T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI GRUP HALKALARINDA KODLARIN YAPISI

MEHMET EMİN KÖROĞLU

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
PROF. DR. BAYRAM ALİ ERSOY

İSTANBUL, 2017

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BAZI GRUP HALKALARINDA KODLARIN YAPISI

Mehmet Emin KÖROĞLU tarafından hazırlanan tez çalışması 03.11.2017 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKROTA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Prof. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi

Prof. Dr. Ahmet Göksel AĞARGÜN

Yıldız Teknik Üniversitesi

Prof. Dr. Ünsal TEKİR

Marmara Üniversitesi

Prof. Dr. Mehmet ÖZEN

Sakarya Üniversitesi

Doç. Dr. Emre KOLOTOĞLU

Yıldız Teknik Üniversitesi

Bu çalışma, **TÜBİTAK BİDEB 2211 Yurt İçi Doktora Burs Programı** ve Yıldız Teknik Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü'nün **2016-01-03-DOP01** numaralı projesi ile desteklenmiştir.

ÖNSÖZ

Yapıcı desteğiyle her daim yanımda olan tez danışmanım Sayın Prof. Dr. Bayram Ali ERSOY'a ve tez jüri üyeleri Sayın Prof. Dr. Ahmet Göksel AĞARGÜN, Sayın Prof. Dr. Ünsal TEKİR, Sayın Prof. Dr. Mehmet ÖZEN ve Sayın Doç. Dr. Emre KOLOTOĞLU'na çok teşekkür ederim.

Tez konusunun belirlenmesi ve ilerlemesi noktasında yol gösteren ve olumlu katkılarını esirgemeyen Sayın Prof. Dr. İrfan ŞİAP'a ve tezin önerisi ile ilk iki izleme komitesinde yer alarak değerli katkılarını sunan Sayın Doç. Dr. Bahattin YILDIZ'a şükranlarımı sunarım.

Doktora eğitimim süresince beni maddi olarak destekleyen TÜBİTAK'a ve bu çalışmayı bilimsel araştırma projesi olarak destekleyen YTÜ Bilimsel Araştırma Projeleri Koordinatörlüğü'ne teşekkürlerimi bildiririm.

Sevgi, ilgi ve destekleriyle hayatımı besleyen, dünyamı güzelleştiren sevgili eşim ve biricik oğluma çok teşekkürler.

Kasım, 2017

Mehmet Emin KÖROĞLU

İÇİNDEKİLER

SİMGE LİSTESİ

RG	R halkası ile G grubunun oluşturduğu grup halkası
FG	F cismi ile G grubunun oluşturduğu grup cebiri
$M_n(R)$	elemanları R halkasından olan $n \times n$ tipindeki matrislerin kümesi
C_n	mertebesi n olan çarpımsal devirli grup
$ZD(R)$	R halkasının sıfır bölenlerinin kümesi
$U(R)$	R halkasının birimsel elemanlarının kümesi
$M(RG,\alpha)$	$\alpha \in RG$ ye karşılık gelen matris
u^T	$u \in RG$ nin transpozesi
$\langle u,z \rangle$	$u,z \in RG$ nin standart iç çarpımı
$ebob(a,b)$	a ile b tam sayılarının en büyük ortak böleni
$R_n = \mathbb{F}_q[x] / \langle x^n - 1 \rangle$	bölüm halkası
$C \leq_{a.v.} \mathbb{F}_q^n$	C, $\mathbb{F}_q^n$ nin alt vektör uzayıdır
$C^{\perp}$	C lineer kodunun duali
$\lvert C \rvert$	C lineer kodunun eleman sayısı
$boy(C)$	C lineer kodunun alt vektör uzayı olarak boyutu
$boy_S(C)$	C, $\mathbb{Z}_4$ – lineer kodunun alt modül olarak serbest boyutu
$boy_{\bar{S}}(C)$	C, $\mathbb{Z}_4$ – lineer kodunun alt modül olarak serbest olmayan boyutu
$\bar{G}$	C lineer kodunun üreteç matrisi
H	C lineer kodunun kontrol matrisi
$d(C)$	C kodunun minimum Hamming uzaklığı
$\forall$	evrensel niceleyici her
$der(f(x))$	$f(x)$ polinomunun derecesi
$\mathbb{F}_q^*$	$\mathbb{F}_q - \{0\}$
$\mathbb{Z}_n^*$	$\mathbb{Z}_n$ halkasının birimsel elemanlarının kümesi

$(n,M)_q$	$\mathbb{F}_q$ alfabesi üzerinde $n-$uzunluklu, M elemanlı kod
$[n,k,d]_q$	$\mathbb{F}_q$ alfabesi üzerinde $n-$uzunluklu, q^k elemanlı lineer kod
$[[n,k,d]]_q$	$\mathbb{C}^{q^n}$ Hilbert uzayının q^k boyutlu alt uzayı
$\mathbb{F}_q^n$	$\mathbb{F}_q$ cismi üzerinde $n-$boyutlu vektör uzayı
$\langle x^n-1\rangle$	$\mathbb{F}_q[x]$ polinom halkasında x^n-1 polinomunun ürettiği ideal
$\langle x,y\rangle$	x ile y vektörlerinin iç çarpımı
$d_H(x,y)$	x ile y vektörleri arasındaki Hamming uzaklığı
$w_H(x)$	x vektörünün Hamming ağırlığı
$a\|b$	a sayısı b sayısını tam böler
$\varphi(n)$	n den küçük ve n ile aralarında asal olan sayıların sayısı
$\lfloor . \rfloor$	alt tam değer fonksiyonu
$\mathrm{supp}(\alpha)$	$\alpha \in RG$ elemanının supportu
$w(M)$	M alt modülünün minimum uzaklığı
$C \oplus C^{\perp}$	C ile dualinin direkt toplamı

KISALTMA LİSTESİ

bkz.	bakınız
LCD	dual kodu ile arakesiti sıfır vektörü olan lineer kod
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
YTÜ	Yıldız Teknik Üniversitesi
v.d.	ve diğerleri

ÇİZELGE LİSTESİ

Sayfa

ÖZET

BAZI GRUP HALKALARINDA KODLARIN YAPISI

Mehmet Emin KÖROĞLU

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Prof. Dr. Bayram Ali ERSOY

Dijital iletişimin öneminin artmasıyla birlikte cebirsel kodlama teorisi bilim alanı yaygın ve hızlı bir şekilde gelişmektedir. Bu anlamda kodlar için yeni inşa yöntemleri, yeni parametreler bulmak veya kodların minimum uzaklığı ya da boyutları üzerinde bazı sınırlar bulmak büyük önem arz etmektedir.

Grup halkası kavramı ilk olarak Arthur Cayley tarafından (bkz. [1]) tanıtıldı. Grup halkaları birimsel elemanlar ve sıfır bölenlerce zengin olduklarından yeni kod parametreleri elde etmek için oldukça elverişli cebirsel yapılardır. Kodların birçok özelliği grup halkalarının kavramları yardımıyla çok rahat bir şekilde ifade edilebilir (bkz. [2], [3]). Grup halkaları üzerinde kodların yapısını incelediğimiz bu çalışma aşağıdaki şekilde düzenlenmiştir.

Birinci bölüm literatür özeti, tezin amacı ve hipoteze ayrılmıştır. İkinci ve üçüncü bölümlerde tezin devamı için gerekli olan grup halkaları ve cebirsel kodlama teorisi hakkındaki kavram ve notasyonlar bir araya getirilmiştir. Dördüncü bölümde devresel sıfır bölen kodların yapısı bir grup halkası ailesinde çalışılmıştır. Ayrıca elde edilen bu kodların eleman sayıları ile dual kodları verilmiştir.

Beşinci bölümde literatürde bir ilk olarak sabit devirli kodlar ile grup cebirleri arasında ilişki kurulmuş ve bu kodların yapısı çalışılmıştır. Ayrıca grup cebirlerindeki sıfır bölenler kullanılarak sabit devirli kodlar için bir inşa yöntemi verilmiştir. Bunlara ek olarak önerilen inşa metodu yardımıyla sabit devirli kodlar için bazı iyi kod parametreleri tablolar halinde verilmiştir. Daha sonra bu kodlar içinde kendine dik ve kendine dual

olan kodlar belirlenmiştir. Bu kodlara bağlı olarak kuantum hata düzelten kodlar için bazı iyi kod parametreleri elde edilmiştir.

Buna ek olarak $\left(\mathbb{F}_q + v\mathbb{F}_q\right)G$ grup halkasındaki sabit devirli kodlardan kendine dik ve kendine dual olan kodlar belirlenmiştir. Belirlenen bu kodlar için uygun bir Gray dönüşümü tanımlanarak $\mathbb{F}_q$ sonlu cismi üzerinde birçok kuantum hata düzelten kod parametresi elde edilmiştir.

Altıncı bölümde grup halkaları üzerinde LCD (dualleri ile kesişimi sıfır vektörü olan lineer kodlar) kodlar için bazı gerek ve yeter koşullar belirlenmiştir. Son bölüm ise sonuç ve önerilere ayrılmıştır.

Anahtar Kelimeler: Grup halkaları, lineer kodlar, devresel kodlar, sabit devresel kodlar, LCD kodlar

ABSTRACT

THE STRUCTURE OF CODES OVER GROUP RINGS

Mehmet Emin KÖROĞLU

Department of Mathematics

PhD. Thesis

Advisor: Prof. Dr. Bayram Ali ERSOY

Due to the increasing importance of digital communications, the area of research in algebraic coding theory is broad and fast developing. In this sense, finding new construction methods, new parameters for codes or finding bounds on minimum distance or dimension of codes have a great importance.

The notion of group rings was introduced by Arthur Cayley (see [1]) for the first time. Since group rings are rich in units and zero divisors, they are quite suitable algebraic structures to obtain new code parameters. Many code properties may more easily be expressed in terms of group ring properties (see [2], [3]). This work, in which we study the structure of codes over group rings, is organized as the following.

