir kapta gerekli enzimler ile desteklenerek hibridizasyonun gerçekleşmesi sağlanır. Hibridizasyon gerçekleştikten sonra ilk olarak elde edilen farklı uzunluktaki DNA zincirlerinden 6 uzunluğundaki zincirler ayrıştırılır, daha sonra ise ayrıştırma yöntemleri kullanılarak Aydın ile başlayıp Bursa ile biten zincirlere ulaşılır. Son olarak kalan DNA dizileri Tablo 1.2.'deki gibi kodlanarak problemin çözümü elde edilir. Burada da açıkça görüldüğü gibi hibridizasyon sonucunda istenilen sonuca ulaşabilmek için DNA hesaplamalarındaki en önemli adımlardan biri problemin DNA dizilerine uygun aktarımını bulmaktır. Bu diziler arasında işe yaramayacak hibridzasyonların da gerçekleşmesi mümkün olabileceğinden problemin doğru çözümüne ulaşabilmek, bu süre zarfında da verimi düşürmemek ve hatalı hibridizasyon oluşma ihtimalinin en düşük seviyeye indirgeyebilmek adına DNA kodlarda bazı kombinatöriyel kısıtların sağlanması gerekir. Detaylı bilgi için [26] ve [27] numaralı makaleler incelenebilir.

n uzunluğundaki DNA kod, $f_i \in \{A,G,C,T\}$ olmak üzere, $(f_0, f_1, \ldots, f_{m-1})$ kodsözlerinin bir kümesi olarak adlandırılır. Bu kodsözler için aşağıdaki kısıtlar mevcuttur.

D bir DNA kod, d ise kodsözler arasındaki uzaklık olmak üzere,

i. Hamming uzaklık kısıtı: Birbirinden farklı her $u,v \in D$ için $d(u,v) \geq d$,

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

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

iv. $GC-$miktar kısıtı: D kodundaki her bir kodsözün G ve C bazlarının toplam sayısının aynı olmasıdır.

Not 1.5.1.1. Bu tezde Hamming uzaklık kısıtı, ters-sıra kısıtı ve ters-sıra tamlayan kısıtı kullanılacak olup $GC-$miktar kısıtı açık bir problem olarak bırakılacaktır.

Tanım 1.5.1.1. D bir DNA kod olmak üzere D kodundan alınan her $u \in D$ kodsözü için u^R vektörü de D kodunun bir kodsözü oluyorsa D koduna ters sıralı DNA kod denir.

Tanım 1.5.1.2. D bir DNA kod olmak üzere D kodundan alınan her $u \in D$ kodsözü için $\overline{u^R}$ vektörü de D kodunun bir kodsözü oluyorsa D koduna ters sıralı tamlayan DNA kod denir.

Ters sıralı DNA kodlar, ters sıralı tamlayan DNA kod elde edebilmek adına büyük önem arz etmektedir ve bu kodlardan ters sıralı tamlayan DNA kodu elde etmek te oldukça kolaydır.

Örnek 1.5.1.2. $D = \{GGGG, AGAT, GCTA, TAGA, ATCG\}$ bir ters sıralı DNA kod, $D' = \{GGGG, CCCC, AGAT, GCTA, TAGA, ATCG, TCTA, CGAT, ATCT, TAGC\}$ ise ters sıralı tamlayan DNA koddur.

BÖLÜM 2. $\mathbb{Z}_4[u]/\langle u^k - u^{k-1}\rangle$ HALKASI ÜZERİNDE DEVİRLİ VE SABİT DEVİRLİ KODLAR

Lineer kodların önemli bir sınıfı olan devirli kodlar üzerine pek çok çalışma mevcut olmasının en temel gerekçesi, polinom halkalarının ideallerine karşılık gelmesi sebebiyle zengin bir cebirsel yapıya sahip olmasıdır. Bu yapı devirli kodların uygulanabilirliğini kolaylaştırdığından lineer kodların en önemli ve üzerine en çok yoğunlaşılan çalışma alanlarından biridir. Devirli kodlar ilk olarak Eugene Prange tarafından [28] numaralı çalışma ile ortaya çıkmıştır. Kodlama teorisinde önemli bir dönüm noktası olarak kabul edilen Hammons ve ark.'nın ufuk açıcı [29] numaralı çalışmasıyla da sonlu halka üzerindeki kodlara ilgi başlamıştır. Bu makalenin ortaya çıkışı, çalışmalara yeni bir boyut kazandırmış ve bu sayede halkalar üzerine birçok araştırma yapılmasına olanak sağlamıştır. Uygulamaları açısından ve yaygın bir çalışma alanına sahip olduğundan pek çok araştırmacının da dikkatini çekerek kodlama teorisinde ilgi çeken bir konu haline gelmiştir. Böylelikle çeşitli halkalar üzerindeki devirli kodların yapısının incelenmesinde önemli oranda artışa neden olmuştur [30-35]. Birçok farklı metot ve farklı yaklaşımlar ile geniş bir alanda ele alınsa da $\mathbb{Z}_4$ üzerindeki kodlar dizayn, kriptoloji, DNA kodlar, latisler, stenografi gibi birçok alanla ilişkili olması nedeniyle kodlama teorisinde seçkin bir yere sahiptir [15, 36-42]. Kodlama teorisinde büyük önem arz eden bu kodlar üzerindeki yoğun çalışmalar neticesinde N. Aydın ve T. Asemov tarafından online bir veritabanı oluşturulmuştur [43]. Sonlu zincir halkası olmayan ancak Frobenius halka olan ve zengin cebirsel yapıya sahip birçok yeni halka aileleri de incelenmiştir. Bu halkalardaki lineer kodları ele alan çalışmalar incelendiğinde Gray dönüşümün önemli bir yere sahip olduğu görülmektedir.

Abualrub ve Şiap [36] numaralı çalışmada, $\mathbb{Z}_4$ halkasında n uzunluğundaki devirli kodların üreteç kümesini oluşturmuş ve bu halkadaki devirli kodların minimum Hamming uzaklığını inceleyerek $5-10$ uzunluktaki ters sıralı devirli kodlara örnekler vermiştir. Al-Ashker ve Hamoudeh [37] numaralı çalışmada, $u^k=0$ iken $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2+\ldots+u^{k-1}\mathbb{Z}_2$ halkasında uzunluğu n olan devirli kodların yapısını araştırmış, rank ve en küçük geren kümeyi oluşturmuşlardır. Ayrıca bazı örnekler de sunmuşlardır. Singh ve Kewat [38] numaralı çalışmada, $u^k=0$ iken $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4+\ldots+u^{k-1}\mathbb{Z}_4$ halkasının çekirdeğinden yararlanarak devirli kodların üreteç polinomunu ve en küçük geren kümeyi oluşturmuşlardır. Ayrıca rank incelemesi de yaparak çeşitli halkalar üzerinde birçok örnek te sunmuşlardır. Bandi ve Bhaintwal [39] numaralı çalışmada, $\mathbb{Z}_4[v]/\langle v^2-v\rangle$ halkasındaki lineer kodları inceleyerek halka üzerindeki $C=C_1+vC_2$ lineer kodunun devirli kod olması için gerek ve yeter koşulları ispatlamışlardır. Devirli kodların üreteçleri için genel bir form oluşturmuş, halka üzerindeki Galois genişlemelerini de ele alarak bu genişlemelerin ideal yapısını incelemişlerdir. Tek uzunluktaki devirli kodların rankını ve en küçük geren uzaylarını araştırarak tek eleman tarafından üretilen devirli kodlara odaklanmış ve bu kodların serbest $R-$modül olması gerektiği sonucuna ulaşmışlardır. Ayrıca halkadaki kodların Lee ağırlık sayacı için MacWilliams özdeşliğini oluşturmuş ve halka üzerindeki kendine dual kodların inşa metotlarını incelemişlerdir. Özen ve ark. [15] numaralı çalışmada, $u^2=1$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkasındaki devirli kodların cebirsel yapısını incelemişlerdir. Bu halka üzerindeki devirli kodların yapısından yararlanarak $(2+u)-$ sabit devirli kodları ele almışlardır. Devirli kodların ve sabit devirli kodların $\mathbb{Z}_4-$ görüntülerini incelemiş ve birçok örnek sunmuşlardır. Bandi ve Bhaintwal [40] numaralı çalışmada, $u^2=0$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkasındaki devirli kodların cebirsel yapısını inceleyerek bu kodların üreteç polinomlarını oluşturmuşlardır. Devirli kodu geren en küçük kümeyi ve bu kodun rankını elde ederek bu kodların $\mathbb{Z}_4$ serbest modül olması için gerek ve yeter koşulu belirlemişlerdir. Ayrıca birçok örnek te sunmuşlardır. Gao ve ark. [41] numaralı çalışmada, $v^2=v$ iken $\mathbb{Z}_4+v\mathbb{Z}_4$ halkası üzerindeki devirli

kodların inşasını ele alarak lineer kodların birçok sınıfını çalışmışlardır. Ayrıca halka üzerindeki devirli kodların önemli bir sınıfı olan kuadratik kalan kodları da inceleyerek yeni lineer $\mathbb{Z}_4$ kodlar bulmuşlardır. Özen ve ark. [42] numaralı çalışmada, $u^3 = 0$ iken $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ halkasında devirli kodların yapısını belirlemiş ve bu kodlardan yararlanarak $\mathbb{Z}_4$ halkası üzerinde yeni kodlar bulmuşlardır. Halka üzerinde Galois genişlemesi ve bu genişlemenin ideal yapısını da incelemişlerdir. Ayrıca devirli kodların üreteç polinomlarından yaralanarak en küçük geren kümeyi belirlemişlerdir.

Blok dizayn, latisler ve modüler formlar gibi diğer matematiksel yapılarla yakından bağlantılı olduğu için hata düzelten kodlar teorisinde önemli bir yere sahip olan kod ailelerinden biri de kendine dual (self dual) kodlardır. Literatürde kendine dualliği kapsayan ve kendine dual kodları karakterize eden birçok çalışma vardır [13, 44-46].

Bazı araştırmacılar tarafından halkalar üzerindeki sabit devirli kodlar, negadevirli (negacyclic) kodlar, parçalı devirli kodlar ve parçalı sabit devirli (quasi twist) kodlar gibi devirli kodların bazı genelleştirmeleri çalışılmış ve bu çalışmalar sonucunda da iyi parametrelere sahip bir çok kod elde edilmiştir. Veri ağlarından uydu iletişimlerine kadar pek çok alanda uygulama sahasına sahip olan sabit devirli kodlar, etkili bir şekilde hata tespiti ve düzeltilmesi hususunda zengin bir cebirsel yapıya sahiptir. Sabit devirli kodlar da devirli kodlar gibi geniş bir literatüre sahiptir [15, 48-52]. Yıldız ve Karadeniz [47] numaralı çalışmada, Gray dönüşümü genelleştirerek çalışılan halka üzerinde n uzunluktaki sabit devirli kodun karakteristik yapısını araştırmışlardır. Ayrıca optimal kodlara da örnek vermişlerdir. Bag ve ark. [48] numaralı çalışmada $\mathbb{Z}_4[u] \big/ \langle u^2 - 3 \rangle$ zincir Frobenius halkası üzerinde $1+2u$ ve $3+2u$ birimsel elemanları için sabit devirli kodların Gray görüntülerini incelemişlerdir. Dinh ve ark. [49] numaralı çalışmada, $v^2 = v$ iken $\mathbb{Z}_4 + v\mathbb{Z}_4$ halkasında yeni bir Gray dönüşüm tanımlayarak devirli kodları, $(1+2v)$ ve $(3+2v)-$sabit devirli kodları incelemişlerdir. Ayrıca negadevirli ve $\theta-$sabit devirli kodların kedine dual kodlarını ele almış ve $\mathbb{Z}_4$ üzerinde birçok yeni kod bulmuşlardır.

Negadevirli kodlar sabit devirli kodların kaydırma sabitinin -1 olduğu spesifik bir durumdur ve ilk olarak Wolfman tarafından [53] numaralı çalışma ile incelenmeye başlanmıştır.

Devirli kodların genelleştirmelerinden biri olan parçalı devirli kodlar, büyük uzunluklarda hata düzeltme kabiliyeti açısından devirli kodlara göre çok daha iyi bir performansa sahiptir. Cao ve Li [54] numaralı çalışmada, tek uzunluktaki her bir devirli kod için teori geliştirmiş ve her bir koddaki kodsözlerin sayısını hesaplamak için bir formül elde etmişlerdir. Halkada tek uzunluktaki her bir kodun duali belirlenerek bu kodların kendine dualliğini araştırmış, spesifik uzunluktaki bazı parçalı devirli kodlar için üreteç matrisi oluşturularak devirli kodlar elde etmişlerdir. Elde edilen bu devirli kodlardan da optimal parçalı devirli kodlar bulmuş, minimal uzaklıklar için de bazı sınırlar oluşturmuşlardır.

Bu bölüm 4 kısımdan oluşmuştur. Bölümün amacı, $u^k = u^{k-1}$ iken $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4 + \ldots + u^{k-1}\mathbb{Z}_4$ halkası üzerindeki devirli kodların karakteristik yapısını belirleyerek üreteç polinomu elde etmek ve elde edilen polinom yardımıyla $\mathbb{Z}_4$ üzerinde yeni kodlar bulmaktır. İlk kısımda halkanın cebirsel yapısı ele alınmış ve yeni bir Gray dönüşüm tanımlanmıştır. İkinci kısımda halka üzerindeki devirli kodların cebirsel yapısı incelenmiş ve üreteç polinomu belirlenmiştir. Üçüncü kısımda devirli kodlar ile sabit devirli kodlar arasında kurulan izometri yardımıyla devirli kodlar için elde edilen teoremler sabit devirli kodlar için de ele alınmıştır. Sabit devirli kodların $\mathbb{Z}_4$ görüntülerinin devirli kod olduğu sonucuna varılmıştır. Dördüncü kısımda ise tanımlanan halka üzerindeki devirli ve sabit devirli kodlardan yararlanarak MAGMA programı ile $\mathbb{Z}_4$ üzerinde birçok yeni, optimal ve bilinen en iyi lineer kodlar elde edilmiştir.

2.1. $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4+u^3\mathbb{Z}_4+\ldots+u^{k-1}\mathbb{Z}_4$ Halkasının Cebirsel Yapısı

Bu bölümde, $u^k=u^{k-1}$ iken $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4+u^3\mathbb{Z}_4+\ldots+u^{k-1}\mathbb{Z}_4$ halkasının cebirsel yapısı çalışılmıştır. Bu halka $\mathbb{Z}_4[u]\Big/\langle u^k-u^{k-1}\rangle$ bölüm halkasına izomorftur ve bölüm boyunca bu bölüm halkası T_k ile temsil edilecektir.

$T_2\cong\mathbb{Z}_4[u]\Big/\langle u^2-u\rangle$ bölüm halkasına izomorf olan $\mathbb{Z}_4+u\,\mathbb{Z}_4=\{a_0+ua_1 \mid u^2=u \text{ ve } a_i\in\mathbb{Z}_4\}$ halkası 16 elemanlı, birimli, değişmeli ve yarı lokal bir halkadır. Karakteristiği 4 olup idealleri kapsama bağıntısına göre karşılaştırılamadığından zincir olmayan bir halkadır. 9 tane ideale sahiptir: $\{(0),(1),(1+u),(2+u),(3+u),(2),(u),(2u+2),(2u)\}$. Halkanın 2 maksimal ideali vardır: $(1+u)$ ve $(2+u)$. 4 tane birimsel elemanı, 4 tane de sıfır böleni mevcuttur. $\{0,1,u,1+3u\}$ halkanın idempotent elemanlarıdır.

$T_3\cong\mathbb{Z}_4[u]\Big/\langle u^3-u^2\rangle$ bölüm halkasına izomorf olan $\mathbb{Z}_4+u\,\mathbb{Z}_4+u^2\mathbb{Z}_4=\{a_0+ua_1+u^2a_2 \mid u^3=u^2 \text{ ve } a_i\in\mathbb{Z}_4\}$ halkası 64 elemanlı, birimli, değişmeli ve yarı lokal bir halkadır. Karakteristiği 4 olup idealleri kapsama bağıntısına göre karşılaştırılamadığından zincir halka özelliği taşımamaktadır. Bu halkanın 21 tane ideali olup $(1+u)$ ve $(2,u)$ halkanın maksimal idealleridir. Temel ideal halkası değildir. 16 tane birimsel eleman, 47 tane sıfır böleni vardır. $\{0,1,u^2,1+3u^2\}$ halkanın idempotent elemanlarıdır.

$T_4 \cong \mathbb{Z}_4[u] \Big/ \langle u^4 - u^3 \rangle$ bölüm halkasına izomorf olan $\mathbb{Z}_4 + u\,\mathbb{Z}_4 + u^2\mathbb{Z}_4 + u^3\mathbb{Z}_4 = \{a_0 + ua_1 + u^2a_2 + u^3a_3 \mid u^4 = u^3 \text{ ve } a_i \in \mathbb{Z}_4\}$ halkası ise 2^8 elemanlı olup 2^6 tane birimsel elemana sahiptir. $\{0, 1, u^3, 1+3u^3\}$ halkanın idempotent elemanlarıdır.

$T_5 \cong \mathbb{Z}_4[u] \Big/ \langle u^5 - u^4 \rangle$ bölüm halkasına izomorf olan $\mathbb{Z}_4 + u\,\mathbb{Z}_4 + u^2\mathbb{Z}_4 + u^3\mathbb{Z}_4 + u^4\mathbb{Z}_4 = \{a_0 + u^2a_2 + u^3a_3 + u^4a_4 \mid u^5 = u^4 \text{ ve } a_i \in \mathbb{Z}_4\}$ halkası ise 2^{10} elemanlı olup 2^8 tane birimsel elemana sahiptir. $\{0, 1, u^4, 1+3u^4\}$ halkanın idempotent elemanlarıdır.

Benzer şekilde devam edildiğinde $T_k \cong \mathbb{Z}_4[u] \Big/ \langle u^k - u^{k-1} \rangle$ bölüm halkasına izomorf olan $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4 + u^3\mathbb{Z}_4 + \ldots + u^{k-1}\mathbb{Z}_4 = \{a_0 + ua_1 + u^2a_2 + \ldots + u^{k-1}a_{k-1} \mid u^k = u^{k-1}$ ve $a_i \in \mathbb{Z}_4\}$ halkasının 2^{2k} elemanlı olduğu ve 2^{2k-2} tane birimsel elemana sahip olduğu görülecektir. Ayrıca yine yukarıdaki akışta halkanın idempotent elemanlarının $\{0, 1, u^{k-1}, 1+3u^{k-1}\}$ formunda olduğu görülecektir.

T_k üzerinde m uzunluğundaki lineer bir C_k kodu, $T_k^{\,m}$ halkasının bir $T_k -$alt modülüdür. Bu lineer kodun elemanları kodsöz olarak adlandırılır. $a_i \in \mathbb{Z}_4$ ve $i = 0,1,\ldots,k-1$ iken T_k halkasının herhangi bir elemanı $a_0 + ua_1 + u^2a_2 + \ldots + u^{k-1}a_{k-1}$ şeklinde tanımlanır. $i = 0,1,\ldots m-1$ olmak üzere, her bir $z_i = a_0^i + ua_1^i + u^2a_2^i + \ldots + u^{k-1}a_{k-1}^i$ elemanı için $z = (z_0, z_1, \ldots, z_{m-1})$ kodsözünün polinom formu $z(x) = z_0 + z_1x + z_2x^2 + \ldots + z_{m-1}x^{m-1}$ şeklinde ifade edilir.

$i = 0,1,\ldots,m-1$ ve herhangi bir $z \in T_k$ için $z_i = a_0^i + ua_1^i + u^2a_2^i + \ldots + u^{k-1}a_{k-1}^i$ olacak şekilde $T_k^{\,m}$ halkasından $\mathbb{Z}_4^{2m}$ halkasına uzaklığı koruyan bir Gray dönüşüm aşağıdaki gibi tanımlansın.

$$\phi : T_k \to \mathbb{Z}_4^{2m}$$

$$\left(a_0 + ua_1 + u^2a_2 + \ldots + u^{k-1}a_{k-1}\right) \to \left(a_0 + a_1 + 3a_2 + \ldots + 3a_{k-1},\ 3a_0 + 3a_1 + a_2 + \ldots + a_{k-1}\right)$$

Bu dönüşüm,

$$\phi : T_k^m \to \mathbb{Z}_4^{2m}$$

$$\left(z_0, z_1, \ldots, z_{m-1}\right) \to \begin{pmatrix} a_0^0 + a_1^0 + 3a_2^0 + \ldots + 3a_{k-1}^0, \ldots, a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1} + \ldots + 3a_{k-1}^{m-1}, \\ 3a_0^0 + 3a_1^0 + a_2^0 + \ldots + a_{k-1}^0, \ldots, 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1} + \ldots + a_{k-1}^{m-1} \end{pmatrix}$$

şeklinde genişletilir.

Teorem 2.1.1. Tanımlanan ϕ dönüşümü lineer ve uzaklığı koruyan bir dönüşümdür.

İspat. $a_j, b_j \in \mathbb{Z}_4$ ve $j = 0,1,\ldots,k-1$ iken $t_i = a_0^i + ua_1^i + u^2a_2^i + \ldots + u^{k-1}a_{k-1}^i$ ve $s_i = b_0^i + ub_1^i + u^2b_2^i + \ldots + u^{k-1}b_{k-1}^i$ olmak üzere, her $t = \left(t_1, t_2, \ldots, t_{m-1}\right)$, $s = \left(s_1, s_2, \ldots, s_{m-1}\right) \in T_3^{\,m}$ ve $y, r \in \mathbb{Z}_4$ için,

$$\phi\left(yt + rs\right) = \phi\Big(y\left(a_0^0 + ua_1^0 + u^2a_2^0 + \ldots + u^{k-1}a_{k-1}^0, a_0^1 + ua_1^1 + u^2a_2^1 + \ldots + u^{k-1}a_{k-1}^1, \ldots, a_0^{m-1} + ua_1^{m-1} + u^2a_2^{m-1} + \ldots + u^{k-1}a_{k-1}^{m-1}\right) + r\left(b_0^0 + ub_1^0 + u^2b_2^0 + \ldots + u^{k-1}b_{k-1}^0, b_0^1 + ub_1^1 + u^2b_2^1 + \ldots + u^{k-1}b_{k-1}^1, \ldots, b_0^{m-1} + ub_1^{m-1} + u^2b_2^{m-1} + \ldots + u^{k-1}b_{k-1}^{m-1}\right)\Big)$$

$$= \phi\Big(ya_0^0 + rb_0^0 + u\left(ya_1^0 + rb_1^0\right) + u^2\left(ya_2^0 + rb_2^0\right) + \ldots + u^{k-1}\left(ya_{k-1}^0 + rb_{k-1}^0\right),\ \ldots\ , ya_0^{m-1} + rb_0^{m-1} + u\left(ya_1^{m-1} + rb_1^{m-1}\right) + u^2\left(ya_2^{m-1} + rb_2^{m-1}\right) + \ldots + u^{k-1}\left(ya_{k-1}^{m-1} + rb_{k-1}^{m-1}\right)\Big)$$

$$=\Bigg(ya_0^0 + rb_0^0 + ya_1^0 + rb_1^0 + 3\sum_{i=2}^{k-1} ya_i^0 + rb_i^0, \ldots, ya_0^{m-1} + rb_0^{m-1} + ya_1^{m-1} + rb_1^{m-1} + 3\sum_{i=2}^{k-1} ya_i^{m-1} +$$

$$rb_i^{m-1},\ 3ya_0^0 + 3rb_0^0 + 3ya_1^0 + 3rb_1^0 + \sum_{i=2}^{k-1} ya_i^0 + rb_i^0, \ldots, 3ya_0^{m-1} + 3rb_0^{m-1} + 3ya_1^{m-1} + 3rb_1^{m-1} +$$

$$\sum_{i=2}^{k-1} ya_i^{m-1} + rb_i^{m-1} \Bigg)$$

$$=\Bigg(y\Bigg(a_0^0 + a_1^0 + 3\sum_{i=2}^{k-1} a_i^0, \ldots, a_0^{m-1} + a_1^{m-1} + 3\sum_{i=2}^{k-1} a_i^{m-1} \Bigg) + r\Bigg(b_0^0 + b_1^0 + 3\sum_{i=2}^{k-1} b_i^0, \ldots, b_0^{m-1} + b_1^{m-1}$$

$$+3\sum_{i=2}^{k-1} b_i^{m-1} \Bigg), y\Bigg(3a_0^0 + 3a_1^0 + \sum_{i=2}^{k-1} a_i^0, \ldots, 3a_0^{m-1} + 3a_1^{m-1} + \sum_{i=2}^{k-1} a_i^{m-1} \Bigg) + r\Bigg(3b_0^0 + 3b_1^0 + \sum_{i=2}^{k-1} b_i^0,$$

$$\ldots, 3b_0^{m-1} + 3b_1^{m-1} + \sum_{i=2}^{k-1} b_i^{m-1} \Bigg)\Bigg)$$

$$= y\Bigg(a_0^0 + a_1^0 + 3\sum_{i=2}^{k-1} a_i^0, \ldots, a_0^{m-1} + a_1^{m-1} + 3\sum_{i=2}^{k-1} a_i^{m-1}, 3a_0^0 + 3a_1^0 + \sum_{i=2}^{k-1} a_i^{m-1}, \ldots, 3a_0^{m-1} + 3a_1^{m-1} +$$

$$\sum_{i=2}^{k-1} a_i^{m-1} \Bigg) + r\Big(b_0^0 + b_1^0 + 3\sum_{i=2}^{k-1} b_i^0, \ldots, b_0^{m-1} + b_1^{m-1} + 3\sum_{i=2}^{k-1} b_i^{m-1}, 3b_0^0 + 3b_1^0 + \sum_{i=2}^{k-1} b_i^0, \ldots, 3b_0^{m-1} + 3$$

$$b_1^{m-1} + \sum_{i=2}^{k-1} b_i^{m-1} \Bigg)$$

$= y\phi(t) + r\phi(s)$ elde edilir. Böylece ϕ dönüşümünün lineer bir dönüşüm olduğu gösterilmiş olur.

Peki ϕ dönüşümü uzaklığı korur mu?

$t - s = (t_0, t_1, \ldots, t_{m-1}) - (s_0, s_1, \ldots, s_{m-1})$ ve ϕ lineer dönüşüm olduğundan $\phi(t-s) = \phi(t) - \phi(s)$ eşitliğinin varlığı bilinmektedir. Lee uzaklık tanımı kullanılarak,

$$d_L(t,s) = w_L(t-s)$$

$$= \sum_{i=0}^{m-1} w_L\left(t_i - s_i\right)$$

$$= \sum_{i=0}^{m-1} w_L\left(\left(a_0^i + ua_1^i + u^2a_2^i + \ldots + u^{k-1}a_{k-1}^i\right) - \left(b_0^i + ub_1^i + u^2b_2^i + \ldots + u^{k-1}b_{k-1}^i\right)\right)$$

$$= \sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + u\left(a_1^i - b_1^i\right) + u^2\left(a_2^i - b_2^i\right) + \ldots + u^{k-1}\left(a_{k-1}^i - b_{k-1}^i\right)\right)$$

eşitliğine ϕ Gray dönüşümü uygulandığı takdirde,

$$\sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3\sum_{j=2}^{k-1} a_j^i - b_j^i\right) + w_L\left(3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + \sum_{j=2}^{k-1} a_j^i - b_j^i\right)$$

elde edilir. Bu da $w_L\left(\phi\left(t-s\right)\right)$ ifadesine eşit olur. ϕ lineer dönüşüm olduğundan $w_L\left(\phi\left(t\right)-\phi\left(s\right)\right) = d_L\left(\phi\left(t\right),\phi\left(s\right)\right)$ eşitliğine ulaşılır.

Diğer taraftan,

$$w_L\left(\phi\left(t-s\right)\right) = \sum_{i=0}^{m-1} w_L\left(\phi\left(t_i - s_i\right)\right)$$

$$= \sum_{i=0}^{m-1} w_L\left(\phi\left(\left(a_0^i + ua_1^i + u^2a_2^i + \ldots + u^{k-1}a_{k-1}^i\right) - \left(b_0^i + ub_1^i + u^2b_2^i + \ldots + u^{k-1}b_{k-1}^i\right)\right)\right)$$

$$= \sum_{i=0}^{m-1} w_L\left(\phi\left(a_0^i - b_0^i + u\left(a_1^i - b_1^i\right) + u^2\left(a_2^i - b_2^i\right) + \ldots + u^{k-1}\left(a_{k-1}^i - b_{k-1}^i\right)\right)\right)$$

$$= \sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3\sum_{j=2}^{k-1} a_j^i - b_j^i, 3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + \sum_{j=2}^{k-1} a_j^i - b_j^i\right)$$

$$= \sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3\sum_{j=2}^{k-1} a_j^i - b_j^i\right) + w_L\left(3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + \sum_{j=2}^{k-1} a_j^i - b_j^i\right)$$

elde edilir.

Burada $w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3\sum_{j=2}^{k-1} a_j^i - b_j^i\right) = \min\left\{\left|a_0^i - b_0^i + a_1^i - b_1^i + 3\sum_{j=2}^{k-1} a_j^i - b_j^i\right|,\right.$

$\left.\left|4 - \left(a_0^i - b_0^i + a_1^i - b_1^i + 3\sum_{j=2}^{k-1} a_j^i - b_j^i\right)\right|\right\}$ ve $w_L\left(3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + \sum_{j=2}^{k-1} a_j^i - b_j^i\right) =$

$\min\left\{\left|3a_0^i-3b_0^i+3a_1^i-3b_1^i+\sum_{j=2}^{k-1}a_j^i-b_j^i\right|,\left|4-\left(3a_0^i-3b_0^i+3a_1^i-3b_1^i+\sum_{j=2}^{k-1}a_j^i-b_j^i\right)\right|\right\}$ olduğu da göz önünde bulundurularak $d_L(t,s)=w_L\left(\phi(t-s)\right)=w_L\left(\phi(t)-\phi(s)\right)=d_L\left(\phi(t),\phi(s)\right)$ eşitliği elde edilir. Böylece ϕ dönüşümünün uzaklık koruyan bir dönüşüm olduğu gösterilmiş olur.

ϕ Gray dönüşümünün Öklit ve Hamming uzaklıkları koruduğu da benzer şekilde gösterilir. □

2.2. T_k Halkası Üzerindeki Devirli Kodların Yapısı

T_k^m üzerinde devirli öteleme operatörü $\sigma(z_0,z_1,\ldots,z_{m-1})=(z_{m-1},z_0,z_1,\ldots,z_{m-2})$ iken σ altında korunan, diğer bir ifadeyle $\sigma(C_k)=C_k$ eşitliğini sağlayan, lineer C_k koduna devirli kod denir. T_k halkası üzerinde uzunluğu m olan lineer kod T_k^m'nin bir T_k – alt modülüdür.

Bölüm boyunca tek uzunluktaki devirli ve sabit devirli kodlar çalışılacak olup $T_k[x]\Big/\langle x^m-1\rangle$ bölüm halkası $T_{k,m}$ ile temsil edilecektir. T_k^m cebirsel yapısında uzunluğu m olan vektürler ile $T_{k,m}$ bölüm halkasındaki polinomlar arasında kurulan

$$\Upsilon: T_k^m \to T_{k,m}$$
$$z=(z_0,\ldots,z_{m-1}) \to z(x)=z_0+z_1x+\ldots+z_{m-1}x^{m-1}$$

lineer dönüşüm bir T_k – modül izomorfizmadır.

T_k üzerinde m uzunluğundaki C_k lineer kodunun devirli olması için gerek ve yeter koşul $\Upsilon(C_k)$'nın T_k^m bölüm halkasının bir ideali olmasıdır.

Bu bilgilendirmeler ışığında, lokal olmayan T_k halkasında tek uzunluktaki devirli kodların üreteç polinomunu oluşturmak için Çin Kalan Teoremi kullanılacaktır. Bunun için öncelikle aşağıdaki tanımlar verilsin.

Tanım 2.2.1. $\mathfrak{R}$ ve $\mathfrak{I}$ iki lineer kod olmak üzere, $\oplus$ toplamı $\mathfrak{R}\oplus\mathfrak{I}=\{d+w \mid d\in\mathfrak{R}, w\in\mathfrak{I}\}$ şeklinde tanımlanır.

Tanım 2.2.2. [55] Bir R-modül olan M modülünün her bir S_i alt modülün direkt toplamı olması için gerek ve yeter koşul her $i=1,\ldots,n$ için, $M=S_1\oplus\cdots\oplus S_n$ ve $S_i\cap\left(\sum_{j\neq i}S_j\right)=\{0\}$ olmasıdır. Sonuç olarak, $M=S\oplus T$ ise S 'ye M modülünde T 'nin tamlayanı, T 'ye ise M modülünde S 'nin bir tamlayanı denir.

Teorem 2.2.1. [55] S ve T, M modülünün tamlayan alt modülleri olmak üzere S modülünün bütün tamlayanları M/S bölüm halkasına, T modülünün tamlayanları ise M/T bölüm halkasına izomorftur.

Çin Kalan Teoremi'nin kullanılabilmesi için öncelikle T_k halkası ayrıştırılmalıdır. Tanım 1.2.27. doğrultusunda $\left(u^{k-1}\right)^2=u^{k-1}$ ve $\left(1+3u^{k-1}\right)^2=1+3u^{k-1}$ olduğu göz önünde bulundurularak T_k halkasının u^{k-1} ve $1+3u^{k-1}$ idempotent ailesi,

i. $u^{k-1}\left(1+3u^{k-1}\right)=u^{k-1}+3u^{k-1}=0$,

ii. $u^{k-1}+\left(1+3u^{k-1}\right)=1$,

iii. $R_1=u^{k-1}T_k$ ve $R_2=\left(1+3u^{k-1}\right)T_k$

olacak şekilde mevcuttur. Bu durumda T_k halkası R_1+R_2 formunda ifade edilecek olup,

$$T_k = u^{k-1}T_k \oplus \left(1+3u^{k-1}\right)T_k$$

şeklinde yazılabilir. Tanım 2.2.2. ve Teorem 2.2.1.'den hareketle T_k halkası

$$T_k \Big/ \left\langle u^{k-1} \right\rangle \cong \left\{ a+ub+\ldots+u^{k-2}t+\left\langle u^{k-1}\right\rangle : a,b \in \mathbb{Z}_4 \right\} \cong \mathbb{Z}_4+u\mathbb{Z}_4+\ldots+u^{k-2}\mathbb{Z}_4,\ u^{k-1}=0$$

ve

$$T_k \Big/ \left\langle 1+3u^{k-1} \right\rangle \cong \left\{ 1+\left\langle 1+3u^{k-1}\right\rangle, 2+\left\langle 1+3u^{k-1}\right\rangle, 3+\left\langle 1+3u^{k-1}\right\rangle, 4+\left\langle 1+3u^{k-1}\right\rangle \right\} \cong \mathbb{Z}_4$$

şeklinde ayrıştırılabilir. $M = S \oplus T \Rightarrow M \big/ S \cong T$ ifadesinden yola çıkarak $T_k = \underset{S}{u^{k-1}T_k} + \underbrace{\left(1+3u^{k-1}\right)T_k}_{T}$ olduğu da bilindiğinden,

$$T_k \Big/ \left\langle u^{k-1} \right\rangle \cong \left(1+3u^{k-1}\right)T_k \cong \mathbb{Z}_4+u\mathbb{Z}_4+\ldots+u^{k-2}\mathbb{Z}_4,\quad u^{k-1}=0$$

ve

$$T_k \Big/ \left\langle 1+3u^{k-1} \right\rangle \cong u^{k-1}T_k \cong \mathbb{Z}_4$$

ifadeleri elde edilir. Böylece, $T_k = u^{k-1}\mathbb{Z}_4 \oplus \left(1+3u^{k-1}\right)\left(\mathbb{Z}_4+u\mathbb{Z}_4+\ldots+u^{k-2}\mathbb{Z}_4\right)$ parçalanışı elde edilir. Burada $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4+\ldots+u^{k-2}\mathbb{Z}_4$ halkasında $u^{k-1}=0$ iken çalıştığı gerçeği unutulmamalıdır. $u^{k-1}=0$ iken $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4+\ldots+u^{k-2}\mathbb{Z}_4$ halkası bölüm boyunca $\zeta_\hbar$ ile temsil edilecektir.

T_k halkası üzerindeki bir C_k kodu için,

$$\Re = \left\{ t+y+h \in \mathbb{Z}_4^m \mid t+uy+u^2h+\ldots+u^{k-1}w \in C_k \right\}$$

ve

$$\mathfrak{I}=\left\{t+uy+\ldots+u^{k-2}d\in\zeta_h^m \mid t+uy+u^2h+\ldots+u^{k-2}w\in C_k,\, t,y,h,\ldots,w\in\mathbb{Z}_4^m\right\}$$

kümeleri tanımlansın. $\mathfrak{R}$ kodu $\mathbb{Z}_4$ üzerinde, $\mathfrak{I}$ ise $\zeta_\hbar$ üzerinde, uzunlukları m olan iki lineer kod olsun. Bu durumda, T_k halkası üzerinde uzunluğu m olan lineer C_k kodu tek türlü olarak $C_k=\left(u^{k-1}\mathfrak{R}\right)\oplus\left(\left(1+3u^{k-1}\right)\mathfrak{I}\right)$ şeklinde belirlenir. Buradan hareketle, lokal olmayan T_k halkası, Çin Kalan Teoremi yardımıyla tek minimal ideale sahip lokal halkaların direkt toplamı olarak yazılabildiğinden bu halka bir Frobenius halkadır.

Tüm bu açıklamalar ışığında;

Teorem 2.2.2. $C_k=\left(u^{k-1}\mathfrak{R}\right)\oplus\left(\left(1+3u^{k-1}\right)\mathfrak{I}\right)$ lineer kodunun devirli olması için gerek ve yeter koşul $\mathfrak{R}$ kodunun $\mathbb{Z}_4$ üzerinde, $\mathfrak{I}$ kodunun ise $\zeta_\hbar$ üzerinde devirli kod olmasıdır.

İspat. $p_i=\left(a_0,a_1,\ldots,a_{m-1}\right)\in\mathfrak{R}$ ve $v_i=\left(b_0,b_1,\ldots,b_{m-1}\right)\in\mathfrak{I}$ olsun. $i=0,1,\ldots,m-1$ iken $b_i=t_i+uq_i+\ldots+u^{k-2}n_i$ olacak şekilde $z_i=u^{k-1}a_i\oplus\left(1+3u^{k-1}\right)b_i$ kabul edilsin. Bu durumda $z_i=\left(z_0,z_1,\ldots,z_{m-1}\right)\in C_k$ yazılabilir. C_k devirli bir kod olduğundan $\sigma\left(z_i\right)\in C_k$ olduğu bilinmektedir. Buradan hareketle $\sigma\left(z_i\right)=u^{k-1}\sigma\left(p_i\right)+\left(1+3u^{k-1}\right)\sigma\left(v_i\right)$ eşitliği elde edilir. Böylece $\sigma\left(p_i\right)\in\mathfrak{R}$ ve $\sigma\left(v_i\right)\in\mathfrak{I}$ olduğu görülür. Bu da $\mathfrak{R}$ kodunun $\mathbb{Z}_4$ üzerinde, $\mathfrak{I}$ kodunun ise $\zeta_\hbar$ üzerinde devirli olduğunun kanıtıdır. Diğer yandan $\mathfrak{R}$ kodu $\mathbb{Z}_4$ üzerinde, $\mathfrak{I}$ kodu ise $\zeta_\hbar$ üzerinde devirli kod olsun. Ayrıca $i=0,1,\ldots,m-1$ iken $z_i=\left(z_0,z_1,\ldots,z_{m-1}\right)$ ve $b_i=t_i+uq_i+\ldots+u^{k-2}n_i$ olacak şekilde $z_i=u^{k-1}a_i\oplus\left(1+3u^{k-1}\right)b_i$ mevcut olsun. Bu durumda $p_i\in\mathfrak{R}$ ve $v_i\in\mathfrak{I}$ olduğu görülür. $\mathfrak{R}$ ve $\mathfrak{I}$ lineer kodları devirli kodlar olduklarından $\sigma\left(p_i\right)\in\mathfrak{R}$ ve $\sigma\left(v_i\right)\in\mathfrak{I}$ bilinmektedir. $\sigma\left(z_i\right)\in C_k$ gerçeğinden $\sigma\left(p_i\right)\in\mathfrak{R}$ ve $\sigma\left(v_i\right)\in\mathfrak{I}$ elde edilir. Böylece

$\sigma(z_i)=u^{k-1}\sigma(p_i)+(1+3u^{k-1})\sigma(v_i)\in u^{k-1}\Re\oplus(1+3u^{k-1})\Im=C_k$ eşitliğine ulaşılır. Bu da C_k kodunun T_k üzerinde devirli bir kod olduğunu ispatlar. □

Teorem 2.2.2'den hareketle $\mathbb{Z}_4$ üzerinde ve $\zeta_\hbar$ üzerindeki devirli kodların [38, Teorem 3.3.] üreteç polinomları kullanılarak T_k üzerinde uzunluğu m olan C_k kodunun üreteç polinomu aşağıdaki gibi ifade edilir.

Teorem 2.2.3. $C_k=(u^{k-1}\Re)\oplus((1+3u^{k-1})\Im)$ kodu T_k halkası üzerinde uzunluğu m olan devirli bir kod olsun. Bu durumda, $i=0,1,\ldots,k$ için $x^m-1=f_i(x)h_i(x)w_i(x)$ ve $g_i(x)=f_i(x)(h_i(x)+2)$ olmak üzere, C_k kodunun üreteç polinomu

$$C_k=(u^{k-1}\langle g_1(x)\rangle)\oplus((1+3u^{k-1})\langle g_2(x)+ut_{1,2}(x)+\ldots+u^{k-1}t_{1,k}(x),ug_3(x)+u^2t_{2,3}(x)$$
$$+\ldots+u^{k-1}t_{2,k}(x),\ u^2g_4(x)+u^3t_{3,4}(x)+\ldots+u^{k-1}t_{3,k}(x),\ \ldots,\ u^{k-1}g_{k-1}(x)\rangle)$$

şeklindedir.

Burada, $\mathbb{Z}_4$ üzerindeki lineer devirli kod $\Re=\langle g_1(x)\rangle$ ile, $\zeta_\hbar$ üzerindeki lineer devirli kod ise $\Im=\langle g_2(x)+ut_{1,2}(x)+\ldots+u^{k-1}t_{1,k}(x),\ ug_3(x)+u^2t_{2,3}(x)+\ldots+u^{k-1}t_{2,k}(x),$ $u^2g_4(x)+u^3t_{3,4}(x)+\ldots+u^{k-1}t_{3,k}(x),\ \ldots,\ u^{k-1}g_{k-1}(x)\rangle)$ ile temsil edilmektedir.

İspat. $\mathbb{Z}_4$ üzerindeki devirli kod $\Re=\langle g_1(x)\rangle$, $\zeta_\hbar$ üzerindeki devirli kod $\Im=\langle g_2(x)+ut_{1,2}(x)+\ldots+u^{k-1}t_{1,k}(x),\ ug_3(x)+u^2t_{2,3}(x)+\ldots+u^{k-1}t_{2,k}(x),\ u^2g_4(x)+$ $u^3t_{3,4}(x)+\ldots+u^{k-1}t_{3,k}(x),\ \ldots,\ u^{k-1}g_{k-1}(x)\rangle)$ ve $\hat{C}_k$ kodunun üreteç polinomu $\hat{C}_k=(u^{k-1}\langle g_1(x)\rangle)\oplus((1+3u^{k-1})\langle g_2(x)+ut_{1,2}(x)+\ldots+u^{k-1}t_{1,k}(x),ug_3(x)+u^2t_{2,3}(x)$ $+\ldots+u^{k-1}t_{2,k}(x),\ \ldots,\ u^{k-1}g_{k-1}(x)\rangle)$ olsun. Bu durumda $\hat{C}_k\subseteq C_k$ olduğu aşikârdır.

$u^k = u^{k-1}$ iken $u^{k-1}\mathfrak{R}$ ve $\left(1+3u^{k-1}\right)\mathfrak{I}$ için sırasıyla, $u^{k-1}\mathfrak{R} = u^{k-1}C_k$ ve $\left(1+3u^{k-1}\right)\mathfrak{I} = \left(1+3u^{k-1}\right)C_k$ eşitlikleri sağlanır. Buradan $\left(u^{k-1}\mathfrak{R}\right)\oplus\left(\left(1+3u^{k-1}\right)\mathfrak{I}\right)\subseteq \hat{C}_k$ ifadesi elde edilir. Bu da $C_k \subseteq \hat{C}_k$ anlamına gelir. $\hat{C}_k \subseteq C_k$ ve $C_k \subseteq \hat{C}_k$ sağlandığından $C_k = \hat{C}_k$ eşitliği gerçeklenir. □

Teorem 2.2.4. $C_k = \left(u^{k-1}\mathfrak{R}\right)\oplus\left(\left(1+3u^{k-1}\right)\mathfrak{I}\right)$ kodu T_k üzerinde m uzunluğunda devirli bir kod, $\mathfrak{R}$ devirli kodunun üreteç polinomu $\tau_1(x)$ ve $\mathfrak{I}$ devirli kodunun üreteç polinomu ise $\tau_2(x)$ olsun. Bu durumda, $C_k = \left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle$ eşitliği elde edilir.

İspat. C_k kodunun $\left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle$ üreteç polinomu tarafından üretildiğini göstermek için $\left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle \subseteq C_k$ ve $C_k \subseteq \left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle$ olduğunu göstermek gerekir. $\tau_1(x)$ polinomu $\mathfrak{R}$ kodunun üreteç polinomu ve $\tau_2(x)$ polinomu da $\mathfrak{I}$ kodunun üreteç polinomu olduğundan $C_k = \left(u^{k-1}\mathfrak{R}\right)\oplus\left(\left(1+3u^{k-1}\right)\mathfrak{I}\right)$ ifadesi de kullanılarak,

$$C_k = \left\{ z(x) = u^{k-1}s_1(x)\tau_1(x) + \left(1+3u^{k-1}\right)s_2(x)\tau_2(x) \;\middle|\; s_1(x), s_2(x) \in T_k[x] \right\}$$

eşitliği elde edilir. Böylece $C_k \subseteq \left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle \subseteq T_{k,m}$ sonucuna ulaşılır.

Diğer taraftan $l_1(x), l_2(x) \in T_{k,m}$ olmak üzere, $u^{k-1}l_1(x)\tau_1(x) + \left(1+3u^{k-1}\right)l_2(x)\tau_2(x)$ ifadesi $\left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle$ üreteç polinomunun bir elemanı olsun. Bu durumda $l_1(x), l_2(x) \in T_{k,m}$ iken $u^{k-1}l_1(x) = u^{k-1}s_1(x)$ ve $\left(1+3u^{k-1}\right)l_2(x) = \left(1+3u^{k-1}\right)s_2(x)$ eşitlikleri elde edilir. Böylece $\left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle \subseteq C_k$ sonucuna ulaşılır ve $C_k = \left\langle u^{k-1}\tau_1(x), \left(1+3u^{k-1}\right)\tau_2(x)\right\rangle$ eşitliği ispatlanmış olur. □

Teorem 2.2.5. $\mathfrak{R}$ kodu $\mathbb{Z}_4$ üzerinde, $\mathfrak{I}$ kodu $\zeta_\hbar$ üzerinde devirli kodlar ve bu kodların üreteç polinomları da sırasıyla $\tau_1(x)$ ve $\tau_2(x)$ polinomları olsun. $C_k=\left(u^{k-1}\mathfrak{R}\right)\oplus\left(\left(1+3u^{k-1}\right)\mathfrak{I}\right)$ eşitliği de verilsin. Bu durumda $\tau(x)=u^{k-1}\tau_1(x)+\left(1+3u^{k-1}\right)\tau_2(x)$ olacak şekilde $T_{k,m}$ halkası üzerinde tek bir $\tau(x)$ polinomu vardır ve $C_k=\langle\tau(x)\rangle$ eşitliğine ulaşılır. Ayrıca $\tau(x)$ polinomu x^m-1 polinomunun bir bölenidir.

İspat. Teorem 2.2.4.'ten $C_k=\left\langle u^{k-1}\tau_1(x),\left(1+3u^{k-1}\right)\tau_2(x)\right\rangle$ eşitliği bilinmektedir. $\tau(x)=u^{k-1}\tau_1(x)+\left(1+3u^{k-1}\right)\tau_2(x)$ olduğu kabul edilsin. Bu durumda $\langle\tau(x)\rangle$ üreteç polinomunun C_k devirli kodunun bir alt kümesi olduğu açıktır. Diğer taraftan $u^{k-1}\tau_1(x)=u^{k-1}\tau(x)$ ve $\left(1+3u^{k-1}\right)\tau_1(x)=\left(1+3u^{k-1}\right)\tau(x)$ eşitlikleri sağlandığından C_k devirli kodu $\langle\tau(x)\rangle$ üreteç polinomunun bir alt kümesi olur. İki yönlü eşitlik sağlandığından $C_k=\langle\tau(x)\rangle$ elde edilir. $\tau_1(x)$ polinomu $\mathbb{Z}_4[x]$ üzerinde; $\tau_2(x)$ polinomu ise $\zeta_\hbar[x]$ üzerinde x^m-1 polinomunun bölenleri olduğundan $x^m-1=y_1(x)\tau_1(x)=y_2(x)\tau_2(x)$ olacak şekilde $y_1(x)\in\mathbb{Z}_4[x]$ ve $y_2(x)\in\zeta_\hbar[x]$ polinomları vardır. $\left(u^{k-1}y_1(x)+\left(1+3u^{k-1}\right)y_2(x)\right)\tau(x)$ ifadesinde $\tau(x)$ polinomunun yerine yazılması durumunda $\left(u^{k-1}y_1(x)+\left(1+3u^{k-1}\right)y_2(x)\right)\left(u^{k-1}\tau_1(x)+\left(1+3u^{k-1}\right)\tau_2(x)\right)$ eşitliği elde edilir. Bu ifade düzenlendiğinde,

$$u^{k-1}y_1(x)\tau_1(x)+\left(1+3u^{k-1}\right)y_2(x)\tau_2(x)=u^{k-1}\left(x^m-1\right)+\left(1+3u^{k-1}\right)\left(x^m-1\right)=x^m-1$$

sonucuna varılır. Bu da $\tau(x)$ polinomunun x^m-1 polinomunun bir böleni olduğunun açık ispatıdır. □

T_k halkası üzerindeki C_k kodunun idempotent üretecinin tek türlü olarak belirlendiği gösterilsin.

Teorem 2.2.6. C_k kodu T_k halkası üzerinde uzunluğu m olan devirli bir kod olmak üzere $C_k = \langle e(x) \rangle$ olacak şekilde bir tek $e(x) = u^{k-1}e_1(x) + (1+3u^{k-1})e_2(x)$ idempotent elemanı vardır.

İspat. $\Re = \langle e_1(x) \rangle$ ve $\Im = \langle e_2(x) \rangle$ olacak şekilde $e_1(x)$ idempotent elemanı $\mathbb{Z}_4[x]$ üzerinde ve $e_2(x)$ idempotent elemanı ise $\zeta_\hbar[x]$ üzerinde tek türlü olarak mevcuttur. Böylece $C_k = \langle u^{k-1}e_1(x) + (1+3u^{k-1})e_2(x) \rangle$ yazılabilir. $e(x) = u^{k-1}e_1(x) + (1+3u^{k-1})$ $e_2(x)$ olsun. Bu eşitliğin her iki tarafının karesi alınırsa $e_1(x)$ ve $e_2(x)$ idempotent elemanlar olduklarından $e^2(x) = u^{k-1}e_1(x) + (1+3u^{k-1})e_2(x)$ elde edilir. Bu da $e(x)$ polinomunun idempotent olduğu anlamına gelir. Peki, bu polinom bir tane mi? $C_k = \langle \ell(x) \rangle$ olacak şekilde idempotent bir $\ell(x) \in C_k$ ele alınsın. $\ell(x)$ idempotent olduğundan $\ell^2(x) = \ell(x)$ eşitliği sağlanır. $\ell(x) \in C_k = \langle e(x) \rangle$ olduğundan $\ell(x) =$ $k(x)e(x)$ olacak şekilde bir $k(x) \in T_{k,m}$ vardır. Her iki taraf $e(x)$ polinomu ile çarpıldığı takdirde $\ell(x)e(x) = k(x)e^2(x)$ eşitliği elde edilir. $e(x)$ idempotent olduğundan bu ifade $k(x)e(x)$ ifadesine eşit olur. Böylece $\ell(x)e(x) = e(x)$ eşitliğine ulaşılır. Bu eşitlikten hareketle $\ell(x) = e(x)$ elde edilir. Bu da $e(x)$ idempotent polinomunun tek türlü olarak belirlendiğini gösterir. □

Şimdi T_k halkasında tanımlanan devirli kodların Bölüm 2.1.'de tanımlanan ϕ Gray dönüşümü yardımıyla $\mathbb{Z}_4$ görüntüleri incelensin.

Önerme 2.2.1. Herhangi bir $z \in T_k^m$ için $\phi\sigma(z) = \upsilon_2\phi(z)$ eşitliği elde edilir.

İspat. $j = 0,1,\ldots,k-1$ ve $i = 0,1,\ldots,m-1$ iken, $z_i = a_0^i + ua_1^i + \ldots + u^{k-1}a_{k-1}^i$ ve $a_j \in \mathbb{Z}_4$ olacak şekilde T_k^m üzerinde $z = (z_0, z_1, \ldots, z_{m-1})$ kodu ele alınsın. Bu durumda,

$\phi(z)=\left(a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\right.$
$\left.\ldots+a_{k-1}^0,\ldots,3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1}\right)$ olduğundan,

$\upsilon_2\phi(z)=\left(a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},\ a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,a_0^{m-2}+a_1^{m-2}+\right.$
$3a_2^{m-2}+\ldots+3a_{k-1}^{m-2},3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+3a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,3a_0^{m-2}$
$\left.+3a_1^{m-2}+a_2^{m-2}+\ldots+a_{k-1}^{m-2}\right)$ elde edilir. Diğer taraftan,

$\sigma(z)=(z_{m-1},z_0,\ldots,z_{m-2})=\left(a_0^{m-1}+ua_1^{m-1}+u^2a_2^{m-1}+\ldots+u^{k-1}a_{k-1}^{m-1},\ a_0^0+ua_1^0+u^2a_2^0+\ldots+\right.$
$\left.u^{k-1}a_{k-1}^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}+\ldots+u^{k-1}a_{k-1}^{m-2}\right)$ olduğundan,

$\phi\sigma(z)=\left(a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},\ a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,\ a_0^{m-2}+a_1^{m-2}+3\right.$
$a_2^{m-2}+\ldots+3a_{k-1}^{m-2},3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,3a_0^{m-2}+$
$\left.3a_1^{m-2}+a_2^{m-2}+\ldots+a_{k-1}^{m-2}\right)$ sonucuna ulaşılır.

Böylece $\phi\sigma(z)=\upsilon_2\phi(z)$ eşitliği sağlanır. □

Bu önerme sonucunda aşağıdaki teorem elde edilir.

Teorem 2.2.7. C_k kodu T_k üzerinde m uzunluğundaki devirli bir kodun ϕ altındaki $\mathbb{Z}_4$ görüntüsü $2m$ uzunluğunda $2-$parçalı devirli koddur.

İspat. C_k kodunun T_k üzerinde uzunluğu m olan bir devirli kod olduğu kabul edilsin. Bu durumda $\sigma(C_k)=C_k$ eşitliği sağlanır. Her iki tarafın ϕ altındaki görüntüsü alınırsa $\phi\sigma(C_k)=\phi(C_k)$ elde edilir. Önerme 2.2.1.'den yararlanılarak $\upsilon_2\phi(C_k)=\phi\sigma(C_k)=\phi(C_k)$ sonucuna varılır. Bu da C_k kodunun ϕ altındaki görüntüsünün $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda $2-$parçalı devirli kod olduğunu gösterir. □

2.3. T_k Halkası Üzerindeki $\left(1+2u^{k-1}\right)-$Sabit Devirli Kodlar

Bu bölümde tek uzunlukta $\left(1+2u^{k-1}\right)-$sabit devirli kodlar incelenecek olup $T_k[x]\Big/\left\langle x^m-\left(1+2u^{k-1}\right)\right\rangle$ bölüm halkası $T_{k,m_{\left(1+2u^{k-1}\right)}}$ ile temsil edilecektir. T_k halkasındaki $\left(1+2u^{k-1}\right)$ birimsel elemanı için $u^k=u^{k-1}$ iken $\left(1+2u^{k-1}\right)^{-1}=\left(1+2u^{k-1}\right)$ olduğu aşikardır. $\left(1+2u^{k-1}\right)$ birimsel elemanının tek kuvvetinin kendisine, çift kuvvetinin ise 1'e eşit olduğu bilgisi verilerek, ilk olarak, sabit devirli bir kodun üreteç polinomunu elde etmek maksadıyla önceki bölümde incelenen devirli kodların cebirsel yapısı ile $\left(1+2u^{k-1}\right)-$sabit devirli kodlar arasında bir izomorfizma tanımlansın.

Önerme 2.3.1. $\widehat{\varepsilon}\left(z(x)\right)=z\left(\left(1+2u^{k-1}\right)x\right)$ olacak şekilde $\widehat{\varepsilon}:T_{k,m}\to T_{k,m_{\left(1+2u^{k-1}\right)}}$ dönüşümü tanımlansın. m pozitif tamsayısının tek olması durumunda $\widehat{\varepsilon}$ bir halka izomorfizmasıdır.

İspat. $\widehat{\varepsilon}$ dönüşümünün bir halka izomorfizması olduğunu göstermek için iyi tanımlılık, birebir, örten ve halka homomorfizması olduğunu göstermek gerekir.

<u>İyi tanımlılık</u>: Her $b(x),\,c(x)\in T_{k,m}$ için $b(x)=c(x)\ \left(\text{mod } x^m-1\right)$ iken $\widehat{\varepsilon}\left(b(x)\right)=\widehat{\varepsilon}\left(c(x)\right)\ \left(\text{mod } x^m-\left(1+2u^{k-1}\right)\right)$ olmalıdır.

$b(x)=c(x)\ \left(\text{mod } x^m-1\right)$ ise $b(x)=\left(x^m-1\right)q(x)+c(x)$ şeklinde ifade edilir. $x\mapsto\left(1+2u^{k-1}\right)x$ yazılırsa,

$$b\left(\left(1+2u^{k-1}\right)x\right)=\left(\left(\left(1+2u^{k-1}\right)x\right)^m-1\right)q\left(\left(1+2u^{k-1}\right)x\right)+c\left(\left(1+2u^{k-1}\right)x\right)$$

$$=\left(\left(1+2u^{k-1}\right)x^m-\left(1+2u^{k-1}\right)^2\right)q\left(\left(1+2u^{k-1}\right)x\right)+c\left(\left(1+2u^{k-1}\right)x\right)$$

$$=\left(1+2u^{k-1}\right)\left(x^m-\left(1+2u^{k-1}\right)\right)q\left(\left(1+2u^{k-1}\right)x\right)+c\left(\left(1+2u^{k-1}\right)x\right)$$

elde edilir. Bu da $\widehat{\varepsilon}\left(b\left(x\right)\right)=\widehat{\varepsilon}\left(c\left(x\right)\right)\ \left(\text{mod } x^m-\left(1+2u^{k-1}\right)\right)$ demektir. Yani, $\widehat{\varepsilon}$ iyi tanımlıdır.

Birebirlik: Her $b\left(x\right),c\left(x\right)\in T_{k,m}$ için $\widehat{\varepsilon}\left(b\left(x\right)\right)=\widehat{\varepsilon}\left(c\left(x\right)\right)\ \left(\text{mod } x^m-\left(1+2u^{k-1}\right)\right)$ iken $b\left(x\right)=c\left(x\right)\ \left(\text{mod } x^m-1\right)$ olmalıdır.

$\widehat{\varepsilon}\left(b\left(x\right)\right)=\widehat{\varepsilon}\left(c\left(x\right)\right)\ \left(\text{mod } x^m-\left(1+2u^{k-1}\right)\right)$ yani $b\left(\left(1+2u^{k-1}\right)x\right)=c\left(\left(1+2u^{k-1}\right)x\right)$ $\left(\text{mod } x^m-\left(1+2u^{k-1}\right)\right)$ olarak yazılır. Bu ifade $b\left(\left(1+2u^{k-1}\right)x\right)=\left(x^m-\left(1+2u^{k-1}\right)\right)$ $q\left(\left(1+2u^{k-1}\right)x\right)+c\left(\left(1+2u^{k-1}\right)x\right)$ anlamına gelir. Buradan hareketle, x yerine $\left(1+2u^{k-1}\right)x$ yazılırsa, $b\left(x\right)=\left(1+2u^{k-1}\right)\left(\ x^m-1\right)q\left(x\right)+c\left(x\right)$ ifadesi elde edilir. Bu da $b\left(x\right)=c\left(x\right)\ \left(\text{mod } x^m-1\right)$ olması demektir. Böylece $\widehat{\varepsilon}$ dönüşümü birebir bir dönüşümdür.

Örtenlik: $\widehat{\varepsilon}$ dönüşümü sonlu ve birebir bir dönüşüm olduğundan örtendir.

Homomorfizma: Her $b\left(x\right),c\left(x\right)\in T_{k,m}$ için $\widehat{\varepsilon}\left(b\left(x\right)+c\left(x\right)\right)=\widehat{\varepsilon}\left(b\left(x\right)\right)+\widehat{\varepsilon}\left(c\left(x\right)\right)$ ve $\widehat{\varepsilon}\left(b\left(x\right)c\left(x\right)\right)=\widehat{\varepsilon}\left(b\left(x\right)\right)\ \widehat{\varepsilon}\left(c\left(x\right)\right)$ olmalıdır. Gerekli düzenlemeler yapıldığında,

$$\begin{aligned}\widehat{\varepsilon}\left(b\left(x\right)+c\left(x\right)\right)&=\widehat{\varepsilon}\left(\left(b+c\right)\left(x\right)\right)=\left(b+c\right)\left(\left(1+2u^{k-1}\right)x\right)\\&=b\left(\left(1+2u^{k-1}\right)x\right)+c\left(\left(1+2u^{k-1}\right)x\right)=\widehat{\varepsilon}\left(b\left(x\right)\right)+\widehat{\varepsilon}\left(c\left(x\right)\right)\end{aligned}$$

$$\begin{aligned}\widehat{\varepsilon}\left(b\left(x\right)c\left(x\right)\right)=\widehat{\varepsilon}\left(\left(bc\right)\left(x\right)\right)=\left(bc\right)\left(\left(1+2u^{k-1}\right)x\right)&=b\left(\left(1+2u^{k-1}\right)x\right)\ c\left(\left(1+2u^{k-1}\right)x\right)\\&=\widehat{\varepsilon}\left(b\left(x\right)\right)\ \widehat{\varepsilon}\left(c\left(x\right)\right)\end{aligned}$$

eşitlikleri elde edilir. Böylelikle $\widehat{\varepsilon}$ dönüşümü bir halka homomorfizmadır.

Bu ispat incelenirken m'nin tek tamsayı olduğu unutulmamalıdır. Yukarıda da gösterildiği gibi $\widehat{\varepsilon}$ dönüşümü iyi tanımlı, birebir, örten ve halka homomorfizması olduğu için bir halka izomorfizmasıdır. □

Bu önermenin sonucunda,

Sonuç 2.3.1. $T_{k,m}$ halkasının idealleri ile $T_{k,m_{\left(1+2u^{k-1}\right)}}$ bölüm halkasının idealleri arasında birebir bir eşleşme vardır.

Sonuç 2.3.2. $\widehat{\varepsilon}(z)=\left(z_0,\left(1+2u^{k-1}\right)z_1,\ldots,\left(1+2u^{k-1}\right)^i z_i,\ldots,\left(1+2u^{k-1}\right)^{m-1} z_{m-1}\right)$ olacak şekilde T_k^m üzerinde bir $\widehat{\varepsilon}$ permütasyonu tanımlansın. $Q\subseteq T_k^m$ olmak koşuluyla Q 'nun devirli bir kod olması için gerek ve yeter koşul Q 'nun $\widehat{\varepsilon}$ permütasyonu altındaki görüntüsünün $\left(1+2u^{k-1}\right)-$sabit devirli kod olmasıdır.

İspat. Q bir devirli kod olsun. Bu durumda $\sigma(z)\in Q$ olur. $\widehat{\varepsilon}$ permütasyonu uygulanırsa, $\widehat{\varepsilon}(z)=\left(z_0,\left(1+2u^{k-1}\right)z_1,\ldots,\ z_{m-1}\right)\in\widehat{\varepsilon}(Q)$ elde edilir. $\widehat{\varepsilon}(Q)$ kodunun $\left(1+2u^{k-1}\right)-$sabit devirli kod olması için gerek ve yeter koşul $\rho_{\left(1+2u^{k-1}\right)}\left(\widehat{\varepsilon}(Q)\right)=$ $\left(\left(1+2u^{k-1}\right)z_{m-1},z_0,\left(1+2u^{k-1}\right)z_1,\ldots,\ z_{m-2}\right)$ olmasıdır. Bu ifade $\left(1+2u^{k-1}\right)$ parantezine alınırsa, $\left(1+2u^{k-1}\right)\left(z_{m-1},\left(1+2u^{k-1}\right)z_0,\ldots,\ z_{m-2}\right)\in\widehat{\varepsilon}(Q)$ elde edilir. $\widehat{\varepsilon}(Q)$ ideal olduğundan $\rho_{\left(1+2u^{k-1}\right)}\left(\widehat{\varepsilon}(Q)\right)\in\widehat{\varepsilon}(Q)$ sonucuna ulaşılır. Bu da $\widehat{\varepsilon}(Q)$ kodunun $\left(1+2u^{k-1}\right)-$sabit devirli kod olması demektir. □

Teorem 2.2.3., Teorem 2.2.4., Teorem 2.2.5. ve $\widehat{\varepsilon}$ izomorfizması kullanılarak $\left(1+2u^{k-1}\right)-$sabit devirli kodlar aşağıdaki gibi karakterize edilebilir.

Teorem 2.3.1. $C_k = u^{k-1}\Re \oplus (1+3u^{k-1})\Im$ kodu $u^k = u^{k-1}$ iken T_k üzerinde m uzunluğunda $\left(1+2u^{k-1}\right)-$sabit devirli kod olsun. Bu durumda $i = 1,2,\ldots,k$ için $x^m - 1 = f_i(x).h_i(x).w_i(x)$ ve $\tilde{x} = \left(1+2u^{k-1}\right)x$ olacak şekilde C_k kodunun üreteç polinomu,

$$C_k = \left(u^{k-1}\left\langle g_1(\tilde{x})\right\rangle\right) \oplus \left(\left(1+3u^{k-1}\right)\left\langle g_2(\tilde{x}) + ut_{1,2}(\tilde{x}) + \ldots + u^{k-1}t_{1,k}(\tilde{x}),\, ug_3(\tilde{x}) + u^2 t_{2,3}(\tilde{x})\right.\right.$$
$$\left.\left. + \ldots + u^{k-1}t_{2,k}(\tilde{x}),\, u^2 g_4(\tilde{x}) + u^3 t_{3,4}(\tilde{x}) + \ldots + u^{k-1}t_{3,k}(\tilde{x}),\, \ldots,\, u^{k-1}g_{k+1}(\tilde{x})\right\rangle\right)$$

şeklindedir.

Teorem 2.3.2. $C_k = \left(u^{k-1}\Re\right) \oplus \left(\left(1+3u^{k-1}\right)\Im\right)$ kodu T_k üzerinde m uzunluğunda $\left(1+2u^{k-1}\right)-$sabit devirli bir kod, $\Re$ kodunun üreteç polinomu $\tau_1(\tilde{x})$ ve $\Im$ kodunun üreteç polinomu ise $\tau_2(\tilde{x})$ olsun. Bu durumda $C_k = \left\langle u^{k-1}\tau_1(\tilde{x}), \left(1+3u^{k-1}\right)\tau_2(\tilde{x})\right\rangle$ eşitliği elde edilir.

Teorem 2.3.3. $\Re$ kodu $\mathbb{Z}_4$ üzerinde, $\Im$ kodu $\zeta_\hbar$ üzerinde $\left(1+2u^{k-1}\right)-$sabit devirli kodlar ve bu kodların üreteç polinomları da sırasıyla $\tau_1(\tilde{x})$ ve $\tau_2(\tilde{x})$ polinomları olsun. $C_k = \left(u^{k-1}\Re\right) \oplus \left(\left(1+3u^{k-1}\right)\Im\right)$ eşitliği de verilsin. Bu durumda $\tau(\tilde{x}) = u^{k-1}\tau_1(\tilde{x})$ $+\left(1+3u^{k-1}\right)\tau_2(\tilde{x})$ olacak şekilde $T_{k,m_{\left(1+2u^{k-1}\right)}}$ halkası üzerinde tek bir $\tau(\tilde{x})$ polinomu vardır ve $C_k = \left\langle \tau(\tilde{x})\right\rangle$ eşitliği mevcuttur. Ayrıca $\tau(\tilde{x})$ polinomu $x^m - \left(1+2u^{k-1}\right)$ polinomunun bir bölenidir.

Not 2.3.1. Teorem 2.3.1. – Teorem 2.3.3.'ün ispatları Teorem 2.2.3. – Teorem 2.2.5.'in ispatlarına benzer şekilde yapılabilir.

Önerme 2.3.2. Herhangi bir $z \in T_k^m$ için $\phi\rho_{\left(1+2u^{k-1}\right)}(z) = \sigma\phi(z)$ eşitliği elde edilir.

İspat: $j=0,1,\ldots,k-1$ ve $i=0,1,\ldots,m-1$ iken, $z_i=a_0^i+ua_1^i+\ldots+u^{k-1}a_{k-1}^i$ ve $a_j\in\mathbb{Z}_4$ olacak şekilde T_k^m üzerinde $z=\left(z_0,z_1,\ldots,z_{m-1}\right)$ kodu ele alınsın. Bu durumda,

$\phi(z)=\left(a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\ldots\right.$
$\left.+a_{k-1}^0,\ \ldots,3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1}\right)$ olduğundan,

$\sigma\phi(z)=\left(3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1},\ a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,a_0^{m-2}+a_1^{m-2}+3\right.$
$a_2^{m-2}+\ldots+3a_{k-1}^{m-2},a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,3a_0^{m-2}+3$
$\left.a_1^{m-2}+a_2^{m-2}+\ldots+a_{k-1}^{m-2}\right)$ elde edilir.

Diğer taraftan, $\rho_{1+2u^{k-1}}(z)=\left(\left(1+2u^{k-1}\right)z_{m-1},z_0,\ldots,z_{m-2}\right)=\left(a_0^{m-1}+ua_1^{m-1}+u^2a_2^{m-1}+\ldots+\right.$
$\left.u^{k-1}\left(2a_0^{m-1}+2a_1^{m-1}+\ldots+2a_{k-2}^{m-1}+3a_{k-1}^{m-1}\right),a_0^0+ua_1^0+u^2a_2^0+\ldots+u^{k-1}a_{k-1}^0,\ldots,a_0^{m-2}+ua_1^{m-2}\right.$
$\left.+u^2a_2^{m-2}+\ldots+u^{k-1}a_{k-1}^{m-2}\right)$ olduğundan,

$\phi\rho_{1+2u^{k-1}}(z)=\left(3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1},\ a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,a_0^{m-2}+a_1^{m-2}\right.$
$+3a_2^{m-2}+\ldots+3a_{k-1}^{m-2},a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,3a_0^{m-2}$
$\left.+3a_1^{m-2}+a_2^{m-2}+\ldots+a_{k-1}^{m-2}\right)$ sonucuna ulaşılır.

Böylece $\phi\rho_{\left(1+2u^{k-1}\right)}(z)=\sigma\phi(z)$ eşitliği sağlanır. □

Bu önerme sonucunda aşağıdaki teorem elde edilir.

Teorem 2.3.4. C_k kodu T_k üzerinde m uzunluğundaki $\left(1+2u^{k-1}\right)-$sabit devirli bir kodun ϕ altındaki görüntüsü $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli bir koddur.

İspat. C_k kodunun T_k üzerinde m uzunluğunda $\left(1+2u^{k-1}\right)-$sabit devirli kod olduğu kabul edilsin. Bu durumda $\rho_{1+2u^{k-1}}\left(C_k\right)=C_k$ eşitliği sağlanır. Her iki tarafın ϕ altındaki görüntüsü alınırsa $\phi\rho_{1+2u^{k-1}}\left(C_k\right)=\phi\left(C_k\right)$ elde edilir. Önerme 2.3.2.'den yararlanarak $\phi\rho_{1+2u^{k-1}}\left(C_k\right)=\sigma\phi\left(C_k\right)=\phi\left(C_k\right)$ sonucuna varılır. Bu da C_k kodunun ϕ altındaki görüntüsünün $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli kod olduğunu gösterir. □

Önerme 2.3.3. $\left(1+2u^{k-1}\right)-$sabit devirli öteleme operatörü $\rho_{\left(1+2u^{k-1}\right)}$, $\delta-$parçalı devirli öteleme operatörü υ_δ, T_k^m üzerinden $\mathbb{Z}_4^{2m}$ üzerine Gray dönüşüm de ϕ olmak üzere $\phi\rho_{\left(1+2u^{k-1}\right)}\left(C\right)=\pi\upsilon_2\phi\left(C\right)$ eşitlikleri sağlanır. $\{0,1,\ldots,2m-1\}$'in bir permütasyonu $\pi^{\bullet}=\left(2i+1,\ m+2i+1\right)$ olsun. $\pi\left(z_0,\ldots,z_{2m-1}\right)=\left(z_{\pi_{(0)}},\ldots,z_{\pi_{(2m-1)}}\right)$ ile tanımlanan bu permütasyona Nechaev permütasyonu adı verilir.

İspat. $j=0,1,\ldots,k-1$ ve $i=0,1,\ldots,m-1$ iken, $z_i=a_0^i+ua_1^i+\ldots+u^{k-1}a_{k-1}^i$ ve $a_j\in\mathbb{Z}_4$ olacak şekilde $T_k^{\ m}$ üzerinde $z=\left(z_0,z_1,\ldots,z_{m-1}\right)$ kodu ele alınsın.

$$\phi\rho_{\left(1+2u^{k-1}\right)}\left(z\right)=\left(3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1},a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,a_0^{m-1}+a_1^{m-1}\right.$$
$$\left.+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},\ 3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,3a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}+\ldots+a_{k-1}^{m-2}\right)$$

olduğu bilinmektedir. Diğer taraftan,

$$\upsilon_2\phi\left(z\right)=\left(a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},\ a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ldots,a_0^{m-2}+a_1^{m-2}+3\right.$$
$$a_2^{m-2}+\ldots+3a_{k-1}^{m-2},3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,3a_0^{m-2}+3$$
$$\left.a_1^{m-2}+a_2^{m-2}+\ldots+a_{k-1}^{m-2}\right)\text{ elde edilir.}$$

$\upsilon_2\phi\left(z\right)$ ifadesine π permütasyonu uygulandığı takdirde $\phi\rho_{\left(1+2u^{k-1}\right)}\left(C\right)=\pi\upsilon_2\phi\left(C\right)$ sonucuna ulaşılır. □

Teorem 2.3.5. T_k üzerinde m uzunluğundaki $\left(1+2u^{k-1}\right)-$sabit devirli bir kodun $\mathbb{Z}_4$ görüntüsü π permütasyonu altında $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda $2-$parçalı devirli koddur.

İspat. C_k kodu T_k üzerinde m uzunluğunda $\left(1+2u^{k-1}\right)-$sabit devirli bir kod olsun. Bu durumda $\rho_{\left(1+2u^{k-1}\right)}\left(C_k\right)=C_k$ eşitliği mevcuttur. Bu eşitliğin her iki tarafının ϕ Gray dönüşümü altındaki görüntüsü alınırsa $\phi\rho_{\left(1+2u^{k-1}\right)}\left(C_k\right)=\phi\left(C_k\right)$ elde edilir. Önerme 2.3.3. kullanılarak $\phi\rho_{\left(1+2u^{k-1}\right)}\left(C_k\right)=\pi\upsilon_2\,\phi\left(C_k\right)=\rho_{\left(1+2u^{k-1}\right)}\left(C_k\right)$ sonucuna ulaşılır. Böylece $\left(1+2u^{k-1}\right)-$sabit devirli bir kodun ϕ dönüşümü altındaki görüntüsü $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda $2-$parçalı devirli bir koda permütasyonca eşit olur. □

Önerme 2.3.4. Herhangi bir $z\in T_k^m$ için, $\phi\,\widehat{\underset{\sim}{\varepsilon}}\left(z\right)=\pi\,\phi\left(z\right)$ eşitliği vardır.

İspat. $j=0,1,\ldots,k-1$ ve $i=0,1,\ldots,m-1$ iken, $z_i=a_0^i+ua_1^i+\ldots+u^{k-1}a_{k-1}^i$ ve $a_j\in\mathbb{Z}_4$ olacak şekilde T_k^m üzerinde $z=\left(z_0,z_1,\ldots,z_{m-1}\right)$ kodu ele alınsın.

$$\widehat{\underset{\sim}{\varepsilon}}\left(z\right)=\left(z_0,\left(1+2u^{k-1}\right)z_1,\ldots,\left(1+2u^{k-1}\right)^i z_i,\ldots,\left(1+2u^{k-1}\right)^{m-1}z_{m-1}\right)$$

$$=\left(a_0^0+ua_1^0+\ldots+u^{k-1}a_{k-1}^0,a_0^1+ua_1^1+\ldots+u^{k-1}\left(2a_0^1+2a_1^1+\ldots+2a_{k-2}^1+3a_{k-1}^1\right),\right.$$

$$\left.a_0^2+ua_1^2+\ldots+u^{k-1}a_{k-1}^2,\ \ldots,a_0^{m-1}+ua_1^{m-1}+\ldots+u^{k-1}a_{k-1}^{m-1}\right)$$

olduğu bilinmektedir. Bu dönüşümün Gray görüntüsü alınırsa,

$\phi\,\widehat{\underset{\sim}{\varepsilon}}\left(z\right)=\left(a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ 3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,\ a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\right.$

$\left.\ldots+3a_{k-1}^{m-1},\ 3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1}\right)$ elde edilir. m uzunluğunun çift olması durumunda $\psi_s=a_0^s+a_1^s+3a_2^s+\ldots+3a_{k-1}^s$ ve $\psi_{m+s}=3a_0^s+3a_1^s+a_2^s+\ldots+a_{k-1}^s$, m uzunluğunun tek olması durumunda ise $\psi_m=3a_0^s+3a_1^s+a_2^s+\ldots+a_{k-1}^s$ ve

$\psi_{m+s} = a_0^s + a_1^s + 3a_2^s + \ldots + 3a_{k-1}^s$ olacak şekilde bir $\psi = (\psi_1, \psi_2, \ldots, \psi_{2m-1}) \in \mathbb{Z}_4^{2m}$ tanımlansın. Burada $s = 0,1,\ldots,m-1$'dir.

$\phi(z) = \left(a_0^0 + a_1^0 + 3a_2^0 + \ldots + 3a_{k-1}^0, \ldots, a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1} + \ldots + 3a_{k-1}^{m-1}, 3a_0^0 + 3a_1^0 + a_2^0 + \ldots + a_{k-1}^0, \ldots, 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1} + \ldots + a_{k-1}^{m-1}\right)$ olduğu bilinmektedir. Buradan hareketle $\pi\phi(z) = \left(a_0^0 + a_1^0 + 3a_2^0 + \ldots + 3a_{k-1}^0, 3a_0^0 + 3a_1^0 + a_2^0 + \ldots + a_{k-1}^0, \ldots, a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1} + \ldots + 3a_{k-1}^{m-1}, 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1} + \ldots + a_{k-1}^{m-1}\right)$ elde edilir. Böylelikle $\phi\hat{\varepsilon}(z) = \pi\phi(z)$ eşitliğine ulaşılır. □

Sonuç 2.3.3. T_k üzerindeki kodun $\mathbb{Z}_4$ görüntüsü δ ile temsil edilirse $\pi(\delta)$ bir devirli koddur.

İspat. Q, T_k üzerinde devirli bir kod ve $\delta = \phi(Q)$ olsun. Önerme 2.3.4. gereğince $\phi\hat{\varepsilon}(z) = \pi\phi(z) = \pi\delta$ eşitliği elde edilir. Sonuç 2.3.2. gereğince $\hat{\varepsilon}(Q)$ kodu $\left(1+2u^{k-1}\right)-$sabit devirli kod olur. Buradan $\phi\hat{\varepsilon}(Q) = \phi(z)$ eşitliği elde edilir. Teorem 2.3.4. kullanılarak $\pi(\delta)$ kodunun devirli bir kod olduğu rahatlıkla ispatlanır. □

Bu açıklamalar doğrultusunda;

Sonuç 2.3.4. T_k üzerindeki kodların Gray dönüşüm altındaki $\mathbb{Z}_4$ görüntüsü devirli koddur.

Tanım 2.3.1. ρ_λ sabit devirli öteleme operatörü, $\mathbb{Z}_4^{2m}$ üzerinde $\delta-$parçalı sabit devirli öteleme operatörü ς_δ olmak üzere, parçalı sabit devirli dönüşüm $\varsigma_\delta\left(z^{(1)} \mid z^{(2)} \mid \ldots \mid z^{(\delta)}\right) = \left(\rho_\lambda\left(z^{(1)}\right) \mid \rho_\lambda\left(z^{(1)}\right) \mid \ldots \mid \rho_\lambda\left(z^{(\delta)}\right)\right)$ ile tanımlansın. $2m$ uzunluğundaki bir kod $\mathbb{Z}_4$ üzerinde $\varsigma_\delta(C_k) = C_k$ şartını sağlıyorsa C_k koduna $\delta-$parçalı sabit devirli kod denir.

$\left(1+2u^{k-1}\right)$ birimsel elemanının yanısıra 3 birimsel elemanı için de aşağıdaki önerme ve teoremden bahsedilebilir. Bunlar T_k üzerindeki $3-$sabit devirli kodun $\mathbb{Z}_4$ görüntüsü kullanılarak elde edilen bir gözlemdir.

Önerme 2.3.5. Herhangi bir $z \in T_k^m$ için, $\phi\rho_3(z)=\sigma\phi(z)$ eşitliği elde edilir.

İspat. $j=0,1,\ldots,k-1$ ve $i=0,1,\ldots,m-1$ iken, $z_i=a_0^i+ua_1^i+\ldots+u^{k-1}a_{k-1}^i$ ve $a_j \in \mathbb{Z}_4$ olacak şekilde T_k^m üzerinde $z=(z_0,z_1,\ldots,z_{m-1})$ kodu ele alınsın. ϕ ve σ tanımları gereğince, $\rho_3(z)=(3z_{m-1},z_0,\ldots,z_{m-2})$ olduğundan,

$\sigma\phi(z)=\phi\rho_3(z)=\left(3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}+\ldots+a_{k-1}^{m-1},\ a_0^0+a_1^0+3a_2^0+\ldots+3a_{k-1}^0,\ \ldots,a_0^{m-2}\right.$
$+a_1^{m-2}+3a_2^{m-2}+\ldots+3a_{k-1}^{m-2},a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}+\ldots+3a_{k-1}^{m-1},3a_0^0+3a_1^0+a_2^0+\ldots+a_{k-1}^0,\ldots,$
$\left.3a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}+\ldots+a_{k-1}^{m-2}\right)$ elde edilir.

Böylelikle $\phi\rho_3(z)=\sigma\phi(z)$ eşitliği ispatlanır. □

Teorem 2.3.6. C_k kodu T_k üzerinde $3-$sabit devirli kod olsun. Bu durumda C_k kodunun ϕ dönüşümü altındaki görüntüsü $\mathbb{Z}_4$ üzerinde devirli koddur.

İspat. C_k kodu T_k üzerinde $3-$sabit devirli kod olsun. Bu durumda $\rho_3(C_k)=C_k$ şeklinde ifade edilebilir. Her iki tarafın ϕ dönüşümü altındaki görüntüsü alınırsa $\phi\rho_3(z)=\sigma\phi(z)$ elde edilir. Önerme 2.3.5. kullanılarak $\phi\rho_3(C_k)=\phi(C_k)=\sigma\phi(C_k)$ eşitliğine ulaşılır. Böylece $\phi(C_k)$ kodu $\mathbb{Z}_4$ üzerinde devirli kod olur. □

2.4. Hesaplama Sonuçları

Bu bölümde özel olarak T_3 halkası üzerindeki devirli kodlar ve $\left(1+2u^2\right)-$sabit devirli kodlar incelenmiştir. Bu kodların tanımlanan ϕ Gray dönüşümü yardımıyla $\mathbb{Z}_4$ görüntüleri araştırılmıştır. Teorem 2.2.3., Teorem 2.2.4., Teorem 2.3.1. ve Teorem 2.3.2. dikkate alınarak T_3 halkası üzerindeki devirli kodların ve $\left(1+2u^2\right)-$sabit devirli kodlar hakkındaki bilgisayar araştırma sonuçları, MAGMA programı kullanılarak elde edilmiştir.

T_3 halkasında uzunluğu m olan $\lambda-$sabit devirli kodu $C_3=\left(u^2\Re\right)\oplus\left(\left(1+3u^2\right)\Im\right)$ için üreteç polinomu, $x^m-1=f_i(x)h_i(x)\,w_i(x)$, $g_i(\tilde{x})=f_i(\tilde{x})\left(h_i(\tilde{x})+2\right)$ ve $i=1,2,3$ olmak üzere, $C_3=\left(u^2\left\langle g_1(\tilde{x})\right\rangle\right)\oplus\left(\left(1+3u^2\right)\left\langle g_2(\tilde{x})+ut_{1,2}(\tilde{x}),u\,g_3(\tilde{x})\right\rangle\right)$ şeklindedir. Her bir bileşenin $\tau_i(\tilde{x})$ ile temsil edilmesi durumunda Teorem 2.2.4. ve Teorem 2.3.2. dikkate alınacaktır. $\lambda=1$ iken devirli kodlardan, $\lambda=1+2u^2$ iken $\left(1+2u^2\right)-$sabit devirli kodlardan söz edileceği unutulmamalıdır. Tüm bu değerlendirmeler sonucunda T_3 halkası üzerinde $\mathbb{Z}_4$ görüntüsü yeni, optimal ve iyi bilinen lineer kodlar olan birçok kod elde edilmiştir. Bu kodların türüne karar verilirken [43] numaralı kaynakta verilen çevrimiçi veritabanı kullanılmıştır.

Tablo 2.1.'de T_3 halkasının elemanları ile bu elemanların temsil edileceği ifadeler verilmiştir. T_3 halkasının elemanlarını temsil eden ifadeler Δ ile gösterilecektir.

Tablo 2.1. T_3 halkasındaki elemanların isimlendirilmesi

T_3 **halkasının elemanları**	Δ	T_3 **halkasının elemanları**	Δ	T_3 **halkasının elemanları**	Δ
0	0	1	1	2	2
3	3	u	4	$2u$	5
$3u$	6	u^2	7	$2u^2$	8
$3u^2$	9	u^2+u	$1'$	u^2+2u	$2'$
u^2+3u	$3'$	$2u^2+u$	$4'$	$2u^2+2u$	$5'$
$2u^2+3u$	$6'$	$3u^2+u$	$7'$	$3u^2+2u$	$8'$
$3u^2+3u$	$9'$	$u+1$	A	$u+2$	B
$u+3$	D	$2u+1$	E	$2u+2$	F
$2u+3$	G	$3u+1$	H	$3u+2$	J
$3u+3$	K	u^2+1	L	u^2+2	M
u^2+3	N	$2u^2+1$	P	$2u^2+2$	R
$2u^2+3$	S	$3u^2+1$	U	$3u^2+2$	V
$3u^2+3$	Y	u^2+u+1	Z	u^2+u+2	b
u^2+u+3	c	$2u^2+u+1$	d	$2u^2+u+2$	e
$2u^2+u+3$	g	$3u^2+u+1$	l	$3u^2+u+2$	n
$3u^2+u+3$	p	u^2+2u+1	r	u^2+2u+2	s
u^2+2u+3	t	$2u^2+2u+1$	v	$2u^2+2u+2$	y
$2u^2+2u+3$	b'	$3u^2+2u+1$	c'	$3u^2+2u+2$	d'
$3u^2+2u+3$	e'	u^2+3u+1	g'	u^2+3u+2	l'
u^2+3u+3	n'	$2u^2+3u+1$	p'	$2u^2+3u+2$	r'
$2u^2+3u+3$	s'	$3u^2+3u+1$	t'	$3u^2+3u+2$	v'
$3u^2+3u+3$	y'				

Tablo 2.2. ve Tablo 2.3.'te, T_3 halkası üzerinde uzunluğu $m=7$ olan devirli ve $\left(1+2u^2\right)-$sabit devirli kodlardan elde edilen Hamming ağırlık, Lee ağırlık ve Öklit ağırlıkları için $\mathbb{Z}_4$ üzerindeki yeni ve optimal parametreler hakkında bilgi verecektir. Kodların $\mathbb{Z}_4$ görüntülerinin uzunluğu, tanımlanan ϕ Gray dönüşümü aracılığıyla 14 olacaktır. Yazımı kolaylaştırmak için polinomların katsayılarının temsil edilen formu x değişkenindeki en yüksek dereceden başlayarak azalan bir şekilde yazılacaktır. Örneğin, $\left(2u^2+2u+2\right)x^5+\left(u+1\right)x^3+3u\,x+1$ polinomu $v0A061$ ile temsil edilecektir. Q katsayısının n defa tekrar etmesi durumunda kısaca Q^n şeklinde ifade edilecektir. Örneğin, $\left(u+3\right)x^3+\left(u+3\right)x^2+\left(u+3\right)x+\left(u+3\right)$ polinomu D^4 ile gösterilecektir.

Aşağıdaki tablolarda her bir üreteç polinomu için Lee, Öklit ve Hamming ağırlıklar hesaplanmıştır. [43] numaralı kaynakta verilen veritabanına göre ilk defa bulunan kodlar "$*$" ile işaretlenmiştir. Aynı uzunluk, boyut ve minimum uzaklıkta bulunan en iyi parametreler optimal kod olarak adlandırılmış ve tabloda "$**$" ile işaretlenmiştir. "$*$" ve "$**$" ile işaretlenmeyen kodlar ise $\mathbb{Z}_4$ üzerinde bilinen en iyi lineer kodlardır. Burada L indisi Lee ağırlığı, E indisi Öklit ağırlığı, H indisi ise Hamming ağırlığı temsil etmektedir.

[43] numaralı kaynakta verilen online veritabanı dayanak noktası olarak kabul edildiği takdirde, T_3 halkasındaki devirli kodların $\mathbb{Z}_4$ görüntüleri kullanılarak $\left(14,4^3 2^2,4_L\right)$, $\left(14,4^3 2^2,8_E\right)$ ve $\left(14,4^3 2^2,2_H\right)$ parametrelerine sahip 245 farklı üreteç polinomu; $\left(14,4^1 2^0,14_H\right)$ ve $\left(14,4^1 2^0,14_E\right)$ parametrelerine sahip 3 farklı üreteç polinomu; $\left(14,4^3 2^4,4_L\right)$ ve $\left(14,4^3 2^4,2_H\right)$ parametrelerine sahip 342 farklı üreteç polinomu; $\left(14,4^3 2^0,8_E\right)$ parametresine sahip 1 üreteç polinomu; $\left(14,4^1 2^6,4_L\right)$ ve $\left(14,4^1 2^6,2_H\right)$ parametrelerine sahip 22 farklı üreteç polinomu, $\left(14,4^0 2^3,32_E\right)$ parametresine sahip 1 üreteç polinomu, $\left(14,4^0 2^5,4_L\right)$ ve $\left(14,4^0 2^5,8_E\right)$ parametrelerine sahip 1 üreteç

polinomu ile yeni kodlar elde edilmiştir. Ayrıca $(14,4^3 2^0,8_H)$ parametresine sahip 1 üreteç polinomu; $(14,4^1 2^3,12_L)$, $(14,4^1 2^3,14_E)$ ve $(14,4^1 2^3,6_H)$ parametrelerine sahip 2 farklı üreteç polinomu; $(14,4^0 2^4,24_E)$ ve $(14,4^0 2^4,6_H)$ parametrelerine sahip 2 farklı üreteç polinomu; $(14,4^3 2^3,8_L)$ ve $(14,4^3 2^3,4_H)$ parametrelerine sahip 6 farklı üreteç polinomu; $(14,4^0 2^6,8_L)$, $(14,4^0 2^6,16_E)$ ve $(14,4^0 2^6,4_H)$ parametrelerine sahip 8 farklı üreteç polinomu ve $(14,4^0 2^3,16_L)$ parametresine sahip 1 üreteç polinomu ile optimal kodlar elde edilmiştir. Ancak yoğunluk olmaması adına bulunan kodların bir kısmı aşağıdaki tablolar ile sunulmuştur.