The first section is devoted to the literature review, aim of the thesis and the hypothesis. Section 2 and Section 3 collects the notions and notations needed in the rest of the dissertation about group rings and algebraic coding theory. In Section 4 we study the structure of cyclic zero divisor codes over a family of group rings. In addition, we determine the number of elements of these codes and we introduced the dual codes.

In Section 5 for the first time in the literature, we establish a relation between constacyclic codes and group algebras and study their algebraic structures. Further, we give a method for constructing constacyclic codes by using zero-divisors in group algebras. Some good parameters for constacyclic codes which are derived from the

proposed construction are also listed. Then, we determine self dual and self orthogonal codes arising from constacyclic codes over group algebras. Also, based on these codes we obtained some good parameters for quantum error-correcting codes. Moreover, we determine self dual and self orthogonal codes arising from negacyclic codes over the group ring $\left(\mathbb{F}_q + v\mathbb{F}_q\right)G.$ By taking gray image of these codes we obtained many parameters for quantum error-correcting codes over the finite field $\mathbb{F}_q$.

In Section 6 we derive some necessary and sufficient conditions for LCD codes (linear codes with complementary duals) from group rings. The last section is reserved for the conclusions and future research directions.

Keywords: Group rings, linear codes, cyclic codes, constacyclic codes, LCD codes

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Grup halkaları üzerinde kodların araştırılması temelde iki esasa dayanmaktadır. Bunlardan birincisi grup halkalarının ilkel idempotentler (primitive idempotents) yardımıyla ayrıştırılarak ayrışımın basit (simple) parçalarına karşılık gelen en küçük kodların (minimal codes) elde edilmesidir. Bu yaklaşım da kendi içinde farklı cebirsel metotlar kullanmaktadır. Kimi çalışmalar RG grup halkasının üzerine inşa edildiği grubun karakterleri yardımıyla ilkel idempotenleri bulurken, kimi çalışmalar söz konusu grubun alt grupları yardımıyla istenen ilkel idempotentleri bulmaktadır. Bu yaklaşıma örnek olarak şu çalışmaları sıralayabiliriz: Berman [4]'te abelyan kodların yapısını, [5]'de ise yarı basit (semisimple) devirli ve abelian kodları çalışmıştır. MacWilliams [6]'da grup cebirleri üzerinde kodlar ve ideallerin yapısını ve [7]'de ise değişmeli (abelian) bir grup üzerine inşa edilen cebirin ideali olan ikili kodların (binary codes) yapısını irdelemiştir. Miller [8]'de belli kısıtlamalar altında $\mathbb{F}_2 G$ (G değişmeli bir grup) grup cebirinde iki minimal kodun aynı Hamming ağırlık dağılımına (weight distrubution) sahip olduğunu göstermiştir. Drensky ve Lakatos [9]'da grup cebirlerinin radikallerini araştırmışlardır. Sabin [10] ve [11]'de grup halkaları üzerinde yarı devirli (quasi cyclic) kodların cebirsel yapısını araştırmıştır. Forney ve Trott [12]'de abelian grup kodları ve dual kodlarını ele almışlardır. Aynı yazarlar [13]'te grup kodların kafes yapısı (trellis structure) ve minimal kodlama yapılarını ele almışlardır. Biglieri ve Elia [14]'te grup blok kodların yapısını incelemişlerdir. Pruthi ve Arora [15]'te ilkel idempotentlerini hesaplamak suretiyle grup halkalarında uzunluğu bir asalın kuvveti olan minimal

kodları ve [16]'da de uzunluğu $2p^n$ olan devirli kodları (cyclic codes) belirlemişlerdir. Bakshi v.d. [17] ve [18]'de sırasıyla uzunluğu 2^n ve $p^n q$ olan minimal devirli kodları belirlemişlerdir. Dutra v.d. [19]'da FG grup halkasında ilkel idempotentleri (primitive idempotents) G grubunun alt grupları yardımıyla hesaplayarak minimal kodlar elde etmişlerdir. Ayrıca elde edilen bu minimal kodların boyut ve ağırlıkları da hesaplanmıştır. Ferraz ve Milies [20]'de yarı basit değişmeli bir grup cebirinin basit bileşenlerinin (simple components) sayısını hesaplayarak minimal abelian kodlar elde etmişlerdir. Pıllado v.d. [21]'de bazı özel durumlar için grup kodların abelian olmaları için gerek ve yeter koşulları vermişlerdir. Milies v.d. [22]'de grup halkaları üzerindeki p^n uzunluklu devirli kodların minimum ağırlık ve boyutunu hesaplamışlardır. Chalom v.d. [23]'te grup halkaları üzerinde ikili minimal kodların üreteç idempotentlerini hesaplamışlardır. Schäfer [24]'te iki taraflı abelian grup halkası kodların yapısını çalışmıştır. Ranjeet ve Pruthi [25]'te $p^n q^m$ uzunluklu indirgenemez devirli quadratik kalan (quadratic residue) kodların yapısını çalışmışlardır.

İkinci yaklaşımda ise grup halkasının elemanlarını sol öteleme (left translation) temsili (representation) yardımıyla matrislerle eşleyip, matrislerin rankı yardımıyla sıfır bölen ve birimsel elemanlar tespit edildikten sonra bu elemanlar kullanılarak kodlar elde edilmektedir. Bu yaklaşım Ted Hurley ve arkadaşları tarafından ortaya konmuştur. Bu yaklaşımın literatürü aşağıdaki gibidir:

Hurley tarafından [26]'da mertebesi n olan bir G grubu üzerinde inşa edilen grup halkasının elemanları ile $n \times n$ tipinde girdileri R halkasından olan matrisler halkası $M_n(R)$'nin bir alt kümesi arasında bire-bir bir eşleme kurularak matrislerin rankı yardımıyla RG grup halkasının birimsel elemanları ve sıfır bölenlerinin tespit edilmesi kolaylaştırılmıştır. Paul Hurley ve Ted Hurley [2] ve [3]'te grup halkalarının sıfır bölen ve birimsel elemanları yardımıyla yeni bir kodlama yöntemi geliştirmişlerdir. Geliştirilen bu yöntem yardımıyla grup halkalarının sıfır bölen ve birimsel elemanları yardımıyla yeni kodlar elde etmek mümkündür. Ted Hurley [27] ve [28]'de grup halkalarındaki birimsel elemanların matris temsilleri yardımıyla konvolüsyon kodlar (convolutional codes) için genel bir inşa yöntemi vermiştir. Bu yöntem [29]'da daha detaylı olarak ele alınmıştır. OShaughnessy tarafından [30]'da grup halkaları üzerinde konvolüsyon

kodları için bir inşa yöntemi verilmiştir. Fu ve Feng [31]'de bazı grup halkaları üzerindeki kendine dik (self orthogonal) kodların yapısını araştırmışlardır. McLoughlin, [32]'de düzgün n-genin simetri grubu (dihedral group) üzerine inşa ettiği grup halkası üzerinde [3] çalışmasındaki yöntemi kullanarak $[48,24,12]_2$ parametrelerine sahip kendine dik kodu grup halkaları yardımıyla yeniden elde etmiştir. Barry Hurley ve Ted Hurley [33]'te birimsel ve idempotent elemanlar yardımıyla MDS (maximum distance separable) kod elde etmek için bir yöntem vermişlerdir.

1.2 Tezin Amacı

Bu tezde, ilk olarak $\mathbb{F}_p C_n$ grup halkaları üzerinde tanımlanan sıfır bölen kod (bkz. [3]) kavramı $\mathbb{Z}_4 C_n$ grup halkalarına genelleştirilecektir. Ayrıca grup halkaları üzerinde henüz tanımı yapılmayan sabit devirli (constacyclic) kodlar için bir inşa yöntemi verilecektir. Bu inşa yöntemi yardımıyla elde edilmesi mümkün olan sabit devirli kodların parametreleri araştırılacaktır. Daha sonra elde edilen bu sabit devirli kodlardan kuantum kod parametreleri elde etmek için kendine dik ve kendine dual olma şartları araştırılacaktır. Ayrıca iki kullanıcılı ikili kanallar için en uygun (optimal) dekodlama yeteneğine sahip olan LCD (dual kodu ile arakesiti sıfır vektörü olan lineer kod) kodların bazı özel grup halkaları üzerinde varlık koşulları belirlenecektir.

1.3 Hipotez

Grup halkalarının grup, halka, cisim gibi cebirsel yapılar ile karşılaştırıldığında daha genel cebirsel yapılar oldukları görülecektir. Dolayısıyla bu yapılar üzerinde farklı özellik ve parametrelere sahip kodların araştırılması daha anlamlı hale gelmektedir. Ayrıca grup halkaları sıfır bölenleri çok olan cebirsel yapılardır. Bu özellik aşikâr olmayan yeni kodların elde edilmesi için oldukça elverişlidir.

BÖLÜM 2

HATA DÜZELTEN KODLAR

Bu bölümde hata düzelten kodlar hakkında gerekli önbilgiler verilecektir. Hata düzelten kodlarla ilgili bilgiler *"The theory of error correcting codes"* (1977) [34], *"Coding Theory: A First Course"* (2004) [35], *"The Art of Error Correcting Coding*" (2006) [36] ve "*Quaternary codes*" (1997) [37] isimli kitaplardan yararlanılarak hazırlanmıştır.

2.1 Hata Düzelten Kodlar

Tanım 2.1 $\mathbb{F}_q$, q (burada q asal bir sayının kuvveti) elemanlı sonlu bir cisim olmak üzere, $\mathbb{F}_q$ üzerinde n-uzunluğunda ve eleman sayısı M olan bir C kodu, $\mathbb{F}_q^n$ uzayının bir alt kümesidir. Böyle bir kod $(n, M)_q$ parametreleriyle gösterilir.