Bunların yanı sıra T_3 halkası üzerinde $(1+2u^2)-$sabit devirli kodların $\mathbb{Z}_4$ görüntüleri aracılığı ile 13 farklı yeni parametre elde edilmiştir. $(14,4^4 2^3,4_L)$, $(14,4^4 2^3,6_E)$ ve $(14,4^4 2^3,2_H)$ parametrelerine sahip 3 farklı üreteç polinomu; $(14,4^4 2^0,6_L)$ ve $(14,4^4 2^0,6_E)$ parametrelerine sahip 1 üreteç polinomu; $(14,4^6 2^1,4_L)$, $(14,4^6 2^1,4_E)$ ve $(14,4^6 2^1,2_H)$ parametrelerine sahip 3 farklı üreteç polinomu; $(14,4^3 2^4,4_L)$ ve $(14,4^3 2^4,2_H)$ parametrelerine sahip 3 farklı üreteç polinomu; $(14,4^3 2^1,4_H)$ parametresine sahip 1 üreteç polinomu; $(14,4^1 2^6,4_L)$ ve $(14,4^3 2^4,2_H)$ parametrelerine sahip 3 farklı üreteç polinomu ile yeni kodlar bulundu. Bunlara ek olarak $(14,4^4 2^0,6_H)$ parametresine sahip 2 farklı üreteç polinomu; $(14,4^3 2^3,8_L)$ ve $(14,4^3 2^3,4_H)$ parametrelerine sahip 1 üreteç polinomu; $(14,4^0 2^7,4_L)$ ve $(14,4^0 2^7,2_H)$ parametrelerine sahip 2 farklı üreteç polinomu; $(14,4^1 2^3,12_L)$, $(14,4^1 2^3,14_E)$ ve $(14,4^1 2^3,6_H)$ parametrelerine sahip 2 farklı üreteç polinomu; $(14,4^3 2^1,8_L)$ ve $(14,4^3 2^1,6_H)$ parametrelerine sahip 5 farklı üreteç polinomu ile birçok optimal kod elde edilmiştir. Burada belirtilmeyen kodlar ise [43] numaralı kaynakta verilen veritabanına göre bilinen en iyi $\mathbb{Z}_4-$lineer kodlardır. Elde edilen tüm bu sonuçlar [56] numaralı makalede yayınlanmıştır.

Tablo 2.2. Bazı devirli kodların $\mathbb{Z}_4$ görüntüleri

$\tau_1(x)$	$\tau_2(x)$	$\tau_3(x)$	Tip	W_L	W_E	W_H
789^3	$U^3De'dD$	$5'5'05'$	$4^32^{2\,*}$	4^*	8^*	2^*
78999	$N^3De'D^2$	$7'7'3'03'$	4^32^4	4^*	8	2^*
7^3979^2	$3'3'3'v'3'v'v'$	$5'5'$	4^12^0	14	14^*	14^*
7^2909	$dv's'Ns'$	$7'7'7'3'3'7'3'$	4^32^4	4^*	8	2^*
789^3	$N^5s'D$	$7'5'3'7'3'$	$4^32^{2\,*}$	4^*	8^*	2^*
78999	$U^2de's'ds'$	$5'5'5'05'$	4^32^1	8^{**}	8	6^{**}
7^2909	$3'3'3'v'3'v'v'$	$3'5'3'7'$	4^32^1	8^{**}	8	6^{**}
70779	N^5D^2	$3'5'3'7'$	4^32^4	4^*	8	2^*
789^3	$U^3s'e'HD$	$5'05'5'5'$	$4^32^{2\,*}$	4^*	8^*	2^*
70779	D^6s'	$3'5'3'7'$	4^32^4	4^*	8	2^*
7^39799	$3'3'3'v'3'v'v'$	$7'7'7'7'7'7'7'$	4^12^6	4^*	8	2^*
70779	$U^3s'e'HD$	$5'05'5'$	$4^32^{2\,*}$	4^*	8^*	2^*
78999	$H^3s's'Hs'$	$3'7'$	4^32^4	4^*	8	2^*
789^3	N^5D^2	$5'05'5'$	$4^32^{2\,*}$	4^*	8^*	2^*
70779	U^3N^2dD	$7'3'3'03'$	4^32^4	4^*	8	2^*
70779	$U^2de's'ds'$	$7'5'7'7'$	4^32^4	4^*	8	2^*
78999	$H^3s's'Hs'$	$7'5'7'7'$	4^32^4	4^*	8	2^*
79909	$7'7'dHs'bs'$	$5'5'5'5'5'5'5'$	4^32^1	8^{**}	8	6^{**}
78999	D^6s'	$7'5'7'7'$	4^32^4	4^*	8	2^*
70779	$U^2de's'ds'$	$7'7'$	4^32^4	4^*	8	2^*
70779	$r^3e'e're'$	$7'7'3'03'$	4^32^4	4^*	8	2^*
70779	$U^3De'dD$	$(5')^3\,05'$	$4^32^{2\,*}$	4^*	8^*	2^*
70779	$U^2de's'ds'$	$7'7'7'3'7'3'3'$	4^32^1	8^{**}	8	6^{**}
70779	$N^2D^2s'e's'$	$3'5'7'3'3'$	$4^32^{2\,*}$	4^*	8^*	2^*
70779	$(e')^7$	$3'5'3'7'$	4^32^4	4^*	8	2^*
78999	$N^2s'e'Ds's'$	$7'5'3'7'3'$	4^32^1	8^{**}	8	6^{**}
70779	$N^5e'e'$	$3'5'3'7'$	4^32^4	4^*	8	2^*
79909	$7'7'dHs'bs'$	$7'5'7'7'$	4^32^1	8^{**}	8	6^{**}
88808	$3'3'3'v'3'v'v'$	$7'7'$	4^02^7	4^{**}	8	2^{**}
78999	$N^2De's'Ds'$	$7'7'3'5'3'$	4^32^4	4^*	8	2^*
70779	$N^3De'D^2$	$5'05'5'5'$	$4^32^{2\,*}$	4^*	8^*	2^*
70779	N^5D^2	$7'5'7'7'$	4^32^4	4^*	8	2^*
789^3	$b^2v'0v'$	$7'3'3'03'$	4^32^3	8^{**}	8	4^{**}

Tablo 2.2. (Devamı)

$\tau_1(x)$	$\tau_2(x)$	$\tau_3(x)$	Tip	W_L	W_E	W_H
88808	$drs'3's'$	$5'5'05'$	$4^0 2^6$	8^{**}	16^{**}	4^{**}
70779	$r^3e'e're'$	$(7')^6 3'$	$4^3 2^1$	8	8	6^{*}
70779	$N^5s'D$	$7'3'5'7'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
70779	$N^3s'e's'D$	$(5')^7$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
789^3	U^3N^2HD	$7'5'3'7'3'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
78999	$N^2e'Ne'e'$	$3'3'7'5'3'$	$4^3 2^4$	4^{*}	8	2^{*}
70779	$U^3De'dD$	$7'7'$	$4^3 2^4$	4^{*}	8	2^{*}
789^3	U^3N^2HD	$5'5'05'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
88808	$drs'3's'$	$3'5'7'3'3'$	$4^0 2^6$	8^{**}	16^{**}	4^{**}
$79^2 09$	$r^2e'Re'$	$7'7'3'03'$	$4^3 2^0$	8	8^{*}	8^{**}
78999	$N^2s'e'Ds's'$	$3'5'3'7'$	$4^3 2^4$	4^{*}	8	2^{*}
78999	$H^3s's'Hs'$	$5'5'5'05'$	$4^3 2^1$	8^{**}	8	6^{**}
78999	$N^3s'e's'D$	$7'7'$	$4^3 2^4$	4^{*}	8	2^{*}
789^3	$N^5s'D$	$3'7'5'7'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
70779	$N^2D^2s'e's'$	$5'5'5'05'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
88808	$drs'3's'$	$3'7'5'7'$	$4^0 2^7$	4^{**}	8	2^{**}
79909	$7'7'dHs'bs'$	$(3')^7$	$4^3 2^1$	8^{**}	8	6^{**}
70779	D^6s'	$3'3'7'5'3'$	$4^3 2^4$	4^{*}	8	2^{*}
70779	$N^2D^2s'e's'$	$5'05'5'5'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
79909	$7'7'dHs'bs'$	$3'7'$	$4^3 2^4$	4^{*}	8	2^{*}
78999	$N^5s'D$	$7'7'3'5'3'$	$4^3 2^4$	4^{*}	8	2^{*}
78999	$b^2v'0v'$	$7'7'7'3'7'3'3'$	$4^3 2^4$	4^{*}	8	2^{*}
70779	U^3N^2dD	$5'05'5'5'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
$7^3 979^2$	$R0R^2$	$7'7'3'03'$	$4^1 2^3$	12^{**}	14^{**}	6^{**}
70779	$N^3s'e's'D$	$5'5'05'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
70779	$N^5s'D$	$5'05'5'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
70779	N^5D^2	$5'5'05'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
$7^3 9^2 79$	$dUDbs'$	$7'5'3'7'3'$	$4^1 2^6$	4^{*}	8	2^{*}
70779	N^5D^2	$7'3'5'7'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
70779	$N^5s'D$	$(7')^6 3'$	$4^3 2^{2\,*}$	4^{*}	8^{*}	2^{*}
88808	$drs'3's'$	$7'5'3'7'3'$	$4^0 2^6$	8^{**}	16^{**}	4^{**}
78999	$U^2de's'd's'$	$(3')^7$	$4^3 2^1$	8^{**}	8	6^{**}
70779	$U^2de's'd's'$	$7'7'3'03'$	$4^3 2^4$	4^{*}	8	2^{*}

Tablo 2.2. (Devamı)

$\tau_1(x)$	$\tau_2(x)$	$\tau_3(x)$	Tip	W_L	W_E	W_H
7^2909	$3'3'3'v'3'v'v'$	$7'5'3'7'3'$	$4^3 2^4$	4^*	8^*	2^*
78999	$N^2De's'Ds'$	$3'7'$	$4^3 2^4$	4^*	8	2^*
8^308	$(3')^3 v'3'v'v'$	$(7')^6 3'$	$4^0 2^4$	12	24^{**}	6^{**}
789^3	$N^2D^2s'e's'$	$3'5'7'3'3'$	$4^3 2^{2\,*}$	4^*	8^*	2^*
707^29	$b^2v'0v'$	$7'5'(3')^3$	$4^3 2^3$	8^{**}	8	4^{**}
78999	$U^2de's'ds'$	$7'7'3'03'$	$4^3 2^4$	4^*	8	2^*
789^3	U^3N^2HD	$5'05'5'5'$	$4^3 2^{2\,*}$	4^*	8^*	2^*
7^3979^2	$3'3'3'v'3'v'v'$	$7'7'7'7'7'7'3'$	$4^1 2^0$	14	14^*	14^*
789^3	$U^3s'e'HD$	$7'3'5'7'$	$4^3 2^{2\,*}$	4^*	8^*	2^*
789^3	$N^3s'e's'D$	$7'07'7'3'$	$4^3 2^{2\,*}$	4^*	8^*	2^*
78999	$U^2de's'ds'$	$7'3'3'03'$	$4^3 2^4$	4^*	8	2^*
70779	d^3D^2ds'	$7'5'7'7'$	$4^3 2^4$	4^*	8	2^*
70779	$U^3De'dD$	$7'5'3'7'3'$	$4^3 2^{2\,*}$	4^*	8^*	2^*
79909	$7'7'dHs'bs'$	$7'5'3'7'3'$	$4^3 2^4$	4^*	8	2^*
70779	$N^3s'e's'D$	$3'7'$	$4^3 2^4$	4^*	8	2^*
70779	$r^3e'e're'$	$7'5'3'7'3'$	$4^3 2^1$	8^{**}	8	6^{**}
8^308	$3'3'v'3'v'v'$	$5'5'$	$4^0 2^4$	12	24^{**}	6^{**}
70779	$r^3e'e're'$	$7'5'7'7'$	$4^3 2^4$	4^*	8	2^*
88808	$drs'3's'$	$3'5'7'3'3'$	$4^0 2^6$	8^{**}	16^{**}	4^{**}
70779	$H^3s's'Hs'$	$3'3'7'5'3'$	$4^3 2^4$	4^*	8	2^*
77909	$5'e'RNr$	$5'5'5'5'5'5'5'$	$4^3 2^1$	8^{**}	8	6^{**}
789^3	N^5D^2	$5'05'5'5'$	$4^3 2^{2\,*}$	4^*	8^*	2^*
70779	$H^3s's'Hs'$	$7'7'3'03'$	$4^3 2^4$	4^*	8	2^*
70779	$r^3e'e're'$	$3'5'3'7'$	$4^3 2^4$	4^*	8	2^*
78999	$r^3e'e're'$	$3'3'7'5'3'$	$4^3 2^4$	4^*	8	2^*
78999	$N^3Ds'e'D$	$5'5'5'05'$	$4^3 2^1$	8^{**}	8	6^{**}
70779	$U^3s'e'HD$	$3'7'$	$4^3 2^4$	4^*	8	2^*
7^39799	$drs'3's'$	$5'5'5'05'$	$4^1 2^6$	4^*	8	2^*

Tablo 2.3. Bazı $\left(1+2u^2\right)-$ sabit devirli kodların $\mathbb{Z}_4$ görüntüleri

$\tau_1(x)$	$\tau_2(x)$	$\tau_3(x)$	Tip	W_L	W_E	W_H
79989	$D^3s'Ds'$	$(5')^7$	4^32^1	8^{**}	8	6^{**}
79	$3'3'7'e'H$	$7'7'7'3'3'7'3'$	4^62^1	4^{*}	4^{*}	2^{*}
78999	$7'5'3'v'v'$	$7'7'7'3'7'3'$	4^32^1	8^{**}	8	6^{**}
7979799	$U^3e'e'Ue'$	$7'07'7'3'$	4^12^3	12^{**}	14^{**}	6^{**}
7789	$3'5'7'v'v'$	$(7')^6\,3'$	4^42^0	6^{*}	6^{*}	6^{*}
79989	$H5'dHs'$	$7'3'5'7'$	4^32^4	4^{*}	8	2^{*}
88808	$drs'3's'$	$7'3'5'7'$	4^02^7	4^{**}	8	2^{**}
97789	$5'5'rFe're'$	$5'5'5'05'$	4^32^1	8^{**}	8	4^{*}
79909	$5'5'e'e'rFe'$	$7'7'7'3'7'3'3'$	4^32^1	8^{**}	8	6^{**}
78979	$7'7'dv'DHs'$	$5'5'05'$	4^32^1	8^{**}	8	6^{**}
9989	$7'7'7'b7'bv'$	$7'5'7'7'$	4^42^3	4^{*}	6^{*}	2^{*}
7979799	$UN^23'D$	$7'5'7'7'$	4^12^6	4^{*}	8	2^{*}
7789	$7'7'dv's'ds'$	$7'7'$	4^42^3	4^{*}	6^{*}	2^{*}
98779	$7'7'3'rH$	$5'05'5'$	4^32^3	8^{**}	8	4^{**}
77909	$5'e'RNr$	$5'5'5'5'5'5'5'$	4^32^1	8^{**}	8	6^{**}
99	$7'7'7'b7'bv'$	$7'7'7'3'7'3'3'$	4^62^1	4^{*}	4^{*}	2^{*}
97789	$N^2D^2s'Ns'$	$7'3'5'7'$	4^32^4	4^{*}	8	2^{*}
9989	$DFDd$	$7'7'7'7'7'7'3'$	4^42^3	4^{*}	6^{*}	2^{*}
7979799	$U3'drD$	$3'7'$	4^12^6	4^{*}	8	2^{*}
9989	$U^3NUe'e'$	$7'5'3'7'3'$	4^42^0	8	8	6^{**}
7977779	$R3'bFb$	$7'5'3'3'3'$	4^12^3	12^{**}	14^{**}	6^{**}
98779	$r^3e're'e'$	$7'5'7'7'$	4^32^4	4^{*}	8	2^{*}
9797979	$7'7'7'dDbH$	$7'7'$	4^12^6	4^{*}	8	2^{*}
79	$7'7'7's'bs'H$	$7'3'5'7'$	4^62^1	4^{*}	4^{*}	2^{*}
88808	$drs'3's'$	$3'5'3'7'$	4^02^7	4^{**}	8	2^{**}

BÖLÜM 3. $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ HALKASI ÜZERİNDE AYKIRI DEVİRLİ VE AYKIRI SABİT DEVİRLİ KODLAR

Kodlar üzerine yapılan çalışmaların çoğu değişmeli yapılar üzerinde olsa da son zamanlarda bazı araştırmacılar değişmeli olmayan halkalarda, diğer bir ifadeyle, aykırı polinom halkalarında kod çalışmalarına odaklanmıştır. Aykırı polinom halkaları üzerindeki polinomlar birden fazla şekilde çarpanlarına ayrıldığından kod elde etme bakımından değişmeli halkalara göre daha avantajlıdır. Bu da araştırmacıların aykırı polinom halkalarına odaklanmalarının en önemli sebebidir. Bu halkalardaki devirli kod sınıfları ilk olarak Boucher ve ark. tarafından [57] numaralı çalışma ile ortaya çıkmıştır. Bu çalışmada $\mathbb{F}_q$ sonlu cismi ve bu cisim üzerinde tanımlı θ otomorfizması ile aykırı polinom halkası $\mathbb{F}_q[x,\theta]$ ile temsil edilmiştir. Boucher ve ark. [58] numaralı çalışmada Galois halkaları üzerindeki aykırı sabit devirli kodları incelemişlerdir. Şiap ve ark. [59] numaralı çalışmada, herhangi uzunluktaki bir kod için aykırı devirli kodların yapısını incelemişlerdir. Abualrub ve ark. [60] numaralı çalışmada, $v^2=v$ iken $\mathbb{F}_2+v\mathbb{F}_2$ halkası üzerinde aykırı devirli kodların yapısını araştırmış ve üreteç polinomlarını oluşturmuşlardır. Ayrıca Öklit ve Hermityen iç çarpımları yardımıyla serbest aykırı devirli kodların duallerinin üreteç polinomlarını tanımlamış, birçok örnek sunmuşlardır. Gürsoy ve ark. [61] numaralı çalışma ile $v^2=v$ iken $\mathbb{F}_q+v\mathbb{F}_q$ halkasında ayrıştırma metodu kullanarak aykırı devirli kodların üreteçlerini ve idempotent üreteçlerini inşa etmişlerdir. Bu halka üzerindeki aykırı devirli kodların tek eleman tarafından üretildiğini göstermiş ve bu kodlara birçok örnek sunmuşlardır. Sharma ve ark. [62] numaralı çalışmada, $u^2=0$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ halkasındaki aykırı sabit devirli kodları ele almış, bu kodların tek eleman tarafından üretilmesi durumunda serbest olması için gerek ve yeter koşulları belirlemişlerdir. Halka üzerinde tanımladıkları Gray dönüşüm yardımıyla iyi kodlar elde etmişlerdir. Üreteç polinomu ile duali arasındaki ilişkiyi inceleyerek örnekler vermişlerdir. Ayrıca çift (double)

aykırı sabit devirli polinomlara da değinmişlerdir. Aykırı polinom halkaları için literatürdeki [63-65] numaralı çalışmalar da incelenebilir.

Bu bölüm 4 kısımdan oluşmaktadır. İlk kısımda halkanın yapısı verilmiş, 3 tane yeni Gray dönüşüm tanımlanmıştır. İkinci kısımda öncelikle halka üzerindeki aşikâr olmayan tüm otomorfizmalar belirlenmiş, aykırı polinom halkası ile ilgili temel tanım ve teoremler ifade edilmiştir. Daha sonra tek uzunluktaki aykırı devirli kodların cebirsel yapısı incelenmiş ve üreteç polinomu belirlenmiştir. Tanımlanan tüm otomorfizmalar ve tüm Gray dönüşümler altındaki aykırı devirli kodların $\mathbb{Z}_4$ görüntüsünün $2-$parçalı devirli kod olduğu sonucuna varılmıştır. Üçüncü kısımda aykırı sabit devirli kodların üreteç polinomlarını elde etmek için aykırı devirli kodlar ile arasında bir izomorfizma kurulmuştur. Daha sonra bu izomorfizmadan yararlanarak aykırı sabit devirli kodların üreteç polinomu elde edilmiştir. Tanımlanan otomorfizmalar altında halkadaki her bir birimsel eleman için aykırı sabit devirli kodların $\mathbb{Z}_4$ görüntüleri incelenerek önemli sonuçlar elde edilmiştir. Dördüncü kısımda ise MAGMA programından yararlanarak hesaba dayalı sonuçlara ulaşılmıştır.

3.1. $\mathbb{Z}_4[u]/\langle u^3-u^2\rangle$ Halkasının Cebirsel Yapısı

$\mathbb{Z}_4+u\,\mathbb{Z}_4+u^2\mathbb{Z}_4=\left\{a_0+ua_1+u^2a_2 \;\middle|\; u^3=u^2 \text{ ve } a_i\in\mathbb{Z}_4\right\}$ halkası 64 elemanlı bir halkadır. Birimli ve değişmeli olan bu halka tez boyunca T_3 ile temsil edilecektir. T_3 halkası $\mathbb{Z}_4[u]/\langle u^3-u^2\rangle$ bölüm halkasına izomorf bir halka olduğundan $T_3\cong\mathbb{Z}_4[u]/\langle u^3-u^2\rangle$ şeklinde ifade edilebilir. Karakteristiği 4 olan T_3 halkasının 21 tane ideali vardır. $(1+u)$ ve $(2,u)$ halkanın maksimal idealleridir. İki maksimal ideale sahip olduğundan yarı lokal bir halkadır. İdealleri kapsama bağıntısına göre karşılaştırılamadığından zincir olmayan bir halkadır. u^2 ve $1+3u^2$ halkanın idempotent elemanları, $\{1,3,1+2u,3+2u,1+u+u^2,3+u+u^2,1+3u+u^2,3+3u+u^2,1$

$+2u^2, 3+2u^2, 1+2u+2u^2, 3+2u+2u^2, 1+u+3u^2, 3+u+3u^2, 1+3u+3u^2, 3+3u+3u^2\}$ elemanları ise halkanın birimsel elemanlarıdır.

T_3 üzerinde m uzunluğunda lineer bir C_3 kodu, T_3^m halkasının bir T_3 – alt modülüdür. Bu lineer kodun elemanları kodsöz olarak adlandırılır. $a_i \in \mathbb{Z}_4$ ve $i = 0,1,2$ iken T_3 halkasının herhangi bir elemanı $z = a_0 + ua_1 + u^2 a_2$ şeklinde tanımlanır. $i = 0,1,\ldots m-1$ olmak üzere her bir $z_i = a_0^i + ua_1^i + u^2 a_2^i$ elemanı için $z = (z_0, z_1, \ldots, z_{m-1})$ kodsözünün polinom formu $z(x) = z_0 + z_1 x + z_2 x^2 + \ldots z_{m-1} x^{m-1}$ şeklinde ifade edilir.

$i = 0,1,\ldots,m-1$ ve herhangi bir $z \in T_3$ için $z_i = a_0^i + ua_1^i + u^2 a_2^i$ olacak şekilde T_3^m halkasından $\mathbb{Z}_4^{2m}$ halkasına uzaklığı koruyan üç farklı Gray dönüşümü aşağıdaki gibi tanımlansın.

$$\phi_1 : T_3 \to \mathbb{Z}_4^{2m}$$
$$(a_0 + ua_1 + u^2 a_2) \to (a_0 + a_1 + 3a_2,\ 3a_0 + 3a_1 + a_2)$$

Bu dönüşüm,

$$\phi_1 : T_3^m \to \mathbb{Z}_4^{2m}$$
$$(z_0, z_1, \ldots, z_{m-1}) \to \begin{pmatrix} a_0^0 + a_1^0 + 3a_2^2, \ldots, a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, \\ 3a_0^0 + 3a_1^0 + a_2^0, \ldots, 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1} \end{pmatrix}$$

şeklinde genişletilir.

Bir diğer dönüşüm,

$$\phi_2 : T_3 \to \mathbb{Z}_4^{2m}$$
$$(a_0 + ua_1 + u^2 a_2) \to (a_0 + a_1 + 3a_2,\ a_0 + 3a_1 + a_2)$$

Bu dönüşüm,

$$\phi_2 : T_3^m \to \mathbb{Z}_4^{2m}$$

$$(z_0, z_1, \ldots, z_{m-1}) \to \begin{pmatrix} a_0^0 + a_1^0 + 3a_2^2, \ldots, a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, \\ a_0^0 + 3a_1^0 + a_2^0, \ldots, a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1} \end{pmatrix}$$

şeklinde genişletilir.

Son olarak tanımlanan üçüncü dönüşüm ise,

$$\phi_3 : T_3 \to \mathbb{Z}_4^{2m}$$

$$(a_0 + ua_1 + u^2 a_2) \to (a_0 + a_1 + 3a_2,\ 3a_0 + a_1 + 3a_2)$$

şeklindedir.

Bu dönüşüm de

$$\phi_3 : T_3^m \to \mathbb{Z}_4^{2m}$$

$$(z_0, z_1, \ldots, z_{m-1}) \to \begin{pmatrix} a_0^0 + a_1^0 + 3a_2^2, \ldots, a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, \\ 3a_0^0 + a_1^0 + 3a_2^0, \ldots, 3a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1} \end{pmatrix}$$

şeklinde genişletir.

Teorem 3.1.1. $i = 1,2,3$ olmak üzere tanımlanan ϕ_i dönüşümleri lineer ve uzaklığı koruyan dönüşümlerdir.

İspat. Öncelikle ϕ_1 dönüşümünün lineer olduğu, daha sonra ise Lee uzaklığın korunduğu gösterilsin. $a_j, b_j \in \mathbb{Z}_4$ ve $j = 0,1,2$ iken $t_i = a_0^i + ua_1^i + u^2 a_2^i$ ve $s_i = b_0^i + ub_1^i + u^2 b_2^i$ olmak üzere, her $t = (t_1, t_2, \ldots, t_{m-1})$, $s = (s_1, s_2, \ldots, s_{m-1}) \in T_3^m$ ve $y, r \in \mathbb{Z}_4$ için,

$$\phi_1(yt_1 + rs) = \phi_1 \begin{pmatrix} y\left(a_0^0 + ua_1^0 + u^2 a_2^0, a_0^1 + ua_1^1 + u^2 a_2^1, \ldots, a_0^{m-1} + ua_1^{m-1} + u^2 a_2^{m-1}\right) + \\ r\left(b_0^0 + ub_1^0 + u^2 b_2^0, b_0^1 + ub_1^1 + u^2 b_2^1, \ldots, b_0^{m-1} + ub_1^{m-1} + u^2 b_2^{m-1}\right) \end{pmatrix}$$

eşitliği düzenlenirse,

$$\phi_1\left(ya_0^0+rb_0^0+u\left(ya_1^0+rb_1^0\right)+u^2\left(ya_2^0+rb_2^0\right),\ \ldots\ ,ya_0^{m-1}+rb_0^{m-1}+u\left(ya_1^{m-1}+rb_1^{m-1}\right)+u^2\left(ya_2^{m-1}+rb_2^{m-1}\right)\right)$$

$$=\left(ya_0^0+rb_0^0+ya_1^0+rb_1^0+3ya_2^0+3rb_2^0,\ldots,ya_0^{m-1}+rb_0^{m-1}+ya_1^{m-1}+rb_1^{m-1}+3ya_2^{m-1}+3rb_2^{m-1},3ya_0^0+3rb_0^0+3ya_1^0+3rb_1^0+ya_2^0+rb_2^0,\ldots,3ya_0^{m-1}+3rb_0^{m-1}+3ya_1^{m-1}+3rb_1^{m-1}+ya_2^{m-1}+rb_2^{m-1}\right)$$

$$=\left(y\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}\right)+r\left(b_0^0+b_1^0+3b_2^0,\ldots,b_0^{m-1}+b_1^{m-1}+3b_2^{m-1}\right),\right.$$
$$\left.y\left(3a_0^0+3a_1^0+a_2^0,\ldots,3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right)+r\left(3b_0^0+3b_1^0+b_2^0,\ldots,3b_0^{m-1}+3b_1^{m-1}+b_2^{m-1}\right)\right)$$

$$=y\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+3a_1^0+a_2^0,\ldots,3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right)+r\left(b_0^0+b_1^0+3b_2^0,\ldots,b_0^{m-1}+b_1^{m-1}+3b_2^{m-1},3b_0^0+3b_1^0+b_2^0,\ldots,3b_0^{m-1}+3b_1^{m-1}+b_2^{m-1}\right)$$

$=y\phi_1(t)+r\phi_1(s)$ elde edilir. Böylece ϕ_1 dönüşümünün lineer bir dönüşüm olduğu gösterilmiş olur.

ϕ_1 dönüşümü uzaklığı koruduğunu göstermek için; $t-s=\left(t_0,t_1,\ldots,t_{m-1}\right)-\left(s_0,s_1,\ldots,s_{m-1}\right)$ olduğu, dönüşümün lineerliği ve Lee uzaklık tanımını kullanılarak,

$$d_L(t,s)=w_L(t-s)=\sum_{i=0}^{m-1}w_L\left(t_i-s_i\right)=\sum_{i=0}^{m-1}w_L\left(\left(a_0^i+ua_1^i+u^2a_2^i\right)-\left(b_0^i+ub_1^i+u^2b_2^i\right)\right)$$
$$=\sum_{i=0}^{m-1}w_L\left(a_0^i-b_0^i+u\left(a_1^i-b_1^i\right)+u^2\left(a_2^i-b_2^i\right)\right)$$

elde edilir. Bu eşitliğe ϕ_1 Gray dönüşümü uygulandığı takdirde,

$$\sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3a_2^i - 3b_2^i\right) + w_L\left(3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + a_2^i - b_2^i\right) = w_L\left(\phi_1(t-s)\right)$$

eşitliğine ulaşılır. ϕ_1 lineer dönüşüm olduğundan bu ifade $w_L\left(\phi_1(t)-\phi_1(s)\right) = d_L\left(\phi_1(t),\phi_1(s)\right)$ eşittir.

Diğer taraftan,

$$\begin{aligned} w_L\left(\phi_1(t-s)\right) &= \sum_{i=0}^{m-1} w_L\left(\phi_1(t_i - s_i)\right) = \sum_{i=0}^{m-1} w_L\left(\phi_1\left(\left(a_0^i + ua_1^i + u^2a_2^i\right) - \left(b_0^i + ub_1^i + u^2b_2^i\right)\right)\right) \\ &= \sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + u\left(a_1^i - b_1^i\right) + u^2\left(a_2^i - b_2^i\right)\right) \\ &= \sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3a_2^i - 3b_2^i, 3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + a_2^i - b_2^i\right) \\ &= \sum_{i=0}^{m-1} w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3a_2^i - 3b_2^i\right) + w_L\left(3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + a_2^i - b_2^i\right) \end{aligned}$$

elde edilir. Burada $w_L\left(a_0^i - b_0^i + a_1^i - b_1^i + 3a_2^i - 3b_2^i\right) = \min\left\{\left|a_0^i - b_0^i + a_1^i - b_1^i + 3a_2^i - 3b_2^i\right|, \left|4 - \left(a_0^i - b_0^i + a_1^i - b_1^i + 3a_2^i - 3b_2^i\right)\right|\right\}$ ve $w_L\left(3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + a_2^i - b_2^i\right) = \min\left\{\left|3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + a_2^i - b_2^i\right|, \left|4 - \left(3a_0^i - 3b_0^i + 3a_1^i - 3b_1^i + a_2^i - b_2^i\right)\right|\right\}$ olduğu Lee ağırlık tanımından bilinmektedir. Böylece $d_L(t,s) = w_L\left(\phi_1(t-s)\right) = w_L\left(\phi_1(t) - \phi_1(s)\right) = d_L\left(\phi_1(t), = d_L\left(\phi_1(t),\phi_1(s)\right)\right.$ eşitliği elde edilir. Böylece ϕ_1 dönüşümünün uzaklık koruyan bir dönüşüm olduğu gösterilmiş olur.

ϕ_2 ve ϕ_3 Gray dönüşümlerinin lineer oldukları ve Lee uzaklığı korudukları da benzer şekilde gösterilebilir. □

Not 3.1.1. Tanımlanan ϕ_i Gray dönüşümlerinin Öklit ve Hamming uzaklıkları koruduğu da benzer şekilde gösterilebilir.

Tanım 3.1.1. Herhangi bir $(z_0, z_1, \ldots, z_{m-1}) \in C_3$ iken $(\lambda\Theta_i(z_{m-1}), \Theta_i(z_0), \ldots, \Theta_i(z_{m-2})) \in C_3$ ise C_3 kodu T_3 halkası üzerinde uzunluğu m olan $(\Theta_i, \lambda)-$ sabit devirli kod olarak adlandırılır. $\lambda = 1$ iken, T_3 halkası üzerinde m uzunluğundaki $(\Theta_i, \lambda)-$ sabit devirli kod Θ_i- devirli kod olarak adlandırılır.

3.2. T_3 Halkası Üzerindeki Aykırı Devirli Kodların Cebirsel Yapısı

Aykırı devirli kodlar hakkında bilgi verebilmek için öncelikle T_3 halkasının aşikâr olmayan otomorfizmaları tanımlanmalıdır. $i = 1, 2, 3$ olmak üzere bu otomorfizmalar Θ_i şeklinde temsil edilsin. Bu durumda T_3 halkasından T_3 halkasına tanımlanan aşikâr olmayan otomorfizmalar

$$\Theta_1(a_0 + ua_1 + u^2a_2) = a_0 + (2+3u)a_1 + u^2a_2$$
$$\Theta_2(a_0 + ua_1 + u^2a_2) = a_0 + (2u^2 + u + 2)a_1 + u^2a_2$$
$$\Theta_3(a_0 + ua_1 + u^2a_2) = a_0 + (2u^2 + 3u)a_1 + u^2a_2$$

şeklindedir. Ve tanımlanan bu otomorfizmaların mertebeleri 2 'dir.

$T_3[x, \Theta_i] = \{a_0 + a_1x + \ldots + a_{m-1}x^{m-1} : a_i \in T_3,\ i = 0, 1, \ldots, m-1,\ m \in \mathbb{N}\}$ halkası aykırı polinom halkası olarak adlandırılır. Bu halkada kullanılan toplama işlemi bilinen toplama işlemi olmasına rağmen bilinen çarpma işleminin aksine $(ax^k)(bx^j) = a\Theta_i^k(b)x^{k+j}$ şeklinde farklı bir çarpma işlemi tanımlanır. Tanımlanan bu çarpma işlemi aykırı polinom halkasının değişmeli olmayan bir yapıda olmasının en temel sebebidir. $f(x) = q(x)p(x)$ olacak şekilde bir $q(x) \in T_3[x, \Theta_i]$ polinomu varsa $p(x) \in T_3[x, \Theta_i]$ polinomuna $f(x)$ polinomunun bir sağ böleni adı verilir. Bu durumda $f(x)$ polinomu $p(x)$ polinomunun bir sol çarpanı olur. Sol bölen ve sağ

çarpan da benzer şekilde tanımlanabilir. Yapı değişmeli olmadığından sol çarpan kavramı büyük önem arz etmektedir.

Bu bölümde sağ bölen kavramı kullanılacaktır ve $T_3[x,\Theta_i]\Big/\langle x^m-1\rangle$ bölüm halkası $T_{3,m_{\Theta_i}}$ ile aykırı devirli kodlar da Θ_i-devirli kodlar ile temsil edilecektir. Diğer bir ifade ile $\sigma_{\Theta_i}(C_3)=C_3$ ise T_3^m halkasının bir T_3-alt modülü Θ_i-devirli kod olarak adlandırılacaktır.

Bu bölüm halkaları $p(x), f(x)\in T_3[x,\Theta_i]$ polinomları için $p(x)\big(f(x)+\langle x^m-\lambda\rangle\big)$ $=p(x)f(x)+\langle x^m-\lambda\rangle$ tanımlanan çarpma işlemine göre bir $T_3[x,\Theta_i]-$sol modüldür.

T_3^m halkasından $T_{3,m_{\Theta_i}}$ halkasına $(z_0, z_1,\ldots,z_{m-1})\to z_0+z_1x+\cdots+z_{m-1}x^{m-1}$ olacak şekilde bir T_3-modül izomorfizması tanımlansın.

Tanım 3.2.1. T_3 halkasında uzunluğu m olan aykırı lineer C_3 kodu, $T_3[x,\Theta_i]$ halkası üzerinde derecesi m olan bir polinom $f(x)$ olmak üzere, $T_3[x,\Theta_i]\Big/_{<f(x)>}-$sol modülünün bir $T_3[x,\Theta_i]-$sol alt modülüdür.

Teorem 3.2.1. $T_{3,m_{\Theta_i}}$ bölüm halkası,

$$\alpha(x)\big(z_0(x),z_1(x),\ldots,z_{m-1}(x)\big)=\big(\alpha(x)z_0(x),\alpha(x)z_1(x),\ldots,\alpha(x)z_{m-1}(x)\big)$$

ile tanımlanan çarpma işlemi altında bir $T_{3,m_{\Theta_i}}-$alt modüldür.

İspat. $z(x)=\big(z_0(x),z_1(x),\ldots,z_{m-1}(x)\big)$ ve $t(x)=\big(t_0(x),t_1(x),\ldots,t_{m-1}(x)\big)$ olmak üzere, her $\alpha(x),\beta(x)\in T_{3,m_{\Theta_i}}$ ve her $z(x),t(x)\in T_{3,m_{\Theta_i}}$ için;

i. $(\alpha+\beta)z=(\alpha+\beta)(z_0,z_1,\ldots,z_{m-1})$

$$=(\alpha z_0+\beta z_0,\alpha z_1+\beta z_1,\ldots,\alpha z_{m-1}+\beta z_{m-1})$$

$$=(\alpha z_0,\alpha z_1,\ldots,\alpha z_{m-1})+(\beta z_0,\beta z_1,\ldots,\beta z_{m-1})=\alpha z+\beta z$$

ii. $\alpha(z+t)=\alpha(z_0+t_0,z_1+t_0,\ldots,z_{m-1}+t_{m-1})$

$$=(\alpha z_0+\alpha t_0,\alpha z_1+\alpha t_1,\ldots,\alpha z_{m-1}+\alpha t_{m-1})$$

$$=(\alpha z_0,\alpha z_1,\ldots,\alpha z_{m-1})+(\alpha t_0,\alpha t_1,\ldots,\alpha t_{m-1})=\alpha z+\alpha t$$

iii. $\alpha(\beta z)=\alpha(\beta z_0,\beta z_1,\ldots,\beta z_{m-1})=(\alpha\beta z_0,\alpha\beta z_1,\ldots,\alpha\beta z_{m-1})$

$$=\alpha\beta(z_0,z_1,\ldots,z_{m-1})=(\alpha\beta)z$$

iv. $1_{T_{3,m_{\Theta_i}}}z=z$

şartları sağlandığından $T_{3,m_{\Theta_i}}$ bölüm halkası $T_3[x,\Theta_i]-$sol modülünün bir $T_{3,m_{\Theta_i}}-$sol alt modülüdür.

Teorem 3.2.2. $T_{3,m_{\Theta_i}}$ halkası üzerinde m uzunluğundaki C_3 kodunun Θ_i-devirli kod olması için gerek ve yeter koşul C_3 kodunun bir $T_{3,m_{\Theta_i}}-$sol modülünün $T_3[x,\Theta_i]-$sol alt modüldür.

İspat. C_3 kodunun $T_{3,m_{\Theta_i}}$ üzerinde Θ_i-devirli kod ve $z(x)=q_0+q_1x+\ldots++q_{m-1}x^{m-1}$ olacak şekilde $z(x)\in C_3$ olsun. C_3 kodu $T_{3,m_{\Theta_i}}$ bölüm halkasının bir alt grubu olduğundan $z_1(x),z_2(x)\in C_3$ polinomları için $z_1(x)-z_2(x)\in C_3$ olduğu söylenebilir. C_3 kodu Θ_i-devirli kod olduğundan $xz(x)$ polinomu da C_3 kodunun bir elemanı olur. Aynı şekilde $x(xz(x))$ polinomunun da C_3 kodunun bir elemanı olduğu elde edilir. Benzer şekilde devam edilmesi durumunda 0'dan büyük eşit her i değeri için $x^iz(x)\in C_3$ elde edilir. C_3 kodu lineer kod olduğundan $T_3[x,\Theta_i]$ halkasından alınan herhangi bir $r(x)$ polinomu için $r(x)z(x)$ polinomu da C_3

kodunun bir elemanı olur. Dolayısıyla C_3 kodu $T_{3,m_{\Theta_i}}$ bölüm halkasının bir $T_3\left[x,\Theta_i\right]-$ sol alt modülü olur.

Diğer taraftan, C_3 kodunun $T_{3,m_{\Theta_i}}-$sol modülünün bir $T_3\left[x,\Theta_i\right]-$sol alt modülü olduğu kabul edilsin. Alt modül şartından C_3 kodu $T_{3,m_{\Theta_i}}$ bölüm halkasının bir alt grubu ve $T_3\left[x,\Theta_i\right]$halkasından alınan her x elemanı için de $x\,z\left(x\right)\in C_3$ olacak şekilde $z\left(x\right)\in C_3$ mevcut olacağından C_3 kodu bir Θ_i-devirli kod olur. □

Önceki bölümde detaylı bir şekilde belirtildiği üzere, T_3 halkasındaki devirli bir kodun üreteç polinomunu oluşturmak için Çin Kalan Teoremi kullanılacaktır.

Çin Kalan Teoremi'nin kullanılabilmesi için öncelikle T_3 halkası ayrıştırılmalıdır. $\mathfrak{R}$ ve $\mathfrak{I}$ kodları lineer iki kod olmak üzere $\oplus$ işleminin $\mathfrak{R}\oplus\mathfrak{I}=\{d+w\mid d\in\mathfrak{R},\ w\in\mathfrak{I}\}$ şeklindeki tanımlaması dikkate alınarak T_3 halkası aşağıdaki gibi parçalanabilir.

$$T_3=u^2T_3\oplus\left(1+3u^2\right)T_3=u^2\mathbb{Z}_4\oplus\left(1+3u^2\right)\left(\mathbb{Z}_4+u\mathbb{Z}_4\right)$$

Burada Tanım 2.2.2. ve Teorem 2.2.1.'den hareketle $\mathbb{Z}_4+u\mathbb{Z}_4$ halkasında $u^2=0$ iken çalıştığı unutulmamalıdır. T_3 halkası tek minimal ideale sahip lokal halkaların direkt toplamı olarak yazılabildiğinden bir Frobenius halkadır.

$\mathfrak{R}$ kodu üzerinde, $\mathfrak{I}$ kodu ise $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde uzunlukları m olan lineer kodlar olmak üzere, $\mathfrak{R}=\left\{t+y+h\in{\mathbb{Z}_4}^m\middle|\,t+uy+u^2h\in C_3\right\}$ ve $\mathfrak{I}=\left\{t+uy\in(\mathbb{Z}_4+u\mathbb{Z}_4)^m\,|t+uy+u^2h\in C_3\right\}$ olarak tanımlansın. Böylece T_3 halkası üzerinde uzunluğu m olan lineer kod tek türlü olarak $C_3=u^2\mathfrak{R}\oplus(1+3u^2)\mathfrak{I}$ şeklinde belirlenir.

Tüm bu açıklamalar ışığında;

Teorem 3.2.3. C_3 kodu T_3 halkası üzerinde lineer bir kod ve $\mathfrak{R}$ kodu $\mathbb{Z}_4$ üzerinde m uzunluğunda bir kod, $\mathfrak{I}$ kodu da $u^2=0$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde m uzunluğunda bir kod olmak üzere $C_3=u^2\mathfrak{R}\oplus(1+3u^2)\mathfrak{I}$ olsun. Bu durumda C_3 kodunun Θ_i-devirli kod olması için gerek ve yeter koşul $\mathfrak{R}$ kodunun $\mathbb{Z}_4$ üzerinde, $\mathfrak{I}$ ise $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerinde Θ_i-devirli kod olmasıdır.

İspat. $i=0,1,\ldots,m-1$ olmak üzere $z=(z_0,z_1,\ldots,z_{m-1})\in C_3$ ve $z_i=u^2p_i+(1+3u^2)v_i$ olsun. $p=(p_0,p_1,\ldots,p_{m-1})\in\mathfrak{R}$ ve $i=0,1,\ldots,m-1$ iken $v_i=a_i+ub_i$ olacak şekilde $v=(v_0,v_1,\ldots,v_{m-1})\in\mathfrak{I}$ mevcut olsun. C_3 kodu Θ_i-devirli kod olduğundan $\left(u^2p_0+(1+3u^2)v_0,\ u^2p_1+(1+3u^2)v_1,\ \ldots,\ u^2p_{m-1}+(1+3u^2)v_{m-1}\right)\in C_3$ iken $\left(\Theta_i\left(u^2p_{m-1}+(1+3u^2)v_{m-1}\right),\Theta_i\left(u^2p_0+(1+3u^2)v_0\right),\ldots,\Theta_i\left(u^2p_{m-2}+(1+3u^2)v_{m-2}\right)\right)\in C_3$ elde edilir. Bu ifade düzenlendiği takdirde $u^2\left(\Theta_i(p_{m-1}),\Theta_i(p_0),\ldots,\Theta_i(p_{m-2})\right)\oplus(1+3u^2)\left(\Theta_i(v_{m-1}),\Theta_i(v_0),\ldots,\Theta_i(v_{m-2})\right)\in C_3$ bulunur. Buradan da $u^2\sigma_{\Theta_i}p+(1+3u^2)\ \sigma_{\Theta_i}v\in C_3$ ifadesine ulaşılır. $\sigma_{\Theta_i}\left(u^2p\oplus(1+3u^2)v\right)=u^2\sigma_{\Theta_i}p+(1+3u^2)\sigma_{\Theta_i}v$ olduğundan $\mathfrak{R}$ ve $\mathfrak{I}$ kodları Θ_i-devirli kodlardır.