Tanım 2.2 (Lineer Kod) $\mathbb{F}_q$ üzerinde n-uzunluğunda ve boyutu k olan bir C lineer kodu, $\mathbb{F}_q^n$ vektör uzayının bir alt uzayıdır. Böyle bir kod $[n, k]_q$ parametreleriyle gösterilir.

Özel olarak $q = 2$ için alfabesi $\mathbb{F}_2$ olan bir koda ikili (binary) kod, $q = 3$ için alfabesi $\mathbb{F}_3$ olan bir koda üçlü (ternary) kod denir.

Tanım 2.3 C alfabesi, $\mathbb{F}_q$ olan bir lineer kod olsun.

i) C lineer kodunun dual kodu $C^{\perp}$ ile gösterilir ve $C^{\perp}=\left\{x\in\mathbb{F}_q^n:\langle x,c\rangle=0,\forall c\in C\right\}$ şeklinde tanımlanır. Burada $\langle x,c\rangle$ ile x ve c vektörlerinin iç çarpımı gösterilmektedir.

ii) C lineer kodunun boyutu, C'nin vektör uzayı olarak boyutudur ve $boy(C)$ ile gösterilir.

Teorem 2.1 C, $\mathbb{F}_q$ üzerinde n-uzunluğunda ve boyutu k olan bir lineer kod olsun. Bu durumda;

i) $|C|=q^{boy(C)}$ yani $M=q^k$ dır.

ii) $C^{\perp}$ bir lineer koddur ve $boy(C)+boy\left(C^{\perp}\right)=n$ dir.

iii) $\left(C^{\perp}\right)^{\perp}=C$ dir.

Tanım 2.4 C, $\mathbb{F}_q$ cismi üzerinde bir lineer kod olsun. Eğer $C\subseteq C^{\perp}$ ise C'ye *kendine dik kod*, eğer $C=C^{\perp}$ ise C'ye *kendine dual kod* denir.

2.1.1 Üreteç ve Kontrol Matrisleri

Tanım 2.5 C, $[n,k]_q$ parametrelerine sahip lineer kodun bir alt vektör uzayı olduğunu ve bu alt vektör uzayının $\{c_1,c_2,\ldots,c_k\}$ şeklinde bir tabana sahip olduğunu daha önce söylemiştik. Tabandaki vektörleri satır kabul eden G matrisine, C lineer kodun *üreteç matrisi* denir. Yani

$$\overline{G}=\begin{pmatrix}-c_1-\\-c_2-\\\vdots\\-c_k-\end{pmatrix}_{k\times n}$$

matrisine $[n,k]_q$ parametrelerine sahip C lineer kodunun *üreteç matrisi* denir.

Bir C lineer kodunun kendine dik olduğunu göstermek için üreteç matrisindeki satırların ikişerli birbirlerine dik olduğunu göstermek yeterlidir.

Tanım 2.6 Bir C lineer kodunun *parite kontrol matrisi* $C^{\perp}$ dual kodun üreteç matrisidir ve genellikle H ile gösterilir. Yani $C=\left\{x\in\mathbb{F}_q^n \middle| Hx^T=0\right\}$ dir.

Tanım 2.7 $\left[n,k\right]_q$ parametreli C lineer kodun üreteç matrisi $G'=\left[I_k \middle| A\right]$ olsun. Bu durumda G''nin *standart formda* olduğu söylenir. Burada I_k, $k\times k$ tipinde birim matris, A ise $k\times\left(n-k\right)$ tipinde bir matristir.

Teorem 2.2 Bir $\left[n,k\right]_q$ parametreli C lineer kodunun üreteç matrisi standart formda verilmişse $H=\left[-A^T \mid I_{n-k}\right]$ matrisi, C için bir kontrol matrisidir.

$C\to\left[n,k\right]_q$ lineer kodunun üreteç ve kontrol matrisleri sırasıyla aşağıdaki gibi olsun.

$$\bar{G}=\begin{pmatrix}-c_1-\\-c_2-\\\vdots\\-c_k-\end{pmatrix}_{k\times n},\quad H=\begin{pmatrix}-h_1-\\-h_2-\\\vdots\\-h_{n-k}-\end{pmatrix}_{(n-k)\times n}$$

Bu durumda $\bar{G}H^T=0$ dır. Burada 0, $k\times\left(n-k\right)$ tipinde sıfır matristir.

2.1.2 Hamming Uzaklık ve Hamming Ağırlık

Tanım 2.8 (Hamming Uzaklığı) $x=\left(x_1,x_2,...,x_n\right)$, $y=\left(y_1,y_2,...,y_n\right)\in\mathbb{F}_q^n$ olsun. $d:\mathbb{F}_q^n\times\mathbb{F}_q^n\to\mathbb{N}$, $d_H\left(x,y\right)=\left|\left\{i:x_i\neq y_i,i=1,2,...,n\right\}\right|$ şeklinde tanımlanan fonksiyona *Hamming uzaklığı* denir.

Teorem 2.3 $d:\mathbb{F}_q^n\times\mathbb{F}_q^n\to\mathbb{N}$, $d_H\left(x,y\right)=\left|\left\{i:x_i\neq y_i,i=1,2,...,n\right\}\right|$ şeklinde tanımlanan fonksiyon $\mathbb{F}_q^n$ vektör uzayı üzerinde bir metriktir.

Tanım 2.9 Bir C kodunun minimum Hamming uzaklığı C'nin birbirinden farklı mümkün tüm kod söz çiftleri arasındaki en küçük Hamming uzaklığıdır ve $d(C)$ ile gösterilir. Yani $d(C)=\min\{d_H(x,y): x\neq y, x,y\in C\}$ olarak tanımlanır. Minimum uzaklığı d olan bir $[n,k]_q$ lineer kod $[n,k,d]_q$ parametreleri ile gösterilir.

Tanım 2.10 (Hamming Ağırlığı) Bir $x\in\mathbb{F}_q^n$ vektörünün Hamming ağırlığı $w_H(x)$ ile gösterilir ve x vektörünün sıfırdan farklı koordinatlarının sayısı olarak tanımlanır. Yani $w_H(x)=\left|\{i: x_i\neq 0, x=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q^n\}\right|$. Bir C kodunun minimum Hamming ağırlığı $w(x)=\min\left|\{i: x_i\neq 0, x=(x_1,x_2,\ldots,x_n)\in C\}\right|$ dir.

Teorem 2.4 $x,y\in\mathbb{F}_q^n$ için $d_H(x,y)=w_H(x-y)$ dir.

Teorem 2.5 Eğer $C\subseteq\mathbb{F}_q^n$ bir lineer kod ise $d(C)=w(C)$.

Teorem 2.6 C lineer kodunun minimum uzaklığının d olabilmesi için gerek ve yeter şart C'nin kontrol matrisinin en az d tane sütununun lineer bağımlı ve herhangi $(d-1)$ tane sütununun lineer bağımsız olmasıdır.

2.1.3 Lineer Kodlarda Kodlama

Tanım 2.11 C $[n,k,d]_q$ parametrelerine sahip bir lineer kod ve $\overline{G}=\begin{pmatrix}-c_1-\\-c_2-\\\vdots\\-c_k-\end{pmatrix}$ C'nin üreteç matrisi olsun. Bu durumda bir $u=(u_1,u_2,\ldots,u_k)\in\mathbb{F}_q^k$ için $u\overline{G}=c\in C\subseteq\mathbb{F}_q^n$ şeklindeki ifadeye bir u sözünün kodlanması ve $c\in C$ vektörüne de bir *kod söz* denir.

2.1.4 Devirli Kodlar

Tanım 2.12 $C \subseteq \mathbb{F}_q^n$ bir lineer kod olsun. Eğer $c = (c_0, c_1, c_2, ..., c_{n-1}) \in C$ iken $c = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$ oluyorsa C'ye bir devirli kod denir.

2.1.4.1 Devirli Kodun Polinom ile Temsili

$C \subseteq \mathbb{F}_q^n$ bir devirli kod olmak üzere;

$$\bar{\varphi} : C \to \mathbb{F}_q[x] / \langle x^n - 1 \rangle = R_n, \quad \bar{\varphi}(c) = \bar{\varphi}(c_0, c_1, ..., c_{n-1}) = c_0 + c_1 x + ... + c_{n-1} x^{n-1} \tag{2.1}$$

şeklindeki dönüşüm her devirli koda bir polinom karşılık getirir. Burada $\mathbb{F}_q[x] / \langle x^n - 1 \rangle = R_n$ bölüm halkası ve $\langle x^n - 1 \rangle$ ise $\mathbb{F}_q[x]$ polinom halkasının bir idealidir.

Her devirli kodun $\bar{\varphi}$ altındaki görüntüsü bir ideal oluşturur ve her ideale karşılık bir devirli kod gelir.

Teorem 2.7 $\bar{\varphi}(C)$, $\mathbb{F}_q[x] / \langle x^n - 1 \rangle = R_n$ bölüm halkasının sıfırdan farklı bir ideali olsun. Bu durumda bir en küçük dereceli monik $g(x) \in \bar{\varphi}(C)$ polinomu vardır ve $g(x) \mid (x^n - 1)$ dir.

Tanım 2.13 Teorem 3.7'de verilen $g(x) \in \bar{\varphi}(C)$ polinomuna $\bar{\varphi}(C)$'nin ve dolayısıyla C devirli kodun üreteç polinomu denir ve $C = \langle g(x) \rangle$ şeklinde gösterilir.

Tanım 2.14 $\bar{\varphi}(C)$, $\mathbb{F}_q[x] / \langle x^n - 1 \rangle = R_n$ bölüm halkasının sıfırdan farklı bir ideali ve $C = \langle g(x) \rangle$, $der(g(x)) = r$ olmak üzere, $\bar{G} = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-r-1} g(x) \end{pmatrix}_{(n-r) \times n}$ ile verilen matrise C devirli kodunun üreteç matrisi denir.

2.1.5 Singleton Sınırı ve MDS Kodlar

Tanım 2.15 (Lineer kodlar için Singleton sınırı) C, $\mathbb{F}_q$ cismi üzerinde $[n,k,d]_q$ parametrelenine sahip lineer bir kod olsun. Bu durumda $k \le n-d+1$ eşitsizliği sağlanır. Bu eşitsizliğe lineer kodlar için Singleton sınırı denir.

Tanım 2.16 (MDS Kodlar) C, $\mathbb{F}_q$ cismi üzerinde $[n,k,d]_q$ parametrelenine sahip lineer bir kod olsun. Eğer $k+d=n+1$ oluyorsa C lineer koduna MDS (maximum distance separable code) kod denir.

2.1.6 $\mathbb{Z}_4$ Lineer Kodlar

Tanım 2.17 $\mathbb{Z}_4=\{0,1,2,3\}$ modülo 4 kalan sınıflarının kümesi ve n pozitif tam sayı olmak üzere $\mathbb{Z}_4^n=\{(a_1,a_2,\ldots,a_n)\,|\,a_i\in\mathbb{Z}_4\}$ olsun. $\varnothing\neq C\subset\mathbb{Z}_4^n$ alt kümesine $\mathbb{Z}_4$-kod denir. Özel olarak, eğer C devirli ise $\mathbb{Z}_4$-devirli kod ve C, $\mathbb{Z}_4^n$ nin bir alt grubu ise $\mathbb{Z}_4$-lineer kod denir.

Teorem 2.8 Herhangi bir C, $\mathbb{Z}_4$-lineer kodu $\overline{G}=\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix}$ matrisi tarafından üretilen koda permütasyon denktir.

Teorem 2.8'deki k_1 tam sayısına C kodunun serbest boyutu ve k_2 tam sayısına da C kodunun serbest olmayan boyutu denir. Dolayısıyla C kodunun eleman sayısı $|C|=4^{k_1}2^{k_2}$ dir. Bir C, $\mathbb{Z}_4$-lineer kodun serbest boyutunu $\dim_s(C)$ ve serbest olmayan boyutunu da $\dim_{\bar{s}}(C)$ ile göstereceğiz.

BÖLÜM 3

GRUP HALKALARI

Bu başlık altında grup halkaları hakkında verilen ön bilgiler "*An introduction to group rings"* ([38]) ve *"The algebraic structure of group rings"* ([39]) isimli kitapları esas almaktadır.

3.1 Grup Halkaları

$G=\{g_1,g_2,\ldots,g_n\}$ sonlu bir grup ve R halka olmak üzere; RG grup halkası $\alpha=\sum_{i=1}^{n}a_ig_i,\ (a_i\in R,\ g_i\in G)$ şeklindeki tüm elemanların kümesidir. Toplama ve çarpma işlemleri aşağıdaki gibi tanımlanırsa;

$$\alpha+\beta=\sum_{i=1}^{n}a_ig_i+\sum_{i=1}^{n}b_ig_i=\sum_{i=1}^{n}(a_i+b_i)g_i \tag{3.1}$$

$$\alpha\beta=\left(\sum_{i=1}^{n}a_ig_i\right)\left(\sum_{j=1}^{n}b_jg_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{n}a_ib_jg_ig_j \tag{3.2}$$

RG bir halka olur. Eğer R ve G değişmeli ise RG değişmeli ve eğer R birimli ise RG birimli olur. Ayrıca bir $\lambda\in R$ için skaler ile çarpım $\lambda.\alpha=\lambda\left(\sum_{i=1}^{n}a_ig_i\right)=\sum_{i=1}^{n}(\lambda a_i)g_i$ ile tanımlıdır. RG bir R modül olarak da düşünülebilir [33,34].

Örnek 3.1: $C_2=\langle g\rangle=\{1,g\}$ mertebesi 2 olan çarpımsal devirli grup ve $\mathbb{F}_3=\{0,1,2\}$ karakteristiği 3 olan sonlu cisim olmak üzere,

$$\mathbb{F}_3C_2 = \{a_0 + a_1 g \,|\, a_0, a_1 \in \mathbb{F}_3\} = \{0,1,2,g,2g,1+g,2+g,1+2g,2+2g\}$$

9 elemanlı, değişmeli bir grup halkasıdır. Bu grup halkasının işlem tabloları Çizelge 3.1 ve Çizelge 3.2'de verilmiştir.

Çizelge 3. 1 $\mathbb{F}_3C_2$ grup halkası için toplama işlemi

+	0	1	2	g	2g	1+g	1+2g	2+g	2+2g
0	0	1	2	g	2g	1+g	1+2g	2+g	2+2g
1	1	2	0	1+g	1+2g	2+g	2+2g	g	2g
2	2	0	1	2+g	2+2g	g	2g	1+g	1+2g
g	g	1+g	2+g	2g	0	1+2g	1	2+2g	2
2g	2g	1+2g	2+2g	0	g	1	1+g	2	2+g
1+g	1+g	2+g	g	1+2g	1	2+2g	2	2g	0
1+2g	1+2g	2+2g	2g	1	1+g	2	2+g	0	g
2+g	2+g	g	1+g	2+2g	2	2g	0	1+2g	1
2+2g	2+2g	2g	1+2g	2	2+g	0	g	1	1+g

Çizelge 3. 2 $\mathbb{F}_3C_2$ grup halkası için çarpma işlemi

x	0	1	2	g	2g	1+g	1+2g	2+g	2+2g
0	0	0	0	0	0	0	0	0	0
1	0	1	2	g	2g	1+g	1+2g	2+g	2+2g
2	0	2	1	2g	g	2+2g	2+g	1+2g	1+g
g	0	g	2g	1	2	1+g	2+g	1+2g	2+2g
2g	0	2g	g	2	1	2+2g	1+2g	2+g	1+g
1+g	0	1+g	2+2g	1+g	2+2g	2+2g	0	0	1+g
1+2g	0	1+2g	2+g	2+g	1+2g	0	1+g	1+2g	0
2+g	0	2+g	1+2g	1+2g	2+g	0	1+2g	2+g	0
2+2g	0	2+2g	1+g	2+2g	1+g	1+g	0	0	2+2g

Tanım 3.1 R değişmeli bir halka ve $0 \neq a,b \in R$ olsun. $ab = 0$ oluyorsa a ve b elemanlarına R halkasında sıfır bölendir denir. Bir halkanın sıfır bölenlerinin kümesi $ZD(R)$ ile gösterilir.

Örnek 3.2 Örnek 3.1'de verilen $\mathbb{F}_3C_2$ grup halkasının sıfır bölenleri $ZD(\mathbb{F}_3C_2) = \{1+g, 2+g, 1+2g, 2+2g\}$ dir.

Tanım 3.2 R birimli, değişmeli bir halka ve $0 \neq a,b \in R$ olsun. $ab=1$ oluyorsa a ve b elemanlarına R halkasında birimseldir denir. Bir halkanın birimsel elemanlarının kümesi $U(R)$ ile gösterilir.

Örnek 3.3 Örnek 3.1'de verilen $\mathbb{F}_3C_2$ grup halkasının birimsel elemanları $U(\mathbb{F}_3C_2)=\{1,2,g,2g\}$ dir.

Sonlu bir grup halkasında $RG=\{0\}\cup ZD(R)\cup U(R)$ olur. Ayrıca $|RG|$, RG grup halkasının eleman sayısını göstermek üzere $|RG|=|R|^{|G|}$ şeklindedir. Örneğin; $|\mathbb{F}_3C_2|=|\mathbb{F}_3|^{|C_2|}=3^2=9.$

3.2 Grup Halkaları ve Matrisler

$\{g_1,g_2,\ldots,g_n\}$ mertebesi n olan bir G grubunun elemanlarının sıralı bir listesi olsun. $u=\sum_{i=1}^{n} a_i g_i \in RG$ elemanı bir temsil yardımıyla $M_n(R)$ nin bir elemanına karşılık getirilebilir. $M(RG,u)$ veya U ile göstereceğimiz bu matris aşağıdaki gibi tanımlıdır.

$$\begin{pmatrix} a_{g_1^{-1}g_1} & a_{g_1^{-1}g_2} & \ldots & a_{g_1^{-1}g_n} \\ a_{g_2^{-1}g_1} & a_{g_2^{-1}g_2} & \ldots & a_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{g_n^{-1}g_1} & a_{g_n^{-1}g_2} & \ldots & a_{g_n^{-1}g_n} \end{pmatrix}.$$

Bu temsil RG grup halkasının elemanları ile girdileri R halkasından olan $n\times n$ tipindeki matrisler halkasının bir alt kümesi arasında birebir bir eşlemeyi mümkün kılar [26].

Ayrıca $\theta: RG \to R^n$, $\theta\left(\sum_{i=1}^{n} a_i g_i\right)=(a_1,a_2,\ldots,a_n)$ dönüşümü ile RG'nin elemanları ve R^n nin elemanları arasında bir bire-bir eşleme kurulabilir.

Örnek 3.4 $\mathbb{F}_3C_2$ grup halkasında $u=1+2g$ elemanına karşılık gelen matris $U=\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ dir.

Eğer G grubu devirli ise bir $\alpha \in RG$ için $M\left(RG,\alpha\right)$ devresel (circulant) bir matris olur.

Tanım 3.3 $\alpha = \sum_{g\in G} a_g g \in RG$ elemanın transpozu $\alpha^T = \sum_{g\in G} a_g g^{-1} \in RG$ dir.

Örnek 3.5 $\mathbb{F}_3 C_2$ grup halkasında $\alpha = 1+2g$ elemanın transpozu $\alpha^T = 1+2g$ olur.

3.3 Grup Halkası Kodlaması ile Elde Edilen Kodlar

Bu alt başlık altında verilen önbilgiler [2] ve [3] numaralı kaynaklardan alınmıştır.