Tersine $\mathfrak{R}$ ve $\mathfrak{I}$ kodları Θ_i-devirli kodlar olsun. Bu durumda devirli kod tanımı gereği $p\in\mathfrak{R}$ iken $\sigma_{\Theta_i}p\in\mathfrak{R}$ ve $v\in\mathfrak{I}$ iken $\sigma_{\Theta_i}v\in\mathfrak{I}$ elde edilir. Burada $u^2\sigma_{\Theta_i}p+(1+3u^2)\sigma_{\Theta_i}v$ ifadesi $\sigma_{\Theta_i}(z_0,z_1,\ldots,z_{m-1})$ ifadesine eşit olduğundan $u^2\sigma_{\Theta_i}p+(1+3u^2)\sigma_{\Theta_i}v\in u^2\mathfrak{R}+(1+3u^2)\mathfrak{I}$ yani $u^2\sigma_{\Theta_i}p+(1+3u^2)\sigma_{\Theta_i}v\in C_3$ sonucuna ulaşılır. Böylelikle C_3 kodunun Θ_i-devirli kod olduğu ispatlanmış olur. □

Teorem 3.2.4. $C_3=u^2\mathfrak{R}\oplus(1+3u^2)\mathfrak{I}$ kodu $u^3=u^2$ iken T_3 üzerinde uzunluğu m olan bir Θ_i-devirli kod olsun. Bu durumda $\mathfrak{R}$ kodu $\mathbb{Z}_4$ üzerinde ve $\mathfrak{I}$ kodu ise $\mathbb{Z}_4+u\mathbb{Z}_4$

üzerinde devirli birer kod olmak üzere $i=1,2,3$ için $x^m-1=f_i(x).h_i(x).w_i(x)$ olacak şekilde C_3 kodunun üreteç polinomu,

$$C_3=\left(u^2\left\langle f_1(x)\left(h_1(x)+2\right)\right\rangle\right)\oplus\left(\left(1+3u^2\right)\left\langle f_2(x)\left(h_2(x)+2\right)+uf_{1,2}(x)\left(h_{1,2}(x)+2\right),\right.$$
$$\left.uf_3(x)\left(h_3(x)+2\right)\right\rangle\Big)$$

şeklindedir.

İspat. $\widehat{C}_3=\left(u^2\left\langle f_1(x)\left(h_1(x)+2\right)\right\rangle\right)\oplus\left(\left(1+3u^2\right)\left\langle f_2(x)\left(h_2(x)+2\right)+uf_{1,2}(x)\left(h_{1,2}(x)+2\right),uf_3(x)\left(h_3(x)+2\right)\right\rangle\right)$ olsun. $\widehat{C}_3\subseteq C_3$ ve $C_3\subseteq\widehat{C}_3$ ifadeleri gösterildiğinde istenilen elde edilmiş olacaktır. $\mathfrak{R}=\left\langle f_1(x)\left(h_1(x)+2\right)\right\rangle$ ve $\mathfrak{I}=\left\langle f_2(x)\left(h_2(x)+2\right)+uf_{1,2}(x)\left(h_{1,2}(x)+2\right),uf_3(x)\left(h_3(x)+2\right)\right\rangle$ olduğundan $\widehat{C}_3\subseteq C_3$ olduğu açıktır. Diğer yandan $u^3=u^2$ iken $u^2\mathfrak{R}=u^2\widehat{C}_3$ ve $\left(1+3u^2\right)\mathfrak{I}=\left(1+3u^2\right)\widehat{C}_3$ eşitlikleri sağlandığından $u^2\mathfrak{R}\oplus(1+3u^2)\mathfrak{I}\subseteq\widehat{C}_3$ ifadesi elde edilir. Böylece $C_3=\widehat{C}_3$ bulunur. □

Teorem 3.2.5. $C_3=u^2\mathfrak{R}\oplus(1+3u^2)\mathfrak{I}$ kodu T_3 halkası üzerinde m uzunluğunda Θ_i – devirli kod olsun. $\tau_1(x)$ polinomu $\mathfrak{R}$ kodunun, $\langle\tau_2(x),\tau_3(x)\rangle$ ise $\mathfrak{I}$ kodunun üreteç polinomları olmak üzere C_3 kodunun üreteç polinomu $C_3=\left\langle u^2\tau_1(x),\left(1+3u^2\right)\left\langle\tau_2(x),\tau_3(x)\right\rangle\right\rangle$ şeklindedir. Bu üreteç polinomu düzenlenirse $C_3=\left\langle u^2\tau_1(x),\left(1+3u^2\right)\tau_2(x),\left(1+3u^2\right)\tau_3(x)\right\rangle$ elde edilir.

İspat. $\mathbb{Z}_4$ üzerindeki aykırı devirli kodun üreteç polinomu $\mathfrak{R}=\left\langle f_1(x)\left(h_1(x)+2\right)\right\rangle$, $u^2=0$ iken $\mathbb{Z}_4+u\mathbb{Z}_4$ üzerindeki aykırı devirli kodun üreteç polinomu $\mathfrak{I}=\left\langle f_2(x)\left(h_2(x)+2\right)+uf_{1,2}(x)\left(h_{1,2}(x)+2\right),uf_3(x)\left(h_3(x)+2\right)\right\rangle$ ve $C_3=u^2\mathfrak{R}\oplus\left(1+3u^2\right)\mathfrak{I}$ olduğundan,

$$C_3 = \left\{ z(x) = u^2 r_1(x)\tau_1(x) + \left(1+3u^2\right) r_2(x)\left\langle \tau_2(x), \tau_3(x)\right\rangle : r_1(x), r_2(x) \in T_3\left[x, \Theta_i\right] \right\}$$

elde edilir. Buradan $C_3 \subseteq \left\langle u^2\tau_1(x) + \left(1+3u^2\right)\left\langle \tau_2(x), \tau_3(x)\right\rangle \right\rangle \subseteq T_{3,m_{\Theta_i}}$ olduğu açıktır. Tersine, $y_1(x), y_2(x) \in T_{3,m_{\Theta_i}}$ iken $u^2 y_1(x)\tau_1(x) + \left(1+3u^2\right) y_2(x)\left\langle \tau_2(x), \tau_3(x)\right\rangle$ ifadesi $\left\langle u^2\tau_1(x), \left(1+3u^2\right)\left\langle \tau_2(x), \tau_3(x)\right\rangle \right\rangle$ idealinin bir elemanıdır. Bu sebeple $T_3\left[x, \Theta_i\right]$ halkasından alınan $b_1(x)$ ve $b_2(x)$ polinomları için $u^2 y_1(x) = u^2 b_1(x)$ ve $\left(1+3u^2\right) y_2(x) = \left(1+3u^2\right) b_2(x)$ eşitlikleri sağlanır. Böylece $\left\langle u^2\tau_1(x), \left(1+3u^2\right)\left\langle \tau_2(x), \tau_3(x)\right\rangle \right\rangle$ ideali C_3 kodunun bir alt kümesi olur. Buradan hareketle $C_3 = \left\langle u^2\tau_1(x), \left(1+3u^2\right)\left\langle \tau_2(x), \tau_3(x)\right\rangle \right\rangle$ eşitliği elde edilir. □

Teorem 3.2.6. $\mathfrak{R}$ kodu $\mathbb{Z}_4$ halkası, $\mathfrak{I}$ kodu ise $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerinde Θ_i – devirli kodlar; $\tau_1(x)$ ve $\left\langle \tau_2(x), \tau_3(x)\right\rangle$ polinomları da sırasıyla bu kodların üreteç polinomları olsun. Ayrıca C_3 kodu da $C_3 = u^2\mathfrak{R} \oplus (1+3u^2)\mathfrak{I}$ şeklinde yazılsın. Bu durumda $T_3\left[x, \Theta_i\right]$ halkasında $\tau(x) = u^2\tau_1(x) + \left(1+3u^2\right)\left(\tau_2(x) + \tau_3(x)\right)$ olacak şekilde C_3 kodu üreten bir $\tau(x)$ polinomu vardır ve bu $\tau(x)$ polinomu $x^m - 1$ polinomunun bir sağ bölenidir.

İspat. Önceki teoremden hareketle $C_3 = \left\langle u^2\tau_1(x), \left(1+3u^2\right)\left\langle \tau_2(x), \tau_3(x)\right\rangle \right\rangle$ eşitliği ele alınsın ve $\tau(x) = u^2\tau_1(x) + \left(1+3u^2\right)\left(\tau_2(x) + \tau_3(x)\right)$ olsun. Bu durumda $\left\langle \tau(x)\right\rangle \subseteq C_3$ olduğu aşikârdır.

Diğer taraftan $u^2\tau_1(x) = u^2\tau(x)$ ve $\left(1+3u^2\right)\left(\tau_2(x) + \tau_3(x)\right) = \left(1+3u^2\right)\tau(x)$ eşitlikleri sağlandığından $C_3 \subseteq \left\langle \tau(x)\right\rangle$ elde edilir. Böylece $C_3 = \left\langle \tau(x)\right\rangle$ eşitliği elde edilir. $\tau_1(x)$ ve $\left(\tau_2(x) + \tau_3(x)\right)$ polinomları sırasıyla $\mathbb{Z}_4\left[x, \Theta_i\right]$ ve $\left(\mathbb{Z}_4 + u\mathbb{Z}_4\right)\left[x, \Theta_i\right]$ halkalarında $x^m - 1$ polinomunun monik bölenleri olduğundan $b_1(x), b_2(x) \in T_{3,m_{\Theta_i}}$

olmak üzere $x^m-1=b_1(x)\tau_1(x)=b_2(x)\left(\tau_2(x)+\tau_3(x)\right)$ şeklinde yazılabilir. Buradan, $\left(u^2b_1(x)+\left(1+3u^2\right)b_2(x)\right)\tau(x)=\left(u^2b_1(x)+\left(1+3u^2\right)b_2(x)\right)\left(u^2\tau_1(x)+\left(1+3u^2\right)\left(\tau_2(x)+\tau_3(x)\right)\right)=u^2b_1(x)\tau_1(x)+\left(1+3u^2\right)b_2(x)\left(\tau_2(x)+\tau_3(x)\right)=u^2\left(x^m-1\right)+\left(1+3u^2\right)\left(x^m-1\right)=x^m-1$ eşitlikleri elde edilir. Böylece $\tau(x)$ polinomu x^m-1 polinomunun bir sağ böleni olur. □

$i=1,2,3$ iken, aykırı devirli öteleme operatörü σ_{Θ_i}, $2-$parçalı devirli kod operatörü υ_2 ve T_3^m halkasından $\mathbb{Z}_4^{2m}$ halkasına tanımlanan Gray dönüşümlerin de ϕ_i olduğu hatırlatılarak aşağıdaki önermeler ve teoremler verilebilir.

Önerme 3.2.1. Herhangi bir $z\in T_3\left[x,\Theta_i\right]^m$ ve $i,j=1,2,3$ için $\phi_j\sigma_{\Theta_i}(z)=\upsilon_2\phi_j(z)$ eşitliği elde edilir.

İspat. $i=1,2,3$ iken $T_3\left[x,\Theta_i\right]^m$ üzerinde $z=\left(z_0,z_1,\ldots,z_{m-1}\right)$ kodu ele alınsın. Burada $a_t\in\mathbb{Z}_4$ ve $j=0,1,\ldots,m-1$ olacak şekilde $z_j=a_0^j+ua_1^j+u^2a_2^j$ ile ifade edilecektir. Bu durumda,

$$\phi_1(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+3a_1^0+a_2^0,\ldots,3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right),$$
$$\phi_2(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},a_0^0+3a_1^0+a_2^0,\ldots,a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right) \text{ ve}$$
$$\phi_3(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+a_1^0+3a_2^0,\ldots,3a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}\right)$$

olduğundan,

$$\upsilon_2\phi_1(z)=\begin{pmatrix}a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},\ a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\\ 3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1},3a_0^0+3a_1^0+a_2^0,\ldots,3a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}\end{pmatrix},$$

$$\upsilon_2\phi_2(z)=\begin{pmatrix}a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},\ a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\\ a_0^{m-1}+3a_1^{m-1}+a_2^{m-1},a_0^0+3a_1^0+a_2^0,\ldots,a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}\end{pmatrix} \text{ ve}$$

$\upsilon_2 \phi_3(z) = \begin{pmatrix} a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1},\ a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ 3a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, 3a_0^0 + a_1^0 + 3a_2^0, \ldots, 3a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2} \end{pmatrix}$ elde edilir.

Diğer taraftan, $\sigma_{\Theta_i}(z) = \left(\Theta_i(z_{m-1}), \Theta_i(z_0), \Theta_i(z_1), \ldots, \Theta_i(z_{m-2})\right)$ bilgisi kullanılarak,

$\sigma_{\Theta_1}(z) = \left(a_0^{m-1} + 2a_1^{m-1} + u3a_1^{m-1} + u^2 a_2^{m-1},\ a_0^0 + ua_1^0 + u^2 a_2^0, \ldots, , a_0^{m-2} + ua_1^{m-2} + u^2 a_2^{m-2}\right)$,

$\sigma_{\Theta_2}(z) = \left(a_0^{m-1} + 2a_1^{m-1} + ua_1^{m-1} + u^2\left(2a_1^{m-1} + a_2^{m-1}\right), a_0^0 + ua_1^0 + u^2 a_2^0, \ldots, a_0^{m-2} + ua_1^{m-2} + u^2 a_2^{m-2}\right)$ ve

$\sigma_{\Theta_3}(z) = \left(a_0^{m-1} + u3a_1^{m-1} + u^2\left(2a_1^{m-1} + a_2^{m-1}\right), a_0^0 + ua_1^0 + u^2 a_2^0, \ldots, a_0^{m-2} + ua_1^{m-2} + u^2 a_2^{m-2}\right)$

ifadelerine ulaşılır. Buradan hareketle

$\phi_1 \sigma_{\Theta_i}(z) = \begin{pmatrix} a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1}, 3a_0^0 + 3a_1^0 + a_2^0, \ldots, 3a_0^{m-2} + 3a_1^{m-2} + a_2^{m-2}, \end{pmatrix}$,

$\phi_2 \sigma_{\Theta_i}(z) = \begin{pmatrix} a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1}, a_0^0 + 3a_1^0 + a_2^0, \ldots, a_0^{m-2} + 3a_1^{m-2} + a_2^{m-2}, \end{pmatrix}$,

$\phi_3 \sigma_{\Theta_i}(z) = \begin{pmatrix} a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ 3a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, 3a_0^0 + a_1^0 + 3a_2^0, \ldots, 3a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \end{pmatrix}$ elde edilir.

Böylece $i, j = 1,2,3$ için $\phi_j \sigma_{\Theta_i}(z) = \upsilon_2 \phi_j(z)$ eşitliği sağlanır. □

Bu önerme sonucunda aşağıdaki teorem elde edilir.

Teorem 3.2.7. C_3 kodu T_3 halkası üzerinde uzunluğu m olan aykırı devirli bir kod olsun. Bu durumda T_3 halkası üzerindeki aykırı devirli bir kodun tüm Gray dönüşümleri altındaki görüntüleri $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda $2-$parçalı devirli koddur.

İspat. $i=1,2,3$ için C_3 kodu T_3 halkası üzerinde m uzunluğunda aykırı devirli kod olsun. Bu durumda $\sigma_{\Theta_i}(C_3)=C_3$ şeklinde ifade edilir. Her iki tarafın istenilen Gray dönüşüm altındaki görüntüsü alındığında elde edilen eşitlikte Önerme 3.2.1. te kullanılarak $\phi_j\sigma_{\Theta_i}(C_3)=\upsilon_2\phi_j(C_3)=\phi_j(C_3)$ elde edilir. Böylece parçalı devirli kodun tanımı gereği $\phi_j(C_3)$ Gray görüntüleri $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda $2-$ parçalı devirli kod olur. □

3.3 T_3 Halkasındaki Aykırı $\lambda-$Sabit Devirli Kodlar

Bu bölümde aykırı devirli kodların cebirsel yapısından yararlanarak aykırı sabit devirli kodlar elde edilecektir. Gerekli tanım ve teoremler verildikten sonra izomorfizma yardımıyla üreteç polinomu elde edilecek ve halkanın tüm birimsel elemanları için $\mathbb{Z}_4$ görüntüleri incelenecektir.

Bu bölüm boyunca $T_3[x,\Theta_i]\Big/_{<x^m-\lambda>}$ bölüm halkası $T_{3,m_{\Theta_i,\lambda}}$ ile temsil edilecek, aykırı $\lambda-$sabit devirli kodlar da $(\Theta_i,\lambda)-$sabit devirli kodlar şeklinde isimlendirilecektir. Diğer bir ifade ile $\rho_{\Theta_i,\lambda}(C_3)=C_3$ ise T_3^m halkasının bir T_3-alt modülü $(\Theta_i,\lambda)-$sabit devirli kod olarak adlandırılacaktır. $\lambda=1$ olması durumunda $(\Theta_i,\lambda)-$sabit devirli kodun Θ_i-devirli kod olacağı unutulmamalıdır.

Teorem 3.3.1. $T_{3,m_{\Theta_i,\lambda}}$ bölüm halkası,

$$\alpha(x)\left(\lambda z_{m-1}(x),z_0(x),\ldots,z_{m-2}(x)\right)=\left(\alpha(x)\lambda z_{m-1}(x),\alpha(x)z_0(x),\ldots,\alpha(x)z_{m-2}(x)\right)$$

ile tanımlanan çarpma işlemi altında bir $T_{3,m_{\Theta_i,\lambda}}$ – modüldür.

İspat. Teorem 3.2.1.'in ispatına benzer şekilde yapılır.

Teorem 3.3.2. $T_{3,m_{\Theta_i,\lambda}}$ halkası üzerinde uzunluğu m olan C_3 kodunun $(\Theta_i,\lambda)-$ sabit devirli kod olması için gerek ve yeter koşul C_3 kodunun bir $T_{3,m_{\Theta_i,\lambda}}$ – sol modülünün $T_3[x,\Theta_i]-$ sol alt modülüdür.

İspat. C_3 kodunun $(\Theta_i,\lambda)-$ sabit devirli kod ve $z(x)\in C_3$ olduğu kabul edilsin. C_3 kodu $T_{3,m_{\Theta_i,\lambda}}$ bölüm halkasının bir alt grubu olduğundan $z_1(x), z_2(x)\in C_3$ polinomları için $z_1(x)-z_2(x)\in C_3$ olduğu söylenir. C_3 kodu $(\Theta_i,\lambda)-$ sabit devirli kod olduğundan $\lambda x\, z(x)$ polinomu da C_3 kodunun bir elemanı olur. Aynı şekilde $\lambda x(\lambda x\, z(x))$ polinomu da C_3 kodunun bir elemanı olduğu elde edilir. Benzer şekilde devam edilmesi durumunda 0 ve 0'dan büyük her i değeri için $\lambda^i x^i\, z(x)\in C_3$ elde edilir. C_3 kodu lineer olduğundan $T_3[x,\Theta_i]$ halkasından alınan her $r(x)$ polinomu için $r(x)z(x)$ polinomu da C_3 kodunun bir elemanı olur. Dolayısıyla C_3 kodu $T_{3,m_{\Theta_i,\lambda}}$ bölüm halkasının bir $T_3[x,\Theta_i]-$ sol alt modülü olur. Diğer taraftan, C_3 kodunun $T_{3,m_{\Theta_i,\lambda}}$ bölüm halkasının bir $T_3[x,\Theta_i]-$ sol alt modülü olduğu kabul edilsin. Alt modül şartından C_3 kodunun $T_{3,m_{\Theta_i,\lambda}}$ bölüm halkasının bir alt grubu, $z(x)$ polinomu C_3 kodunun bir elemanı ve $T_3[x,\Theta_i]-$ halkasından alınan her x elemanı için $\lambda x\, z(x)\in C_3$ olacağından C_3 kodu bir $(\Theta_i,\lambda)-$ sabit devirli kod olur. □

Halkadaki birimsel elemanlar tek kuvveti kendisi çift kuvveti ise 1'e eşit olanlar ve karesi $1+2u+2u^2$ dolayısıyla da dördüncü kuvveti 1'e eşit olanlar şeklinde ikiye ayrılmaktadır. Bu bilgi ışığında aşağıdaki önerme ve sonuçlar ortaya çıkmaktadır.

Önerme 3.3.1. $T_{3,m_{\Theta_i}}$ halkasından $T_{3,m_{\Theta_i,\lambda}}$ halkasına

I. Karesi 1 olan birimsel elemanlar için, $\xi\left(z\left(x\right)\right)=z\left(\lambda x\right)$ olacak şekilde bir ξ dönüşümü tanımlansın. Her bir Θ_i otomorfizması ve T_3 halkasındaki tüm birimsel elemanlar için m uzunluğu tek uzunluk olmak kaydıyla bu dönüşüm bir halka izomorfizması olur.

II. Karesi $1+2u+2u^2$ olan birimsel elemanlar için $\xi\left(z\left(x\right)\right)=z\left(\lambda^2 x\right)$ olacak şekilde bir ξ dönüşümü tanımlansın.

   i. Θ_3 otomorfizmalarının kullanılması halinde T_3 halkasındaki tüm birimsel elemanlar için m uzunluğu tek uzunluk,

   ii. Θ_1 ve Θ_2 otomorfizmalarının kullanılması durumunda ise m uzunluğu $k\in\mathbb{Z}$ olmak üzere $m=4k+1$ uzunluğunda

olmak kaydıyla bu dönüşüm bir halka izomorfizması olur.

İspat. ξ dönüşümünün bir halka izomorfizması olduğunu göstermek için iyi tanımlılık, birebir, örten ve halka homomorfizması olduğunu göstermek gerekir.

<u>İyi tanımlılık</u>:

i. Karesi 1 olan birimsel elemanlar için;

$\forall\ b(x),\ c(x)\in T_{3,m_{\Theta_i}}$ için $b(x)=c(x)\ \left(\text{mod } x^m-1\right)$ iken $\xi\left(b(x)\right)=\ \xi\left(c(x)\right)$ $\left(\text{mod } x^m-\lambda\right)$ olmalıdır.

$b(x)=c(x)\ \left(\text{mod } x^m-1\right)$ ise $b(x)=\left(x^m-1\right)q(x)+c(x)$ şeklinde ifade edilir. $x\mapsto\lambda x$ yazılırsa, $b(\lambda x)=\left(\left(\lambda x\right)^m-1\right)q(\lambda x)+c(\lambda x)$ ifadesi elde edilir. Burada 1 yerine λ^2 yazıldığı takdirde $\left(\lambda x^m-\lambda^2\right)q(\lambda x)+c(\lambda x)=\lambda\left(x^m-\lambda\right)q(\lambda x)+c(\lambda x)$ elde edilir. Bu da $\xi\left(b(x)\right)=\xi\left(c(x)\right)\ \left(\text{mod } x^m-\lambda\right)$ demektir. Yani, ξ dönüşümü iyi tanımlıdır.

ii. Karesi $1+2u+2u^2$ olan birimsel elemanlar için;

$\forall\ b(x), c(x) \in T_{3,m_{\Theta_i}}$ için $b(x)=c(x) \pmod{x^m-1}$ iken $\xi(b(x))=\xi(c(x)) \pmod{x^m-\lambda^2}$ olmalıdır.

$b(x)=c(x) \pmod{x^m-1}$ ise $b(x)=(x^m-1)q(x)+c(x)$ şeklinde ifade edilir. $x \mapsto \lambda^2 x$ yazılırsa, $b(\lambda^2 x)=\left((\lambda^2 x)^m-1\right)q(\lambda^2 x)+c(\lambda^2 x)$ ifadesi elde edilir. Burada 1 yerine λ^4 yazıldığı takdirde $(\lambda^2 x^m-\lambda^4)q(\lambda^2 x)+c(\lambda^2 x)=\lambda^2(x^m-\lambda^2)q(\lambda^2 x)+c(\lambda^2 x)$ elde edilir. Bu da $\xi(b(x))=\xi(c(x)) \pmod{x^m-\lambda^2}$ demektir. Yani, ξ dönüşümü iyi tanımlıdır.

<u>Birebirlik</u>:

i. Karesi 1 olan birimsel elemanlar için;

$\forall\ b(x), c(x) \in T_{3,m_{\Theta_i}}$ için $\xi(b(x))=\xi(c(x)) \pmod{x^m-\lambda}$ olması durumunda $b(x)=c(x) \pmod{x^m-1}$ olmalıdır.

$\xi(b(x))=\xi(c(x)) \pmod{x^m-\lambda}$ yani $b(\lambda x)=c(\lambda x) \pmod{x^m-\lambda}$ olarak yazılır. Bu ifade $b(\lambda x)=(x^m-\lambda)q(\lambda x)+c(\lambda x)$ anlamına gelir. Buradan hareketle, $x \mapsto \lambda x$ yazılırsa $b(x)=\lambda(x^m-1)q(x)+c(x)$ ifadesi elde edilir. Bu da $b(x)=c(x) \pmod{x^m-1}$ olması anlamına gelir. Böylece ξ dönüşümünün birebir bir dönüşüm olduğu söylenir.

ii. Karesi $1+2u+2u^2$ olan birimsel elemanlar için;

$\forall\ b(x), c(x) \in T_{3,m_{\Theta_i}}$ için $\xi(b(x))=\xi(c(x)) \pmod{x^m-\lambda^2}$ olması durumunda $b(x)=c(x) \pmod{x^m-1}$ olmalıdır.

$\xi(b(x))=\xi(c(x))\ \ (\text{mod } x^m-\lambda^2)$ yani $b(\lambda^2 x)=c(\lambda^2 x)\ (\text{mod } x^m-\lambda^2)$ olarak yazılır. Bu ifade $b(\lambda^2 x)=(x^m-\lambda^2)q(\lambda^2 x)+c(\lambda^2 x)$ anlamına gelir. Buradan hareketle, $x\mapsto\lambda^2 x$ yazılırsa $b(x)=\lambda^2(x^m-1)q(x)+c(x)$ ifadesi elde edilir. Bu da $b(x)=c(x)\ (\text{mod } x^m-1)$ olması anlamına gelir. Böylece ξ dönüşümünün birebir bir dönüşüm olduğu söylenir.

Örtenlik: Tanımlanan ξ dönüşümleri sonlu ve birebir bir dönüşüm olduğundan örtendir.

Homomorfizma: $\forall\ b(x),\ c(x)\in T_{3,m_{\Theta_i}}$ için $\xi(b(x)+c(x))=\xi(b(x))+\xi(c(x))$ ve $\xi(b(x)c(x))=\xi(b(x))\ \xi(c(x))$ olmalıdır. Gerekli düzenlemeler yapıldığında,

i. Karesi 1 olan birimsel elemanlar için;

$$\xi(b(x)+c(x))=\xi((b+c)(x))=(b+c)(\lambda x)=b(\lambda x)+c(\lambda x)=\xi(b(x))+\xi(c(x))$$

$$\xi(b(x)c(x))=\xi((bc)(x))=(bc)(\lambda x)=b(\lambda x)\ c(\lambda x)=\xi(b(x))\ \xi(c(x))\ \text{ ve}$$

ii. Karesi $1+2u+2u^2$ olan birimsel elemanlar için;

$$\xi(b(x)+c(x))=\xi((b+c)(x))=(b+c)(\lambda^2 x)=b(\lambda^2 x)+c(\lambda^2 x)=\xi(b(x))+\xi(c(x))$$

$$\xi(b(x)c(x))=\xi((bc)(x))=(bc)(\lambda^2 x)=b(\lambda^2 x)\ c(\lambda^2 x)=\xi(b(x))\ \xi(c(x))$$

eşitlikleri elde edilir. Böylelikle ξ dönüşümleri bir halka homomorfizmasıdır.

Bu ispat incelenirken kullanılan otomorfizmalar için farklı uzunlukların mevcut olduğu dikkate alınmalıdır. Aksi takdirde izomorfizma sağlanmayacaktır. Yukarıda da gösterildiği gibi tanımlanan ξ dönüşümleri iyi tanımlı, birebir, örten ve halka homomorfizması olduğu için bir halka izomorfizmasıdır. □

Bu önermenin sonucunda aşağıdaki sonuç edilir.

Sonuç 3.3.1. Yukarıdaki önermeden yararlanarak $T_{3,m_{\Theta_i}}$ halkasının idealleri ile $T_{3,m_{\Theta_i,\lambda}}$ halkasının idealleri arasında birebir bir ilişki vardır.

Önerme 3.3.2. C_3 kodu T_3 halkası üzerinde m uzunluğunda lineer bir kod ve $\bar{\xi}\left(z_0,\, z_1,\ldots,z_{m-1}\right)=\left(z_0,\, \lambda z_1,\, \lambda^2 z_2,\, \ldots,\, \lambda^{m-1} z_{m-1}\right)$ olsun. Bu durumda C_3 kodunun devirli bir kod olması için gerek ve yeter koşul C_3 kodunun $\bar{\xi}$ dönüşümü altındaki görüntüsünün T_3 halkası üzerinde m uzunluğunda $\lambda-$sabit devirli kod olmasıdır.

İspat. C_3 kodunun devirli bir kod olduğu kabul edilsin. Bu durumda $\left(z_0,\, z_1,\ldots,z_{m-1}\right)\in C_3$ iken $\left(z_{m-1}, z_0,\, z_1,\ldots,z_{m-2}\right)$ de C_3 kodunun bir elemanıdır. $\left(z_0,\, z_1,\ldots,z_{m-1}\right)$ kodunun $\bar{\xi}$ dönüşümü altındaki görüntüsü alınırsa $\left(z_0,\lambda z_1, z_2,\ldots,z_{m-1}\right)\in\bar{\xi}\left(C_3\right)$ elde edilir. $\rho_{\Theta_i,\lambda}$ ifadesi aykırı $\lambda-$sabit devirli öteleme operatörü olmak üzere, C_3 kodunun $\bar{\xi}$ dönüşümü altındaki görüntüsünün $\lambda-$sabit devirli bir kod olması için $\left(\lambda z_{m-1}, z_0,\, \lambda z_1, z_2,\ldots,z_{m-2}\right)=\rho_{\Theta_i,\lambda}\left(\bar{\xi}\left(C_3\right)\right)$ olması gerekir. Bu da $\lambda\left(z_{m-1},\lambda z_0,\, z_1,\ldots,z_{m-2}\right)$ anlamına gelir. $\lambda\,\rho_{\Theta_i,\lambda}\left(\bar{\xi}\left(C_3\right)\right)=\left(z_{m-1},\lambda z_0, z_1,\ldots,\right.$ $\left.z_{m-2}\right)\in\xi\left(C_3\right)$ olup $\xi\left(C_3\right)$ te bir ideal olduğundan $\rho_{\Theta_i,\lambda}\left(\bar{\xi}\left(C_3\right)\right)\in\bar{\xi}\left(C_3\right)$ elde edilir. Böylece C_3 kodunun $\bar{\xi}$ dönüşümü altındaki görüntüsünün $\lambda-$sabit devirli kod olduğu ispatlanmış olur. □

$$\tilde{x}=\begin{cases}\text{Karesi 1 olan birimsel elemanlar için,} & \lambda x\\ \text{Karesi } 1+2u+2u^2 \text{ olan birimsel elemanlar için,} & \lambda^2 x\end{cases}$$

olacak şekilde, Teorem 3.2.4. ve ξ halka izomorfizması kullanılarak T_3 halkası üzerinde uzunluğu m olan $\left(\Theta_i,\lambda\right)-$sabit devirli kodların üreteç polinomu aşağıdaki gibi ifade edilir.

Teorem 3.3.3. $C_3 = u^2\Re \oplus (1+3u^2)\Im$ kodu T_3 üzerinde uzunluğu m olan $(\Theta_i, \lambda)-$ sabit devirli bir kod olsun. Bu durumda;

i. $i = 1,2,3$ için $x^m - 1 = f_i(x).h_i(x).w_i(x)$ olmak üzere C_3 kodunun üreteç polinomu,

$$C_3 = \left(u^2 \left\langle f_1(\tilde{x})\left(h_1(\tilde{x})+2\right)\right\rangle\right) \oplus \left(\left(1+3u^2\right)\left\langle f_2(\tilde{x})\left(h_2(\tilde{x})+2\right) + uf_{1,2}(\tilde{x})\left(h_{1,2}(\tilde{x})+2\right),\right.$$
$$\left. uf_3(\tilde{x})\left(h_3(\tilde{x})+2\right)\right\rangle\right)$$

şeklinde ifade edilir.

ii. Diğer bir ifade ile, en klasik yöntem olan ve hesaplamalarda sıklıkla kullanılan formuyla C_3 kodunun üreteç polinomu, $i = 1,2,3$ için $x^m - \lambda = f_i(x).h_i(x).w_i(x)$ olacak şekilde,

$$C_3 = \left(u^2 \left\langle f_1(x)\left(h_1(x)+2\right)\right\rangle\right) \oplus \left(\left(1+3u^2\right)\left\langle f_2(x)\left(h_2(x)+2\right) + uf_{1,2}(x)\left(h_{1,2}(x)+2\right),\right.$$
$$\left. uf_3(x)\left(h_3(x)+2\right)\right\rangle\right)$$

şeklindedir.

Teorem 3.3.4. $C_3 = u^2\Re \oplus (1+3u^2)\Im$ kodu T_3 halkası üzerinde m uzunluğunda $\Theta_i -$ devirli kod olsun. $\tau_1(\tilde{x})$ polinomu $\Re$ kodunun, $\langle \tau_2(\tilde{x}), \tau_3(\tilde{x})\rangle$ ise $\Im$ kodunun üreteç polinomları olmak üzere C_3 kodunun üreteç polinomu $C_3 = \left\langle u^2\tau_1(\tilde{x}), \left(1+3u^2\right)\langle \tau_2(\tilde{x}), \tau_3(\tilde{x})\rangle\right\rangle$ şeklindedir. Bu üreteç polinomu düzenlenirse $C_3 = \left\langle u^2\tau_1(\tilde{x}), \left(1+3u^2\right)\tau_2(\tilde{x}), \left(1+3u^2\right)\tau_3(\tilde{x})\right\rangle$ elde edilir.

Teorem 3.3.5. $\Re$ kodu $\mathbb{Z}_4$ halkası, $\Im$ kodu ise $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerinde $\Theta_i -$ devirli kodlar; $\tau_1(\tilde{x})$ ve $\langle \tau_2(\tilde{x}), \tau_3(\tilde{x})\rangle$ polinomları da sırasıyla bu kodların üreteç polinomları olsun. Ayrıca C_3 kodu da $C_3 = u^2\Re \oplus (1+3u^2)\Im$ şeklinde yazılsın. Bu durumda $T_3[x, \Theta_i]$ halkasında $\tau(\tilde{x}) = u^2\tau_1(\tilde{x}) + (1+3u^2)\left(\tau_2(\tilde{x}) + \tau_3(\tilde{x})\right)$ olacak

şekilde C_3 kodu üreten bir $\tau(\tilde{x})$ polinomu vardır ve bu $\tau(\tilde{x})$ polinomu $x^m-\lambda$ polinomunun bir sağ bölenidir.

Not 3.3.1. Teorem 3.3.3., Teorem 3.3.4. ve Teorem 3.3.5.'in ispatları, sırasıyla, Teorem 3.2.4., Teorem 3.2.5. ve Teorem 3.2.6.'nın ispatlarına benzer şekilde yapılır.

Bölüm 3.1.'de tanımlanan ϕ_i Gray dönüşümleri yardımıyla T_3 halkası üzerindeki $(\Theta_i,\lambda)-$ sabit devirli kodların $\mathbb{Z}_4$ görüntüleri incelensin.

$i=1,2,3$ olmak üzere; ρ_{Θ_i} aykırı $\lambda-$sabit devirli öteleme operatörü, υ_2 $2-$parçalı devirli kod operatörü ve T_3^m halkasından $\mathbb{Z}_4^{2m}$ halkasında tanımlanan Gray dönüşümlerin de ϕ_i olduğu hatırlatılsın. Aşağıda verilen teoremler ve önermeler, önemli gözlemlerin sonuçlarının birer yansımasıdır. Halkadaki tüm birimsel elemanların $\mathbb{Z}_4$ görüntüleri incelenecektir.

Önerme 3.3.3. $i=1,2,3$ iken herhangi bir $z\in T_3[x,\Theta_i]^m$ için, $\lambda=3,\,1+2u,\,1+2u^2,$ $3+2u+2u^2$ olmak üzere $\phi_1\rho_{\Theta_i,\lambda}(z)=\sigma\phi_1(z)$ eşitliği elde edilir.

İspat. $T_3[x,\Theta_1]^m$ üzerinde $z=(z_0,z_1,\ldots,z_{m-1})$ kodu ele alınsın. Burada $a_t\in\mathbb{Z}_4$ ve $j=0,1,\ldots,m-1$ olacak şekilde $z_j=a_0^j+ua_1^j+u^2a_2^j$ ile ifade edilecektir. Bu durumda,

$$\rho_{\Theta_i,3}(z)=\left(3\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,1+2u}(z)=\left((1+2u)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,1+2u^2}(z)=\left(\left(1+2u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,3+2u+2u^2}(z)=\left(\left(3+2u+2u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right)$$

bilgileri kullanılarak,

$$\rho_{\Theta_1,3}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+ua_1^{m-1}+u^2 3a_2^{m-1}, a_0^0+ua_1^0+u^2a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,1+2u}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}++u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,1+2u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u3a_1^{m-1}+u^2\left(2a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,3+2u+2u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+a_1^{m-1}\right)+u^2\left(2a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\right.$$
$$\left.\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,3}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u3a_1^{m-1}+u^2\left(2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+u\right.$$
$$\left.a_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,1+2u}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+a_1^{m-1}\right)+u^2 3a_2^{m-1},\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+u\right.$$
$$\left.a_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,1+2u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+ua_1^{m-1}+u^2\left(2a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+u\right.$$
$$\left.a_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,3+2u+2u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(2a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+\right.$$
$$\left.ua_1^0+u^2a_2^0,\ \ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,3}(z)=\left(3a_0^{m-1}+ua_1^{m-1}+u^2\left(2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,a_0^{m-2}+ua_1^{m-2}+u^2\right.$$
$$\left.a_2^{m-2}\right),$$

$\rho_{\Theta_3,1+2u}(z)=\left(a_0^{m-1}+u\left(2a_0^{m-1}+3a_1^{m-1}\right)+u^2 3a_2^{m-1},\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2 a_2^{m-2}\right)$,

$\rho_{\Theta_3,1+2u^2}(z)=\left(a_0^{m-1}+u3a_1^{m-1}+u^2\left(2a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right)$,

$\rho_{\Theta_3,3+2u+2u^2}(z)=\left(3a_0^{m-1}+u\left(2a_0^{m-1}+a_1^{m-1}\right)+u^2\left(2a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2 a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right)$ eşitlikleri elde edilir. Buradan hareketle,

$\phi_1(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+3a_1^0+a_2^0,\ldots,3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right)$

Gray dönüşümü de kullanılarak,

$\phi_1\rho_{\Theta_i,\lambda}(z_0,z_1,\ldots,z_{m-1})=\left(3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1},a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\right.$

$\left.a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},\ a_0^0+3a_1^0+a_2^0,\ \ldots,\ 3a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}\right)$ sonucuna ulaşılır.

Diğer taraftan, ϕ_1 Gray dönüşümü kullanılarak,

$\sigma\phi_1(z)=\left(3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1},\ a_0^0+a_1^0+3a_2^0,\ \ldots,\ a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\ a_0^{m-1}+a_1^{m-1}+3\right.$

$\left.a_2^{m-1},\ 3a_0^0+3a_1^0+a_2^0,\ \ldots,\ 3a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}\right)$ elde edilir.

Böylece $i=1,2,3$ için $\phi_1\rho_{\Theta_i,\lambda}(z)=\sigma\phi_1(z)$ eşitliği sağlanır. □

Bu önerme sonucunda aşağıdaki teorem elde edilir.

Teorem 3.3.6. C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i,\lambda)-$ devirli kod olsun. Bu durumda $\lambda=3,\ 1+2u,\ 1+2u^2,\ 3+2u+2u^2$ olmak üzere T_3 halkası

üzerindeki $(\Theta_i,\lambda)-$ sabit devirli bir kodun tanımlanan ϕ_1 Gray dönüşümü altındaki görüntüsü $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli bir koddur.

İspat. $i=1,2,3$ için C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i,\lambda)-$ devirli kod olsun. Bu durumda $\rho_{\Theta_i,\lambda}(C_3)=C_3$ şeklinde ifade edilir. Önerme 3.3.3. kullanılarak $\phi_1\rho_{\Theta_i,\lambda}(C_3)=\sigma\phi_1(C_3)=\phi_1(C_3)$ elde edilir. Bu da $(\Theta_i,\lambda)-$ sabit devirli devirli kodun $\phi_1(C_3)$ görüntüsünün, $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli kod olmasıdır. □

Önerme 3.3.4. $i=1,2,3$ iken herhangi bir $z\in T_3[x,\Theta_i]^m$ için, $\lambda=1+u+u^2,3+3u+u^2,\ 3+u+3u^2,\ 1+3u+3u^2$ olmak üzere $\phi_2\rho_{\Theta_i,\lambda}(z)=\sigma\phi_2(z)$ eşitliği elde edilir.

İspat. $T_3[x,\Theta_i]^m$ üzerinde $z=(z_0,z_1,\ldots,z_{m-1})$ kodu ele alınsın. Burada $a_t\in\mathbb{Z}_4$ ve $j=0,1,\ldots,m-1$ olacak şekilde $z_j=a_0^j+ua_1^j+u^2a_2^j$ ile ifade edilecektir. Bu durumda,

$$\rho_{\Theta_i,1+u+u^2}(z)=\left(\left(1+u+u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,3+3u+u^2}(z)=\left(\left(3+3u+u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,3+u+3u^2}(z)=\left(\left(3+u+3u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,1+3u+3u^2}(z)=\left(\left(1+3u+3u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right)$$

eşitlikleri kullanılarak,

$$\rho_{\Theta_1,1+u+u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+a_1^{m-1}\right)+u^2\left(a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,1+u+u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,1+u+u^2}(z)=\left(a_0^{m-1}+u\left(a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,3+3u+u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,3+3u+u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+a_1^{m-1}\right)+u^2\left(a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,3+3u+u^2}(z)=\left(3a_0^{m-1}+u\left(3a_0^{m-1}+a_1^{m-1}\right)+u^2\left(a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,3+u+3u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,3+u+3u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,3+u+3u^2}(z)=\left(3a_0^{m-1}+u\left(a_0^{m-1}+a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ \ldots,\ a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,1+3u+3u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\right.$$
$$\left.\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,1+3u+3u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+2a_1^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0\right.$$
$$\left.+u^2a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,1+3u+3u^2}(z)=\left(a_0^{m-1}+u\left(3a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+3a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right)$$ eşitlikleri elde edilir. Böylece,

$$\phi_2(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},a_0^0+3a_1^0+a_2^0,\ldots,a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right)$$

Gray dönüşümü de uygulanarak,

$$\phi_2\,\rho_{\Theta_i,\lambda}(z_0,z_1,\ldots,z_{m-1})=\begin{pmatrix}a_0^{m-1}+3a_1^{m-1}+a_2^{m-1},a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\\ a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},a_0^0+3a_1^0+a_2^0,\ldots,a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}\end{pmatrix}$$

sonucuna ulaşılır. Diğer taraftan,

$$\sigma\phi_2(z)=\begin{pmatrix}a_0^{m-1}+3a_1^{m-1}+a_2^{m-1},a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\\ a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},a_0^0+3a_1^0+a_2^0,\ldots,a_0^{m-2}+3a_1^{m-2}+a_2^{m-2}\end{pmatrix}$$

elde edilir. Böylece $i=1,2,3$ için $\phi_2\,\rho_{\Theta_i,\lambda}(z)=\sigma\phi_2(z)$ eşitliği sağlanır. □

Bu önerme sonucunda aşağıdaki teorem elde edilir.

Teorem 3.3.7. C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i,\lambda)-$ devirli kod olsun. Bu durumda $\lambda=1+u+u^2,\ 3+3u+u^2,\ 3+u+3u^2,\ 1+3u+3u^2$ olmak üzere T_3

halkası üzerindeki $(\Theta_i, \lambda)-$ sabit devirli bir kodun tanımlanan ϕ_2 Gray dönüşümü altındaki görüntüsü $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli bir koddur.

İspat. $i=1,2,3$ ve $\lambda=1+u+u^2$, $3+3u+u^2$, $3+u+3u^2$, $1+3u+3u^2$ olmak üzere, C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i, \lambda)-$ sabit devirli kod olsun. Bu durumda $\rho_{\Theta_i,\lambda}(C_3)=C_3$ şeklinde ifade edilir. Önerme 3.3.4. kullanılarak $\phi_2\,\rho_{\Theta_i,\lambda}(C_3)=\sigma\phi_2(C_3)=\phi_2(C_3)$ elde edilir. Bu da $(\Theta_i, \lambda)-$ sabit devirli devirli kodun $\phi_2(C_3)$ görüntüsünün, $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli kod olmasıdır. □

Önerme 3.3.5. Herhangi bir $z \in T_3^m$ ve $i=1,2,3$ için, $\lambda=3+u+u^2$, $1+3u+u^2$, $1+u+3u^2$, $3+3u+3u^2$ olmak üzere $\phi_3\,\rho_{\Theta_i,\lambda}(z)=\sigma\phi_3(z)$ eşitliği elde edilir.