RG, G grubunun R halkası üzerindeki grup halkası olsun. $G = \left\{g_1, g_2, \ldots, g_n\right\}$, G grubunun elemanlarının sıralı bir listesi olsun. $W \subseteq RG$ alt modül ve $u \in RG$ olsun.

Tanım 3.4 Grup halkası kodlaması $f : W \to RG,\ f\left(x\right) = xu$ (ya da $f\left(x\right) = ux$) kuralı ile verilen bir dönüşümdür. İlk durum sol kodlama, ikinci durum ise sağ kodlama olarak adlandırılır. Eğer G grubu değişmeli ise sol ve sağ kodlama birbirine eşittir.

Dolayısıyla seçilen bir $u \in RG$ için grup halkası kodlamasından elde edilen bir C kodu $C = \left\{ux \middle| x \in W\right\}$ veya $C = \left\{xu \middle| x \in W\right\}$ kümelerinden birisidir. W alt modülünün boyutu r olsun. $r \le n$ dir.

Tanım 3.5 $u \in RG$ sıfır bölen olsun. Yani en az bir $0 \ne v \in RG$ için $uv = 0$ olsun. W, RG grup halkasının bir $S \subset G$ alt kümesi tarafından üretilen alt modülü olsun. $C = \left\{ux \middle| x \in W\right\}$ veya $C = \left\{xu \middle| x \in W\right\}$ kümelerine sıfır bölen kod denir.

Dolayısıyla C kodunun inşası $u \in RG$ sıfır böleni, W alt modülü ve RG grup halkasının değişmeli olup olmamasına bağlıdır. $u \in RG$ elemanına $C = Wu$ kodunun W alt modülüne göre üreteci denir.

- Bu çalışmada kullanılan grup halkaları değişmeli olduğundan $C = \left\{ux \middle| x \in W\right\} = \left\{xu \middle| x \in W\right\}$ olacaktır.

Tanım 3.6 $T \subset RG$ olmak üzere $\sum_{x\in T} a_x x = 0\ \left(a_x \in R,\ x \in T\right)$ iken $a_x = 0$ oluyorsa T kümesine lineer bağımsızdır denir. Aksi halde T kümesi lineer bağımlıdır denir.

T kümesinin lineer bağımsız elemanlarının maksimum sayısına T'nin rankı denir ve $rank(T)$ ile gösterilir.

W, RG grup halkasının bir $S \subset G$ alt kümesi tarafından üretilen alt modülü olsun. Dikkat edilirse $u \in RG$ sıfır böleni tarafından üretilen $C = Wu$ kodu $\sum_{g \in S} a_g gu$ şeklindeki bütün elemanların kümesidir. Dolayısıyla bu alt modülün boyutu $rank(Su)$ olur.

Örnek 3.6 $\mathbb{F}_2 C_3 = \{0, 1, g, g^2, 1+g, 1+g^2, g+g^2, 1+g+g^2\}$ grup halkasında $u = 1+g$ ve $v = 1+g+g^2$ alalım. Ayrıca W, RG grup halkasının $S = \{1, g\}$ alt kümesi tarafından üretilen alt modülü olsun. Yani $W = \{0, 1, g, 1+g\}$ olsun. $(Su) = \{1, g\}(1+g) = \{1+g, g+g^2\}$ buradan $rank(Su) = 2$ olur. Ayrıca $C = Wu = \{0, 1+g, 1+g^2, g+g^2\}$ olmak üzere $\theta(C)$ bir $[3, 2, 2]_2$ lineer kod belirler.

Tanım 3.7 $\{g_1, g_2, \ldots, g_n\}$ mertebesi n olan bir G grubunun elemanlarının sıralı bir listesi olsun. $u \in RG$ sıfır bölen ve $rank(U) = rank(Gu) = k$ olsun. Bir $0 \neq v \in RG$ için $uv = 0$ ve $rank(V) = rank(Gv) = n - k$ oluyorsa $u \in RG$ sıfır bölenine esas sıfır bölen denir.

Örnek 3.7 $u = 1+g$ ve $v = 1+g+g^2 \in \mathbb{F}_2 C_3$ elemanları esas sıfır bölen olurlar. Gerçekten de $U = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \end{pmatrix}$ ve $V = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$ olup $rank(U) = 2$ iken $rank(V) = 3 - 2 = 1$.

Teorem 3.1 $C = \{xu \mid x \in W\}$ olmak üzere (Su) lineer bağımsız ve $|S| = rank(U) = r$ diyelim. Ayrıca $uv = 0$ ve $rank(V) = n - r$ olsun. $y \in RG$ nin kodsöz olması için gerek ve yeter şart $yv = 0$ olmasıdır.

$v \in RG$ elemanına $C = \{xu \mid x \in W\}$ kodunun kontrol elemanı denir.

Örnek 3.8 $v = 1+g+g^2 \in \mathbb{F}_2 C_3$ Örnek 3.6'da verilen kodun kontrol elemanıdır.

Teorem 3.2 $u \in RG$ ve $rank(U) = t$ olmak üzere $S \subset G$ ve $|S| = t+1$ olsun. Bu durumda (Su) lineer bağımlıdır.

Örnek 3.9 $\mathbb{F}_2 C_3$ grup halkası için $S = \{1, g, g^2\}$ ve $u = 1+g$ olarak alınırsa $(Su) = \{1+g, g+g^2, 1+g^2\}$ kümesi lineer bağımlı olur. Çünkü $1.(1+g)+1.(g+g^2)+1.(1+g^2) = 0$ dır.

Sonuç 3.1 $C = \{xu \,|\, x \in W\}$ kodunun tek kontrol elemanının olması için gerek ve yeter şart $u \in RG$ elemanının esas sıfır bölen olmasıdır.

Tanım 3.8 $x = \sum_{g \in G} a_g g$ ve $y = \sum_{g \in G} b_g g \in RG$ olmak üzere $\langle x, y \rangle = \sum a_g b_g$ ile tanımlanan toplama x ve y elemanlarının iç çarpımı denir.

Tanım 3.9 $C = \{xu \,|\, x \in W\}$ kodunun duali $C^{\perp} = \{y \in RG \,|\, \langle xu, y \rangle = 0 \quad \forall x \in W\}$ dir.

Teorem 3.3 $u, v \in RG$ esas sıfır bölenler olmak üzere $rank(U) = r$ ve $rank(V) = n - r$ olsun. Ayrıca, $S \subset G$ için $W = \langle S \rangle$ alt modülünün rankı r olacak şekilde (Su) lineer bağımsız ve $W^{\perp} = \langle G - S \rangle$ olsun. Bu durumda $C = \{xu \,|\, x \in W\}$ kodunun duali $C^{\perp} = \{xv^T \,|\, x \in W^{\perp}\} = \{y \in RG \,|\, yu^T = 0\}$ kümesidir.

İspat: v^T sıfır bölen ve $rank(V) = n - r$ olduğundan $W^{\perp}$ alt modülü için $xv^T = 0$ olacak şekilde $x \in W^{\perp}$ yoktur. Dolayısıyla $W^{\perp}$ alt modülü ile $\{xv^T \,|\, x \in W^{\perp}\}$ kümesi arasında bire-bir eşleme vardır.

Şimdi $\{xv^T \,|\, x \in W^{\perp}\}$ kümesinin $C = \{xu \,|\, x \in W\}$ kümesine dik olduğunu gösterelim. Bunun için $0 \neq z \in \{xv^T \,|\, x \in W^{\perp}\}$ olsun. Her $x \in W$ için $\langle xu, z \rangle = 0$ olduğunu göstermeliyiz. $x, y \in RG$ olmak üzere $z = yv^T$ alalım. $\theta : RG \to R^n, \quad \theta\left(\sum_{i=1}^{n} a_i g_i\right) = (a_1, a_2, \ldots, a_n)$ iken $\theta(x) = (x_1, x_2, \ldots, x_n)$ ve

$\theta(y)=(y_1,y_2,\ldots,y_n)$ alalım. O halde $\langle xu,z\rangle=\langle xu,yv^T\rangle=\theta(x)U\left(\theta(y)V^T\right)^T=\theta(x)UV\theta(y)^T=0$ elde edilir.

Tersine her $x\in W$ için $\langle xu,z\rangle=0$ olsun. Genelliği bozmadan $1\in W$ alabiliriz. Bu durumda $\langle u,z\rangle=0$ ise $zu^T=0$ demektir. u^T, v^T tarafından üretilen kodun kontrol elemanı olduğundan en az bir tane $y\in W^T$ için $z=yv^T$ olur.

Örnek 3.10 $\mathbb{F}_2C_7$ grup halkası ve $S=\{g,g^5,g^6\}\subset C_7$ ile $S^\perp=\{1,g^2,g^3,g^4\}\subset C_7$ alt kümeleri verilsin. Ayrıca $uv=0$ ve $rank(u)+rank(v)=3+4=7$ olacak şekilde $u,v\in\mathbb{F}_2C_7$ aşağıdaki gibi verilsin.

$u=1+g^2+g^3+g^4$	$u^T=1+g^3+g^4+g^5$
$v=1+g^2+g^3$	$v^T=1+g^4+g^5$

Bu durumda Wu ve $W^\perp(v^T)$ alt modülleri aşağıdaki gibi elde edilir.

Alt Modül	Eleman Sayısı
$Wu=\begin{Bmatrix}0,1+g^2+g^3+g^4,1+g+g^2+g^5,g+g^3+g^4+g^5,g+g^2+g^3+g^6,\\1+g+g^4+g^6,1+g^3+g^5+g^6,g^2+g^4+g^5+g^6\end{Bmatrix}$	2^3
$W^\perp(v^T)=\begin{Bmatrix}0,1+g+g^3,g+g^2+g^4,1+g^2+g^3+g^4,1+g+g^2+g^5,\\g^2+g^3+g^5,1+g^4+g^5,g+g^3+g^4+g^5,1+g^2+g^6,\\g+g^2+g^3+g^6,1+g+g^4+g^6,g^3+g^4+g^6,g+g^5+g^6,\\1+g^3+g^5+g^6,g^2+g^4+g^5+g^6,1+g+g^2+g^3+g^4+g^5+g^6\end{Bmatrix}$	2^4

θ dönüşümü yardımıyla $\theta(Wu)=C$ ve $\theta\left(W^\perp\left(v^T\right)\right)=C^\perp$ aşağıdaki gibi elde edilir.

$C=\{0000000,1011100,1110010,0101110,0111001,1101010,10010110,0010111\}$

$C^\perp=\begin{Bmatrix}0000000,1101000,0110100,1011100,1110010,0011010,1000110,0101110,\\1010001,0111001,1100101,0001101,0100011,1001011,0010111,1111111\end{Bmatrix}$.

BÖLÜM 4

$\mathbb{Z}_4C_n$ DEVİRLİ KODLAR

Bu bölümde [3] numaralı referansta verilen grup cebirleri üzerindeki sıfır bölen kod kavramı $\mathbb{Z}_4C_n$ grup halkalarına genişletildi. Elde edilen bu kodların eleman sayıları, dual kodları ve dual kodlarının eleman sayıları belirlendi.

4.1 $\mathbb{Z}_4C_n$ Devirli Kodlar

Tanım 4.1 $G = C_n = \langle g \rangle$ mertebesi n olan devirli bir grup, $R = \mathbb{Z}_4 = \{0,1,2,3\}$ dört elemanlı halka, n tek tam sayı ve $u \in \mathbb{Z}_4C_n$ bir sıfır bölen olsun. u sıfır bölen elemanının rankını $rank(u) = n - boy_S\left(\left(\mathbb{Z}_4C_n\right)u\right)$ şeklinde tanımlansın.

Örnek 4.1 $C_3 = \{1, g, g^2\}$ olmak üzere $u = g^2 + 3g \in \mathbb{Z}_4C_3$ elemanının rankı aşağıdaki gibi bulabiliriz.

$$\mathbb{Z}_4C_3\left(3g+g^2\right) = \begin{Bmatrix} 0,3+g,2+2g,1+3g,3+g^2,2+g+g^2,1+2g+g^2, \\ 3g+g^2,2+2g^2,1+g+2g^2,2g+2g^2,3+3g+2g^2, \\ 1+3g^2,g+3g^2,3+2g+3g^2,2+3g+3g^2 \end{Bmatrix}$$

kümesinin eleman sayısı $\left|\left(\mathbb{Z}_4C_3\right)\left(3g+g^2\right)\right| = 4^2$ olduğundan $\dim\left(\left(\mathbb{Z}_4C_3\right)\left(3g+g^2\right)\right) = 2$ ve $rank(u) = 3 - boy_S\left(\left(\mathbb{Z}_4C_3\right)u\right) = 3-2 = 1$ dir.

- $\mathbb{Z}_4C_n$ grup halkasında sıfır bölen kodların dual kodlarını ve bu kodların eleman sayılarını kontrol edebilmek için aşağıdaki tanımlama ve kısıtlamalar verilmiştir.

$G=\{1,g,\ldots,g^{n-1}\}$, G grubunun elemanlarının sıralı bir listesi ve $u,v,w\in RG$ için $uvw=0$ olmak üzere $rank(u)+rank(v)+rank(w)=n$ şartı sağlansın. Ayrıca, $S(uw)$, $S(2uv)\subset RG$ alt kümeleri lineer bağımsız olacak şekilde bir $S\subset G$ alt kümesi için $W=\langle S\rangle$, $W^{\perp}=\langle G-S\rangle\subseteq RG$ alt modüllerini oluşturalım.

Tanım 4.2 $u,v,w\in RG$ elemanları için $uvw=0$ ve $rank(u)+rank(v)+rank(w)=n$ şartı sağlansın. Ayrıca W, $\mathbb{Z}_4C_n$ grup halkasının $S(uw)$ ve $S(2uv)$ lineer bağımsız olacak şekilde bir $S\subset C_n$ alt kümesi tarafından üretilen alt modülü olsun. $C=W(uw)+W(2uv)=\{xuw+y2uv\mid x,y\in W\}$ kümesine bir $\mathbb{Z}_4C_n$-grup halkası kod denir.

Teorem 4.1 $C=W(uw)+W(2uv)=\{xuw+y2uv\mid x,y\in W\}$ ile verilen $\mathbb{Z}_4C_n$-grup halkası kodunun eleman sayısı $|C|=4^{rank(v)}2^{rank(w)}$ dir.

İspat: Dikkat edilirse $C=W(uw)+W(2uv)$ ile verilen küme $\sum_{g\in S}a_g g(uw)+\sum_{g\in S}b_g g(2uv)$ şeklindeki lineer toplamlardan oluşmaktadır. Ayrıca $W(uw)\cap W(2uv)=W(2uvw)=\{0\}$ dir. Dolayısıyla bu kümenin eleman sayısı $|S(uw)||S(2uv)|$ dir. O halde $|C|=|W(uw)||W(2uv)|=|S(uw)||S(2uv)|=4^{rank(v)}2^{rank(w)}$ elde edilir.

Teorem 4.2 $C=W(uw)+W(2uv)=\{xuw+y2uv\mid x,y\in W\}$ ile verilen $\mathbb{Z}_4C_n$-grup halkası kodunun dual kodu $C^{\perp}=\{x(v^Tw^T)+y(2u^Tv^T)\mid x,y\in W^{\perp}\}=W^{\perp}(v^Tw^T)+W^{\perp}(2u^Tv^T)$ şeklindedir. Ayrıca, $C^{\perp}$ kodunun eleman sayısı $|C^{\perp}|=4^{rank(u)}2^{rank(w)}$ dir.

İspat: Sıfır bölen kodun dualinin tanımından $(Wu)^{\perp}=W^{\perp}(v^Tw^T)$ yazılabilir. $W(uw)$ ve $W(2uv)\subset W(u)$ olduğundan $C=W(uw)+W(2uv)\subset W(u)$ dir. Bu da $(W(u))^{\perp}\subset C^{\perp}$ küme kapsamasını gerektirir. Bu yüzden $W^{\perp}(v^Tw^T)\subseteq C^{\perp}$. Benzer

şekilde $W^{\perp}\left(2u^{T}v^{T}\right)\subseteq W^{\perp}(v^{T})=\left(W\left(uw\right)\right)^{\perp}$ olur. Ayrıca $W^{\perp}\left(2u^{T}v^{T}\right)\subseteq\left(W\left(2uv\right)\right)^{\perp}$ dir. Bu yüzden $W^{\perp}\left(2u^{T}v^{T}\right)\subseteq\left(W\left(uw\right)\right)^{\perp}\cap\left(W\left(2uv\right)\right)^{\perp}=C^{\perp}$. Sonuç olarak $W^{\perp}\left(v^{T}w^{T}\right)+W^{\perp}\left(2u^{T}v^{T}\right)\subseteq C^{\perp}$ elde edilir.

Diğer taraftan $|C|=4^{rank(v)}2^{rank(w)}$ ve $\left|W^{\perp}\left(v^{T}w^{T}\right)+W^{\perp}\left(2u^{T}v^{T}\right)\right|=4^{rank(u)}2^{rank(w)}=\left|C^{\perp}\right|$ olduğundan $C^{\perp}=W^{\perp}\left(v^{T}w^{T}\right)+W^{\perp}\left(2u^{T}v^{T}\right)$.

Örnek 4.2 $R=\mathbb{Z}_4$ halkası ve $G=C_3=\langle g\rangle=\left\{1,g,g^2\right\}$ mertebesi 3 olan devirli grup iken aşağıda verilen $u,v,w\in\mathbb{Z}_4C_3$ sıfır bölen elemanlarını düşünelim.

$u=g^2+3g$	$u^T=g+3g^2$
$v=g^2+g+1$	$v^T=g^2+g+1$
$w=1$	$w^T=1$

Bu durumda aşağıda verilen elemanlar hesaplanabilir.

$uw=g^2+3g$	$uw+2uv=g^2+3g$
$2uv=0$	
$v^Tw^T=g^2+g+1$	$v^Tw^T+2u^Tv^T=g^2+g+1$
$2u^Tv^T=0$	

Bazı hesaplamalardan sonra $uvw=0$ ve $rank(u)+rank(v)+rank(w)=1+2+0=3$ olduğu görülür. Ayrıca, $S=\left\{1,g\right\}\subset C_3$ için $W=\langle S\rangle$ alalım. Bu durumda $W^{\perp}=\langle C_3-S\rangle$ olur.

$$W\left(uw\right)=\left\{\begin{matrix}0,3+g,2+2g,1+3g,3+g^2,2+g+g^2,1+2g+g^2,3g+g^2,2+2g^2,\\1+g+2g^2,2g+2g^2,3+3g+2g^2,1+3g^2,g+3g^2,3+2g+3g^2,2+3g+3g^2\end{matrix}\right\}$$

kümesi $4^{rank(v)}2^{rank(w)}=4^2=16$ elemanlıdır.

Ayrıca, $W^{\perp}\left(v^T w^T\right)=\left\{0,1+g+g^2,2+2g+2g^2,3+3g+3g^2\right\}$ olarak bulunur. Dikkat edilirse $\forall c\in W\left(uw\right)$ ve $\forall c'\in W^{\perp}\left(v^T w^T\right)$ için $\left\langle c,c'\right\rangle=0$ ve $\left|W^{\perp}\left(v^T w^T\right)\right|=4^{rank(v)}2^{rank(w)}=4^1=4$ dir. Bu durumda $W\left(uw\right)$ ve $W^{\perp}\left(v^T w^T\right)$ kümeleri birbirlerini dik tümleyeni olurlar. Bu kümelerin her biri birer $\mathbb{Z}_4C_3$-grup halkası kodu belirler.