İspat. $T_3[x,\Theta_i]^m$ üzerinde $z=(z_0,z_1,\ldots,z_{m-1})$ kodu ele alınsın. Burada $a_t \in \mathbb{Z}_4$ ve $j=0,1,\ldots,m-1$ olacak şekilde $z_j=a_0^j+ua_1^j+u^2a_2^j$ ile ifade edilecektir. Bu durumda,

$$\rho_{\Theta_i,3+u+u^2}(z)=\left(\left(3+u+u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,1+3u+u^2}(z)=\left(\left(1+3u+u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,1+u+3u^2}(z)=\left(\left(1+u+3u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,3+3u+3u^2}(z)=\left(\left(3+3u+3u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right)$$ kullanılarak,

$$\rho_{\Theta_1,3+u+u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(a_0^{m-1}+a_2^{m-1}\right),a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,3+u+u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+a_1^{m-1}\right)+u^2\left(a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),a_0^0+ua_1^0+u^2\right.$$
$$\left.a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,3+u+u^2}(z)=\left(3a_0^{m-1}+u\left(a_0^{m-1}+a_1^{m-1}\right)+u^2\left(a_0^{m-1}+a_2^{m-1}\right),a_0^0+ua_1^0+u^2a_2^0,\ldots,a_0^{m-2}+u\right.$$
$$\left.a_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,1+3u+u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+a_1^{m-1}\right)+u^2\left(a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2\right.$$
$$\left.a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,1+3u+u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(a_0^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,1+3u+u^2}(z)=\left(a_0^{m-1}+u\left(3a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,1+u+3u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+\right.$$
$$\left.u^2a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,1+u+3u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,1+u+3u^2}(z)=\left(a_0^{m-1}+u\left(a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$$
$$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_1,3+3u+3u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\right.$$
$$\left.\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,3+3u+3u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(3a_0^{m-1}+a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),a_0^0+ua_1^0+\right.$$
$$\left.u^2a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,3+3u+3u^2}(z)=\left(3a_0^{m-1}+u\left(3a_0^{m-1}+a_1^{m-1}\right)+u^2\left(3a_0^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,a_0^{m-2}+\right.$$
$$\left.ua_1^{m-2}+u^2a_2^{m-2}\right)$$ eşitlikleri elde edilir. Böylece,

$$\phi_3(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+a_1^0+3a_2^0,\ldots,3a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}\right)$$

Gray dönüşümü de uygulanarak,

$$\phi_3\rho_{\Theta_i,\lambda}(z_0,z_1,\ldots,z_{m-1})=\begin{pmatrix}3a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\\ a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+a_1^0+3a_2^0,\ldots,3a_0^{m-2}+a_1^{m-2}+3a_2^{m-2}\end{pmatrix}$$

elde edilir. Diğer taraftan,

$$\sigma\phi_3(z)=\begin{pmatrix}3a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-2}+a_1^{m-2}+3a_2^{m-2},\\ a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+a_1^0+3a_2^0,\ldots,3a_0^{m-2}+a_1^{m-2}+3a_2^{m-2}\end{pmatrix}$$

sonucuna ulaşılır. Böylece $i=1,2,3$ için $\phi_3\rho_{\Theta_i,\lambda}(z)=\sigma\phi_3(z)$ eşitliği sağlanır. □

Bu önerme sonucunda aşağıdaki teorem elde edilir.

Teorem 3.3.8. C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i,\lambda)-$devirli kod olsun. Bu durumda $\lambda=3+u+u^2,\ 1+3u+u^2,\ 1+u+3u^2,\ 3+3u+3u^2$ olmak üzere T_3 halkası üzerindeki $(\Theta_i,\lambda)-$sabit devirli bir kodun tanımlanan ϕ_3 Gray dönüşümü altındaki görüntüsü $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli bir koddur.

İspat. $i=1,2,3$ ve $\lambda=3+u+u^2, 1+3u+u^2, 1+u+3u^2, 3+3u+3u^2$ olmak üzere, C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i,\lambda)-$ sabit devirli kod olsun. Bu durumda $\rho_{\Theta_i,\lambda}(C_3)=C_3$ şeklinde ifade edilir. Önerme 3.3.5. kullanılarak $\phi_3\,\rho_{\Theta_i,\lambda}(C_3)=\sigma\phi_3(C_3)=\phi_3(C_3)$ elde edilir. Bu da $(\Theta_i,\lambda)-$ sabit devirli devirli kodun $\phi_3(C_3)$ görüntüsünün, $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda devirli kod olmasıdır. □

Önerme 3.3.6. Herhangi bir $z\in T_3^m$ ve $i,j=1,2,3$ için, $\lambda=1+2u+2u^2,3+2u,3+2u^2$ olmak üzere $\phi_j\,\rho_{\Theta_i,\lambda}(z)=\upsilon_2\,\phi_j(z)$ eşitliği elde edilir.

İspat. üzerinde $z=(z_0,z_1,\ldots,z_{m-1})$ kodu ele alınsın. Burada $a_t\in\mathbb{Z}_4$ ve $j=0,1,\ldots,m-1$ olacak şekilde $z_j=a_0^j+ua_1^j+u^2a_2^j$ ile ifade edilecektir. Bu durumda,

$$\rho_{\Theta_i,1+2u+2u^2}(z)=\left(\left(1+2u+2u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$$\rho_{\Theta_i,3+2u}(z)=\left((3+2u)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right),$$

$\rho_{\Theta_i,3+2u^2}(z)=\left(\left(3+2u^2\right)\Theta_i(z_{m-1}),\Theta_i(z_0),\Theta_i(z_1),\ldots,\Theta_i(z_{m-2})\right)$ kullanılarak,

$$\rho_{\Theta_1,1+2u+2u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(2a_0^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\right.$$
$$\left.\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_2,1+2u+2u^2}(z)=\left(a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+a_1^{m-1}\right)+u^2\left(2a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+\right.$$
$$\left.u^2a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$$\rho_{\Theta_3,1+2u+2u^2}(z)=\left(a_0^{m-1}+u\left(2a_0^{m-1}+3a_1^{m-1}\right)+u^2\left(2a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\right.$$
$$\left.\ldots,a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$$

$\rho_{\Theta_1,3+2u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+ua_1^{m-1}+u^2\left(2a_0^{m-1}+2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$
$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$

$\rho_{\Theta_2,3+2u^2}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u3a_1^{m-1}+u^2\left(2a_0^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,a_0^{m-2}+\right.$
$\left.ua_1^{m-2}+u^2a_2^{m-2}\right),$

$\rho_{\Theta_3,3+2u^2}(z)=\left(3a_0^{m-1}+ua_1^{m-1}+u^2\left(2a_0^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2\right.$
$\left.a_2^{m-2}\right),$

$\rho_{\Theta_1,3+2u}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+a_1^{m-1}\right)+u^2\left(2a_1^{m-1}+a_2^{m-1}\right),\ a_0^0+ua_1^0+u^2a_2^0,\ldots,\right.$
$\left.a_0^{m-2}+ua_1^{m-2}+u^2a_2^{m-2}\right),$

$\rho_{\Theta_2,3+2u}(z)=\left(3a_0^{m-1}+2a_1^{m-1}+u\left(2a_0^{m-1}+3a_1^{m-1}\right)+u^2a_2^{m-1},\ a_0^0+ua_1^0+u^2a_2^0,\ldots,a_0^{m-2}+u\right.$
$\left.a_1^{m-2}+u^2a_2^{m-2}\right),$

$\rho_{\Theta_3,3+2u}(z)=\left(3a_0^{m-1}+u\left(2a_0^{m-1}+a_1^{m-1}\right)+u^2a_2^{m-1},\ a_0^0+ua_1^0+u^2a_2^0,\ldots,a_0^{m-2}+ua_1^{m-2}+u^2\right.$
$\left.a_2^{m-2}\right)$ elde edilir. Buradan hareketle,

$\phi_1(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+3a_1^0+a_2^0,\ldots,3a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right),$

$\phi_2(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},a_0^0+3a_1^0+a_2^0,\ldots,a_0^{m-1}+3a_1^{m-1}+a_2^{m-1}\right)$ ve

$\phi_3(z)=\left(a_0^0+a_1^0+3a_2^0,\ldots,a_0^{m-1}+a_1^{m-1}+3a_2^{m-1},3a_0^0+a_1^0+3a_2^0,\ldots,3a_0^{m-1}+a_1^{m-1}+3a_2^{m-1}\right)$

Gray dönüşümleri de kullanılarak,

$$\phi_1 \rho_{\Theta_i,\lambda}(z_0, z_1, \ldots, z_{m-1}) = \begin{pmatrix} 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, 3a_0^0 + 3a_1^0 + a_2^0, \ldots, 3a_0^{m-2} + 3a_1^{m-2} + a_2^{m-2} \end{pmatrix}$$

,

$$\phi_2 \rho_{\Theta_i,\lambda}(z_0, z_1, \ldots, z_{m-1}) = \begin{pmatrix} a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + 3a_1^0 + a_2^0, \ldots, a_0^{m-2} + 3a_1^{m-2} + a_2^{m-2} \end{pmatrix},$$

$$\phi_3 \rho_{\Theta_i,\lambda}(z_0, z_1, \ldots, z_{m-1}) = \begin{pmatrix} 3a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, 3a_0^0 + a_1^0 + 3a_2^0, \ldots, 3a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2} \end{pmatrix}$$

sonucuna varılır. Diğer taraftan,

$$\upsilon_2 \phi_1(z) = \begin{pmatrix} a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1}, 3a_0^0 + 3a_1^0 + a_2^0, \ldots, 3a_0^{m-2} + 3a_1^{m-2} + a_2^{m-2} \end{pmatrix},$$

$$\upsilon_2 \phi_2(z) = \begin{pmatrix} a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1}, a_0^0 + 3a_1^0 + a_2^0, \ldots, a_0^{m-2} + 3a_1^{m-2} + a_2^{m-2} \end{pmatrix},$$

$$\upsilon_2 \phi_3(z) = \begin{pmatrix} a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, a_0^0 + a_1^0 + 3a_2^0, \ldots, a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2}, \\ 3a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, 3a_0^0 + a_1^0 + 3a_2^0, \ldots, 3a_0^{m-2} + a_1^{m-2} + 3a_2^{m-2} \end{pmatrix}$$ elde edilir.

Böylece $i, j = 1,2,3$ için $\phi_j \rho_{\Theta_i,\lambda}(z) = \upsilon_2 \phi_j(z)$ eşitliği sağlanır. □

Bu önerme sonucunda aşağıdaki teorem elde edilir.

Teorem 3.3.9. $i, j = 1,2,3$ ve $\lambda = 1 + 2u + 2u^2, 3 + 2u, 3 + 2u^2$ olmak üzere, C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i, \lambda)-$ sabit devirli kod ise T_3 halkası üzerindeki $(\Theta_i, \lambda)-$ sabit devirli bir kodun tanımlanan ϕ_j Gray dönüşümü altındaki $\mathbb{Z}_4$ görüntüsü, $2m$ uzunluğunda $2-$ parçalı devirli bir kod olur.

İspat. $i, j = 1,2,3$ ve $\lambda = 1+2u+2u^2, 3+2u, 3+2u^2$ için, C_3 kodu T_3 halkası üzerinde m uzunluğunda $(\Theta_i, \lambda)-$ devirli kod olsun. Bu durumda $\rho_{\Theta_i,\lambda}(C_3) = C_3$ şeklinde ifade edilir. Önerme 3.3.6. kullanılarak $\phi_j \rho_{\Theta_i,\lambda}(C_3) = \upsilon_2 \phi_j(C_3) = \phi_j(C_3)$ elde edilir. Bu da $(\Theta_i, \lambda)-$ sabit devirli devirli bir kodun $\phi_j(C_3)$ görüntüsünün, $\mathbb{Z}_4$ üzerinde $2m$ uzunluğunda $2-$parçalı devirli bir kod olmasıdır. □

3.4. Hesaplama Sonuçları

Bu bölümde, özel olarak Θ_1-otomorfizması ve ϕ_1 dönüşümü kullanılarak T_3 halkası üzerinde 7 uzunluktaki aykırı devirli kodlar ve aykırı $(u^2+3u+3)-$sabit devirli kodlar araştırılmıştır. Teorem 3.2.4., Teorem 3.3.3. ve MAGMA programı kullanılarak Θ_1-devirli kodların $\mathbb{Z}_4$ görüntüleri incelenmiştir. Yapılan incelemeler sonucunda T_3 halkası üzerinde $\mathbb{Z}_4$ görüntüsü yeni, optimal ve iyi bilinen lineer kodlar elde edilmiştir. Bu kodların türüne karar verilirken [43] numaralı kaynakta verilen çevrimiçi veritabanı kullanılmıştır. Tablo 2.1.'deki T_3 halkasındaki elemanların temsilleri kullanılarak elde edilen kodlar Tablo 3.1. ve Tablo 3.2.'de sunulmuştur. Tablodaki yazımı kolaylaştırmak adına, en yüksek dereceli değişkenin katsayısından başlayarak polinomun katsayıları azalan formda yazılacaktır. Örneğin; $(2u^2)x^5+(1+3u)x^3+(2+u)x+(1+2u+3u^2)$ polinomu $80H0Bc'$ şeklinde, $(2+u+3u^2)x^3+(2+u+3u^2)x^2+(2+u+3u^2)x+(2+u+3u^2)$ polinomu ise n^4 şeklinde ifade edilecektir.

Bu bilgiler doğrultusunda, T_3 halkasındaki devirli kodların $\mathbb{Z}_4$ görüntüleri kullanılarak $(14, 4^4 2^1, 4_L)$, $(14, 4^4 2^1, 6_E)$ ve $(14, 4^4 2^1, 2_H)$ parametrelerine sahip 3 farklı üreteç polinomu; $(14, 4^6 2^1, 4_L)$, $(14, 4^6 2^1, 4_E)$ ve $(14, 4^6 2^1, 2_H)$ parametrelerine sahip 1 üreteç polinomu; $(14, 4^1 2^4, 4_L)$, $(14, 4^1 2^4, 8_E)$ ve $(14, 4^1 2^4, 2_H)$

parametrelerine sahip 1 üreteç polinomu; $\left(14,4^4 2^0,6_L\right)$ ve $\left(14,4^4 2^0,6_E\right)$ parametrelerine sahip 1 üreteç polinomu; $\left(14,4^6 2^0,4_L\right)$ ve $\left(14,4^6 2^0,4_E\right)$ parametrelerine sahip 1 üreteç polinomu; $\left(14,4^0 2^5,4_L\right)$, $\left(14,4^0 2^5,8_E\right)$ ve $\left(14,4^0 2^5,2_H\right)$ parametrelerine sahip 1 üreteç polinomu ile yeni kodlar elde edilmiştir. Ayrıca $\left(14,4^4 2^3,4_L\right)$, $\left(14,4^4 2^3,6_E\right)$ ve $\left(14,4^4 2^3,2_H\right)$ parametrelerine sahip 5 farklı üreteç polinomu; $\left(14,4^3 2^2,4_L\right)$, $\left(14,4^3 2^2,8_E\right)$ ve $\left(14,4^3 2^2,2_H\right)$ parametrelerine sahip 10 farklı üreteç polinomu; $\left(14,4^3 2^4,4_L\right)$ ve $\left(14,4^3 2^4,2_H\right)$ parametrelerine sahip 7 farklı üreteç polinomu; $\left(14,4^1 2^6,4_L\right)$ ve $\left(14,4^1 2^6,2_H\right)$ parametrelerine sahip 4 farklı üreteç polinomu; $\left(14,4^3 2^3,8_L\right)$ ve $\left(14,4^3 2^3,4_H\right)$ parametrelerine sahip 3 farklı üreteç polinomu; $\left(14,4^0 2^7,4_L\right)$ ve $\left(14,4^0 2^7,2_H\right)$ parametrelerine sahip 9 farklı üreteç polinomu;$\left(14,4^1 2^3,12_L\right)$, $\left(14,4^1 2^3,14_E\right)$ ve $\left(14,4^1 2^3,6_H\right)$ parametrelerine sahip 2 farklı üreteç polinomu; $\left(14,4^0 2^4,24_E\right)$ ve $\left(14,4^0 2^4,6_H\right)$ parametrelerine sahip 3 farklı üreteç polinomu; $\left(14,4^3 2^0,8_E\right)$ ve $\left(14,4^3 2^0,8_H\right)$ parametrelerine sahip 2 farklı üreteç polinomu; $\left(14,4^3 2^1,8_L\right)$ ve $\left(14,4^3 2^1,6_H\right)$ parametrelerine sahip 9 farklı üreteç polinomu; $\left(14,4^4 2^0,6_H\right)$ parametresine sahip 1 üreteç polinomu; $\left(14,4^6 2^0,4_H\right)$ parametresine sahip 1 üreteç polinomu ile optimal kodlar elde edilmiştir.

Ayrıca T_3 halkasındaki $\left(u^2+3u+3\right)-$sabit devirli kodların $\mathbb{Z}_4$ görüntüleri ile $\left(14,4^0 2^2,12_L\right)$, $\left(14,4^0 2^2,24_E\right)$ ve $\left(14,4^0 2^2,6_H\right)$ parametrelerine sahip 1 üreteç polinomu, $\left(14,4^3 2^1,4_H\right)$ parametresine sahip 2 farklı üreteç polinomu ve $\left(14,4^3 2^3,4_L\right)$ ve $\left(14,4^3 2^3,2_H\right)$ parametrelerine sahip 1 üreteç polinomu ile yeni kodlar bulunmuştur. $\left(14,4^3 2^1,8_L\right)$ ve $\left(14,4^3 2^1,8_E\right)$ parametrelerine sahip 2 farklı üreteç polinomu, $\left(14,4^6 2^0,4_L\right)$, $\left(14,4^6 2^0,4_E\right)$ ve $\left(14,4^6 2^0,4_H\right)$ parametresine sahip 1 üreteç polinomu, $\left(14,4^3 2^2,4_L\right)$, $\left(14,4^3 2^2,8_E\right)$ ve $\left(14,4^3 2^2,2_H\right)$ parametrelerine sahip

3 farklı üreteç polinomu, $(14,4^3 2^1,8_L)$, $(14,4^3 2^1,8_E)$ ve $(14,4^3 2^1,6_H)$ parametrelerine sahip 2 farklı üreteç polinomu, $(14,4^1 2^6,4_L)$ ve $(14,4^1 2^6,2_H)$ parametrelerine sahip 2 farklı üreteç polinomu, $(14,4^1 2^4,4_L)$, $(14,4^1 2^4,8_E)$ ve $(14,4^1 2^4,2_H)$ parametrelerine sahip 2 farklı üreteç polinomu, $(14,4^4 2^3,4_L)$, $(14,4^4 2^3,6_E)$ ve $(14,4^4 2^3,2_H)$ parametrelerine sahip 3 farklı üreteç polinomu, $(14,4^4 2^0,6_H)$ parametresine sahip 1 üreteç polinomu, $(14,4^3 2^4,4_L)$ ve $(14,4^3 2^4,2_H)$ parametrelerine sahip 2 farklı üreteç polinomu, $(14,4^0 2^7,4_L)$ ve $(14,4^0 2^7,2_H)$ parametresine sahip 1 üreteç polinomu, $(14,4^4 2^1,4_L)$, $(14,4^4 2^1,6_E)$ ve $(14,4^4 2^1,2_H)$ parametresine sahip 1 üreteç polinomu, $(14,4^0 2^6,8_L)$, $(14,4^0 2^6,16_E)$ ve $(14,4^0 2^6,4_H)$ parametresine sahip 1 üreteç polinomu ile optimal kodlar kodlar elde edilmiştir. Bölüm 2.4.'te de belirtildiği üzere bu parametrelerdeki L indisi Lee ağırlığı, E indisi Öklit ağırlığı, H indisi ise Hamming ağırlığı temsil etmektedir. Ayrıca [43] numaralı kaynakta verilen veritabanına göre ilk defa bulunan kodlar "*" ile işaretlenmiştir. Aynı uzunluk, boyut ve minimum uzaklıkta bulunan en iyi parametreler optimal kod olarak adlandırılmış ve tabloda "**" ile işaretlenmiştir.

Tablo 3.1. Bazı aykırı devirli kodların $\mathbb{Z}_4$ görüntüleri

$\tau_1(x)$	$\tau_2(x)$	$\tau_3(x)$	Tip	W_L	W_E	W_H
808^3	$v'5'v'b$	$7'7'7'7'7'7'3'$	$4^0 2^7$	4^{**}	8	2^{**}
78979	$b^3v'bv'v'$	$7'3'5'7'$	$4^3 2^1$	8^{**}	8	6^{**}
8088	$H^3s's'Hs'$	$5'5'5'05'$	$4^0 2^4$	12	24^{**}	6^{**}
7987	$3'rDv'H$	$7'7'7'3'7'3'3'$	$4^4 2^0$	6^{*}	6^{*}	6^{**}
7^3979^2	$R^3v'000$	$7'7'$	$4^1 2^6$	4^{**}	8	2^{**}
7^2989	$7'Dv'NH$	$5'5'5'5'5'5'5'$	$4^3 2^1$	8^{**}	8	6^{**}
77	$5'5'5'F5'F^2$	$5'5'5'05'$	$4^6 2^0$	4^{*}	4^{*}	4^{**}
707^29	$U^3e'000$	$7'7'7'3'3'7'3'$	$4^3 2^1$	8^{**}	8	6^{**}
7^2909	$s'v'de's'$	$7'7'7'7'7'7'3'$	$4^3 2^4$	4^{**}	8	2^{**}
79^209	$bv'v'0v'$	$7'5'3'3'3'$	$4^3 2^3$	8^{**}	8	4^{**}
79^209	U^2drHds'	$7'7'3'5'3'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
7^69	$7'DHFH$	$7'5'3'7'3'$	$4^1 2^6$	4^{**}	8	2^{**}
78979	$3'5'7'H^2$	$7'5'3'7'3'$	$4^3 2^3$	8^{**}	8	4^{**}
77909	$R^27'b$	$7'7'7'3'7'3'3'$	$4^3 2^4$	4^{**}	8	2^{**}
789^3	$R^3v'Fv'b$	$3'7'5'7'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
789^3	U^2dH^2Us'	$3'5'7'3'3'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
7^2989	$UrNFe'$	$5'5'5'5'5'5'5'$	$4^3 2^0$	8	8^{**}	8^{**}
8^208	d^3H^2ds'	$7'5'7'7'$	$4^0 2^7$	4^{**}	8	2^{**}
7^39^279	D^2HRs'	$3'5'3'7'$	$4^1 2^3$	12^{**}	14^{**}	6^{**}
8^208	R^5F^2	$3'3'7'5'3'$	$4^0 2^7$	4^{**}	8	2^{**}
77	d^3D^2ds'	$7'3'3'03'$	$4^6 2^1$	4^{*}	4^{*}	2^{*}
7^3979^2	$3'3'3'3'3'H^2$	$7'7'3'03'$	$4^1 2^4$	4^{*}	8^{*}	2^{*}
7987	$7'7'Ds'dv's'$	$7'7'7'3'3'7'3'$	$4^4 2^1$	4^{*}	6^{*}	2^{*}
7^2989	$7'7'3'Fv'$	$7'7'3'03'$	$4^3 2^0$	8	8^{**}	8^{**}
9^2789	$e'e'e'e'e'e'e'$	$7'7'7'3'3'7'3'$	$4^3 2^1$	8^{**}	8	6^{**}
7^2989	$UHe'v'D$	$7'5'3'3'3'$	$4^3 2^4$	4^{**}	8	2^{**}
7^39^279	$Ube'D^2$	$7'7'3'03'$	$4^1 2^6$	4^{**}	8	2^{**}
9787	$5'5'5'Ur$	$7'7'7'7'7'7'3'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
79^209	$HrDv's'$	$5'5'5'05'$	$4^3 2^3$	8^{**}	8	4^{**}
79909	U^2drHds'	$7'7'3'5'3'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}

Tablo 3.1. (Devamı)

$\tau_1(x)$	$\tau_2(x)$	$\tau_3(x)$	Tip	W_L	W_E	W_H
7987	$7'7'Ds'dv's'$	$7'7'3'5'3'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
9787	$3'3'7'rH$	$7'7'7'3'3'7'3'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
77989	$3'3'Hv's's's'$	$5'5'5'5'5'5'5'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
$707^2 9$	$7'7'7'3'3'DH$	$7'3'5'7'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
70779	$7'7'D^2 dbs'$	$7'7'7'3'3'7'3'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
88	$7'7'b3'v'bv'$	$3'3'7'5'3'$	$4^0 2^7$	4^{**}	8	2^{**}
$7^3 979^2$	$v'UFr$	$3'3'3'3'3'3'3'$	$4^1 2^3$	12^{**}	14^{**}	6^{**}
$7^3 9^2 79$	$De'Hv's'$	$5'5'5'05'$	$4^1 2^6$	4^{**}	8	2^{**}
$79^2 09$	$Ude'7'D$	$7'7'7'7'7'7'3'$	$4^3 2^1$	8^{**}	8	6^{**}
$9^2 789$	$e'e'e'e'e'e'e'$	$7'3'3'03'$	$4^3 2^1$	8^{**}	8	6^{**}
$8^3 08$	$5'rFUr$	$3'5'7'3'3'$	$4^0 2^7$	4^{**}	8	2^{**}
789^3	$U^3 Ds'rD$	$7'7'3'5'3'$	$4^3 2^4$	4^{**}	8	2^{**}
$707^2 9$	$7'7'D^2 dbs'$	$5'5'05'5'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
9897	$7'F3'bv'$	$7'7'7'3'7'3'3'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
$79^2 909$	$U^2 drHds'$	$7'5'7'7'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
9897	$U^2 rUr^2 e'$	$7'5'3'3'3'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
77909	$s'v'de's'$	$7'7'7'7'7'7'3'$	$4^3 2^4$	4^{**}	8	2^{**}
$79^2 09$	$N^3 e'e'e'e'$	$3'5'3'7'$	$4^3 2^1$	8^{**}	8	6^{**}
$9^2 789$	$3's'be'H$	$3'3'3'3'3'3'3'$	$4^3 2^1$	8^{**}	8	6^{**}
8808	$dUD7's'$	$7'7'7'7'7'7'3'$	$4^0 2^7$	4^{**}	8	2^{**}
8088	$H^3 s's'Hs'$	$7'07'7'3'$	$4^0 2^7$	4^{**}	8	2^{**}
$7^2 989$	$3'3'Hv's's'$	$3'5'7'3'3'$	$4^3 2^4$	4^{**}	8	2^{**}
78979	$5'5'e'Fre'e'$	$7'5'7'7'$	$4^3 2^4$	4^{**}	8	2^{**}
$8^2 08$	$d^3 H^2 ds'$	$5'5'$	$4^0 2^4$	12	24^{**}	6^{**}
$9^2 789$	$3's'be'H$	$5'5'5'5'5'5'5'$	$4^3 2^1$	8^{**}	8	6^{**}
8088	$dbs'e's'$	$7'7'7'3'7'3'3'$	$4^0 2^7$	4^{**}	8	2^{**}
8808	$7'7'dHs'7's'$	$7'5'3'3'3'$	$4^0 2^{5*}$	4^*	8^*	2^*
9787	$U^3 DrD^2$	$7'3'5'7'$	$4^4 2^1$	4^*	6^*	2^*
70779	$7'7'7'3'3'DA$	$5'05'5'5'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
8^7	$7'v'3'Rv'$	$7'7'7'3'3'7'3'$	$4^0 2^4$	12	24^{**}	6^{**}
787^2	$7'7'dv's'ds'$	$5'5'05'$	$4^4 2^1$	4^*	6^*	2^*

Tablo 3.2. Bazı aykırı $\left(u^2+3u+3\right)-$ devirli kodların $\mathbb{Z}_4$ görüntüleri

$\tau_1(x)$	$\tau_2(x)$	$\tau_3(x)$	Tip	W_L	W_E	W_H
8^7	$FR7'7'7'Rb$	$7'7'3'7'3'7'7'$	$4^0 2^{2^*}$	12^*	24^*	6^*
98779	$FR3'b3'5'v'$	$7'03'7'7'$	$4^3 2^1$	8^{**}	8^{**}	4^*
79	$FR0^3RR$	$7'5'7'3'7'$	$4^6 2^0$	4^{**}	4^{**}	4^{**}
70799	$3'7'7'Hbs'U$	$5'5'05'005'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
98779	$7'3'3'7'7'v'v'$	$7'03'3'7'$	$4^3 2^1$	8^{**}	8^{**}	6^{**}
7979799	$7'DUFe'$	$7'5'3'7'$	$4^1 2^6$	4^{**}	8	2^{**}
9797979	$UDs'rdDd$	$7'03'3'7'$	$4^1 2^4$	4^{**}	8^{**}	2^{**}
97789	$rde'de'Hr$	$5'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
9899	$7'7'HUdr'D$	$3'7'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
9989	$FR5'b7'0v'$	$7'5'7'3'7'$	$4^4 2^0$	8	8	6^{**}
78999	$FR3'3'b5'b$	$7'03'7'7'$	$4^3 2^1$	8^{**}	8^{**}	4^*
9899	$rs'e'HUDU$	$7'3'5'3'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
79989	$3'7'Fb$	$3'7'7'3'3'7'7'$	$4^3 2^4$	4^{**}	8	2^{**}
98779	$5'5'UdU5'N$	$5'5'0^3 5'5'$	$4^3 2^2$	4^{**}	8^{**}	2^{**}
7789	$3'Ue'v'e'$	$7'7'3'7'3'7'7'$	$4^4 2^3$	4^{**}	6^{**}	2^{**}
8088	$HUs'rDUd$	$7'5'7'3'7'$	$4^0 2^7$	4^{**}	8	2^{**}
77909	$FR0^3bv'$	$7'3'5'3'$	$4^3 2^4$	4^{**}	8	2^{**}
78979	$d7's'Dd$	$5'5'005'05'$	$4^3 2^3$	4^*	8	2^*
7977999	$7'de'FN$	$7'3'3'7'7'3'7'$	$4^1 2^6$	4^{**}	8	2^{**}
7879	$7'3'HrH7's'$	$3'7'7'3'3'7'7'$	$4^4 2^1$	4^{**}	6^{**}	2^{**}
98779	$7'3'3'7'7'v'v'$	$5'5'5'05'$	$4^3 2^1$	8^{**}	8^{**}	6^{**}
7977779	$FR7'7'7'Rb$	$3'7'5'3'$	$4^1 2^4$	4^{**}	8^{**}	2^{**}
88808	$7'03'bv'$	$7'03'3'7'$	$4^0 2^6$	8^{**}	16^{**}	4^{**}

BÖLÜM 4. $\mathbb{Z}_4 + u\,\mathbb{Z}_4 + u^2\mathbb{Z}_4$ HALKASI ÜZERİNDE TERS SIRALI DNA KODLAR

Şeker, fosfat ve baz gruplarının bir araya gelmesiyle oluşan DNA, birbirine sarmal şekilde bağlı iki zincirden meydana gelir. Bu teori ilk defa J. Watson ve F. Crick tarafından ortaya atılmış ve sonrasında yapılan tüm çalışmaların temel dayanağı haline gelmiştir [66-71]. Tüm canlı türlerinde kalıtsal bilgilerin taşınması hususunda ve hücrelerin hayati tüm fonksiyonlarında önemli bir rol oynayan DNA, birçok karmaşık problemin çözümünde yer aldığından ve bilgiyi uzun süre saklayabildiğinden disiplinler arası çalışma sahasına sahiptir. DNA'nın hata düzeltme kapasitesi son zamanlarda hata düzelten kodlar teorisinde de ilgi çekmeye başlamıştır. Bu hususstaki bazı çalışmalar ele alınacak olursa; Şiap ve ark. [71] numaralı çalışmada, $u^2 = 1$ iken $F_2[u] \big/ \langle u^2 - 1 \rangle$ halkasındaki devirli kodların cebirsel yapısından yararlanarak devirli DNA kodları inşa etmişlerdir. Ayrıca bu kodların $CG-$miktar ve silme mesafesini de inceleyerek örnekler sunmuşlardır. Bayram ve ark. [72] numaralı çalışmada, $v^2 = v$ iken $F_4 + vF_4$ halkasında devirli, sabit devirli ve aykırı sabit devirli kodların yapısını incelemişlerdir. DNA kodlar için önemli bir referans olan terslenebilen kodları oluşturmuş ve birçok örnek sunmuşlardır. Yıldız ve Şiap [73] numaralı çalışmada, $F_2[u] \big/ \langle u^4 - 1 \rangle$ halkasında devirli kodların üreteç polinomlarından yararlanarak devirli DNA kodların yapısını incelemiş ve farklı tek uzunluktaki birçok örnek ile makaleyi zenginleştirmişlerdir. Öztaş ve ark. [74] numaralı çalışmasında farklı alfabeler üzerinde ters sıralı ve ters sıralı tamlayan DNA kodlar bulmak için yeni bir yaklaşım inşa etmişlerdir. Yeni bir polinom tipi (coterm polinom) tanımlayarak bu polinoma uygun bir modül inşa metodu oluşturmuş ve bu sayede pek çok optimal ters sıralı kod bulmuşlardır.

Bu bölüm 2 kısımdan oluşmaktadır. İlk kısımda, DNA kodlar hakkındaki bazı temel tanım ve teoremler verilmiştir. Önceki bölümlerde de kullanılan ϕ_1 Gray dönüşümü vasıtasıyla halkanın elemanları ile DNA $2-$baz arasındaki ilişki oluşturulmuştur. İkinci kısımda ise yeni bir polinom (unit reverse polinom) tanımlanarak yeni bir üretim metotu inşa edilmiştir. Bu üretim metodu ters sıralı DNA kod bulma hususunda yardımcı olacaktır.

4.1. DNA Kodlar Hakkında Temel Bilgiler

DNA'nın temel yapı birimi olan nükleotitler bir fosfat, $5C$'lu şeker ve bir azotlu organik bazdan oluşur. DNA'da bulunan dört çeşit nükleotitin üçlü kombinasyonlar halinde bir araya gelmesiyle oluşan kodonlar ise protein oluşumu için gerekli şifreyi oluşturur. Diğer bir ifadeyle, genler protein sentezi için gerekli olan kodu içerir ve her bir kodon da protein sentezi esnasında tek bir aminoasit kodlar. Vücuttaki hücresel faaliyetlerin hepsi enzim kontrolünde gerçekleştiğinden ve oluşan mevcut tüm enzimler de protein yapılı olduğundan dolayı enzimsiz herhangi bir reaksiyonun gerçekleşmesi mümkün değildir. Dolayısıyla DNA hayati tüm fonksiyonlarda önemli bir rol oynar.

Bu bölümde ilk olarak bazı notasyonlar hakkında konuşulacak ve temel tanımlar verilecektir. Daha sonra, önceki bölümlerde tanımlanan Gray dönüşüm hatırlatılacaktır. Bu dönüşüm, $u^3=u^2$ iken $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ halkasının elemanları ile DNA $2-$bazı arasında ilişki kurmaya yarayacaktır.

Tanım 4.1.1. Sonlu bir $\tilde{\Lambda}$ kümesinde herhangi bir m uzunluğundaki D kodu için,

i. $(z_0,z_1,\ldots,z_{m-1})\in D$ iken $(z_{m-1},z_{m-2},\ldots,z_0)\in D$ oluyorsa, diğer bir ifade ile, D kodundaki herhangi bir z kodsözü için z^R kodsözü de D kodunun bir elemanı oluyorsa D koduna ters sıralı kod adı verilir.

ii. $(z_0, z_1, \ldots, z_{m-1}) \in D$ iken $(\overline{z}_{m-1}, \overline{z}_{m-2}, \ldots, \overline{z}_0) \in D$ oluyorsa diğer bir ifade ile, D kodundaki herhangi bir z kodsözü için $\overline{z^R}$ kodsözü de D kodunun bir elemanı oluyorsa D koduna ters sıralı tamlayan kod adı verilir.

Tanım 4.1.2. $s(x) = s_0 + s_1 x + \ldots s_t x^t \in T_3[x]$ polinomu derecesi t olan bir polinom olsun. $i = 1,2,3$ ve $j = 0, \ldots, t$ olmak üzere; $s(x)$ polinomunun katsayıları için; $s_j(x) = s_{t-j}(x)$ eşitliği sağlanıyorsa $s(x)$ polinomuna palindromik polinom denir.

Önceki bölümde de anlatıldığı gibi; T_3 halkası üzerinde m uzunluğundaki lineer C_3 kodu, T_3^m halkasının bir T_3 – alt modülüdür. Bu lineer kodun elemanları kodsöz olarak adlandırılır. $i = 0,1,2$ ve $a_i \in \mathbb{Z}_4$ iken T_3 halkasının herhangi bir elemanı $z = a_0 + ua_1 + u^2 a_2$ şeklinde tanımlanır. $i = 0,1,\ldots m-1$ olmak üzere her bir $z_i = a_0^i + ua_1^i + u^2 a_2^i$ elemanı için $z = (z_0, z_1, \ldots, z_{m-1})$ kodsözünün polinom formu $z(x) = z_0 + z_1 x + z_2 x^2 + \ldots z_{m-1} x^{m-1}$ şeklinde ifade edilir.

$i = 0,1,\ldots,m-1$ ve herhangi bir $z \in T_3$ için $z_i = a_0^i + ua_1^i + u^2 a_2^i$ olacak şekilde T_3^m halkasından $\mathbb{Z}_4^{2m}$ halkasına uzaklığı koruyan ve lineer olan aynı zamanda da T_3 halkasındaki elemanlar ile $\{A,G,C,T\}^2$ alfabesi üzerinde 64 kodon arasındaki ilişkiyi sağlayacak olan Gray dönüşüm aşağıdaki gibidir.

$$\phi : T_3 \to \mathbb{Z}_4^{2m}$$

$$(a_0 + ua_1 + u^2 a_2) \to (a_0 + a_1 + 3a_2,\ 3a_0 + 3a_1 + a_2)$$

Bu dönüşüm,

$$\Phi : T_3^m \to \mathbb{Z}_4^{2m}$$

$$(z_0, z_1, \ldots, z_{m-1}) \to \begin{pmatrix} a_0^0 + a_1^0 + 3a_2^2, \ldots, a_0^{m-1} + a_1^{m-1} + 3a_2^{m-1}, \\ 3a_0^0 + 3a_1^0 + a_2^2, \ldots, 3a_0^{m-1} + 3a_1^{m-1} + a_2^{m-1} \end{pmatrix}$$

şeklinde genişletilir. Bu Gray dönüşümün önceki bölümlerde de kullanıldığı hatırlatılsın.

4.2. T_3 Halkasında Ters Sıralı DNA Kodlar

Ters sıralı DNA kodlar ele alınmadan önce ters sıralılık problemi incelensin. $\eta(0)=A, \eta(1)=T, \eta(2)=G$ ve $\eta(3)=C$ iken $t_1=3u+u^2$, $t_2=3+3u+u^2$, $t_3=2+3u^2$, $t_4=3+u+2u^2$ ve $t_5=1+u+2u^2$ olmak üzere (t_1,t_2,t_3,t_4,t_5) kodsözü ele alınsın. Bu durumda ϕ_1 Gray dönüşümü göz önünde bulundurularak bu kodsözün DNA karşılığı *GGTCCTGGAA* olmaktadır. (t_1,t_2,t_3,t_4,t_5) kodsözünün ters sıralısı (t_5,t_4,t_3,t_2,t_1) iken bu kodsözün DNA zinciri ise *AAGGCTTCGG* olmaktadır. Ancak *GGTCCTGGAA* DNA zincirinin ters sıralısı *AAGGCTTCGG* değildir. Böylece (t_1,t_2,t_3,t_4,t_5) kodsözünün ters sıralısının DNA zincirinin *AAGGCTTCGG* olmadığı açık bir şekilde görülmektedir. Buradan hareketle, halkanın elemanı Gray dönüşüm vasıtasıyla ikili veya daha fazla DNA bazına dönüştürüldüğünde ters sıralılık problemi ile karşılaşıldığı görülmektedir.

Bu bölümde, ilk olarak, önceki bölümlerde T_3 olarak isimlendirilen, $u^3=u^2$ iken $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4$ halkasında ters sıralı DNA kod bulmak için yeni bir polinom tanımlanacaktır. Bu polinomu oluşturmak için öncelikle,

$$U_A=\{1,3+2u,1+u+u^2,3+3u+u^2,3+2u^2,1+2u+2u^2,3+u+3u^2,1+3u+3u^2\},$$

$$U_B=\{3,1+2u,3+u+u^2,1+3u+u^2,1+2u^2,3+2u+2u^2,1+u+3u^2,3+3u+3u^2\},$$

$$\kappa=\{0,2\}$$

kümeleri tanımlansın. Burada U_A kümesi ile U_B kümesi birbirinin ters sıralısı olan birimsel elemanlardan oluşmaktadır. Bu kümelerdeki elemanların 3 ile çapılması durumunda bir diğer kümenin içine düştüğü, 2 ile çarpılması durumunda ise sadece 2 ve $2+2u+2u^2$ elemanlarının elde edildiğine dikkat edilsin. Şimdi U_A ve U_B kümelerinden yardım alınarak birimsel ters sıralı polinom tanımı yapılsın.

Tanım 4.2.1. (Unit Reverse Polinom) z elemanı T_3 halkasının bir elemanı ve $g(x)$ polinomu da T_3 halkasında derecesi t olan bir polinom olsun. Bu durumda, $z_S \in U_A$, $z_Y \in U_B$, $\beta_S \in U_A$ ve $\beta_Y \in U_B$ olmak üzere,

i. $g(x)$ polinomu çift dereceli ise birimsel ters sıralı polinom

$$U_R(x) = z_S + z_Y x^t + \left(\sum_{i=1}^{(t/2)-1} \beta_S x^i + \beta_Y x^{t-i} \right) + \kappa x^{t/2} ,$$

ii. $g(x)$ polinomu tek dereceli ise birimsel ters sıralı polinom

$$U_R(x) = \sum_{i=0}^{(t-1)/2} \beta_S x^i + \beta_Y x^{t-i}$$

şeklindedir. Burada $z_S \in U_B$ ise $z_Y \in U_A$, $\beta_S \in U_B$ ise $\beta_Y \in U_A$'dır.

Örnek 4.2.1. $1+(u^2+u+1)x+(2u+3)x^2+2x^3+(3u^2+3u+3)x^4+(u^2+3u+1)x^5+(2u+1)x^6$ polinomu $T_3[x]$ halkası üzerinde çift dereceli birimsel ters sıralı bir polinomdur. $(3+2u^2)+(2u+3)x+(2u+1)x^2+(3u^2+u+1)x^3$ polinomu ise $T_3[x]$ halkası üzerinde tek dereceli bir birimsel ters sıralı polinomdur.

Şimdi Öztaş ve ark.'nın [74] makalesindeki $\dagger-$modül kod tanımı verilsin. Ayrıca $\dagger$ kodunun $x \in R$ tarafından üretilmesi durumunda $\dagger-$modül kodun $x-$modül kod olarak adlandırılabileceği hatırlatması yapılsın.

Tanım 4.2.2. [74] $\dagger$, R halkasının bir alt halkası, E de $\dagger$'nin bir üreteç kümesi olmak üzere, $R[x]/\langle x^n-1\rangle$ üzerinde $p(x)$ tarafından üretilen kod C kodu olsun. Burada,

$$C=\left\{\left(y_0+y_1x+\ldots+y_{n-1}x^{n-1}\right)p(x)\ :\ y_i\in\dagger\right\}$$

veya

$$C=\left\{\left(y_0c_1+y_1c_2+\ldots+y_ac_a\right)p(x)\ :\ y_i\in\dagger\right\}$$

şeklinde temsil edilen C kodu R^n'nin bir alt kümesidir.

[74] makalesinde DNA'nın herhangi bir $k-$bazınının yaşadığı bir halka bulunarak, bu halkanın elemanlarıyla DNA zincirinin $k-$bazları tanımlanmıştır. $k-$bazlarının tanımlanmasıyla elde edilen tersinirlik sorununun çözülmesi için yukarıda da anlatıldığı gibi yeni gösterimler ve yeni tanımlar sunulmuştur. $\dagger-$modül kod kullanılarak DNA $k-$bazının n bileşeni için verilen notasyonlar halkadaki DNA $k-$bazlarının tersini bulmaya yardımcı olmuştur.

Bu çalışmadan hareketle; çalışılan T_3 halkası 3'lü 64 elemana sahip olsa bile 3 ayrı parça halinde ayrıştırılamadığı için halka elemanları DNA $3-$bazlı olarak yazılamaz. Böylece tanımlanan Gray yapısı gereği halka elemanları DNA $2-$baza karşılık gelmektedir ve bu da kısıtlı elemanlar üzerinden olmaktadır.

Bu strateji doğrultusunda; T_3 halkasının elemanlarından DNA $2-$baza bir dönüşüm tanımlansın.

Bunun için ilk olarak, DNA bazları ile $\mathbb{Z}_4$ elemanlarındaki eşleşme kullanılarak

$$\eta:\mathbb{Z}_4\to\{A,T,G,C\}$$

şeklinde bir η dönüşümü oluşturulsun. Burada, $\eta(0)=A,\ \eta(1)=T,\eta(2)=G$ ve $\eta(3)=C$ olarak tanımlansın. Tüm $\mathbb{Z}_4$ ve DNA dizileri arasındaki η karşılaştırmasının 24 farklı şekilde olabileceği de göz önünde bulundurulmalıdır. Mesela; $\eta(0)=C,\ \eta(1)=A,\eta(2)=T$ ve $\eta(3)=G$ veya $\eta(0)=A,\ \eta(1)=G,\eta(2)=C$ ve $\eta(3)=T$ gibi. Bu tip bir çoklu dönüşüm kullanımı, Teorem 4.2.1. ile elde edilen örneklerin çeşitliliğini sağlayacaktır.

Önceki bölümde hatırlatılan ϕ_1 Gray dönüşümü ve $\mathbb{Z}_4$ ile DNA bazlarını eşleştiren η dönüşümü kullanılarak T_3 halkasının elemanları ile DNA $2-$baz arasındaki eşleşme için,

$$\vartheta=\eta o\phi_1$$

dönüşümü

$$\vartheta:T_3\to\{A,T,G,C\}^2$$
$$a_0+ua_1+u^2a_2\to\left(\eta(a_0+a_1+3a_2),\eta(3a_0+3a_1+a_2)\right)$$

ile tanımlansın.

Bu dönüşüm $i=0,1,\ldots,m-1$ iken $z_i=a_0^i+ua_1^i+u^2a_2^i$ olmak üzere,

$$\vartheta:T_3^m\to\{A,T,G,C\}^{2m}$$
$$(z_0,z_1,\ldots,z_{m-1})\to\left(\eta(\phi_1(z_0)),\eta(\phi_1(z_1)),\ldots,\eta(\phi_1(z_{m-1}))\right)$$

şeklinde çoklu bileşen formuna genişletilsin. Tanımlanan tüm bu dönüşümler yardımıyla eşleşen kodonlar WCC özelliğini sağlamaktadır.

Şimdi T_3 halkası üzerindeki ters sıralı kodları inşa etmek için birimsel ters sıralı polinomların üreteç metodu inşa edilsin.

Tanım 4.2.3. (Birimsel Ters Sıralı Polinomlar ile $\hbar_4 -$Modül Üretimi) T_3 halkasında m uzunluğundaki kodlar için, tanımlanan $U_R(x)$ polinomunun üreteç matrisleri $\hbar_4(U_R(x))$ ve $\hbar_4^{+1}(U_R(x))$ ile aşağıdaki gibi tanımlanmaktadır.

$$h_4(U_R(x)) = \begin{bmatrix} U_R(x) \\ xU_R(x) \\ \vdots \\ x^{m-t-1}U_R(x) \end{bmatrix}$$

ve

$$h_4^{+1}(U_R(x)) = \begin{bmatrix} U_R(x) \\ xU_R(x) \\ \vdots \\ x^{m-t-1}U_R(x) \\ \rho_3(x) \end{bmatrix}.$$

Burada $\lambda = \{b, b'\}$ ve $\alpha \in \kappa$ olmak üzere, $\rho_3(x)$ polinomu

$$\rho_3(x) = \begin{cases} \sum_{i=0}^{m-2/2} bx^i + b'x^{m-i-1}, & m \text{ uzunluğu çift ise,} \\ \sum_{i=0}^{m-1/2} bx^i + b'x^{m-i-1} + \alpha x^{m-1/2}, & m \text{ uzunluğu tek ise,} \end{cases}$$

şeklindedir ve $\lambda = \{1, 3\}$ olarak belirlenmektedir.

$\varepsilon_i \in T_3$ olmak üzere $U_R(x) = \varepsilon_0 + \varepsilon_1 x + \ldots + \varepsilon_t x^t$ polinomu ele alınsın. Bu durumda, $U_R(x)$ polinomunun $\hbar_4(U_R(x))$ üreteç matrisi,

$$\begin{bmatrix} \varepsilon_0 & \varepsilon_1 & & \cdots & & & \varepsilon_t & 0 & 0 & \cdots & 0 \\ 0 & \varepsilon_0 & \varepsilon_1 & & \cdots & & & \varepsilon_t & 0 & \cdots & 0 \\ \vdots & & & & \ddots & & & & & & \vdots \\ 0 & & \cdots & 0 & \varepsilon_0 & \varepsilon_1 & & \cdots & & & \varepsilon_t \end{bmatrix}$$

ve $\hbar_4^{+1}(U_R(x))$ üreteç matrisi ise

$$\begin{bmatrix} \varepsilon_0 & \varepsilon_1 & & \cdots & & & \varepsilon_t & 0 & 0 & \cdots & 0 \\ 0 & \varepsilon_0 & \varepsilon_1 & & & & & \varepsilon_t & 0 & \cdots & 0 \\ \vdots & & & & \ddots & & & & & & \vdots \\ 0 & & \cdots & 0 & \varepsilon_0 & \varepsilon_1 & & \cdots & & & \varepsilon_t \\ \rho_3(x) & & \cdots & & \rho_3(x) & & & \cdots & & & \rho_3(x) \end{bmatrix}$$

şeklindedir.

Teorem 4.2.1. C_3 (veya C_3^{+1}) kodu, $U_R(x)$ polinomu tarafından $\hbar_4(U_R(x))$ (veya $\hbar_4^{+1}(U_R(x))$) üreteç matrisi ile üretilirse, $\phi_1(C_3)$ (veya $\phi_1(C_3^{+1})$) ters sıralı bir $\mathbb{Z}_4$ – kod, $\vartheta(C_3)$ ve $\vartheta(C_3^{+1})$ kodları ise ters sıralı DNA kodlardır.

İspat. $U_R(x) = \varepsilon_0 + \varepsilon_1 x + \ldots + \varepsilon_t x^t$ birimsel ters sıralı polinomu için, tanımdan da görüleceği üzere, $\delta \in \{0, 1, \ldots, m-t-1\}$ için, $\hbar_4(U_R(x))$ üreteç matrisinin herhangi bir satırı $x^\delta U_R(x)$ olsun. Bu durumda polinomlar,

$$x^\delta U_R(x) = \varepsilon_0 x^\delta + \varepsilon_1 x^{\delta+1} + \ldots + \varepsilon_t x^{\delta+t}$$

ve

$$x^{m-t-\delta} U_R(x) = \varepsilon_0 x^{m-t-\delta} + \varepsilon_1 x^{m-t-\delta+1} + \ldots + \varepsilon_t x^{m-\delta}$$

şeklinde yazılabilir. Bu polinomlar herhangi bir $q \in \mathbb{Z}_4^*$ skaleri ile çarpıldığında,

$$qx^{\delta}U_R(x) = q\varepsilon_0 x^{\delta} + q\varepsilon_1 x^{\delta+1} + \ldots + q\varepsilon_t x^{\delta+t}$$

ve

$$qx^{m-t-\delta}U_R(x) = q\varepsilon_0 x^{m-t-\delta} + q\varepsilon_1 x^{m-t-\delta+1} + \ldots + q\varepsilon_t x^{m-\delta}$$

elde edilir. Bu durumda, ε_i 'lerin seçiminden dolayı

$$\phi_1\left(\left(qx^{\delta}U_R(x)\right)\right)^R = \phi_1\left(qx^{m-t-\delta-1}U_R(x)\right)$$

eşitliğine ulaşılır. $\vartheta = \eta o \phi_1$ olduğundan ve $\mathbb{Z}_4 -$ tersleri bulunduğundan istenildiği şekilde DNA tersleri de bulunabilir. Böylece,

$$\vartheta\left(qx^{\delta}U_R(x)\right)^R = \vartheta\left(qx^{m-t-\delta}U_R(x)\right)$$

eşitliğine ulaşılır.

Not 4.2.1. Tamlayan DNA kodları için; DNA bazları $\mathbb{Z}_4$ elemanlara karşılık gelen bir kurala sahiptir. Örneğin; 1 ve 3 seçildiğinde birbirinin tamlayanı olur. Ayrıca 0 ve 2 de birbirinin tamlayanıdır. Bu bilgiden hareketle, $\hbar_4\left(U_R(x)\right)$ $\hbar_4\left(U_R(x)\right)$üreteç matrisine tüm bileşenleri 2 olan bir satır eklendiğinde, tanımlanan DNA kuralı kullanarak ters sıralı ve tamlayan DNA kod elde edilebilir.

Örnek 4.2.2. T_3 halkası üzerinde uzunluğu 8 olan bir $U_R(x) = (2u+3) + (u^2+u+1)x + (3u^2+u+3)x^2 + 2x^3 + (2u^2+1)x^4 + (3u^2+u+1)x^5 + (2u^2+2u+3)x^6$ birimsel ters sıralı polinomu ele alınsın. Bu polinomun $\hbar_4\left(U_R(x)\right)$ üreteç matrisi,

$$\begin{bmatrix} 2u+3 & u^2+u+1 & 3u^2+u+3 & 2 & 2u^2+1 & 3u^2+u+1 & 2u^2+2u+3 & 0 \\ 0 & 2u+3 & u^2+u+1 & 3u^2+u+3 & 2 & 2u^2+1 & 3u^2+u+1 & 2u^2+2u+3 \end{bmatrix}$$

$\hbar_4^{+1}\left(U_R(x)\right)$ üreteç matrisi ise

$$\begin{bmatrix} 2u+3 & u^2+u+1 & 3u^2+u+3 & 2 & 2u^2+1 & 3u^2+u+1 & 2u^2+2u+3 & 0 \\ 0 & 2u+3 & u^2+u+1 & 3u^2+u+3 & 2 & 2u^2+1 & 3u^2+u+1 & 2u^2+2u+3 \\ 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 \end{bmatrix}$$

şeklindedir. Buradan

$$\phi_1\left(\hbar_4\left(U_R(x)\right)\right)=\begin{bmatrix} 1 & 3 & 1 & 3 & 1 & 3 & 2 & 2 & 3 & 1 & 3 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 & 1 & 3 & 1 & 3 & 2 & 2 & 3 & 1 & 3 & 1 & 3 & 1 \end{bmatrix}$$

ve

$$\phi_1\left(\hbar_4^{+1}\left(U_R(x)\right)\right)=\begin{bmatrix} 1 & 3 & 1 & 3 & 1 & 3 & 2 & 2 & 3 & 1 & 3 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 & 1 & 3 & 1 & 3 & 2 & 2 & 3 & 1 & 3 & 1 & 3 & 1 \\ 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 \end{bmatrix}$$

elde edilir. $\hbar_4\left(U_R(x)\right)$ ve $\hbar_4^{+1}\left(U_R(x)\right)$ üreteç matrislerindeki satırlar bir $q\in\mathbb{Z}_4^*$ skaleri ile çarpıldığında birinci satır ile ikinci satır birbirinin ters sıralısıdır. Örneğin; $\phi_1\left(\hbar_4\left(U_R(x)\right)\right)$ matrisi 3 ile çarpıldığında,

$$\begin{bmatrix} 3 & 1 & 3 & 1 & 3 & 1 & 2 & 2 & 1 & 3 & 1 & 3 & 1 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 & 3 & 1 & 3 & 1 & 2 & 2 & 1 & 3 & 1 & 3 & 1 & 3 \end{bmatrix}$$

matrisi elde edilmektedir. Buradan birinci ve ikinci satırın birbirinin ters sıralısı olduğu açık bir şekilde görülmektedir.

$\phi_1\left(\hbar_4\left(U_R(x)\right)\right)$ üreteç matrisindeki birinci ve ikinci satırlar toplandığında elde edilen

$$[1 \quad 3 \quad 2 \quad 2 \quad 2 \quad 2 \quad 3 \quad 1 \quad 1 \quad 3 \quad 2 \quad 2 \quad 2 \quad 2 \quad 3 \quad 1]$$

dizi palindromiktir. Yani bu dizinin ters sıralısının kendisine eşit olduğu söylenir.

$\hbar_4\left(U_R\left(x\right)\right)$ üreteç matrisine 2 satırının eklenmesiyle,

$$\begin{bmatrix} 2u+3 & u^2+u+1 & 3u^2+u+3 & 2 & 2u^2+1 & 3u^2+u+1 & 2u^2+2u+3 & 0 \\ 0 & 2u+3 & u^2+u+1 & 3u^2+u+3 & 2 & 2u^2+1 & 3u^2+u+1 & 2u^2+2u+3 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix}$$

matrisi elde edilmektedir. Bu matrisin $\mathbb{Z}_4$ görüntüsü ise,

$$\begin{bmatrix} 1 & 3 & 1 & 3 & 1 & 3 & 2 & 2 & 3 & 1 & 3 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 & 1 & 3 & 1 & 3 & 2 & 2 & 3 & 1 & 3 & 1 & 3 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix}$$

olmaktadır. Bu matrisin birinci ve üçüncü satır toplandığında elde edilen

$$[3 \quad 1 \quad 3 \quad 1 \quad 3 \quad 1 \quad 0 \quad 0 \quad 1 \quad 3 \quad 1 \quad 3 \quad 1 \quad 3 \quad 2 \quad 2]$$

dizisi birinci satırın tamlayanıdır. İkinci ve üçüncü satırı toplandığında elde edilen

$$[2 \quad 2 \quad 3 \quad 1 \quad 3 \quad 1 \quad 3 \quad 1 \quad 0 \quad 0 \quad 1 \quad 3 \quad 1 \quad 3 \quad 1 \quad 3]$$

dizisi ise ikinci satırın tamlayanı olmaktadır.

$\phi_1\left(\hbar_4^{+1}\left(U_R\left(x\right)\right)\right)$ üreteç matrisinde ise birinci ve üçüncü satırlar toplandığında elde edilen

$$[2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 3 \quad 1 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 3 \quad 1]$$

dizisi ile ikinci ve üçüncü satırlar toplandığında elde edilen

$$[1 \quad 3 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 1 \quad 3 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2]$$

dizisi birbirinin ters sıralısıdır. Herhangi bir $q \in \mathbb{Z}_4^*$ skaleri ile çarpılıp aynı kombinasyonlar uygulandığında da satırların birbirinin ters sıralısı olduğu açık bir şekilde görülecektir.

Örnek 4.2.3. T_3 halkası üzerinde 9 uzunluktaki bir birimsel ters sıralı polinom $U_R(x) = (2u^2+1) + 3x + (2u+1)x^2 + (u^2+3u+3)x^3 + (2u^2+3)x^4 + (2u+3)x^5$ olsun. Bu durumda, $U_R(x)$ polinomunun $\hbar_4(U_R(x))$ üreteç matrisi,

$$\begin{bmatrix} 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 & 0 & 0 & 0 \\ 0 & 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 & 0 & 0 \\ 0 & 0 & 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 & 0 \\ 0 & 0 & 0 & 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 \end{bmatrix}$$

ve $\hbar_4^{+1}(U_R(x))$ üreteç matrisi ise

$$\begin{bmatrix} 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 & 0 & 0 & 0 \\ 0 & 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 & 0 & 0 \\ 0 & 0 & 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 & 0 \\ 0 & 0 & 0 & 2u^2+1 & 3 & 2u+1 & u^2+3u+3 & 2u^2+3 & 2u+3 \\ 3 & 3 & 3 & 3 & 2 & 1 & 1 & 1 & 1 \end{bmatrix}$$

şeklindedir. Bu matrislerin $\mathbb{Z}_4$ görüntüsü incelenirse,

$$\phi_1\left(\hbar_4\left(U_R(x)\right)\right)=\begin{bmatrix}3&1&3&1&3&1&1&3&1&3&1&3&0&0&0&0&0&0\\0&0&3&1&3&1&3&1&1&3&1&3&1&3&0&0&0&0\\0&0&0&0&3&1&3&1&3&1&1&3&1&3&1&3&0&0\\0&0&0&0&0&0&3&1&3&1&3&1&1&3&1&3&1&3\end{bmatrix}$$

ve

$$\phi_1\left(\hbar_4^{+1}\left(U_R(x)\right)\right)=\begin{bmatrix}3&1&3&1&3&1&1&3&1&3&1&3&0&0&0&0&0&0\\0&0&3&1&3&1&3&1&1&3&1&3&1&3&0&0&0&0\\0&0&0&0&3&1&3&1&3&1&1&3&1&3&1&3&0&0\\0&0&0&0&0&0&3&1&3&1&3&1&1&3&1&3&1&3\\3&1&3&1&3&1&3&1&2&2&1&3&1&3&1&3&1&3\end{bmatrix}$$

elde edilir.

$\phi_1\left(\hbar_4\left(U_R(x)\right)\right)$ ve $\phi_1\left(\hbar_4^{+1}\left(U_R(x)\right)\right)$ matrisleri herhangi bir $q\in\mathbb{Z}_4^*$ ile çarpıldığında birinci ile dördüncü satır; ikinci ile üçüncü satır birbirlerinin ters sıralısı olmaktadır. Örneğin; $\phi_1\left(\hbar_4\left(U_R(x)\right)\right)$ matrisi 3 ile çarpıldığında;

$$\begin{bmatrix}1&3&1&3&1&3&3&1&3&1&3&1&0&0&0&0&0&0\\0&0&1&3&1&3&1&3&3&1&3&1&3&1&0&0&0&0\\0&0&0&0&1&3&1&3&1&3&3&1&3&1&3&1&0&0\\0&0&0&0&0&0&3&1&3&1&3&1&1&3&1&3&1&3\end{bmatrix}$$

matrisi elde edilmektedir. Buradan birinci ile dördüncü satırın ve ikinci ile üçüncü satırın birbirlerinin ters sıralısı olduğu görülmektedir.

Yine $\phi_1\left(\hbar_4\left(U_R(x)\right)\right)$ matrisinde, birinci ve dördüncü satırlar toplandığında elde edilen

$$\begin{bmatrix}3&1&3&1&3&1&2&2&0&0&0&0&1&3&1&3&1&3\end{bmatrix}$$

dizisi ve ikinci ve üçüncü satırlar toplandığında elde edilen

$$[0 \quad 0 \quad 3 \quad 1 \quad 2 \quad 2 \quad 2 \quad 2 \quad 0 \quad 0 \quad 2 \quad 2 \quad 2 \quad 2 \quad 1 \quad 3 \quad 0 \quad 0]$$

dizisi palindromiktir. Böylece bu dizilerin ters sıralalılarının kendisine eşit olduğu söylenir.

$\phi_1\left(\hbar_4^{+1}\left(U_R(x)\right)\right)$ matrisinde birinci ve beşinci satırların toplanmasıyla elde edilen

$$[2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 0 \quad 0 \quad 3 \quad 1 \quad 2 \quad 2 \quad 1 \quad 3 \quad 1 \quad 3 \quad 1 \quad 3]$$

dizisi ile dördüncü ve beşinci satırların toplanmasıyla elde edilen

$$[3 \quad 1 \quad 3 \quad 1 \quad 3 \quad 1 \quad 2 \quad 2 \quad 1 \quad 3 \quad 0 \quad 0 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2]$$

dizisi birbirinin ters sıralısıdır. Ayrıca, ikinci ve beşinci satırların toplanmasıyla elde edilen

$$[3 \quad 1 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 3 \quad 1 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 1 \quad 3]$$

dizisi ile üçüncü ve beşinci satırların toplanmasıyla elde edilen

$$[3 \quad 1 \quad 3 \quad 1 \quad 2 \quad 2 \quad 2 \quad 2 \quad 1 \quad 3 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 1 \quad 3]$$

dizisi birbirlerinin ters sıralısıdır.

$\phi_1\left(\hbar_4\left(U_R(x)\right)\right)$ matrisi herhangi bir $q \in \mathbb{Z}_4^*$ ile çarpılıp aynı komine işlemleri yapıldığında satırların birbirinin ters sıralısı olduğu aşikar bir şekilde görülmektedir.

BÖLÜM 5. $\mathbb{Z}_4(\mathbb{Z}_4+u\mathbb{Z}_4)$ HALKASI ÜZERİNDEKİ DEVİRLİ VE AYKIRI DEVİRLİ KODLAR

Hata düzelten kodlar teorisinde dikkat çeken başlıklardan biri de karma alfabeler üzerinde çalışılan toplamsal (additive) kodlardır. Değişmeli bir grubun alt grubu olarak tanımlanan toplamsal kodlar ilk olarak Delsarte ve Levenshtein tarafından [75] çalışması ile ele alınmıştır. Borges ve ark. [76] numaralı çalışma ile $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kod olarak adlandırılan yeni bir hata düzelten kod sınıfı ortaya çıkarmıştır. Bileşenleri ikili ve dörtlü alfabeden oluşan bu kod sınıfı son zamanlarda birçok araştırmacının odağı haline gelmiştir [76-82]. Aydoğdu ve ark. [80] numaralı çalışmada, $\mathbb{Z}_2\mathbb{Z}_2[u]-$ lineer devirli, sabit devirli ve bu kodların duallerinin cebirsel yapısını inşa etmişlerdir. Ayrıca bu kodların tanımlanan Gray dönüşüm altındaki görüntülerini inceleyerek optimal kod parametresine yakın kod elde etmişlerdir. Melakhessou ve ark. [81] numaralı çalışmada, $u^2=0$ ve $q=p^s$ iken $\mathbb{Z}_q\left(\mathbb{Z}_q+u\mathbb{Z}_q\right)$ halkasındaki lineer aykırı sabit devirli kodları araştırmak için öncelikle $\mathbb{Z}_q+u\mathbb{Z}_q$ halkasındaki aykırı polinom halkalarını tanımlayarak bu halka üzerindeki aykırı sabit devirli kodları incelemişlerdir. Daha sonra $\mathbb{Z}_q\left(\mathbb{Z}_q+u\mathbb{Z}_q\right)$ halkasındaki lineer aykırı sabit devirli kodların cebirsel yapısını ele almışlardır. Bu halkanın üreteç polinomlarını ve geren kümelerini elde etmişlerdir. Ayrıca, halka üzerindeki aykırı sabit devirli kodların Gray görüntülerini incelemiş, double aykırı sabit devirli kodlara da değinmişlerdir. Buldukları yeni $\mathbb{Z}_4$ kodlar ile makaleyi güçlendirmişlerdir. Diao ve ark. [82] numaralı çalışmada, $v^2=v$ ve p asal iken $\mathbb{Z}_p\mathbb{Z}_p[v]$ halkasında toplamsal devirli kodların cebirsel yapısını ve dualliğini incelemişlerdir. Optimal kodlar elde etmiş, Singleton sınırına dayanarak maksimum uzaklığa ayrılabilir kodlara bazı örnekler sunmuşlardır. Ayrıca kuantum kodlara da değinerek örnekler sunmuşlardır.

Bu bölüm 6 kısımdan oluşmaktadır. İlk kısımda, halkanın yapısı incelenmiş ve toplamsal kodlar ile ilgili temel tanım ve teoremlere yer verilmiştir. İkinci kısımda, $\mathbb{Z}_4T_2-$devirli kodunun üreteç polinomu ve kodu geren en küçük küme tespit edilmiştir. Üçüncü kısımda, halka üzerindeki devirli kodlar ile tüm sabit devirli kodlar arasında kurulan izomorfizma yardımı ile halka üzerindeki sabit devirli kodların üreteç polinomuna ulaşılmıştır. Dördüncü kısımda, yeni bir Gray dönüşüm tanımlanarak $\mathbb{Z}_4T_2-$devirli ve sabit devirli kodların Gray görüntüleri incelenmiştir. Beşinci kısımda, halkadaki âşikar olmayan otomorfizma tanımlanmış ve sabit devirli kodlar için üreteç polinomu oluşturulmuştur. Altıncı bölümde ise yeni bir Gray dönüşüm tanımlanarak aykırı devirli ve aykırı $3-$sabit devirli kodun görüntüsü incelenmiştir.

5.1. $\mathbb{Z}_4R$ Halkasının Yapısı ve Temel Bilgiler

$T_2=\{r_0+ur_1 \ : \ r_0,r_1\in\mathbb{Z}_4,\ u^2=u\}=\{0,1,2,3,u,2u,3u,1+u,1+2u,1+3u,2+u,2+2u,2+3u,3+u,3+2u,3+3u\}$ halkası ilerleyen kısımlarda indislerin karışmaması açısından bölüm boyunca R ile temsil edilecektir.

$\mathbb{Z}_4R$ halkası birimli, değişmeli bir halkadır. 64 elemanlı olan $\mathbb{Z}_4R$ halkası birden fazla maksimal ideale sahip olduğundan aynı zamanda lokal olmayan bir halkadır. Frobenius olan $\mathbb{Z}_4R$ halkasının birimsel elemanları $\{(1,1),(1,3),(3,1),(3,3),(1,1+2u),(1,3+2u),(3,1+2u),(3,3+2u)\}$ şeklindedir. Halkanın maksimal idealleri, $\{(1,1+u),(1,2+u),(2,1)\}$ olup minimal idealleri ise $\{(0,2+2u),(0,2u),(2,0)\}$'dir.

α ve β pozitif tamsayılar olmak üzere $\alpha+\beta$ uzunluğundaki C kodunun ilk α bileşeni $\mathbb{Z}_4$ alfabesinden, son β bileşeni ise $\mathbb{Z}_4+u\mathbb{Z}_4$ alfabesinden olacak şekilde parçalanabiliyorsa bu koda $\mathbb{Z}_4R-$kodu adı verilir.

Bu şekilde tanımlanan kod $\mathbb{Z}_4{}^{\alpha}\times R^{\beta}$ halkasının bir $R-$alt modülü olur mu?

Öncelikle $\mathbb{Z}_4R$ halkası $\mathbb{Z}_4R=\{(e_1,e_2):e_1\in\mathbb{Z}_4,e_2\in R\}$ şeklinde tanımlansın. Bu halka bilinen toplama işlemine göre kapalıdır ancak $u\in R$ skaleri ile bilinen çarpma işlemine göre kapalı değildir. Bu durumda $\mathbb{Z}_4R$ halkası standart skaler ile çarpma işlemine göre $R-$modül olmaz. Bu halkayı $R-$modül yapmak ve halkanın cebirsel yapısını zenginleştirmek için skaler ile yeni bir çarpma işlemi aşağıdaki gibi tanımlanabilir. Bu çarpma işlemini oluşturmak için öncelikle

$$\eta:R\to\mathbb{Z}_4$$
$$r_0+ur_1\to r_0+r_1$$

dönüşümü tanımlanmalıdır. Bu durumda R halkasındaki elemanların η dönüşümü altındaki görüntüleri,

$$\eta(0)=\eta(1+3u)=\eta(2+2u)=\eta(3+u)=0,$$
$$\eta(1)=\eta(u)=\eta(2+3u)=\eta(3+2u)=1,$$
$$\eta(2)=\eta(1+u)=\eta(2u)=\eta(3+3u)=2,$$
$$\eta(3)=\eta(1+2u)=\eta(3u)=\eta(2+u)=3$$

şeklindedir.

$\forall r_0+ur_1,r_2+ur_3\in R$ için,

i. $\eta((r_0+ur_1)+(r_2+ur_3))=\eta((r_0+r_2)+u(r_1+r_3))=r_0+r_1+r_2+r_3$
$=\eta(r_0+ur_1)+\eta(r_2+ur_3)$

ii. $\eta((r_0+ur_1).(r_2+ur_3))=\eta(r_0r_2+u(r_0r_3+r_1r_2+r_1r_3))$
$=r_0r_2+r_0r_3+r_1r_2+r_1r_3=r_2(r_0+r_1)+r_3(r_0+r_1)$
$=(r_0+r_1)(r_2+r_3)=\eta(r_0+ur_1)\eta(r_2+ur_3)$

eşitlikleri sağlandığından tanımlanan η dönüşümü bir halka homomorfizmadır. Bu homomorfizma yardımı ile herhangi bir $(e_1,e_2)\in\mathbb{Z}_4R$ ve $r\in R$ için, skaler çarpım $r*(e_1,e_2)=(\eta(r)e_1,re_2)$ şeklinde tanımlanabilir.

Bu çarpım $r \in R$ ve $z = \left(e_1^{\,0}, e_1^{\,1}, \ldots, e_1^{\,\alpha-1}, e_2^{\,0}, e_2^{\,1}, \ldots, e_2^{\,\beta-1}\right) \in \mathbb{Z}_4^{\,\alpha} \times R^{\beta}$ olmak üzere

$$r * z = r * \left(e_1^{\,0}, e_1^{\,1}, \ldots, e_1^{\,\alpha-1}, e_2^{\,0}, e_2^{\,1}, \ldots, e_2^{\,\beta-1}\right)$$

$$= \left(\eta(r)e_1^{\,0}, \eta(r)e_1^{\,1}, \ldots, \eta(r)e_1^{\,\alpha-1}, re_2^{\,0}, re_2^{\,1}, \ldots, re_2^{\,\beta-1}\right)$$ şeklinde genişletilebilir.

Lemma 5.1.1. $\mathbb{Z}_4^{\,\alpha} \times R^{\beta}$ halkası yukarıda tanımlanan skaler ile çarpma işlemine göre bir $R-$modüldür.

İspat. $\forall a, b \in R$ ve $\forall (e_1, e_2), (e_3, e_4) \in \mathbb{Z}_4^{\,\alpha} \times R^{\beta}$ için,

i. $$a * \left[(e_1, e_2) + (e_3, e_4)\right] = a * (e_1 + e_3, e_2 + e_4)$$
$$= \left[\eta(a)(e_1 + e_3), a(e_2 + e_4)\right]$$
$$= \left[\eta(a)e_1 + \eta(a)e_3, ae_2 + ae_4\right]$$
$$= \left(\eta(a)e_1, ae_2\right) + \left(\eta(a)e_3, ae_4\right)$$
$$= a * (e_1, e_2) + a * (e_3, e_4)$$

ii. $$(a+b) * (e_1, e_2) = \left[\eta(a+b)e_1, (a+b)(e_2)\right]$$
$$= \left(\eta(a)e_1 + \eta(b)e_1, ae_2 + be_2\right)$$
$$= \left(\eta(a)e_1, ae_2\right) + \left(\eta(b)e_1, be_2\right)$$
$$= a * (e_1, e_2) + b * (e_1, e_2)$$

iii. $$a * \left[b * (e_1, e_2)\right] = a * \left[\eta(b)e_1, b(e_2)\right] = \left(\eta(a)\eta(b)e_1, ab(e_2)\right) = ab * (e_1, e_2)$$

iv. $$1_R * (e_1, e_2) = \left(\eta(1_R)e_1, 1_R e_2\right) = (e_1, e_2)$$

şartları sağlandığından $\mathbb{Z}_4^{\,\alpha} \times R^{\beta}$ halkası skaler ile çarpma işlemine göre bir $R-$modüldür.

Tanım 5.1.1. $\mathbb{Z}_4^{\,\alpha} \times R^{\beta}$ halkasının herhangi bir C alt kümesi $\mathbb{Z}_4^{\,\alpha} \times R^{\beta}$ halkasının bir $R-$alt modülü ise C koduna $\mathbb{Z}_4 R-$lineer kod adı verilir. Açıktır ki; C kodu, $\alpha = 0$ iken R üzerinde lineer kod, $\beta = 0$ iken $\mathbb{Z}_4$ üzerinde lineer kod olur.

C kodu $\mathbb{Z}_4R-$lineer kod olmak üzere, C kodunun ilk α koordinatı üzerindeki izdüşümü C_α ve son β koordinatı üzerindeki izdüşümü ise C_β olsun. İzdüşüm lineer bir dönüşüm olduğundan C_α kodu $\mathbb{Z}_4$ üzerinde α uzunluğunda, C_β kodu ise R üzerinde β uzunluğunda lineer bir koddur. C kodu C_α ve C_β kodlarının direkt çarpımı yani $C_\alpha \times C_\beta$ ise C kodu ayrıştırılabilirdir.

Tanım 5.1.2. Herhangi bir $z=\left(e_1^{\,0},e_1^{\,1},\ldots,e_1^{\,\alpha-1},e_2^{\,0},e_2^{\,1},\ldots,e_2^{\,\beta-1}\right)\in {\mathbb{Z}_4}^{\alpha}\times R^{\beta}$ için $\sigma(z)=\left(e_1^{\,\alpha-1},e_1^{\,0},\ldots,e_1^{\,\alpha-2},e_2^{\,\beta-1},e_2^{\,0},\ldots,e_2^{\,\beta-2}\right)\in {\mathbb{Z}_4}^{\alpha}\times R^{\beta}$ şeklinde bir devirsel öteleme operatörü tanımlansın. $\mathbb{Z}_4R-$lineer C kodu σ devirli öteleme opreatörü altında sabit kalıyorsa yani $\sigma(C)=C$ oluyorsa C koduna $\mathbb{Z}_4R-$devirli kod denir.

Koda daha fazla cebirsel özellik kazandırmak için kodsözler polinomlar ile temsil edilsin. ${\mathbb{Z}_4}^{\alpha}\times R^{\beta}$ halkasının elemanları ile $\mathbb{Z}_4[x]\Big/\langle x^{\alpha}-1\rangle \times R[x]\Big/\langle x^{\beta}-1\rangle$ halkasının elemanları arasında birebir eşleme

$$ {\mathbb{Z}_4}^{\alpha}\times R^{\beta}\rightarrow \mathbb{Z}_4[x]\Big/\langle x^{\alpha}-1\rangle \times R[x]\Big/\langle x^{\beta}-1\rangle $$

$$ \left(e_1^{\,0},e_1^{\,1},\ldots,e_1^{\,\alpha-1},e_2^{\,0},e_2^{\,1},\ldots,e_2^{\,\beta-1}\right)\rightarrow\left(e_1^{\,0}+e_1^{\,1}x+\ldots+e_1^{\,\alpha-1}x^{\alpha-1},e_2^{\,0}+e_2^{\,1}x+\ldots+e_2^{\,\beta-1}x^{\beta-1}\right) $$

dönüşümü ile verilecektir. Yukarıdaki dönüşüm altında C kodunun görüntüsü de C ile gösterilsin.

Bu bölümde, $\mathbb{Z}_4[x]\Big/\langle x^{\alpha}-1\rangle \times R[x]\Big/\langle x^{\beta}-1\rangle$ halkası $\Re_{\alpha,\beta}$ ile $\left(e_1^{\,0}+e_1^{\,1}x+\ldots+e_1^{\,\alpha-1}\right.$ $\left.x^{\alpha-1},e_2^{\,0}+e_2^{\,1}x+\ldots+e_2^{\,\beta-1}x^{\beta-1}\right)$ ifadesi ise $\left(e_1(x),e_2(x)\right)$ ile temsil edilecektir.

Tanım 5.1.3. $r(x)=r_0+r_1x+\ldots+r_tx^t\in R[x]$ ve $(e_1(x),e_2(x))\in R_{\alpha,\beta}$ elemanları için, $\eta(r(x))=\eta(r_0)+\eta(r_1)x+\ldots+\eta(r_t)x^t\in R[x]$ olmak üzere $r(x)*(e_1(x),e_2(x))$ çarpımı $r(x)*(e_1(x),e_2(x))=(\eta(r(x))e_1(x),r(x)e_2(x))$ şeklinde tanımlanabilir.

Teorem 5.1.1. $\Re_{\alpha,\beta}$ halkası yukarıda tanımlanan çarpma işlemine göre bir $R[x]-$ modüldür.

İspat. Her $a(x),b(x)\in R[x]$ ve her $(e_1(x),e_2(x)),(e_3(x),e_4(x))\in\Re_{\alpha,\beta}$ için,

i. $$\begin{aligned}a(x)*[(e_1(x),e_2(x))+(e_3(x),e_4(x))]&=a(x)*(e_1(x)+e_3(x),e_2(x)+e_4(x))\\&=[\eta(a(x))(e_1(x)+e_3(x)),a(x)(e_2(x)+e_4(x))]\\&=[\eta(a(x))e_1(x)+\eta(a(x))e_3(x),a(x)e_2(x)+a(x)e_4(x)]\\&=(\eta(a(x))e_1(x),a(x)e_2(x))+(\eta(a(x))e_3(x),a(x)e_4(x))\\&=a(x)*(e_1(x),e_2(x))+a(x)*(e_3(x),e_4(x))\end{aligned}$$

ii. $$\begin{aligned}(a(x)+b(x))*(e_1(x),e_2(x))&=[\eta(a(x)+b(x))e_1(x),(a(x)+b(x))(e_2(x))]\\&=(\eta(a(x))e_1(x)+\eta(b(x))e_1(x),a(x)e_2(x)+b(x)e_2(x))\\&=[(\eta(a(x))e_1(x),a(x)e_2(x))+(\eta(b(x))e_1(x),b(x)e_2(x))]\\&=a(x)*(e_1(x),e_2(x))+b(x)*(e_1(x),e_2(x))\end{aligned}$$

iii. $$\begin{aligned}a(x)*[b(x)*(e_1(x),e_2(x))]&=a(x)*[\eta(b(x))e_1(x),b(x)(e_2(x))]\\&=(\eta(a(x))\eta(b(x))e_1(x),a(x)b(x)e_2(x))\\&=a(x)b(x)*(e_1(x),e_2(x))\end{aligned}$$

iv. $1_{R[x]}*(e_1(x),e_2(x))=(\eta(1_{R[x]})e_1(x),1_{R[x]}e_2(x))=(e_1(x),e_2(x))$ elde edilir.

Böylece $\Re_{\alpha,\beta}$ halkası tanımlanan skaler çarpma işlemine göre bir $R[x]-$modüldür.

$\mathbb{Z}_4R-$devirli kodun polinom tanımı aşağıdaki gibidir.

Tanım 5.1.4. $\Re_{\alpha,\beta}$ halkasının boştan farklı bir alt kümesi olan C kümesi $\Re_{\alpha,\beta}$ halkasının bir alt grubu ve $z(x)=\left(e_1^{\,0}+e_1^{\,1}x+\ldots+e_1^{\,\alpha-1}x^{\alpha-1},e_2^{\,0}+e_2^{\,1}x+\ldots+e_2^{\,\beta-1}x^{\beta-1}\right)$ olacak şekilde herhangi bir $r\in R$ ve her $z(x)\in C$ elemanları için,

$$r\,x^{*}\left(e_1(x),e_2(x)\right)=r\,x^{*}\left(e_1^{\,0}+e_1^{\,1}x+\ldots+e_1^{\,\alpha-1}x^{\alpha-1},e_2^{\,0}+e_2^{\,1}x+\ldots+e_2^{\,\beta-1}x^{\beta-1}\right)$$
$$=\left(\eta(r)\left(e_1^{\,\alpha-1}+e_1^{\,0}x+\ldots+e_1^{\alpha-2}x^{\alpha-1}\right),r\left(e_2^{\,\beta-1}+e_2^{\,0}x+\ldots+e_2^{\beta-2}x^{\beta-1}\right)\right)$$

ifadesi de C kümesinin bir elemanı ise C kümesine $\mathbb{Z}_4R-$devirli kod denir.

Teorem 5.1.2. $\Re_{\alpha,\beta}$ halkasının boştan farklı bir alt kümesi olan C kodunun $\mathbb{Z}_4R-$devirli kod olması için gerek yeter koşul C kodunun $\Re_{\alpha,\beta}$ halkasının bir $R[x]-$alt modülü olmasıdır.

İspat. C kodunun $\mathbb{Z}_4R-$devirli kod ve $z(x)=\left(e_1(x),e_2(x)\right)\in C$ olduğu kabul edilsin. C kodu $\Re_{\alpha,\beta}$ halkasının bir alt grubu olduğundan C kodundan alınan $z_1(x)$ ve $z_2(x)$ kodsözleri için $z_1(x)-z_2(x)\in C$ elde edilir. C kodu $\mathbb{Z}_4R-$devirli kod olduğundan $x*z(x)\in C$ olduğu bilinmektedir. Aynı nedenden ötürü, $x*\left(x*z(x)\right)$ ifadesi $x*\left(x*z(x)\right)=x^2*z(x)\in C$ şeklinde yazılabilir. Benzer şekilde devam edilirse, sıfır ve sıfırdan büyük her i değeri için $x^i*z(x)\in C$ olur. C kodu lineer bir kod olduğundan $R[x]$ halkasından alınan her $r(x)$ polinomu için $r(x)*z(x)$ çarpımı yine C kodunun içine düşer. Böylece C kodunun $\Re_{\alpha,\beta}$ halkasının bir $R[x]-$alt modülü olduğu sonucuna ulaşılır. Diğer taraftan, C kodu $\Re_{\alpha,\beta}$ halkasının bir $R[x]-$

alt modülü olsun. Alt modül şartı gereğince, C kodu $\Re_{\alpha,\beta}$ halkasının bir alt grubudur. Ayrıca C kodundan alınan her $z(x)$ kodsözü ve $R[x]$ halkasından alınan her x için $x*z(x)$ çarpımı da yine C kodunun içine düşer. Buradan, C kodunun $\mathbb{Z}_4R-$devirli bir kod olduğu sonucuna varılır. □

5.2. $\mathbb{Z}_4R-$Devirli Kodun Üreteç Polinomu

[41] numaralı çalışma ile R halkası üzerindeki C_β devirli kodunun $C_\beta = uC_\Delta + (1+3u)C_\nabla$ şeklinde parçalandığı ve C_β devirli kodunun üreteç polinomu bilinmektedir. Bölüm boyunca C_β devirli kodunun üreteç polinomu $\kappa(x)$ ile temsil edilecektir.

$\mathbb{Z}_4R$ halkasında tek uzunluktaki C devirli kodunun üreteç polinomu oluşturulmadan önce bazı açıklamalar yapılsın.

C kodu $\mathbb{Z}_4R-$devirli kod, ve C kodundaki bir eleman $z(x)=(e_1(x),e_2(x))$ olsun. $\mathrm{X}=\left\{(e_1(x),0)\in C : e_1(x)\in \mathbb{Z}_4[x]\Big/\langle x^\alpha-1\rangle\right\}$ olsun. Bu durumda tanımlanan X kümesi C kodunun bir alt modülüdür.

Şimdi X kümesi $\mathbb{Z}_4[x]\Big/\langle x^\alpha-1\rangle$ bölüm halkasının bir ideali olduğu gösterilsin.

i. $s_1(x),s_2(x)\in \mathrm{X}$ için $(s_1(x),0),(s_2(x),0)\in C$ vardır. Böylece $(s_1(x),0)+(s_2(x),0)=(s_1(x)+s_2(x),0)\in C$ olur. X kümesinin tanımı gereği $s_1(x)+s_2(x)\in \mathrm{X}$ elde edilir.

ii. $p(x) \in \mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle$ ve $s(x) \in \mathrm{X}$ için $(s(x),0) \in C$ vardır. $p(x)(s(x),0) = (p(x)s(x),0) \in C$ olur. X kümesinin tanımı gereği $p(x)s(x) \in \mathrm{X} \bmod(x^\alpha - 1)$ elde edilir.

Böylece X kümesi $\mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle$ bölüm halkasının bir idealidir. Bu da X kümesinin devirli kod olduğu ve $x^\alpha - 1$ polinomunun böleni olduğu anlamına gelir. Buradan hareketle $e_1(x) \mid \langle x^\alpha - 1 \rangle$ olacak şekilde $\mathrm{X} = \langle e_1(x) \rangle$ ifadesi elde edilir.

Herhangi bir $(y(x),0) \in C$ için $y(x) \in \mathrm{X}$ olduğundan $y(x) = n(x)e_1(x)$ olacak şekilde $n(x) \in \mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle$ vardır. $(y(x),0) = (n(x)e_1(x),0) = n(x) * (e_1(x),0)$ olup $n(x) \in \mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle$ ve $(e_1(x),0) \in C$ olduğundan $\mathrm{X} = \langle (e_1(x),0) \rangle$ elde edilir. Böylece X kümesi, $\mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle$ halkasında $x^\alpha - 1$ polinomunun böleni tarafından üretilen bir ideal olarak yorumlanabilir.

$\Lambda = \left\{ e_2(x) \in R[x] / \langle x^\beta - 1 \rangle , (l(x), e_2(x)) \in C \, : \, l(x) \in \mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle \right\}$ olsun. Λ kümesi $R[x] / \langle x^\beta - 1 \rangle$ halkasının bir alt modülü olduğu gösterilsin.

i. $q_1(x), q_2(x) \in \Lambda$ için $(l_1(x), q_1(x)), (l_2(x), q_2(x)) \in C$ olacak şekilde $l_1(x), l_2(x) \in \mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle$ vardır. $(l_1(x), q_1(x)) + (l_2(x), q_2(x)) = (l_1(x) + l_2(x), q_1(x) + q_2(x)) \in C$ olduğundan $q_1(x) + q_2(x) \in \Lambda$ elde edilir.

ii. $r(x) \in R[x] / \langle x^{\beta} - 1 \rangle$ ve $(l(x), e_2(x)) \in C$ için $l(x) \in \mathbb{Z}_4[x] / \langle x^{\alpha} - 1 \rangle$ olmak üzere C kodu $R_{\alpha,\beta}$ halkasının $R[x]-$ alt modülü olduğundan $r(x) * (l(x), e_2(x)) = (\eta(r(x)) l(x), r(x) e_2(x)) \in C$ olur. Buradan $r(x) e_2(x) \bmod(x^{\beta} - 1) \in \Lambda$ ve $\eta(r(x)) l(x) \bmod(x^{\alpha} - 1) \in X$ elde edilir.

Böylece Λ kümesi $R[x] / \langle x^{\beta} - 1 \rangle$ halkasının bir alt modülüdür. Böylelikle $\Lambda = (l(x), e_2(x))$ olduğu söylenebilir.

Tüm bu açıklamalar doğrultusunda $\mathbb{Z}_4 R-$ devirli kodun üreteç polinomu aşağıdaki gibi inşa edilebilir.

Teorem 5.2.1. $C_{\beta} = \langle \kappa(x) \rangle$ olmak üzere $f(x), l(x) \in \mathbb{Z}_4[x] / \langle x^{\alpha} - 1 \rangle$ ve $\kappa(x) \in R[x] / \langle x^{\beta} - 1 \rangle$ olacak şekilde $f(x) \mid x^{\alpha} - 1$ iken $\mathbb{Z}_4 R$ halkasındaki C devirli kodunun üreteç polinomu,

$$C = \langle (f(x), 0), (l(x), \kappa(x)) \rangle$$

şeklindedir.

İspat. $C = \langle (f(x), 0), (l(x), \kappa(x)) \rangle$ olduğunu gösterebilmek için çift taraflı kapsama gösterilmelidir.

$\langle (f(x), 0), (l(x), \kappa(x)) \rangle \subseteq C$ olduğu aşikârdır. $C \subseteq \langle (f(x), 0), (l(x), \kappa(x)) \rangle$ olduğunu göstermek için ise, öncelikle $b(x) \in \mathbb{Z}_4^{\alpha}$ ve $t(x) \in R^{\beta}$ olmak üzere herhangi bir $(b(x), t(x)) \in C$ elemanı alınsın. $t(x) \in \Lambda$ olduğundan $t(x) = a(x) \kappa(x)$ olacak

şekilde bir $a(x)\in {R[x]}/{\langle x^{\beta}-1\rangle}$ ve $\kappa(x)\in\Lambda$ olduğundan $(l(x),\kappa(x))\in C$ olacak şekilde bir $l(x)\in {\mathbb{Z}_4[x]}/{\langle x^{\alpha}-1\rangle}$ vardır. Böylelikle,

$$(b(x),t(x))-a(x)*(l(x),\kappa(x))=(b(x),t(x))-(\eta(a(x))l(x),a(x)\kappa(x))$$
$$=(b(x)-\eta(a(x))l(x),t(x)-a(x)\kappa(x))$$

elde edilir. $t(x)=a(x)\kappa(x)$ ifadesi yerine yazıldığı takdirde bu ifade $(b(x)-\eta(a(x))l(x),0)$ ifadesine eşit olur ve böylece X kümesinin içine düşer. $(b(x)-\eta(a(x))l(x),0)\in \mathrm{X}$ olduğundan $(b(x)-\eta(a(x))l(x),0)=r(x)(f(x),0)$ olacak şekilde bir $r(x)\in {\mathbb{Z}_4[x]}/{\langle x^{\alpha}-1\rangle}$ vardır.

Bu durumda, $(b(x),t(x))=a(x)*(l(x),\kappa(x))+(b(x)-\eta(a(x))l(x),0)$
$$=a(x)*(l(x),\kappa(x))+r(x)(f(x),0)$$
ifadesi elde edilir. Böylece $C\subseteq\langle(f(x),0),(l(x),\kappa(x))\rangle$ sağlanır.