Örnek 4.3 $R=\mathbb{Z}_4$ ve $G=C_7=\left\langle g\right\rangle=\left\{1,g,g^2,g^3,g^4,g^5,g^6\right\}$ mertebesi 7 olan devirli grup iken aşağıda verilen $u,v,w\in\mathbb{Z}_4C_7$ sıfır bölen elemanlarını düşünelim.

$u=g^2+3g$	$u^T=3g^6+g^5$
$v=g^5+2g^4+g^3+3g^2$	$v^T=3g^5+g^4+2g^3+g^2$
$w=g^6+3g^5+2g^4+3g^3$	$w^T=3g^4+2g^3+3g^2+g$

Bu durumda aşağıda verilen elemanlar ve alt modüller hesaplanabilir.

$uw=2+g+g^4+g^5+3g^6$	$uw+2uv=g+2g^3+g^4+3g^5+g^6$
$2uv=2+2g^3+2g^5+2g^6$	
$v^T w^T=1+g+g^2+g^3+g^4+g^5+g^6$	$v^T w^T+2u^T v^T=3+3g+3g^2+g^3+3g^4+g^5+g^6$
$2u^T v^T=2+2g+2g^2+2g^4$	

Alt Modül	Boyut	Alt Modül	Boyut
$W\left(uw\right)$	4^3	$W\left(uw\right)+W\left(2uv\right)$	4^32^3
$W\left(2uv\right)$	2^3		
$W^{\perp}\left(v^T w^T\right)$	4^1	$W^{\perp}\left(v^T w^T\right)+W^{\perp}\left(2u^T v^T\right)$	4^12^3
$W^{\perp}\left(2u^T v^T\right)$	2^3		

Bazı aritmetik işlemlerden sonra $uvw = 0$ ve $rank(u) + rank(v) + rank(w) = 1 + 3 + 3 = 7$ olarak hesaplanır. Ayrıca, $S = \{1, g, g^2\} \subset C_7$ için $W = \langle S \rangle$ olsun. Bu durumda $W^{\perp} = \langle C_7 - S \rangle$ olur. $W(uw) + W(2uv)$ kümesi

$$\overline{G} = \begin{pmatrix} 2 & 1 & 0 & 0 & 1 & 1 & 3 \\ 1 & 0 & 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 1 & 1 & 3 & 2 & 1 \\ 2 & 0 & 0 & 2 & 0 & 2 & 2 \\ 0 & 0 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 0 & 2 & 2 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}$$

matrisi tarafından üretilen $4^{rank(v)}2^{rank(w)} = 4^3 2^3 = 512$ elemanlı bir $\mathbb{Z}_4$-devirli lineer kod belirler. Ayrıca, $W^{\perp}(v^T w^T) + W^{\perp}(2u^T v^T)$ kümesi de

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 & 2 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 2 & 2 \end{pmatrix}$$

matrisi tarafından üretilen $4^{rank(u)}2^{rank(w)} = 4^1 2^3 = 32$ elemanlı bir $\mathbb{Z}_4$-devirli lineer kod belirler. Dikkat edilirse $\forall c \in W(uw) + W(2uv)$ ve $\forall c' \in W^{\perp}(v^T w^T) + W^{\perp}(2u^T v^T)$ için $\langle c, c' \rangle = 0$ şartı sağlanır. Bu durumda $W(uw) + W(2uv)$ ve $W^{\perp}(v^T w^T) + W^{\perp}(2u^T v^T)$ kümeleri birbirlerinin dik tümleyeni olurlar.

BÖLÜM 5

SABİT DEVİRLİ KODLAR

Sabit devirli kodlar (constacyclic codes) verimli kodlama işlemleri sayesinde birçok mühendislik uygulamasında tercih edilir. Sabit devirli kodlar sınıfı devresel ve nega devresel kodları içerir. Bu bölümde grup halkalarının sıfır bölenleri yardımıyla grup cebirleri üzerinde sabit devresel kodlar için bir inşa yöntemi verildi. İnşa edilen bu yöntem ile şu ana kadar bilinen en iyi kod parametrelerinden bazıları doğrudan elde edildi.

5.1 Sabit Devirli (Constacyclic) Kodlar

Sabit devirli kodların cebirsel yapısı [40] numaralı referansta verilmiştir. Bu alt başlık altında devirli kodların tanımı verilecektir.

Tanım 5.1 n pozitif tam sayı ve $0 \neq \alpha \in \mathbb{F}_q$ olsun. Ayrıca C, n-uzunluğunda bir $\mathbb{F}_q$ lineer kod olsun. Her $(c_0, c_1, \ldots, c_{n-1}) \in C$ için $(\alpha c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ oluyorsa C lineer koduna α-sabit devirli kod denir.

5.2 Grup Halkalarında Sabit Devirli Kodların Yapısı

Bu bölüm boyunca aşağıdaki gösterim ve kısıtlamalar vardır.

p tek asal sayı,

$\mathbb{F}_q$, q elemanlı sonlu cisim

$p^k + 1 \neq 0, 1 \pmod{q}$ ve $ebob(q, n) = 1$ olmak üzere $n = 2p^k$

Sabit devirli kodların grup halkaları üzerindeki yapısını vermeden önce bunu bir örnek ile açıklayalım.

$\mathbb{Z}_{10}=\{0,1,2,3,4,5,6,7,8,9\}$ modülo 10 kalan sınıflarının kümesi ve $G=2\mathbb{Z}_{10}^{*}=\{2,4,6,8\}\subset\mathbb{Z}_{10}$ olsun. Bu durumda G kümesi birimi 6 olan çarpımsal devirli bir grup belirler. Bu grubun işlem tablosu aşağıdaki gibidir.

Çizelge 5. 1 G grubu için işlem tablosu

x	***2***	***4***	***6***	***8***
2	*4*	*8*	*2*	*6*
4	*8*	*6*	*4*	*2*
6	*2*	*4*	*6*	*8*
8	*6*	*2*	*8*	*4*

Dolayısıyla, devirli grup tanımından en az bir $g\in G$ için $g^4=e$ ve $g^i\neq e\ \ i=1,2,3$ dir. $\mathbb{F}_7$ karakteristiği 7 olan sonlu cisim olsun. Bu durumda $\mathbb{F}_7G$ grup halkasının elemanları $i=0,1,2,3$ için $a_i\in\mathbb{F}_7$ olmak üzere $\sum_{i=0}^{3}a_ig^i$ şeklindedir. $u=1+3g+g^2$, $v=1+4g+g^2\in\mathbb{F}_7G$ için $uv=0$ ve $rank(u)+rank(v)=4$ şartı sağlanır. $(\mathbb{F}_7G)u=\{xu\,|\,x\in\mathbb{F}_7G\}$ kümesi $\mathbb{F}_7G$ nin vektör uzayı olarak 2 boyutlu bir alt uzayıdır. Dolayısıyla $\theta((\mathbb{F}_7G)u)$ de $\mathbb{F}_7^4$ vektör uzayının 2 boyutlu bir alt uzayı olur. Magma programı yardımıyla $\theta((\mathbb{F}_7G)u)$ kümesinin $\overline{G}=\begin{pmatrix}1&0&6&4\\0&1&3&1\end{pmatrix}$ matrisi tarafından üretilen ve $[4,2,3]_7$ parametrelerine sahip bir $6-$sabit devirli lineer kod olduğu görülür. Bu kodun dual kodu ise $(\mathbb{F}_7G)v^T=\{xv^T\,|\,x\in\mathbb{F}_7G\}$ kümesi ile verilen $\mathbb{F}_7G$ grup halkasının iki taraflı idealidir. Aynı zamanda $\theta((\mathbb{F}_7G)v^T)$ kümesi de $H=\begin{pmatrix}1&0&6&3\\0&1&4&1\end{pmatrix}$ matrisi tarafından üretilen ve $[4,2,3]_7$ parametrelerine sahip bir sabit devirli lineer koddur. Bu kodların her ikisi de singleton sınırını eşitlik hali için sağladıklarından birer MDS kod belirler.

Yukarıda verilen örnekte görüldüğü gibi $G = 2\mathbb{Z}_n^*$ kümesinin ne zaman çarpımsal bir grup olduğu n uzunluğundaki sabit devirli kodların varlığı için önem arz etmektedir. Aşağıda verilecek lemmalar dizisi yardımıyla $n = 2p^k$ için $G = 2\mathbb{Z}_n^*$ kümesinin birim elemanı $e = p^k + 1$ olan devirli bir grup olduğu gösterilecektir.

Lemma 5.1 p tek asal sayı ve bir k pozitif tam sayısı için $n = 2p^k$ olsun. Bu durumda $G = 2\mathbb{Z}_n^*$ kümesi çarpma işlemi altında kapalıdır.

İspat: p tek asal sayı ve bir k pozitif tam sayısı için $n = 2p^k$ olsun. $n = 2, 4, p^k$ ve $2p^k$ için Gauss Teoremi'den biliyoruz ki $\mathbb{Z}_n^*$ kümesi devirli bir gruptur. Buradan $n = 2p^k$ için $g^{\varphi(2p^k)} \equiv 1 \pmod{2p^k}$ şartını sağlayan bir $g \in \mathbb{Z}_n^*$ vardır. O halde $\langle g \rangle = \mathbb{Z}_n^*$ $= \left\{1, g, g^2, \ldots, g^{\varphi(p^k)-1}\right\}$ yazarız. Ayrıca $G = 2\mathbb{Z}_n^*$ kümesini $G = 2\mathbb{Z}_n^* = \left\{a \in \mathbb{Z}_n \middle| p \nmid a\right\}$ $= \left\{a \in \mathbb{Z}_n \middle| ebob\left(a, 2p^k\right) = 2\right\} = \left\{2, 2g, 2g^2, \ldots, 2g^{\varphi(p^k)-1}\right\}$ şeklinde ifade edebiliriz. Keyfi $x, y \in G = 2\mathbb{Z}_n^*$ alalım. Bu durumda $0 \le i, j \le \varphi\left(2p^k\right)$ olacak şekilde $x = 2g^i$ ve $y = 2g^j$ dir. Eğer $xy = 2g^i 2g^j = 4g^i g^j \notin G = 2\mathbb{Z}_n^*$ ise $p \mid 4g^i g^j$ olur. Ancak $\left(4, p\right) = 1$ ve $\left(4, g^i g^j\right) = 1$ olduğundan bu bir çelişkidir. Sonuç olarak $p \nmid 4g^i g^j$ ve $0 \le t \le \varphi\left(2p^k\right)$ şartını sağlayan bir t tam sayısı için $xy = 2g^t \in 2\mathbb{Z}_n^*$ dir. Bu da $G = 2\mathbb{Z}_n^*$ kümesinin çarpma işlemi altında kapalı olduğunu gösterir.