$\langle(f(x),0),(l(x),\kappa(x))\rangle\subseteq C$ ve $C\subseteq\langle(f(x),0),(l(x),\kappa(x))\rangle$ gösterildiği için $C=\langle(f(x),0),(l(x),\kappa(x))\rangle$ eşitliği mevcuttur. □

Lemma 5.2.1. $C=\langle(f(x),0),(l(x),\kappa(x))\rangle$ kodu $\mathbb{Z}_4R-$devirli kod ise $der(l(x))<der(f(x))$ olarak kabul edilebilir.

İspat. $der(l(x))\geq der(f(x))$ olduğu varsayılsın. Bu durumda, $l(x)=f(x)q_1(x)+r_1(x)$ olacak şekilde $0\leq der(r_1(x))\leq der(f(x))$ şartını sağlayan

$q_1(x), r_1(x) \in \mathbb{Z}_4[x] / \langle x^\alpha - 1 \rangle$ polinomları vardır. $l(x)$ polinomu üreteç polinomunda yerine yazılırsa,

$$\langle (f(x),0),(l(x),\kappa(x)) \rangle = \langle (f(x),0),(f(x)q_1(x)+r_1(x),\kappa(x)) \rangle$$
$$= \langle (f(x),0),(r_1(x),\kappa(x)) \rangle$$

olduğu görülür. Yani $der(l(x)) < der(f(x))$ olduğu kabul edilebilir. □

Lemma 5.2.2. $\kappa(x) = u\tau_1(x) + (1+3u)\tau_2(x)$ olmak üzere $\tau_1(x) \mid x^\beta - 1$ ve $\tau_2(x) \mid x^\beta - 1$ iken $C = \langle (f(x),0),(l(x),\kappa(x)) \rangle$ kodu $\mathbb{Z}_4R-$devirli kod olsun. Bu durumda $\kappa(x) \mid x^\beta - 1$ olmaktadır.

İspat. $\tau_1(x) \mid x^\beta - 1$ ve $\tau_2(x) \mid x^\beta - 1$ kabul edildiğinden $x^\beta - 1 = \tau_1(x)w_1(x) = \tau_2(x)w_2(x)$ olacak şekilde bir $w_1(x), w_2(x) \in R[x] / \langle x^\beta - 1 \rangle$ polinomları mevcuttur. Böylece, $x^\beta - 1$ polinomu $x^\beta - 1 = (u\tau_1(x) + (1+3u)\tau_2(x))(u\,w_1(x) + (1+3u)w_2(x))$ şeklinde yazılabildiğinden $\kappa(x) \mid x^\beta - 1$ olmaktadır. □

Lemma 5.2.3. $\kappa(x) = u\tau_1(x) + (1+3u)\tau_2(x)$ ve $x^\beta - 1 = \tau_1(x)w_1(x) = \tau_2(x)w_2(x)$ olmak üzere, $C = \langle (f(x),0),(l(x),\kappa(x)) \rangle$ kodu $\mathbb{Z}_4R-$devirli kod ise $f(x) \mid w_1(x)l(x)$ olacaktır.

İspat. Lemma 5.2.2.'den hareketle $x^\beta - 1 = \tau_1(x)w_1(x) = \tau_2(x)w_2(x)$ eşitliği de kullanılarak $(u\,w_1(x) + (1+3u)w_2(x)) * (l(x),\kappa(x))$ ifadesinin $(w_1(x)l(x),0)$

ifadesine eşit olduğu kolaylıkla görülmektedir. $\left(w_1(x)l(x),0\right)$ ifadesi de X kümesinin içine düştüğünden $f(x)\,|\,w_1(x)l(x)$ elde edilir. □

Teorem 5.2.2. $x^{\beta}-1=\tau_1(x)w_1(x)=\tau_2(x)w_2(x)$ olmak üzere $C=\langle(f(x),0),(l(x),\kappa(x))\rangle$ kodu (α,β) uzunluğunda $\mathbb{Z}_4R-$devirli kod ve

$$\wp_1=\bigcup_{i=0}^{\alpha-der(f(x))-1}\{x^i*(f(x),0)\},$$

$$\wp_2=\bigcup_{i=0}^{der(w_1(x))-1}\{x^i*(l(x),u\tau_1(x))\}$$

ve

$$\wp_3=\bigcup_{i=0}^{der(w_2(x))-1}\{x^i*(0,(1+3u)\tau_2(x))\}$$

olsun. Bu durumda $\wp=\wp_1\cup\wp_2\cup\wp_3$ kümesi C kodunu geren en küçük kümedir.

İspat. $C=\langle(f(x),0),(l(x),\kappa(x))\rangle$ olsun. $z(x)\in C$ ve $a_1(x),a_2(x)\in R[x]$ olacak şekilde bir $z(x)=a_1(x)*(f(x),0)+a_2(x)*(l(x),\kappa(x))$ polinomu mevcuttur.

Burada $der(a_1(x))<\alpha-der(f(x))-1$ ise $a_1(x)*(f(x),0)\in Span\wp_1$ elde edilir. Aksi takdirde bölme algoritması uygulanır. Bu durumda $s_1(x),r_1(x)\in R[x]$ polinomları için $0\le der(r_1(x))\le\alpha-der(f(x))-1$ olacak şekilde $a_1(x)=\dfrac{x^{\alpha}-1}{f(x)}s_1(x)+r_1(x)$ eşitliği vardır. Böylece,

$$a_1(x)*(f(x),0)=\left(\frac{x^{\alpha}-1}{f(x)}s_1(x)+r_1(x)\right)*(f(x),0)$$

$$=s_1(x)*\left(\frac{x^{\alpha}-1}{f(x)}f(x),0\right)+r_1(x)*(f(x),0)$$

$$=r_1(x)*(f(x),0)$$

elde edilir. Bu da $a_1(x)*(f(x),0)\in Span\wp_1$ anlamına gelir.

$i=0,1,\ldots,v$ iken $p_i=uq_i+(1+3u)n_i$ olacak şekilde $a_2(x)=p_0+p_1x+\ldots+p_vx^v$ olsun. Bu durumda $a_2(x)=u\left(q_0+q_1x+\ldots+q_vx^v\right)+(1+3u)\left(n_0+n_1x+\ldots+n_vx^v\right)$ elde edilir. Burada $q_0+q_1x+\ldots+q_vx^v$ polinomu $q(x)$ ile $n_0+n_1x+\ldots+n_vx^v$ polinomu ise $n(x)$ ile ifade edilirse $a_2(x)=u\,q(x)+(1+3u)n(x)$ eşitliği elde edilir. Böylece,

$$a_2(x)*(l(x),\kappa(x))=(u\,q(x)+(1+3u)n(x))*(l(x),\kappa(x))$$

$$=q(x)*(l(x),u\,\tau_1(x))+n(x)*(0,\,(1+3u)\tau_2(x))$$

elde edilir. Ayrıca $f(x)\,|\,w_1(x)l(x)$ olduğu da bilindiğinden $w_1(x)l(x)=f(x)k(x)$ şeklinde yazılabilir.

Eğer $der(n(x))\le der(w_1(x))-1$ ise $n(x)*(l(x),u\,\tau_1(x))\in Span\wp_2$ olduğu açıktır. Aksi takdirde bölme algoritması uygulanır. $0\le der(r_2(x))\le der(w_1(x))-1$ için $n(x)=w_1(x)s_2(x)+r_2(x)$ olacak şekilde $s_2(x),r_2(x)\in R[x]$ polinomları vardır. Bu durumda,

$$n(x)*(l(x),u\,\tau_1(x))=(w_1(x)s_2(x)+r_2(x))*(l(x),u\,\tau_1(x))$$

$$=s_2(x)*(w_1(x)l(x),\,0)+r_2(x)*(l(x),u\,\tau_1(x))$$

elde edilir. $w_1(x)l(x)$ ifadesinin $f(x)k(x)$ ifadesine eşitliği bilindiğinden $s_2(x)*(w_1(x)l(x),\,0)\in Span\wp_1$ ve $r_2(x)*(l(x),u\,\tau_1(x))\in Span\wp_2$ elde edilir.

Eğer $der(q(x)) \le der(w_2(x)) - 1$ ise $n(x) * (0, (1+3u)\tau_2(x)) \in Span\wp_3$ olduğu açıktır. Aksi takdirde bölme algoritması uygulanır. $0 \le der(r_3(x)) \le der(w_2(x)) - 1$ için $q(x) = w_2(x)s_3(x) + r_3(x)$ olacak şekilde $s_3(x), r_3(x) \in R[x]$ polinomları mevcuttur. Bu durumda,

$$\begin{aligned} q(x) * (0,(1+3u)\tau_2(x)) &= (w_2(x)s_3(x) + r_3(x)) * (0, (1+3u)\tau_2(x)) \\ &= s_3(x) * (0, (1+3u)\tau_2(x)w_2(x)) + r_3(x) * (0,(1+3u)\tau_2(x)) \\ &= r_3(x) * (0,(1+3u)\tau_2(x)) \end{aligned}$$

elde edilir. Bu da $r_3(x) * (0,(1+3u)\tau_2(x)) \in Span\wp_3$ olduğu anlamına gelir.

Böylece $\wp = \wp_1 \cup \wp_2 \cup \wp_3$ kümesi C kodu için geren küme olur. $\wp$ kümesindeki diğer elemanlar ile lineer bağımlı bir eleman mevcut olmadığından $\wp$ kümesine C kodu için kodu geren en küçük küme adı verilir. □

5.3. $\mathbb{Z}_4R$ Halkasında Sabit Devirli Kodlar

Tanım 5.3.1. Herhangi bir $z = (e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_2^{\beta-1}) \in \mathbb{Z}_4{}^{\alpha} \times R^{\beta}$ için $\rho_\lambda(z) = (e_1^{\alpha-1}, e_1^0, \ldots, e_1^{\alpha-2}, \lambda e_2^{\beta-1}, e_2^0, \ldots, e_2^{\beta-2}) \in \mathbb{Z}_4{}^{\alpha} \times R^{\beta}$ şeklinde bir sabit devirsel öteleme operatörü tanımlansın. $\mathbb{Z}_4R-$lineer C kodu ρ_λ devirli öteleme opreatörü altında sabit kalıyorsa yani $\rho_\lambda(C) = C$ oluyorsa C koduna $\mathbb{Z}_4R-$lineer sabit devirli kod denir.

Koda daha fazla cebirsel özellik kazandırmak için kodsözler polinomlar ile temsil edilsin. $\mathbb{Z}_4{}^{\alpha} \times R^{\beta}$ halkasının elemanları ile $\mathbb{Z}_4[x]/\langle x^\alpha - 1\rangle \times R[x]/\langle x^\beta - \lambda\rangle$ halkasının elemanları arasında birebir eşleme

$$\mathbb{Z}_4{}^{\alpha} \times R^{\beta} \to {\mathbb{Z}_4[x]}\Big/{\langle x^{\alpha}-1\rangle} \times {R[x]}\Big/{\langle x^{\beta}-\lambda\rangle}$$

$$\left(e_1{}^0, e_1{}^1, \ldots, e_1{}^{\alpha-1}, e_2{}^0, e_2{}^1, \ldots, e_2{}^{\beta-1}\right) \to \left(e_1{}^0 + e_1{}^1 x + \ldots + e_1{}^{\alpha-1}x^{\alpha-1}, \lambda e_2{}^0 + e_2{}^1 x + \ldots + e_2{}^{\beta-1}x^{\beta-1}\right)$$

dönüşümü ile verilecektir. Yukarıdaki dönüşüm altında C kodunun görüntüsü de C ile gösterilsin.

$\mathbb{Z}_4 R-$lineer sabit devirli kodun polinom tanımı aşağıdaki gibidir.

Tanım 5.3.2. $\Re_{\alpha,\beta_\lambda}$ halkasının boştan farklı bir alt kümesi olan C kümesi için $\Re_{\alpha,\beta_\lambda}$ halkasının bir alt grubu ve $z(x) = \left(e_1{}^0 + e_1{}^1 x + \ldots + e_1{}^{\alpha-1}x^{\alpha-1}, e_2{}^0 + e_2{}^1 x + \ldots + e_2{}^{\beta-1}x^{\beta-1}\right)$ olacak şekilde herhangi bir $r \in R$ ve her $z(x) \in C$ elemanları için,

$$\begin{aligned} r\,x^*\left(e_1(x), e_2(x)\right) &= r\,x^*\left(e_1{}^0 + e_1{}^1 x + \ldots + e_1{}^{\alpha-1}x^{\alpha-1}, e_2{}^0 + e_2{}^1 x + \ldots + e_2{}^{\beta-1}x^{\beta-1}\right) \\ &= \left(\eta(r)\left(e_1{}^{\alpha-1} + e_1{}^0 x + \ldots + e_1^{\alpha-2}x^{\alpha-1}\right), r\left(\lambda e_2{}^{\beta-1} + e_2{}^0 x + \ldots + e_2^{\beta-2}x^{\beta-1}\right)\right) \end{aligned}$$

ifadesi de C kümesinin bir elemanı ise C kümesine $\mathbb{Z}_4 R-$lineer sabit devirli kod denir.

Bu kısımda $\mathbb{Z}_4 R$ halkasındaki sabit devirli kodlar ele alınırken, devirli kodların tanımlandığı halka ile sabit devirli kodları temsil eden halka arasında bir izomorfizma kurulacaktır. Sabit devirli kodların üreteç polinomu oluşturulurken devirli kodlarda olduğu gibi tek uzunluktaki kodlar çalışılacaktır. Öncelikle R halkasındaki birimsel elemanların tek kuvvetinin kendisi, çift kuvvetlerinin ise 1 olduğu hatırlatılarak aşağıdaki gibi bir izomorfizma kurulsun.

Önerme 5.3.1. β tek tamsayı, R halkasındaki birimsel elemanlar da λ ile temsil edilmek üzere,

$$\Omega : \mathbb{Z}_4[x]/\langle x^\alpha - 1\rangle \times R[x]/\langle x^\beta - 1\rangle \rightarrow \mathbb{Z}_4[x]/\langle x^\alpha - 1\rangle \times R[x]/\langle x^\beta - \lambda\rangle$$

$$\Omega\left(e_1(x), e_2(x)\right) = \left(e_1(x), e_2(\lambda x)\right)$$

dönüşümü tanımlansın. Bu durumda Ω dönüşümü bir halka izomorfizmasıdır.

İspat. Birebirlik, örtenlik, iyi tanımlılık ve halka homomorfizma olduğu gösterildiği takdirde Ω dönüşümünün halka izomorfizması olduğu ispatlanmış olur. Buradan hareketle,

$e_1(x) = e_1^0 + e_1^1 x + \ldots + e_1^{\alpha-1} x^{\alpha-1}$, $e_2(x) = e_2^0 + e_2^1 x + \ldots + e_2^{\beta-1} x^{\beta-1}$, $e_3(x) = e_3^0 + e_3^1 x + \ldots + e_3^{\alpha-1} x^{\alpha-1}$ ve $e_4(x) = e_4^0 + e_4^1 x + \ldots + e_4^{\beta-1} x^{\beta-1}$ olmak üzere,

<u>İyi tanımlılık</u>: Her $\left(e_1(x), e_2(x)\right), \left(e_3(x), e_4(x)\right) \in \Re_{\alpha,\beta}$ için, $\left(e_1(x), e_2(x)\right) = \left(e_3(x), e_4(x)\right) \bmod\left(x^\alpha - 1\right) \times \left(x^\beta - 1\right)$ iken $\Omega\left(e_1(x), e_2(x)\right) = \Omega\left(e_3(x), e_4(x)\right) \bmod\left(x^\alpha - 1\right) \times \left(x^\beta - \lambda\right)$ olmalıdır.

$\left(e_1(x), e_2(x)\right) = \left(e_3(x), e_4(x)\right) \bmod\left(x^\alpha - 1\right) \times \left(x^\beta - 1\right)$ ise $\left(e_1^0 + e_1^1 x + \ldots + e_1^{\alpha-1} x^{\alpha-1}, e_2^0 + e_2^1 x + \ldots + e_2^{\beta-1} x^{\beta-1}\right) = \left(x^{\alpha-1}, x^{\beta-1}\right) q(x) + \left(e_3^0 + e_3^1 x + \ldots + e_3^{\alpha-1} x^{\alpha-1}, e_4^0 + e_4^1 x + \ldots + e_4^{\beta-1} x^{\beta-1}\right)$ şeklinde yazılır. Bu ifadede x yerine λx yazıldığı takdirde, $\left(e_1^{\alpha-1} + e_1^0 x + \ldots + e_1^{\alpha-2} x^{\alpha-1}, e_2^{\beta-1} + e_2^0 x + \ldots + e_2^{\beta-2} x^{\beta-1}\right) = \left(\lambda^\alpha x^\alpha - 1, \lambda^\beta x^\beta - 1\right) q(\lambda x) + \left(e_3^{\alpha-1} + e_3^0 x + \ldots + e_3^{\alpha-2} x^{\alpha-1}, e_4^{\beta-1} + e_4^0 x + \ldots + e_4^{\beta-2} x^{\beta-1}\right)$ elde edilir. α ve β tek tamsayı olduğundan bu ifade $\left(\lambda x^\alpha - \lambda^2, \lambda x^\beta - \lambda^2\right) q(\lambda x) + \left(e_3^{\alpha-1} + e_3^0 x + \ldots + e_3^{\alpha-2} x^{\alpha-1}, e_4^{\beta-1} + e_4^0 x + \ldots + e_4^{\beta-2} x^{\beta-1}\right) = \lambda \left(x^\alpha - \lambda, x^\beta - \lambda\right) q(\lambda x) + \left(e_3^{\alpha-1} + e_3^0 x + e_3^{\alpha-2} x^{\alpha-1}, e_4^{\beta-1} + e_4^0 x + \ldots + e_4^{\beta-2} x^{\beta-1}\right)$ ifadesine eşit olur. Böylece $\left(e_1(\lambda x), e_2(\lambda x)\right) = \lambda \left(x^\alpha - \lambda, x^\beta - \lambda\right) q(\lambda x) + \left(e_3(\lambda x), e_4(\lambda x)\right)$ elde

edilir. Bu da $\Omega(e_1(x),e_2(x))=\Omega(e_3(x),e_4(x)) \mod(x^\alpha-1)\times(x^\beta-\lambda)$ anlamına gelir. Buradan Ω dönüşümünün iyi tanımlı bir dönüşüm olduğu gösterilmiş olur.

Birebirlik: Her $(e_1(x),e_2(x)),(e_3(x),e_4(x))\in\Re_{\alpha,\beta}$ için, $\Omega(e_1(x),e_2(x))=\Omega(e_3(x),e_4(x)) \mod(x^\alpha-1)\times(x^\beta-\lambda)$ iken $(e_1(x),e_2(x))=(e_3(x),e_4(x)) \mod(x^\alpha-1)\times(x^\beta-1)$ olur mu?

$\Omega(e_1(x),e_2(x))=\Omega(e_3(x),e_4(x)) \mod(x^\alpha-1)\times(x^\beta-\lambda)$ yani $(e_1(x),e_2(\lambda x))=(e_3(x),e_4(\lambda x)) \mod(x^\alpha-1)\times(x^\beta-\lambda)$ ise $(e_1(x),e_2(\lambda x))=(x^\alpha-1,x^\beta-\lambda)q(\lambda x)+(e_3(x),e_4(\lambda x)) \mod(x^\alpha-1)\times(x^\beta-\lambda)$ şeklinde yazılır. Bu ifadede x yerine λx yazıldığı takdirde, $(e_1(x),e_2(\lambda x))=(\lambda^\alpha x^\alpha-1,\lambda^\beta x^\beta-\lambda)q(x)+(e_3(x),e_4(x))$ $=\lambda(x^\alpha-1,x^\beta-1)q(x)+(e_3(x),e_4(x)) \mod(x^\alpha-1)\times(x^\beta-1)$ elde edilir. Bu da Ω dönüşümünün birebir bir dönüşüm olduğu anlamına gelir.

Örtenlik: Ω dönüşümü sonlu ve birebir olduğundan örten bir dönüşümdür.

Homomorfizma: Her $(e_1(x),e_2(x)),(e_3(x),e_4(x))\in\Re_{\alpha,\beta}$ için, $\Omega((e_1(x),e_2(x))+(e_3(x),e_4(x)))=\Omega(e_1(x),e_2(x))+\Omega(e_3(x),e_4(x))$ ve $\Omega((e_1(x),e_2(x)).(e_3(x),e_4(x)))=\Omega(e_1(x),e_2(x)).\Omega(e_3(x),e_4(x))$ eşitlikleri sağlanmalıdır.

$$\begin{aligned}\Omega(e_1(x),e_2(x))+\Omega(e_3(x),e_4(x))&=\Omega((e_1(x),e_2(x)),(e_3(x),e_4(x)))\\&=\Omega((e_1+e_3)(x),(e_2+e_4)(x))\\&=((e_1+e_3)(x),(e_2+e_4)(\lambda x))\\&=((e_1(x)+e_3(x)),(e_2(\lambda x)+e_4(\lambda x)))\end{aligned}$$

$$= \left(\left(e_1(x), e_2(\lambda x) \right) + \left(e_3(x), e_4(\lambda x) \right) \right)$$

$$= \Omega\left(\left(e_1(x), e_2(x) \right) + \Omega\left(e_3(x), e_4(x) \right) \right)$$

elde edilir.

$$\Omega\left(\left(e_1(x), e_2(x) \right).\left(e_3(x), e_4(x) \right) \right) = \Omega\left(\left(e_1(x), e_3(x) \right), \left(e_2(x), e_4(x) \right) \right)$$

$$= \Omega\left(\left(e_1 e_3 \right)(x), \left(e_2 e_4 \right)(x) \right)$$

$$= \left(\left(e_1 e_3 \right)(x), \left(e_2 e_4 \right)(\lambda x) \right)$$

$$= \left(\left(e_1(x) e_3(x) \right), \left(e_2(\lambda x) e_4(\lambda x) \right) \right)$$

$$= \left(\left(e_1(x), e_2(\lambda x) \right).\left(e_3(x), e_4(\lambda x) \right) \right)$$

$$= \Omega\left(\left(e_1(x), e_2(x) \right).\Omega\left(e_3(x), e_4(x) \right) \right)$$

elde edilir. Dolayısıyla Ω dönüşümü bir halka homomorfizmadır.

Ω dönüşümü iyi tanımlılık, birebirlik, örtenlik ve halka homomorfizma özelliklerini sağladığından bir halka izomorfizması olur. □

Bu önermeden yararlanarak aşağıdaki sonuç elde edilir.

Sonuç 5.3.1. Yukarıdaki önermeden yararlanarak $\Re_{\alpha,\beta}$ halkasının idealleri ile $\mathbb{Z}_4[x] \Big/ \langle x^\alpha - 1 \rangle \times R[x] \Big/ \langle x^\beta - \lambda \rangle$ halkasının idealleri arasında birebir bir ilişki vardır.

Bölüm boyunca $\mathbb{Z}_4[x] \Big/ \langle x^\alpha - 1 \rangle \times R[x] \Big/ \langle x^\beta - \lambda \rangle$ halkası $\Re_{\alpha,\beta_\lambda}$ ile temsil edilecektir. Toplamsal sabit devirli kodları ele alabilmek için öncelikle aşağıdaki teoremlere ihtiyaç duyulacaktır.

Teorem 5.3.1. $\Re_{\alpha,\beta_\lambda}$ halkası Tanım 5.1.3'te tanımlanan çarpma işlemine göre bir $R[x]-$modüldür.

Teorem 5.3.2. $C \subseteq \Re_{\alpha,\beta_\lambda}$ kodunun $\lambda-$sabit devirli $\mathbb{Z}_4R-$kod olması için gerek ve yeter koşul C kodunun $\Re_{\alpha,\beta_\lambda}$ halkasının bir $R[x]-$alt modülü olmasıdır.

Not 5.3.1. Teorem 5.3.1. ve Teorem 5.3.2.'nin ispatları, tanımlanan Ω izomorfizması göz önünde bulundurularak Teorem 5.1.1. ve Teorem 5.1.2.'nin ispatlarına benzer şekilde yapılır.

Sonuç 5.3.2. J'nin $\Re_{\alpha,\beta}$ halkasının bir ideali olması durumunda $\Omega(J)$ de $\Re_{\alpha,\beta_\lambda}$ halkasının bir idealidir. Tersi de geçerlidir.

Teorem 5.2.1. ve Ω halka izomorfizması kullanılarak $\Re_{\alpha,\beta_\lambda}$ halkası üzerindeki $\lambda-$sabit devirli kodların üreteç polinomu aşağıdaki gibi ifade edilir.

Teorem 5.3.3. $\tilde{x}=\lambda x$ ve $C_\beta=\langle\kappa(\tilde{x})\rangle$ olmak üzere, $f(x),l(x)\in \mathbb{Z}_4[x]/\langle x^\alpha-1\rangle$ ve $\kappa(\tilde{x})\in R[x]/\langle x^\beta-\lambda\rangle$ olacak şekilde $f(x)\mid x^\alpha-1$ ve $\kappa(\tilde{x})\mid x^\beta-\lambda$ iken $\mathbb{Z}_4R$ halkasındaki $\lambda-$sabit devirli C kodunun üreteç polinomu,

$$C=\langle(f(x),0),(l(x),\kappa(\tilde{x}))\rangle$$

şeklindedir.

Teorem 5.3.4. C_α kodu $\mathbb{Z}_4$ üzerinde uzunluğu α olan lineer bir kod, C_β kodu R halkası üzerinde uzunluğu β olan lineer bir kod, $C=C_\alpha\times C_\beta$ kodu ise $\mathbb{Z}_4R$ halkasında lineer bir kod olsun. Bu durumda,

i. C kodunun devirli kod olması için gerek ve yeter koşul C_α kodunun $\mathbb{Z}_4$ üzerinde, C_β kodunun da R halkası üzerinde devirli kod olmasıdır.

ii. $\lambda = 3,1+2u,3+2u$ olmak üzere, C kodunun $\lambda-$sabit devirli kod olması için gerek ve yeter koşul C_α kodunun $\mathbb{Z}_4$ üzerinde devirli kod, C_β kodunun da R halkası üzerinde $\lambda-$sabit devirli kod olmasıdır.

İspat. Öncelikle $\mathbb{Z}_4R$ halkasındaki $C = C_\alpha \times C_\beta$ kodu sabit devirli bir kod olması durumunda C_α kodunun $\mathbb{Z}_4$ üzerinde devirli, C_β kodunun ise R halkası üzerinde $\lambda-$sabit devirli bir kod olduğu gösterilsin. $\left(e_1^0, e_1^1, \ldots, e_1^{\alpha-1}\right) \in C_\alpha$ ve $\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) \in C_\beta$ olmak üzere, C kodu $\lambda-$sabit devirli bir kod ise tanım gereği $\left(e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) \in C$ iken $\left(e_1^{\alpha-1}, e_1^0, \ldots, e_1^{\alpha-2}, \lambda e_2^{\beta-1}, e_2^0, \ldots, e_2^{\beta-2}\right) \in C$ olur. Bu da $\left(e_1^{\alpha-1}, e_1^0, \ldots, e_1^{\alpha-2}\right) \in C_\alpha$ ve $\left(\lambda e_2^{\beta-1}, e_2^0, \ldots, e_2^{\beta-2}\right) \in C_\beta$ olması demektir. $\left(e_1^0, e_1^1, \ldots, e_1^{\alpha-1}\right) \in C_\alpha$ iken $\left(e_1^{\alpha-1}, e_1^0, \ldots, e_1^{\alpha-2}\right) \in C_\alpha$ olduğundan C_α kodu $\mathbb{Z}_4$ üzerinde devirli bir koddur. $\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) \in C_\beta$ iken $\left(\lambda e_2^{\beta-1}, e_2^0, \ldots, e_2^{\beta-2}\right) \in C_\beta$ olduğundan C_β kodu R halkası üzerinde $\lambda-$sabit devirli koddur. Burada $\lambda = 1$ olması durumunda (i) şıkkı, $\lambda = 3,\ 1+2u,\ 3+2u$ olması durumunda ise (ii) şıkkı ispatlanmış olur. Tersi de benzer şekilde gösterilir. □

5.4. $\mathbb{Z}_4R$ Halkasındaki Devirli ve Sabit Devirli Kodların Gray Görüntüsü

R halkasından $\mathbb{Z}_4^2$ yapısına aşağıdaki gibi bir Gray dönüşüm tanımlansın.

$$\varpi_1 : R \to \mathbb{Z}_4^2$$
$$e_2 = r_0 + ur_1 \to \left(r_0 + r_1, 3r_0 + 3r_1\right)$$

Tanımlanan bu dönüşüm R^β yapısından $\mathbb{Z}_4^{2\beta}$ yapısına genişletilirse,

$$\varpi_1 : R^\beta \to \mathbb{Z}_4^{2\beta}$$

$$\left(e_2{}^0, e_2{}^1, \ldots, e_2{}^{\beta-1}\right) \to \begin{pmatrix} r_0{}^0 + r_1{}^0, r_0{}^1 + r_1{}^1, \ldots, r_0{}^{\beta-1} + r_1{}^{\beta-1}, \\ 3r_0{}^0 + 3r_1{}^0, 3r_0{}^1 + 3r_1{}^1, \ldots, 3r_0{}^{\beta-1} + 3r_1{}^{\beta-1} \end{pmatrix}$$

elde edilir.

Teorem 5.4.1. Tanımlanan ϖ_1 dönüşümü $\left(R^\beta, \text{Lee uzaklık}\right) \to \left(R^\beta, \text{Hamming uzaklık}\right)$ uzaklığı koruyan lineer bir dönüşümdür.

İspat. $t_1 = a_1 + ub_1$ ve $t_2 = a_2 + ub_2$ olmak üzere,

$$\begin{aligned} \varpi_1\left(yt_1 + kt_2\right) &= \varpi_1\left(ya_1 + uyb_1 + ka_2 + ukb_2\right) = \varpi_1\left(ya_1 + ka_2 + u\left(yb_1 + kb_2\right)\right) \\ &= \left(ya_1 + ka_2 + yb_1 + kb_2, 3ya_1 + 3ka_2 + 3yb_1 + 3kb_2\right) \\ &= \left(y\left(a_1 + b_1\right) + k\left(a_2 + b_2\right), y\left(3a_1 + 3b_1\right) + k\left(3a_2 + 3b_2\right)\right) \\ &= y\left(a_1 + b_1, 3a_1 + 3b_1\right) + k\left(a_2 + b_2, 3a_2 + 3b_2\right) == y\varpi_1\left(t_1\right) + k\varpi_1\left(t_2\right) \end{aligned}$$

eşitliği sağlandığından ϖ_1 dönüşümü lineer bir dönüşüm olur.

$$\begin{aligned} d_L\left(t_1, t_2\right) = w_L\left(t_1 - t_2\right) &= w_L\left(a_1 - a_2 + u\left(b_1 - b_2\right)\right) \\ &= w_H\left(\varpi_1\left(\left(a_1 - a_2\right) + u\left(b_1 - b_2\right)\right)\right) \\ &= w_H\left(a_1 - a_2 + b_1 - b_2, 3a_1 - 3a_2 + 3b_1 - 3b_2\right) \\ &= w_H\left(\left(a_1 + b_1, 3a_1 + 3b_1\right) - \left(a_2 + b_2, 3a_2 + 3b_2\right)\right) \\ &= w_H\left(\varpi_1\left(a_1 + ub_1\right) - \varpi_1\left(a_2 + ub_2\right)\right) \\ &= w_H\left(\varpi_1\left(t_1\right) - \varpi_1\left(t_2\right)\right) = d_H\left(\varpi_1\left(t_1\right), \varpi_1\left(t_2\right)\right) \end{aligned}$$

olduğundan uzaklık korunur.

Böylece ϖ_1 Gray dönüşümü $\left(R^\beta, \text{Lee uzaklık}\right) \to \left(R^\beta, \text{Hamming uzaklık}\right)$ uzaklığı koruyan lineer bir dönüşümdür. □

Buradan hareketle $\mathbb{Z}_4 R$ halkasından $\mathbb{Z}_4^3$ yapısına aşağıdaki gibi bir Gray dönüşüm tanımlanabilir.

$$\partial : \mathbb{Z}_4 R \to \mathbb{Z}_4^3$$
$$(e_1, e_2) \to (e_1, \varpi_1(e_2))$$

$e_2 = r_0 + ur_1$ olduğu hatırlatılarak, ∂ fonksiyonu $\mathbb{Z}_4^{\alpha} R^{\beta}$ yapısından $\mathbb{Z}_4^{\alpha+2\beta}$ yapısına aşağıdaki gibi genişletilebilir.

$$\partial : \mathbb{Z}_4{}^{\alpha} R^{\beta} \to \mathbb{Z}_4{}^{\alpha+2\beta}$$
$$\partial\left(e_1{}^0, e_1^1, \ldots, e_1{}^{\alpha-1}, e_2{}^0, e_2^1, \ldots, e_2{}^{\beta-1}\right) \to \begin{pmatrix} e_1{}^0, e_1^1, \ldots, e_1{}^{\alpha-1}, r_0{}^0 + r_1^0, r_0^1 + r_1^1, \ldots, r_0{}^{\beta-1} + r_1^{\beta-1}, \\ 3r_0{}^0 + 3r_1^0, 3r_0^1 + 3r_1^1, \ldots, 3r_0{}^{\beta-1} + 3r_1^{\beta-1} \end{pmatrix}$$

$\mathbb{Z}_4^{\alpha} R^{\beta}$ halkasından alınan herhangi bir (e_1, e_2) elemanın Lee ağırlığı,

$$w_L(e_1, e_2) = w_H(e_1) + w_L(e_2) = w_H(e_1) + w_H(\varpi_1(e_2))$$

ile tanımlanır.

$\lambda -$ sabit devirli öteleme operatörü ρ_λ, devirsel öteleme operatörü σ, $l -$ parçalı devirli kod operatörü υ_l ve parçalı sabit devirli öteleme operatörü ς_l olmak üzere aşağıdaki teoremler ve önermeler oluşturulabilir.

Önerme 5.4.1. C_β kodu R üzerinde β uzunluğunda devirli kod ise C_β kodunun görüntüsü $\varpi_1(C_\beta)$, $\mathbb{Z}_4$ üzerinde 2β uzunluğunda $2 -$ parçalı devirli koddur.

İspat. $i = 0, \ldots, \beta - 1$ olmak üzere, R halkasından herhangi bir $e_2{}^i = r_0{}^i + ur_1^i$ elemanı alınsın.

C_β kodu R üzerinde devirli kod ise tanım gereği $\sigma\left(e_2{}^0, e_2{}^1, \ldots, e_2{}^{\beta-1}\right) = \left(e_2{}^{\beta-1}, e_2{}^0, \ldots, e_2{}^{\beta-2}\right)$ eşitliği yazılır. Buradan $\sigma\left(e_2{}^0, e_2{}^1, \ldots, e_2{}^{\beta-1}\right) = \left(r_0{}^{\beta-1} + ur_1{}^{\beta-1}, r_0{}^0 + ur_1{}^0, \ldots, r_0{}^{\beta-2} + ur_1{}^{\beta-2}\right)$ olduğu görülür. Bu dönüşümün $\mathbb{Z}_4$ görüntüsü dikkate alınırsa,

$$\varpi_1 \sigma\left(e_2{}^{\beta-1}, e_2{}^0, \ldots, e_2{}^{\beta-2}\right) = \begin{pmatrix} r_0{}^{\beta-1} + r_1{}^{\beta-1}, r_0{}^0 + r_1{}^0, \ldots, r_0{}^{\beta-2} + r_1{}^{\beta-2}, \\ 3r_0{}^{\beta-1} + 3r_1{}^{\beta-1}, 3r_0{}^0 + 3r_1{}^0, \ldots, 3r_0{}^{\beta-2} + 3r_1{}^{\beta-2} \end{pmatrix}$$

elde edilir.

Diğer taraftan $i = 0, \ldots, \beta - 1$ iken $e_2{}^i = \left(e_2{}^0, e_2{}^1, \ldots, e_2{}^{\beta-1}\right)$ ifadesinin yarı devirsel öteleme operatörü υ_2 altındaki görüntüsü,

$$\upsilon_2 \varpi_1\left(e_2{}^0, e_2{}^1, \ldots, e_2{}^{\beta-1}\right) = \begin{pmatrix} r_0{}^{\beta-1} + r_1{}^{\beta-1}, r_0{}^0 + r_1{}^0, \ldots, r_0{}^{\beta-2} + r_1{}^{\beta-2}, \\ 3r_0{}^{\beta-1} + 3r_1{}^{\beta-1}, 3r_0{}^0 + 3r_1{}^0, \ldots, 3r_0{}^{\beta-2} + 3r_1{}^{\beta-2} \end{pmatrix}$$

olarak bulunur. Buradan R halkasındaki C_β devirli kodunun tanımlanan Gray altındaki görüntüsü $\varpi_1\left(C_\beta\right)$'nın $\mathbb{Z}_4$ üzerinde 2β uzunluğunda $2-$parçalı devirli kod olduğu görülür. □

Teorem 5.4.2. C kodu $\Re_{\alpha,\beta}$ halkasında devirli kod olsun.

i. $\alpha = \beta$ olması durumunda, C kodunun tanımlanan Gray altındaki görüntüsü $\mathbb{Z}_4$ üzerinde $3-$parçalı devirli bir koddur.

ii. $\alpha \neq \beta$ olması durumunda ise $\partial(C)$, genelleştirilmiş $3-$parçalı devirli koddur.

İspat. C kodunun $\Re_{\alpha,\beta}$ halkasında devirli kod olduğu kabul edilsin. C kodundan bir $z = \left(e_1, e_2\right) = \left(e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_1^{\beta-1}\right) \in C$ kod sözü alınsın. Bu durumda,

$$\begin{pmatrix} e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, r_0^0 + r_1^0, r_0^1 + r_1^1, \ldots, r_0^{\beta-1} + r_1^{\beta-1}, \\ 3r_0^0 + 3r_1^0, 3r_0^1 + 3r_1^1, \ldots, 3r_0^{\beta-1} + 3r_1^{\beta-1} \end{pmatrix} \in \partial(C)$$

elde edilir. C kodu devirli bir kod olduğundan $(e_1, e_2) = (e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_2^{\beta-1}) \in C$ iken $\sigma(e_1, e_2) = (e_1^{\alpha-1}, e_1^0, e_1^1, \ldots, e_1^{\alpha-2}, e_1^{\beta-1}, e_2^0, \ldots, e_1^{\beta-2}) \in C$ yazılabilir. Bu ifadenin tanımlanan Gray altındaki görüntüsü alınırsa,

$$\partial\sigma(C) = \begin{pmatrix} e_1^{\alpha-1}, e_1^0, e_1^1, \ldots, e_1^{\alpha-2}, r_0^{\beta-1} + r_1^{\beta-1}, r_0^0 + r_1^0, \ldots, r_0^{\beta-2} + r_1^{\beta-2}, \\ 3r_0^{\beta-1} + 3r_1^{\beta-1}, 3r_0^0 + 3r_1^0, \ldots, 3r_0^{\beta-2} + 3r_1^{\beta-2} \end{pmatrix}$$

elde edilir.

$\alpha = \beta$ olması durumunda uzunluk 3α olur. $\partial(C)$ ifadesine parçalı devirli öteleme operatörü uygulandığı takdirde, C kodunun Gray altındaki görüntüsünün 3α uzunluğunda $3-$parçalı devirli kod olduğu görülür.

$\alpha \neq \beta$ olması durumunda ise $\partial(C)$'nin genelleştirilmiş $3-$parçalı devirli kod olacağı aşikârdır. □

Önerme 5.4.2. $\lambda = 3$ ve $\lambda = 1 + 2u$ olmak üzere, C_β kodu R üzerinde β uzunluğunda $\lambda-$sabit devirli kod ise C_β kodunun $\mathbb{Z}_4$ görüntüsü, uzunluğu 2β olan devirli koddur.

İspat. $i = 0, \ldots, \beta - 1$ olmak üzere, R halkasından herhangi bir $e_2^i = r_0^i + ur_1^i$ elemanı alınsın. C_β kodu R üzerinde $3-$sabit devirli kod ise tanım gereği $\rho_3(e_2^0, e_2^1, \ldots, e_2^{\beta-1}) = (3e_2^{\beta-1}, e_2^0, \ldots, e_2^{\beta-2}) = (3r_0^{\beta-1} + u3r_1^{\beta-1}, r_0^0 + ur_1^0, \ldots, r_0^{\beta-2} + ur_1^{\beta-2})$ eşitliği yazılır. Bu dönüşümün $\mathbb{Z}_4$ görüntüsü dikkate alınırsa,

$$\varpi_1\rho_3\left(3e_2^{\beta-1},e_2^0,\ldots,e_2^{\beta-2}\right)=\begin{pmatrix}3r_0^{\beta-1}+3r_1^{\beta-1},r_0^0+r_1^0,\ldots,r_0^{\beta-2}+r_1^{\beta-2},\\ r_0^{\beta-1}+r_1^{\beta-1},3r_0^0+3r_1^0,\ldots,3r_0^{\beta-2}+3r_1^{\beta-2}\end{pmatrix}$$

elde edilir.

C_β kodu R üzerinde $(1+2u)-$sabit devirli kod ise tanım gereği $\rho_{1+2u}\left((1+2u)e_2^{\beta-1},\right.$ $\left.e_2^0,e_2^1,\ldots,e_2^{\beta-2}\right)=\left(r_0^{\beta-1}+u\left(2r_0^{\beta-1}+3r_1^{\beta-1}\right),r_0^0+ur_1^0,\ldots,r_0^{\beta-2}+ur_1^{\beta-2}\right)$ yazılabilir. Bu dönüşümün $\mathbb{Z}_4$ görüntüsü dikkate alınırsa,

$$\varpi_1\rho_{1+2u}\left((1+2u)e_2^{\beta-1},e_2^0,\ldots,e_2^{\beta-2}\right)=\begin{pmatrix}3r_0^{\beta-1}+3r_1^{\beta-1},r_0^0+r_1^0,\ldots,r_0^{\beta-2}+r_1^{\beta-2},\\ r_0^{\beta-1}+r_1^{\beta-1},3r_0^0+3r_1^0,\ldots,3r_0^{\beta-2}+3r_1^{\beta-2}\end{pmatrix}$$

elde edilir.

Diğer taraftan $i=0,\ldots,\beta-1$ iken $e_2^i=\left(e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)$ ifadesinin devirsel öteleme operatörü σ altındaki görüntüsü,

$$\sigma\varpi_1\left(e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)=\begin{pmatrix}3r_0^{\beta-1}+3r_1^{\beta-1},r_0^0+r_1^0,\ldots,r_0^{\beta-1}+r_1^{\beta-1},\\ r_0^0+r_1^0,3r_0^1+3r_1^1,\ldots,3r_0^{\beta-2}+3r_1^{\beta-2}\end{pmatrix}$$

olarak bulunur. Buradan $\varpi_1\rho_{1+2u}\left(C_\beta\right)=\varpi_1\rho_3\left(C_\beta\right)=\sigma\varpi_1\left(C_\beta\right)$ elde edilir. Bu da R halkasından alınan $3-$sabit devirli ve $(1+2u)-$sabit devirli C_β kodunun $\mathbb{Z}_4$ görüntüsünün, uzunluğu olan devirli bir kod olduğu anlamına gelir. □

Önerme 5.4.3. C_β kodu R üzerinde β uzunluğunda $(3+2u)-$sabit devirli kod ise C_β kodunun $\mathbb{Z}_4$ görüntüsü, 2β uzunluğunda $2-$parçalı devirli koddur.

İspat. $i=0,\ldots,\beta-1$ olmak üzere, R halkasından herhangi bir $e_2^i=r_0^i+ur_1^i$ elemanı alınsın. C_β kodu R üzerinde $(3+2u)-$sabit devirli kod ise tanım gereği

$\rho_{3+2u}\left(e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)=\left((3+2u)e_2^{\beta-1},e_2^0,\ldots,e_2^{\beta-2}\right)$ yazılır. Buradan $\rho_{3+2u}\left(e_2^0,e_2^1,\ldots\right.$ $\left.e_2^{\beta-1}\right)=\left(3r_0^{\beta-1}+u\left(2r_0^{\beta-1}+r_1^{\beta-1}\right),r_0^0+ur_1^0,\ldots,r_0^{\beta-2}+ur_1^{\beta-2}\right)$ olduğu görülür. Bu dönüşümün $\mathbb{Z}_4$ görüntüsü dikkate alınırsa,

$$\varpi_1\rho_{3+2u}\left((3+2u)e_2^{\beta-1},e_2^0,\ldots,e_2^{\beta-2}\right)=\begin{pmatrix} r_0^{\beta-1}+r_1^{\beta-1},r_0^0+r_1^0,\ldots,r_0^{\beta-2}+r_1^{\beta-2}, \\ 3r_0^{\beta-1}+3r_1^{\beta-1},3r_0^0+3r_1^0,\ldots,3r_0^{\beta-2}+3r_1^{\beta-2}\end{pmatrix}$$

elde edilir.

Diğer taraftan, $i=0,\ldots,\beta-1$ iken $e_2^i=\left(e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)$ ifadesinin $2-$parçalı devirli öteleme operatörü υ_2 altındaki görüntüsü,

$$\upsilon_2\varpi_1\left(e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)=\begin{pmatrix} r_0^{\beta-1}+r_1^{\beta-1},r_0^0+r_1^0,\ldots,r_0^{\beta-2}+r_1^{\beta-2}, \\ 3r_0^{\beta-1}+3r_1^{\beta-1},3r_0^0+3r_1^0,\ldots,3r_0^{\beta-2}+3r_1^{\beta-2}\end{pmatrix}$$

olarak bulunur. Buradan $\varpi_1\rho_{3+2u}\left(C_\beta\right)=\upsilon_2\varpi_1\left(C_\beta\right)$ elde edilir. Bu da R halkasındaki $\left(3+2u\right)-$sabit devirli C_β kodunun $\mathbb{Z}_4$ görüntüsünün, 2β uzunluğunda $2-$parçalı devirli kod olması anlamına gelir. □

Teorem 5.4.3. $\lambda=3+2u$ olmak üzere, C kodu R_{α,β_λ} halkasında $\lambda-$sabit devirli kod olsun. $\alpha=\beta$ iken, C kodunun tanımlanan Gray altındaki görüntüsü $\mathbb{Z}_4$ üzerinde 3α uzunluğunda $3-$parçalı devirli bir koddur. Aksi takdirde $\partial(C)$, genelleştirilmiş $3-$parçalı devirli koddur.

İspat. C kodu R_{α,β_λ} halkasında $\left(3+2u\right)-$sabit devirli kod olsun. C kodundan alınan bir $z=\left(e_1,e_2\right)=\left(e_1^0,e_1^1,\ldots,e_1^{\alpha-1},e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)\in C$ kodsözü için,

$$\begin{pmatrix} e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, r_0^0 + r_1^0, \ldots, r_0^{\beta-1} + r_1^{\beta-1}, \\ 3r_0^0 + 3r_1^0, 3r_0^1 + 3r_1^1, \ldots, 3r_0^{\beta-1} + 3r_1^{\beta-1} \end{pmatrix} \in \partial(C)$$

yazılabilir.

C kodu $(3+2u)-$sabit devirli kod olduğundan $(e_1, e_2) = (e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_2^{\beta-1}) \in C$ iken $\rho_{3+2u}(e_1, e_2) = (\eta(3+2u)e_1^{\alpha-1}, e_1^0, \ldots, e_1^{\alpha-2}, (3+2u)e_2^{\beta-1}, e_2^0, \ldots, e_1^{\alpha-2}) \in C$ olup bu ifadenin $\mathbb{Z}_4$ görüntüsü düzenlenirse,

$$\left(e_1^{\alpha-1}, e_1^0, \ldots, e_1^{\alpha-2}, 3r_0^{\beta-1} + u\left(2r_0^{\beta-1} + r_1^{\beta-1}\right), r_0^0 + r_1^0, \ldots, r_0^{\beta-2} + r_1^{\beta-2}\right) \in \partial(C)$$

elde edilir. Bu ifadenin tanımlanan Gray altındaki $\mathbb{Z}_4$ görüntüsü

$$\partial\rho_{3+2u}(C) = \begin{pmatrix} e_1^{\alpha-1}, e_1^0, e_1^1, \ldots, e_1^{\alpha-2}, r_0^{\beta-1} + r_1^{\beta-1}, r_0^0 + r_1^0, \ldots, r_0^{\beta-2} + r_1^{\beta-2}, \\ 3r_0^{\beta-1} + 3r_1^{\beta-1}, 3r_0^0 + 3r_1^0, \ldots, 3r_0^{\beta-2} + 3r_1^{\beta-2} \end{pmatrix}$$

şeklinde yazılır. $\alpha = \beta$ olması durumunda, parçalı devirli kod tanımı gereği, C kodunun Gray altındaki görüntüsünün 3α uzunluğunda $3-$parçalı devirli kod olduğu görülür. Aksi takdirde $\partial(C)$, genelleştirilmiş $3-$parçalı devirli kod olur.□

5.5. $\mathbb{Z}_4R$ Halkasındaki Aykırı Devirli Kodlar

Toplamsal aykırı devirli kodlardan (skew additive) söz edebilmek için öncelikle R halkasındaki aşikâr olmayan bir otomorfizma tanımlanmalıdır. Bu halkadaki âşikar olmayan tek otomorfizma Θ ile temsil edilmek üzere,

$$\Theta(r_0 + ur_1) = r_0 + (1+3u)r_1$$

şeklindedir ve mertebesi 2 'dir.

$R[x,\Theta]=\{a_0+a_1x+\ldots+a_{\beta-1}x^{\beta-1}:a_i\in R,\ \beta\in\mathbb{N}\}$ halkası katsayıları R halkasından alınan aykırı polinom halkası olarak adlandırılır. Bu halkada kullanılan toplama işlemi bilinen toplama işlemi olmasına rağmen bilinen çarpma işleminin aksine $(ax^k)(bx^j)=a\Theta^k(b)x^{k+j}$ şeklinde farklı bir çarpma işlemi tanımlanır. Aykırı polinom halkasının değişmeli olmayan bir yapıda olmasının en temel sebebi tanımlanan çarpma işlemidir. $w(x)=s(x)a(x)$ olacak şekilde bir $s(x)\in R[x,\Theta]$ polinomu varsa $a(x)\in R[x,\Theta]$ polinomuna $w(x)$ polinomunun bir sağ böleni adı verilir. Bu durumda $w(x)$ polinomu $a(x)$ polinomunun bir sol çarpanı olur. Sol bölen ve sağ çarpan da benzer şekilde tanımlanabilir. Yapı değişmeli olmadığından sol çarpan kavramı büyük önem arz etmektedir.

Not 5.5.1. Bu bölümde sol çarpan kavramı kullanılacaktır ve $\mathbb{Z}_4[x]/\langle x^\alpha-1\rangle\times R[x,\Theta]/\langle x^\beta-\lambda\rangle$ bölüm halkası $\Re_{\alpha,\beta_{\Theta,\lambda}}$ ile temsil edilecektir. $\lambda=1$ olması durumunda aykırı devirli kodlardan söz edilecek olup bu bölüm halkası $\Re_{\alpha,\beta_\Theta}$ ile temsil edilecektir. Aykırı devirli kodlar, kısaca, $\Theta-$devirli kod, λ birimsel elemanının 1'den farklı olması durumunda ise aykırı sabit devirli kodlar $(\lambda,\Theta)-$devirli kod şeklinde isimlendirilecektir. Diğer bir ifade ile $\Re_{\alpha,\beta_\Theta}(C)=C$ ise R^β halkasının bir $R-$alt modülü $\Theta-$devirli kod, $\Re_{\alpha,\beta_{\Theta,\lambda}}(C)=C$ ise R^β halkasının bir $R-$alt modülü ise $(\lambda,\Theta)-$devirli kod olarak adlandırılacaktır.

Bu bölüm halkası $a(x),w(x)\in R[x,\Theta]$ polinomları için $a(x)\left(w(x)+\langle x^\beta-\lambda\rangle\right)=a(x)w(x)+\langle x^\beta-\lambda\rangle$ tanımlanan çarpma işlemine göre bir $R[x,\Theta]-$sol modüldür.

R^β halkasından $R[x,\Theta]/\langle x^\beta-1\rangle$ halkasına $(e_2^0,e_2^1,\ldots,e_2^{\beta-1})\to e_2^0+e_2^1x+\ldots+e_2^{\beta-1}x^{\beta-1}$ olacak şekilde bir $R-$modül izomorfizması tanımlansın.

Tanım 5.5.1. R halkasında uzunluğu β olan aykırı lineer C_β kodu, $R[x,\Theta]$ halkası üzerinde derecesi β olan bir polinom $w(x)$ olmak üzere, $R[x,\Theta]\big/\langle w(x)\rangle$ – sol modülünün bir $R[x,\Theta]$ – sol alt modülüdür.

$\mathbb{Z}_4^\alpha \times R^\beta$ halkasının skaler ile çarpma işlemine göre bir R – modül olduğundan, $\Re_{\alpha,\beta_\Theta}$ ve $\Re_{\alpha,\beta_{\Theta,\lambda}}$ halkalarının da Tanım 5.1.3.'te tanımlanan çarpma işlemine göre bir $R[x]$ – modül olduğundan Bölüm 5.2.'de ifade edilmişti. Şimdi $\mathbb{Z}_4 R$ halkasındaki toplamsal aykırı sabit devirli kodların üreteç polinomu ele alınsın. Bu kodlar $\Re_{\alpha,\beta_{\Theta,\lambda}}$ halkasının bir $R[x,\Theta]$ – sol modülüdür.

Tanım 5.5.2. Θ, R halkasında tanımlanan aşikâr olmayan bir otomorfizma olsun. C kodu, $\mathbb{Z}_4^\alpha R^\beta$ halkasının bir R – alt modülü ve $\left(e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) \in C$ iken $\left(e_1^{\alpha-1}, e_1^0, e_1^1, \ldots, e_1^{\alpha-2}, \lambda\Theta\left(e_2^{\beta-1}\right), \Theta\left(e_2^0\right), \Theta\left(e_2^1\right), \ldots, \Theta\left(e_2^{\beta-2}\right)\right) \in C$ şartları sağlanıyorsa lineer C koduna $\mathbb{Z}_4^\alpha R^\beta$ halkası üzerinde aykırı λ – sabit devirli kod adı verilir.

Teorem 5.5.1. C_α kodu $\mathbb{Z}_4$ üzerinde uzunluğu α olan lineer bir kod ve C_β kodu R üzerinde uzunluğu β olan lineer bir kod olmak üzere, $\mathbb{Z}_4 R$ halkasında (α,β) uzunluğundaki lineer bir kod $C = C_\alpha \times C_\beta$ olsun. C kodunun aykırı λ – sabit devirli kod olması için gerek ve yeter koşul C_α kodunun $\mathbb{Z}_4$ üzerinde devirli kod, C_β kodunun ise R üzerinde aykırı λ – sabit devirli kod olmasıdır.

İspat. $C = C_\alpha \times C_\beta$ kodunun aykırı λ – sabit devirli kod olduğu kabul edilsin. Aykırı sabit devirli kod tanımı gereği $\left(e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) \in C$ iken $\left(e_1^{\alpha-1}, e_1^0, e_1^1, \ldots, e_1^{\alpha-2}, \lambda\Theta\left(e_2^{\beta-1}\right), \Theta\left(e_2^0\right), \Theta\left(e_2^1\right), \ldots, \Theta\left(e_2^{\beta-2}\right)\right) \in C$ olmasıdır. Bu da

$\left(e_1^{\alpha-1},e_1^0,e_1^1,\ldots,e_1^{\alpha-2}\right)\in C_\alpha$ ve $\left(\lambda\Theta\left(e_2^{\beta-1}\right),\Theta\left(e_2^0\right),\Theta\left(e_2^1\right),\ldots,\Theta\left(e_2^{\beta-2}\right)\right)\in C_\beta$ anlamına gelir. Bu durumda $\left(e_1^0,e_1^1,\ldots,e_1^{\alpha-1}\right)\in C_\alpha$ iken $\left(e_1^{\alpha-1},e_1^0,e_1^1,\ldots,e_1^{\alpha-2}\right)\in C_\alpha$ olduğundan, tanım gereği, C_α kodu $\mathbb{Z}_4$ üzerinde uzunluğu α olan devirli bir kod olur. $\left(e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)\in C_\beta$ iken $\left(\lambda\Theta\left(e_2^{\beta-1}\right),\Theta\left(e_2^0\right),\Theta\left(e_2^1\right),\ldots,\Theta\left(e_2^{\beta-2}\right)\right)\in C_\beta$ olduğundan, tanım gereği, C_β kodu da R üzerinde uzunluğu β olan aykırı $\lambda-$sabit devirli bir kod olur.

Tersine, C_α kodunun $\mathbb{Z}_4$ üzerinde uzunluğu α olan devirli bir kod, C_β kodunun ise R üzerinde uzunluğu β olan aykırı $\lambda-$sabit devirli bir kod olduğu kabul edilsin. C_α kodu devirli kod ise $\left(e_1^0,e_1^1,\ldots,e_1^{\alpha-1}\right)\in C_\alpha$ iken $\left(e_1^{\alpha-1},e_1^0,e_1^1,\ldots,e_1^{\alpha-2}\right)\in C_\alpha$, aykırı $\lambda-$sabit devirli kod ise $\left(e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)\in C_\beta$ iken $\left(\lambda\Theta\left(e_2^{\beta-1}\right),\Theta\left(e_2^0\right),\Theta\left(e_2^1\right),\right.$ $\left.\ldots,\Theta\left(e_2^{\beta-2}\right)\right)\in C_\beta$ yazılabilir. Böylece $\left(e_1^{\alpha-1},e_1^0,e_1^1,\ldots,e_1^{\alpha-2},\lambda\Theta\left(e_2^{\beta-1}\right),\Theta\left(e_2^0\right),\right.$ $\left.\Theta\left(e_2^1\right),\ldots,\Theta\left(e_2^{\beta-2}\right)\right)\in C_\beta$ sonucuna ulaşılır. Bu da $C=C_\alpha\times C_\beta$ kodunun $\mathbb{Z}_4R$ üzerinde aykırı $\lambda-$sabit devirli kod olması anlamına gelir. □

C kodu $\mathbb{Z}_4R-$aykırı devirli kod, $l(x)\in{\mathbb{Z}_4[x]}\Big/{\left\langle x^\alpha-1\right\rangle}$ ve C kodundaki bir eleman $z(x)=\left(e_1(x),e_2(x)\right)$ olsun. Bölüm 5.2.'de tanımlanan X kümesi C kodunun bir alt modülü ve ${\mathbb{Z}_4[x]}\Big/{\left\langle x^\alpha-1\right\rangle}$ bölüm halkasının da bir ideali olduğundan aynı zamanda devirli bir koddur. Bu da $x^\alpha-1$ polinomunun bir böleni olduğu anlamına gelir. Buradan hareketle $e_1(x)\left|\left\langle x^\alpha-1\right\rangle\right.$ olacak şekilde $\mathrm{X}=\left\langle e_1(x)\right\rangle$ elde edilir.

$\Lambda'=\left\{e_2(x)\in{R[x,\Theta]}\Big/{\left\langle x^\beta-\lambda\right\rangle},\left(l(x),e_2(x)\right)\in C\ :\ l(x)\in{\mathbb{Z}_4[x]}\Big/{\left\langle x^\beta-1\right\rangle}\right\}$ olsun.

Λ' kümesinin ${R[x,\Theta]}\Big/{\left\langle x^\beta-\lambda\right\rangle}$ halkasının bir alt modülü olması ve $\Lambda'=\left(l(x),e_2(x)\right)$

ifadesinin gösterimi daha önce tanımlanan Λ kümesinin ispatına benzer şekilde yapılabilir.

R halkasındaki birimsel eleman λ'nın tek kuvvetlerinin kendisi, çift kuvvetlerinin ise 1 olduğu hatırlatılsın. Bu bilgiler doğrultusunda $\mathbb{Z}_4R-$aykırı sabit devirli bir kodun üreteç polinomu aşağıdaki gibi inşa edilir.

Teorem 5.5.2. $\tilde{x}=\lambda x$ ve $C_\beta=\langle\kappa(\tilde{x})\rangle$ olmak üzere, $f(x),l(x)\in {\mathbb{Z}_4[x]}/{\langle x^\beta-1\rangle}$ ve $\kappa(\tilde{x})\in {R[x,\Theta]}/{\langle x^\beta-\lambda\rangle}$ olacak şekilde $f(x)\,|\,x^\alpha-1$ iken $\mathbb{Z}_4R$ halkasındaki $\lambda-$aykırı sabit devirli bir C kodunun üreteç polinomu

$$C=\langle(f(x),0),(l(x),\kappa(\tilde{x}))\rangle$$

şeklindedir.

Lemma 5.5.1. $C=\langle(f(x),0),(l(x),\kappa(\tilde{x}))\rangle$ kodu $\mathbb{Z}_4R-$aykırı sabit devirli kod ise $der(l(x))<der(f(\tilde{x}))$'dir.

Not 5.5.2. Teorem 5.5.2. ve Lemma 5.5.1.'in ispatları Teorem 5.2.1. ve Lemma 5.2.1.'nin ispatlarına benzer şekilde yapılır. □

5.6. $\mathbb{Z}_4R$ Halkasındaki Aykırı Devirli ve Aykırı Sabit Devirli Kodun Görüntüsü

R halkasından $\mathbb{Z}_4^2$ yapısına aşağıdaki gibi bir Gray dönüşüm tanımlansın.

$$\varpi_2:R\to\mathbb{Z}_4^2$$

$$e_2=r_0+ur_1\to(2r_0+3r_1,2r_0+r_1)$$

Tanımlanan bu dönüşüm R^β yapısından $\mathbb{Z}_4^{2\beta}$ yapısına genişletilirse,

$$\varpi_2 : R^\beta \to \mathbb{Z}_4^{2\beta}$$

$$\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) \to \begin{pmatrix} 2r_0^0 + 3r_1^0, 2r_0^1 + 3r_1^1, \ldots, 2r_0^{\beta-1} + 3r_1^{\beta-1}, \\ 2r_0^0 + r_1^0, 2r_0^1 + r_1^1, \ldots, 2r_0^{\beta-1} + r_1^{\beta-1} \end{pmatrix}$$

elde edilir.

Teorem 5.6.1. Tanımlanan ϖ_2 dönüşümü $\left(R^\beta, \text{Lee uzaklık}\right) \to \left(R^\beta, \text{Hamming uzaklık}\right)$ uzaklığı koruyan lineer bir dönüşümdür.

İspat. $t_1 = a_1 + ub_1$ ve $t_2 = a_2 + ub_2$ olmak üzere,

$$\begin{aligned} \varpi_2\left(yt_1 + kt_2\right) &= \varpi_2\left(ya_1 + uyb_1 + ka_2 + ukb_2\right) = \varpi_2\left(ya_1 + ka_2 + u\left(yb_1 + kb_2\right)\right) \\ &= \left(2ya_1 + 2ka_2 + 3yb_1 + 3kb_2, 2ya_1 + 2ka_2 + yb_1 + kb_2\right) \\ &= \left(y\left(2a_1 + 3b_1\right) + k\left(2a_2 + 3b_2\right), y\left(2a_1 + b_1\right) + k\left(2a_2 + b_2\right)\right) \\ &= \left(y\left(2a_1 + 3b_1, 2a_1 + b_1\right) + k\left(2a_2 + 3b_2, 2a_2 + b_2\right)\right) \\ &= y\varpi_2 t_1 + k\varpi_2 t_2 \end{aligned}$$

eşitliği sağlandığından ϖ_2 dönüşümü lineer bir dönüşüm olur.

$$\begin{aligned} d_L\left(t_1, t_2\right) = w_L\left(t_1 - t_2\right) &= w_L\left(a_1 - a_2 + u\left(b_1 - b_2\right)\right) \\ &= w_L\left(\varpi_2\left(\left(a_1 - a_2\right) + u\left(b_1 - b_2\right)\right)\right) \\ &= w_H\left(2a_1 - 2a_2 + 3b_1 - 3b_2, 2a_1 - 2a_2 + b_1 - b_2\right) \\ &= w_H\left(\left(2a_1 + 3b_1, 2a_1 + b_2\right) - \left(2a_2 + 3b_1 + 2a_2 + b_2\right)\right) \\ &= w_H\left(\varpi_2\left(a_1 + ub_1\right) - \varpi_2\left(a_2 + ub_1\right)\right) \\ &= w_H\left(\varpi_2 t_1 - \varpi_2 t_2\right) = d_H\left(\varpi_2 t_1 - \varpi_2 t_2\right) \end{aligned}$$

olduğundan uzaklık korunur.

Böylece ϖ_2 Gray dönüşümü $\left(R^\beta, \text{Lee uzaklık}\right) \to \left(R^\beta, \text{Hamming uzaklık}\right)$ uzaklığı koruyan lineer bir dönüşümdür. □

Buradan hareketle $\mathbb{Z}_4 R$ halkasından $\mathbb{Z}_4^3$ yapısına aşağıdaki gibi bir Gray dönüşüm tanımlanabilir.

$$\partial' : \mathbb{Z}_4 R \to \mathbb{Z}_4^3$$
$$\left(e_1, e_2\right) \to \left(e_1, \varpi_2\left(e_2\right)\right)$$

$e_2 = r_0 + u\, r_1$ olduğu hatırlatılarak, ∂' fonksiyonu yapısından $\mathbb{Z}_4^{\alpha+2\beta}$ yapısına aşağıdaki gibi genişletilebilir.

$$\partial' : \mathbb{Z}_4^\alpha R^\beta \to \mathbb{Z}_4^{\alpha+2\beta}$$
$$\partial'\left(e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) \to \begin{pmatrix} e_1^0, e_1^1, \ldots, e_1^{\alpha-1}, 2r_0^0 + 3r_1^0, 2r_0^1 + 3r_1^1, \ldots, 2r_0^{\beta-1} \\ +3r_1^{\beta-1}, 2r_0^0 + r_1^0, 2r_0^1 + r_1^1, \ldots, 2r_0^{\beta-1} + r_1^{\beta-1} \end{pmatrix}$$

$\mathbb{Z}_4^\alpha R^\beta$ halkasından alınan herhangi bir $\left(e_1, e_2\right)$ elemanın Lee ağırlığı,

$$w_L\left(e_1, e_2\right) = w_H\left(e_1\right) + w_L\left(e_2\right) = w_H\left(e_1\right) + w_H\left(\varpi_2\left(e_2\right)\right)$$

ile tanımlanır.

Aykırı $\lambda-$sabit devirli öteleme operatörü $\rho_{\Theta,\lambda}$, aykırı devirsel öteleme operatörü σ_Θ ve $l-$parçalı devirli kod operatörü υ_l olmak üzere aşağıdaki teorem ve önermeler verilebilir.

Önerme 5.6.1. C_β kodu üzerinde β uzunluğunda aykırı devirli kod ise C_β kodunun görüntüsü $\varpi_2\left(C_\beta\right)$, $\mathbb{Z}_4$ üzerinde 2β uzunluğunda $2-$parçalı devirli koddur.

İspat. $i=0,\ldots,\beta-1$ olmak üzere, R halkasından herhangi bir $e_2^i = r_0^i + u\, r_1^i$ elemanı alınsın.

C_β kodu R üzerinde aykırı devirli kod ise tanım gereği $\sigma\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) = \left(\Theta\left(e_2^{\beta-1}\right), \Theta\left(e_2^0\right), \ldots, \Theta\left(e_2^{\beta-2}\right)\right)$ eşitliği yazılır. Buradan,

$$\sigma_\Theta\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) = \left(r_0^{\beta-1} + r_1^{\beta-1} + u3r_1^{\beta-1}, r_0^0 + r_1^0 + u3r_1^0, \ldots, r_0^{\beta-2} + r_1^{\beta-2} + u3r_1^{\beta-2}\right)$$

olduğu görülür. Bu dönüşümün $\mathbb{Z}_4$ görüntüsü dikkate alınırsa

$$\varpi_2\sigma_\Theta\left(e_2^{\beta-1}, e_2^0, \ldots, e_2^{\beta-2}\right) = \begin{pmatrix} 2r_0^{\beta-1} + 3r_1^{\beta-1}, 2r_0^0 + 3r_1^0, \ldots, 2r_0^{\beta-2} + 3r_1^{\beta-2}, \\ 2r_0^{\beta-1} + r_1^{\beta-1}, 2r_0^0 + r_1^0, \ldots, 2r_0^{\beta-2} + r_1^{\beta-2} \end{pmatrix}$$

elde edilir.

Diğer taraftan $i=0,\ldots,\beta-1$ iken $e_2^i = \left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right)$ ifadesinin $2-$parçalı devirli öteleme operatörü υ_2 altındaki görüntüsü,

$$\upsilon_2\varpi_2\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) = \begin{pmatrix} 2r_0^{\beta-1} + 3r_1^{\beta-1}, 2r_0^0 + 3r_1^0, \ldots, 2r_0^{\beta-2} + 3r_1^{\beta-2}, \\ 2r_0^{\beta-1} + r_1^{\beta-1}, 2r_0^0 + r_1^0, \ldots, 2r_0^{\beta-2} + r_1^{\beta-2} \end{pmatrix}$$

olarak bulunur. Buradan R halkasındaki aykırı devirli C_β kodunun tanımlanan Gray altındaki görüntüsü $\varpi_2\left(C_\beta\right)$'nın $\mathbb{Z}_4$ üzerinde 2β uzunluğunda $2-$parçalı devirli kod olduğu görülür. □

Teorem 5.6.2. C kodu $\Re_{\alpha,\beta_\Theta}$ halkasında aykırı devirli kod olsun.

i. $\alpha=\beta$ olması durumunda, C kodunun ∂' altındaki görüntüsü $\mathbb{Z}_4$ üzerinde $3-$parçalı devirli bir koddur.

ii. $\alpha \neq \beta$ olması durumunda ise $\partial'(C)$, genelleştirilmiş $3-$parçalı devirli koddur.

İspat. C kodunun $\Re_{\alpha,\beta_\Theta}$ halkasında aykırı devirli kod olduğu kabul edilsin. C kodundan bir $z=(e_1,e_2)=\left(e_1^0,e_1^1,\ldots,e_1^{\alpha-1},e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)\in C$ kodsözü alınsın. Bu durumda,

$$\begin{pmatrix} e_2^0,e_2^1,\ldots,e_2^{\alpha-1},\ 2r_0^0+3r_1^0,2r_0^1+3r_1^1,\ldots,2r_0^{\beta-1}+3r_1^{\beta-1}, \\ 2r_0^0+r_1^0,2r_0^1+r_1^1,\ldots,2r_0^{\beta-1}+r_1^{\beta-1} \end{pmatrix}\in\partial'(C)$$

elde edilir.

C kodu aykırı devirli bir kod olduğundan tanım gereği, $(e_1,e_2)=\left(e_1^0,e_1^1,\ldots,e_1^{\alpha-1},\right.$ $\left.e_2^0,e_2^1,\ldots,e_2^{\beta-1}\right)\in C$ iken $\sigma_\Theta(e_1,e_2)=\left(e_1^{\alpha-1},e_1^0,\ldots,e_1^{\alpha-2},\Theta\left(e_1^{\beta-1}\right),\Theta\left(e_1^0\right),\ldots,\Theta\left(e_1^{\beta-2}\right)\right)$ de C kodunun elemanıdır. Bu ifadenin tanımlanan Gray altındaki görüntüsü alınırsa

$$\partial'\sigma(C)=\begin{pmatrix} e_1^{\alpha-1},e_1^0,\ldots,e_1^{\alpha-2},2r_0^{\beta-1}+3r_1^{\beta-1},2r_0^0+3r_1^0,\ldots,2r_0^{\beta-2}+3r_1^{\beta-2}, \\ 2r_0^{\beta-1}+r_1^{\beta-1},2r_0^0+r_1^0,\ldots,2r_0^{\beta-2}+r_1^{\beta-2} \end{pmatrix}$$

elde edilir.

$\alpha=\beta$ olması durumunda uzunluk 3α olacağı âşikardır. $\partial'(C)$ ifadesine parçalı devirli öteleme operatörü uygulandığı takdirde, C kodunun ∂' altındaki görüntüsünün 3α uzunluğunda $3-$parçalı devirli kod olduğu görülür.

$\alpha\neq\beta$ olması durumunda ise $\partial'(C)$'nin genelleştirilmiş $3-$parçalı devirli kod olacağı açıktır. □

Önerme 5.6.2. $\lambda=3$ olmak üzere, C_β kodu R üzerinde β uzunluğunda $\lambda-$sabit devirli kod ise C_β kodunun $\mathbb{Z}_4$ görüntüsü, uzunluğu 2β olan devirli koddur.

İspat. $i=0,\ldots,\beta-1$ olmak üzere, R halkasından herhangi bir $e_2^i = r_0^{\,i} + u\, r_1^{\,i}$ elemanı alınsın. C_β kodu R üzerinde aykırı $3-$sabit devirli kod ise tanım gereği, $\rho_3\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) = \left(3\Theta\left(e_2^{\beta-1}\right), \Theta\left(e_2^0\right), \ldots, \Theta\left(e_2^{\beta-2}\right)\right) = \left(3r_0^{\beta-1} + 3r_1^{\beta-1} + ur_1^{\beta-1}, r_0^0 + r_1^0 + u\right.$ $\left. 3r_1^0, \ldots, r_0^{\beta-2} + r_1^{\beta-2} + u3r_1^{\beta-2}\right)$ eşitliği yazılır. Bu dönüşümün $\mathbb{Z}_4$ görüntüsü alındığı takdirde,

$\varpi_2\rho_3\left(3\Theta\left(e_2^{\beta-1}\right), \Theta\left(e_2^0\right), \ldots, \Theta\left(e_2^{\beta-2}\right)\right) = \left(2r_0^{\beta-1} + r_1^{\beta-1}, 2r_0^0 + 3r_1^0, \ldots, 2r_0^{\beta-2} + 3r_1^{\beta-2}, 2r_0^{\beta-1}\right.$ $\left. +3r_1^{\beta-1}, 2r_0^0 + r_1^0, 2r_0^1 + r_1^1, \ldots, 2r_0^{\beta-2} + r_1^{\beta-2}\right)$ elde edilir.

Diğer taraftan $i=0,\ldots,\beta-1$ iken $e_2^i = \left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right)$ ifadesinin devirsel öteleme operatörü σ altındaki görüntüsü,

$$\sigma\varpi_2\left(e_2^0, e_2^1, \ldots, e_2^{\beta-1}\right) = \begin{pmatrix} 2r_0^{\beta-1} + r_1^{\beta-1}, 2r_0^0 + 3r_1^0, \ldots, 2r_0^{\beta-1} + 3r_1^{\beta-1}, \\ 2r_0^0 + r_1^0, 2r_0^1 + r_1^1, \ldots, 2r_0^{\beta-2} + r_1^{\beta-2} \end{pmatrix}$$

olarak bulunur.

Böylece $\varpi_2\rho_3\left(C_\beta\right) = \sigma\varpi_2\left(C_\beta\right)$ elde edilir. Bu da R halkasından alınan aykırı $3-$ sabit devirli C_β kodunun $\mathbb{Z}_4$ görüntüsünün, uzunluğu 2β olan devirli bir kod olduğu anlamına gelir. □

BÖLÜM 6. TARTIŞMA VE SONUÇ

Hem değişmeli hem de değişmeli olmayan halkalar üzerinde, uygulamaları ve cebirsel yapısı bakımından kodlama teorisinde yaygın bir çalışma alanına sahip olan devirli kod aileleri çalışılmıştır.

T_k olarak isimlendirilen $u^k = u^{k-1}$ iken $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4 + \ldots + u^{k-1}\mathbb{Z}_4$ halkasındaki devirli kodlar inşa edilmiş, ve izomorfizma yardımıyla halka üzerindeki sabit devirli kodların üreteç polinomuna ulaşılmıştır. Devirli ve sabit devirli kodların Gray altındaki görüntüleri incelenerek önemli sonuçlar tespit edilmiştir. Özel olarak, T_3 adı verilen, $u^3 = u^2$ iken $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ halkası üzerindeki devirli kodlar ve $\left(1+2u^2\right)-$sabit devirli kodların tanımlanan ϕ_1 Gray dönüşümü altındaki görüntülerinin $\mathbb{Z}_4$ üzerinde, sırasıyla, $2-$parçalı devirli kod ve devirli lineer kod oldukları gözlemlenmiştir. T_3 halkası üzerindeki devirli ve sabit devirli kodların Gray görüntüleri ile minimum Lee, Öklit ve Hamming uzaklıklar kullanılarak literatüre yeni $\mathbb{Z}_4-$lineer kodlar kazandırılmış ve birçok optimal kod elde edilmiştir.

Değişmeli olmayan yapılarda halkalar üzerindeki polinomlar birden fazla şekilde çarpanlarına ayrıldığından değişmeli halka yapısına göre daha fazla kod elde edilmesine olanak sağlar. Bu sebepten ötürü aykırı devirli ve aykırı sabit devirli kod yapılarının daha avantajlı olduğu dikkate alınarak T_3 halkası üzerinde aşikâr olmayan tüm otomorfizmalar belirlenmiş, aykırı devirli ve aykırı sabit devirli kodların karakteristik yapısı incelenmiştir. Aykırı devirli kodlar için üreteç polinomu inşa edilerek izomorfizma yardımıyla aykırı sabit devirli kodların üreteç polinomu oluşturulmuştur. Halka üzerindeki tüm birimsel elemanlar için uygun olan Gray dönüşüm ve otomorfizma kullanılarak aykırı devirli ve aykırı $\left(3+3u+u^2\right)-$sabit

devirli kodların $\mathbb{Z}_4$ görüntüleri incelenmiştir. Minimum Lee, Öklit ve Hamming uzaklıklar kullanılarak literatüre yeni $\mathbb{Z}_4-$lineer kodlar kazandırılmış ve birçok optimal kod elde edilmiştir.

Birçok karmaşık problemin çözümünde yer alan ve bilgiyi uzun süre saklayabilen DNA, hata düzeltme kapasitesi bakımından önemli bir rol oynamaktadır. Bu çalışmada, T_3 halkasındaki ters sıralı DNA kodlar ele alınmıştır. İlk olarak halkanın elemanları ile DNA $2-$baz arasında bağlantı sağlayan bir dönüşüm tanımlanmıştır. Daha sonra, T_3 halkasındaki ters sıralı DNA kodları elde edebilmek için birimsel ters sıralı polinom tanımı yapılmıştır. Halkadaki ters sıralı DNA kodları ve tamlayan DNA kodları elde edebilmek için birimsel ters sıralı polinomdan yararlanarak yeni bir üretim metodu inşa edilmiştir. Bu inşa metoduna örnekler sunulmuştur.

$u^2=u$ iken $\mathbb{Z}_4T_2$ halkasındaki devirli kodların üreteç yapısı ve kodu geren en küme inşa edilmiş, aynı zamanda izomorfizma yardımıyla halka üzerindeki sabit devirli kodların üreteç polinomuna da ulaşılmıştır. Halka üzerindeki tüm birimsel elemanlar için sabit devirli kodların $\mathbb{Z}_4$ görüntüleri elde edilmiştir. Aykırı devirli kodların yapısı incelenmiş, aykırı devirli ve aykırı $3-$sabit devirli kodun $\mathbb{Z}_4$ görüntüsü araştırılmıştır.

KAYNAKLAR

[1] Fraleigh, J.B., A first course in absract algebra. Pearson Education, Boston, 2003.

[2] Çallıalp, F., Örneklerle Soyut Cebir. Birsen Yayınevi, İstanbul, 2013.

[3] Hungerford, T.W., Algebra. Springer-Verlag, 1974.

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

[5] Wood, J.A., Duality for Modules over Finite Rings and Applications to Coding Theory. American Journal of Mathematics, 121 (3), 555-575, 1999.

[6] Shannon, C.E., A mathematical theory of communication. The Bell System Technical Journal, 27 (3), 379–423, 1948.

[7] Hamming, R.W., Error detecting and error correcting codes. Bell Labs Tech. J, 29 (2), 147–160, 1950.

[8] Ling, S., Xing C., Coding Theory A First Course. Cambridge University, 2004.

[9] Roman, S., Coding and Information Theory. Springer Verlag, 1992.

[10] Hill, R, Kolman, B., Elementary Linear Algebra. Prentice Hall, 2000.

[11] Huffman, W.C., Pless, V., Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.

[12] Wan, Z.X., Series on Applied Mathematics: Quaternary codes. World Scientific, Singapore, 1997.

[13] Dougherty, S.T., Algebraic Coding theory over finite commutative rings. Springer Briefs in Mathematics, Springer, 2017.

[14] Dougherty, S.T., Shiromoto, K., Maksimum Distance Codes over Rings of Order 4. IEEE, Transactions on Information Theory, 47 (1), January 2001.

[15] Ozen, M., Uzekmek, F.Z., Aydın, N, Ozzaim, N.T., Cyclic and some constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$. Finite Fields and Their Applications, 38: 27-39, 2016.

[16] Prange, E., Cyclic Error Correcting Codes in Two Symbols. Air Force Cambridge Research Center, Cambridge Mass., AFCRC-TN-57, 103, 1957.

[17] Skjærbæk, T. H., Quasi Cyclic Code Represented by Gröbner Bases. Aalborg University Department of Mathematical Sciences, 2010.

[18] Boucher, D., Geiselmann, W., Ulmer, F., Skew cyclic codes. AAECC, 18 (4), 379-389, 2007.

[19] MacDonald, B. R., Finite rings with identity. Marcel Deccer, New York, 1974.

[20] Şiap, İ., Abualrub, T., Aydın, N., Seneviratne, P., Skew cyclic codes of arbitrary length. International Journal of Information and Coding Theory, 2: 10-20, 2011.

[21] Boucher, D., Ulmer, F., A note on the dual codes of module skew codes. Lecture Notes in Computer Science, 7089: pp230-243.

[22] https://bilimgenc.tubitak.gov.tr/makale/dnanin-kesfinden-bugune, Erişim Tarihi: 18.01.2020.

[23] https://www.slideserve.com/pegeen/n-kleik-asitler, Erişim Tarihi: 18.01.2020.

[24] L. Adleman, Molecular computation of solutions to combinatorial problems. Science, 266 (5187), 1021–1024, 1994.

[25] Adleman L., Computing with DNA. Scientific American, August: 54-61.

[26] R. W. Hamming, "Error detecting and error correcting codes," Bell Labs Tech. J, 29 (2), 147–160, 1950.

[27] Adleman. L., On applying moleculaer computation to the data encryption standard. J. Comput. Biol. 6 (1), 53–63, 1999.

[28] Prange, E., Cyclic Error Correcting Codes in Two Symbols. Air Force. Cambridge Research Center, Cambridge Mass., AFCRC-TN-57, 103, 1957.

[29] Hammons, A.R., Kumar, V., Calderbank, A.R., Sloane, N.J.A., Sole, P. The $\mathbb{Z}_4-$linearity of Kerdock, Preparata, Goethals and related codes. IEEE Transactions on Information Theory, 40 (2), 301-319, 1994.

[30] Pless, V.S., Qian, Z., Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Transactions on Information Theory, 42 (5),1594-1600, 1996.

[31] Dougherty, S. T., Liu, H. Independence of vectors in codes over rings. Des. Code Crypt., 51 (1), 55-68, 2009.

[32] Zhu, S., Wang, Y., Shi, M., Some results on Cyclic Codesover $\mathbb{F}_2+u\mathbb{F}_2$. IEEE Transactions on Information Theory, 56 (4),1680-1684, 2010.

[33] Islam, H., Prakash, O., A study of cyclic and constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4$. Int. J. Information and Coding Theory, 5 (2), 155-168, 2018.

[34] Yıldız, B., Karadeniz, S., Cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$. Designs, Codes and Cryptography, 58 (3), 221-234, 2011.

[35] Aydın, N., Asamov, T., A Database of $\mathbb{Z}_4-$codes. J Comb Inf Syst Sci., 34, 1-12, 2009.

[36] Abualrub, T., Şiap, I., Reversible cyclic codes over $\mathbb{Z}_4$. Australasian Journal of Combinatorics, 38: 195-206, 2007.

[37] Al-Ashker, M., Hamoudeh, M., Cyclic codes over $\mathbb{Z}_2+u\mathbb{Z}_2+\ldots+u^{k-1}\mathbb{Z}_2$. Turkish Journal of Mathematics, 35: 737-749, 2011.

[38] Singh, A.K., Kewat, P.K., On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k\rangle$. Des. Codes Cryptogr., 74, 1-13, 2015.

[39] Bandi, R.K., Bhaintwal, M., Codes over $\mathbb{Z}_4+v\mathbb{Z}_4$. IEEE, International Conferance on Advances in Computing, Communications and Informatics, 422-427, 2014.

[40] 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), 17 pages, 2016.

[41] Gao, J., Fu, F.W:, Gao, Y., Some classes of linear codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ and their applications to construct good and new $\mathbb{Z}_4-$linear codes. Applicable Algebra in Engineering, Communication Computing, 28: 131-153, 2016.

[42] Ozen, M., Ozzaim, N.T., Aydın, N., Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$. Turkish Journal of Mathematics, 41: 1235-1247, 2017.

[43] www.Z4Codes.info, Erişim Tarihi: 22.10.2020.

[44] Pless, V., Sole, P., Qian, Z., Cyclic self-dual $\mathbb{Z}_4 -$ codes, Finite Fields and Their Applications, 3(1), 48-69, 1997.

[45] 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.

[46] Yıldız, B., Karadeniz, S., Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: MacWilliams identities, projections and formally self-dual codes. Finite Fields and Their Applications, 27 (1), 24-40, 2014.

[47] Karadeniz, S., Yıldız, B., $(1+v)-$constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Journal of Franklin Institute, 348: 2625-2632, 2011.

[48] Bag, T., Islam, H., Prakash, O., Upadhyay, A.K., A study of constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 3\rangle$. Discrete Mathematics, Algorithms and Applications, 10 (4), 10 pages, 2018.

[49] Dinh, H.Q., Singh, A.K., Kumar, N., Sriboonchitta, S., On constacyclic codes over $\mathbb{Z}_4[v]/\langle v^2 - v\rangle$ and their Gray images. IEEE, Communcations Letters, 22 (9), 1758-1761, 2018.

[50] Qian, J.F., Zhang, L.N., Zhu, S.X., $(1+u)-$constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Appl. Math. Lett., 19: 820-823, 2006.

[51] Abualrub, T., Siap, İ., Constacyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2$. J. Franklin Inst. 346: 520-529, 2009.

[52] Cengellenmis, Y., Dertli, A., Aydın, N., On some constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$, their $\mathbb{Z}_4 -$images and new codes. Designs, Codes and Cryptography, 86: 1249-1255, 2018.

[53] Wolfmann, J., Binary images of cyclic codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory, 47: 1773-1779, 2001.

[54] Cao, Y., Li, Q., Cyclic codes of odd length over $\mathbb{Z}_4[u]/\langle u^k \rangle$. Cryptogr. Commun. 9(5), 599-624, 2016.

[55] Roman, S., Advanced Linear Algebra. Third Edition, Springer, 2010.

[56] Özen, M., Uzekmek, F.Z:, Oztas, E.S., Cyclic and constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^3 - u^2 \rangle$. and their Gray image. Turkish Journal of Mathematics, 45: 579-596, 2021.

[57] Boucher, D., Geiselmann, W., Ulmer, F., Skew cyclic codes. Applicable Algebra in Engineering, Communication and Computing, 18 (4), 379-389, 2007.

[58] Boucher D, Sole P, Ulmer F. Skew constacyclic codes over Galois rings. Adv. Math. Commun., 2008; 2: 273-292.

[59] 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.

[60] Abualrub, T., Aydın, N., Seneviratne, P., $\theta-$Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Australasian J. Combinatorics, 54, 115-126, 2012.

[61] 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.

[62] Sharma A, Bhaintwal M. A class of skew-constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. Int. J. Information and Coding Theory, 2017; 4: 289-302.

[63] Boucher D, Ulmer F. Coding with skew polynomial rings. J. Symb. Comput., 44: 1644-1656, 2009.

[64] 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.

[65] Ashraf, M., Mohammad, G., Skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. Asian-Europan Journal of Mathematics, 11 (5), 11 pages, 2018.

[66] Gaborit, P., King, O., Linear constructions for DNA codes. Theoretical Computer Science, vol. 334, no. 1–3, pp. 99–103, 2005.

[67] Abulraub, T., Ghrayeb, A., Zeng, X.N., Construction of cyclic codes over $GF(4)$ for DNA computing. J. Franklin Inst., 343 (4-5), 448–457, 2006.

[68] Oztas, E.S:, Siap, I., Lifted polynomials over $\mathbb{F}_{16}$ and their applications to DNA codes, Filomat, 27 (3), 459–466, 2013.

[69] Oztas, E.S:, Siap, On a generalization of lifted polynomials over finite fields and their applications to DNA codes. Int. J. Comput. Math., 92 (9), 1976–1988, 2015.

[70] Limbachiya, D., Rao, B., Gupta, M.K., The art of DNA strings: Sixteen years of DNA Coding Theory. Arxiv: 1607.00266.

[71] Bayram, A., Oztas, E.S., Siap, I., Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications. Des. Codes Cryptogr., 80 (2): 379-393, 2015.

[72] Siap, İ., Abualrub, T., Ghrayeb, A., Cyclic DNA codes over the ring $\mathbb{F}_2[u]/\langle u^2-1\rangle$ based on the deletion distace. Journal of Franklin Int., 346:731-740, 2009.

[73] Yıldız, B., Siap, İ., Cyclic Codes over $\mathbb{F}_2[u]/\langle u^4-1\rangle$ and applications to DNA codes, Computers and Math. with Applications, 63: 1169-1176, 2012.

[74] Oztas, E.S:, Yildiz, B., Siap, I., A novel approach for constructing reversible codes and application to DNA codes over the ring $\mathbb{F}_2[u]/\langle u^{2k}-1\rangle$. Finite Fields and Their Applications, 46: 217–234, 2017.

[75] Delsarte, P., Levenshtein, V.I., Association shemes and Coding theory. IEEE Trans. Inform. Theory, 44: 2477-2504, 1998.

[76] 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.

[77] Abualrub, T., Şiap, İ., Aydın, N., $\mathbb{Z}_2\mathbb{Z}_4$ – additive Cyclic Codes. IEEE Trans. Inf. Theory, 60 (3), 1508-1514, 2014.

[78] 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.

[79] Borges, J., Fernández-Córdoba, C., Ten-Valls, $\mathbb{Z}_2\mathbb{Z}_4$ – additive cyclic codes, generator polynomials and dual codes. IEEE Trans. Inform. Theory, 62: 6348–6354, 2016.

[80] Aydoğdu, İ., Abualrub, T., Siap, İ., $\mathbb{Z}_2\mathbb{Z}_2[u]-$Cyclic and Constacyclic Codes. IEEE Trans. on Inf. Theory, 2016.

[81] Melakhessou, A., Aydın, N., Hebbache, Z., Guenda, K., $\mathbb{Z}_q\left(\mathbb{Z}_q+u\mathbb{Z}_q\right)-$ linear skew constacyclic codes. J. Algebra Comb. Discrete Appl. 7 (1), 85-101, 2019.

[82] Diao, L., Gao, J., Lu, J., Some results one $\mathbb{Z}_p\mathbb{Z}_p[u]-$additive cyclic codes. Advances in Mathematics of Communications, 14 (4), 555-572, 2020.

ÖZGEÇMİŞ

Adı Soyadı **:** Fatma Zehra UZEKMEK

ÖĞRENİM DURUMU

Derece	**Eğitim Birimi**	**Mezuniyet Yılı**
Doktora	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Matematik	2021
Yüksek Lisans	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Matematik	2015
Lisans	Sakarya Üniversitesi / Fen Edebiyat Fakültesi / Matematik	2013
Lise	Özel Zaim Anadolu Lisesi	2008

YABANCI DİL

İngilizce

ESERLER (makale, bildiri, proje vb.)

1. Ozen, M., Uzekmek, F.Z., Aydın, N, Ozzaim, N.T., Cyclic and some constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$. Finite Fields and Their Applications, 38: 27-39, 2016.

2. Ozen, M., Uzekmek, F.Z., Macwilliams identities of linear codes over the ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$. Tojsat, 6 (1): 40-44, 2016.

3. Ozen, M., Uzekmek, F.Z., Oztas, E.S., Cyclic and constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^3-u^2\rangle$. and their Gray image. Turkish Journal of Mathematics, 45: 579-596, 2021.