Lemma 5.2 p tek asal sayı ve bir k pozitif tam sayısı için $n = 2p^k$ olsun. Bu durumda $G = 2\mathbb{Z}_n^*$ kümesinin çarpımsal birimi $e = p^k + 1$ dir.

İspat: $x \in G = \left\{a \in \mathbb{Z}_n \middle| ebob\left(a, 2p^k\right) = 2\right\} = \left\{2, 2g, 2g^2, \ldots, 2g^{\varphi(p^k)-1}\right\}$ olsun. O halde $0 \le i \le \varphi\left(2p^k\right)$ için $x = 2g^i$ olduğundan $xe = 2g^i\left(p^k + 1\right) \equiv 2g^i \pmod{2p^k}$ elde edilir. Buradan $e = p^k + 1$ elemanının $G = 2\mathbb{Z}_n^*$ kümesinin çarpımsal birimi olduğu görülür.

Sonuç 5.1 p tek asal sayı ve bir k pozitif tam sayısı için $n = 2p^k$ olsun. Ayrıca $G = 2\mathbb{Z}_n^*$ kümesinin çarpımsal birimi $e = p^k + 1$ olsun. Bu durumda $e \equiv 1 \pmod{p}$ dir.

Lemma 5.3 p tek asal sayı ve bir k pozitif tam sayısı için $n=2p^k$ olsun. Bu durumda $r|\varphi\left(p^k\right)$ sayısı için $2^r \equiv p^k+1\left(\mathrm{mod}\ 2p^k\right)$ denkliği sağlanır.

İspat: Tanımdan dolayı $2\in G$ olur. Eğer 2 elemanı G kümesinde ilkel ise $2^{\varphi\left(p^k\right)} \equiv p^k+1\left(\mathrm{mod}\ 2p^k\right)$ olur. Diğer taraftan, eğer 2 elemanı G kümesinde ilkel eleman değilse $r|\varphi\left(p^k\right)$ için $2^r \equiv p^k+1\left(\mathrm{mod}\ 2p^k\right)$ dir.

Lemma 5.4 p tek asal sayı ve bir k pozitif tam sayısı için $n=2p^k$ olsun. Bu durumda $G=2\mathbb{Z}_n^*$ kümesindeki her elemanın çarpımsal tersi vardır.

İspat: $G=\left\{2,2g,2g^2,\ldots,2g^{\varphi\left(p^k\right)-1}\right\}$ olduğunu biliyoruz. O halde G kümesindeki her bir y elemanı $0\le j\le\varphi\left(2p^k\right)$ için $y=2g^j$ şeklindedir. G kümesinin tüm elemanlarını $x=2g^i$ ile çarpalım. Bu durumda $xG=\left\{2.2g^i,2g.2g^i,2g^2.2g^i,\ldots,2g^{\varphi\left(p^k\right)-1}.2g^i\right\}$ yazarız. G kümesi çarpma işlemine göre kapalı olduğundan keyfi bir $z\in xG$ için $z=2g^l$ $0\le l\le\varphi\left(2p^k\right)$ veya $z=p^k+1=e$ olur. Son durum $G=2\mathbb{Z}_n^*$ kümesindeki her elemanın çarpımsal tersinin olduğunu gösterir.

Sonuç 5.2 p tek asal sayı ve bir k pozitif tam sayısı için $n=2p^k$ olsun. Ayrıca $0\le i,j\le\varphi\left(2p^k\right)$ olacak şekilde $x=2g^i$ ve $y=2g^j$ için $xy=p^k+1\left(\mathrm{mod}\ 2p^k\right)$ olsun. Bu durumda $x=2g^i$ elemanının çarpımsal tersi $r|\varphi\left(p^k\right)$ için $2^r \equiv p^k+1\left(\mathrm{mod}\ 2p^k\right)$ olmak üzere $y=2^{r-1}g^{\varphi\left(2p^k\right)-i-1}$ dir.

Teorem 5.1 p tek asal sayı ve bir k pozitif tam sayısı için $n=2p^k$ olsun. Bu durmda $G=2\mathbb{Z}_n^*$ kümesi birimi $e\equiv 1\left(\mathrm{mod}\ p\right)$ olan devirli bir gruptur.

İspat: $G=2\mathbb{Z}_n^*$ kümesinin birimi $e=p^k+1$ olan bir grup olduğunu yukarıda verilen lemmalar serisinde gösterdik. $G=2\mathbb{Z}_n^*$ kümesinin bir üretecinin olduğunu göstermek yeterlidir. Gauss Teoremi'nden $n=2p^k$ için $g^{\varphi\left(2p^k\right)} \equiv 1\left(\mathrm{mod}\, 2p^k\right)$ şartını sağlayan bir

$g \in \mathbb{Z}_n^*$ vardır. Yani $\langle g \rangle = \mathbb{Z}_n^* = \left\{1, g, g^2, \ldots, g^{\varphi(p^k)-1}\right\}$ dir. Ayrıca $(2, p) = 1$ aldığımızdan $2^{\varphi(p^k)} \equiv 1 \pmod{p^k}$ dır. Sonuç olarak bir $h \in G = 2\mathbb{Z}_n^*$ için $\langle h \rangle = 2\mathbb{Z}_n^*$ olur.

Sonuç 5.3 p tek asal sayı ve bir k pozitif tam sayısı için $n = 2p$ olsun. Bu durumda $G = 2\mathbb{Z}_n^*$ kümesi birimi $e \equiv 1 \pmod{p}$ olan devirli bir gruptur.

$\mathbb{F}_q$ cismi üzerinde $\varphi(2p^k)$ uzunluklu bir $e = (p^k + 1)$-sabit devirli kod $G = 2\mathbb{Z}_n^*$ olmak üzere $\mathbb{F}_q G$ grup cebirinin bir ideali olarak görülebilir.

Teorem 5.2 $\mathbb{F}_q$, q elemanlı sonlu cisim ve k pozitif tam sayısı için $n = 2p^k$ iken $G = 2\mathbb{Z}_n^*$ olsun. Ayrıca $(q, \varphi(p^k)) = 1$ alalım. $u, v \in \mathbb{F}_q G$ asal sıfır bölenler olmak üzere $(\mathbb{F}_q G)u$ kümesi $\varphi(2p^k)$ uzunluklu ve boyutu $rank(u)$ olan bir $e = (p^k + 1)$-sabit devirli kod belirler.

İspat: Teorem 5.1 ve sıfır bölen kodun tanımından rahatlıkla görülür.

Sonuç 5.4 Teorem 5.2'de verilen kodun duali $\varphi(2p^k)$ uzunluklu ve boyutu $rank(v)$ olan bir $(p^k + 1)^{-1} \pmod{q}$-sabit devirli kod belirler.

Verilen her $\varphi(2p^k)$ uzunluğu için $s \mid \varphi(2p^k)$ olacak şekilde $\mathbb{F}_q$ üzerinde s-uzunluklu e-sabit devirli kodlar elde edilebilir. Burada $e \equiv p^k + 1 \pmod{q}$ dur. Aşağıdaki sonuç bu durumu ifade etmektedir.

Sonuç 5.5 p tek asal sayı ve bir k pozitif tam sayısı için $n = 2p^k$ olsun. Ayrıca $(q, \varphi(p^k)) = 1$ olacak şekilde $\mathbb{F}_q$, q elemanlı sonlu cisim alalım. Bu durumda $\varphi(2p^k)$'i bölen her s için $\mathbb{F}_q$ üzerinde s-uzunluklu bir $e \equiv p^k + 1 \pmod{q}$-sabit devirli kod vardır.

Örnek 5.1 $p = 3, k = 6$ ve $q = 7$ olsun. Bu durumda $\varphi(2p^k) = \varphi(p^k)$ $= \varphi(729) = 3^6 - 3^5 = 486$ ve $e \equiv p^k + 1 = 730 = 2 \pmod{7}$ olduğundan $1, 2, 3, 6, 9, 18, 27, 54, 81, 162, 243, 486$ uzunluklu 2-sabit devirli kodlar vardır.

Eğer $p=5,k=5$ ve $q=7$ olarak alırsak $\varphi\left(2p^k\right)=\varphi\left(p^k\right)=\varphi\left(5^5\right)=5^5-5^4=2500$ ve $e\equiv p^k+1=3126=4\left(\mathrm{mod}\,7\right)$ olduğundan $1,2,4,5,10,20,25,50,100,125,250,500,625,1250,2500$ uzunluklu 4-sabit devirli kodlar vardır.

5.3 Bazı Seçilmiş Örnekler

Çizelge 5.1 ve Çizelge 5.2'de verilen parametrelerin çoğu Grassl'ın Kod Tablosu'nda (bkz. [41]) verilen ve şu ana kadar bilinen en iyi kod parametreleri ile aynıdır. Grassl'ın Kod Tablosu'nda birçok adımda verilen parametreler bizim verdiğimiz inşa yöntemiyle doğrudan elde edilmektedir. Bu bölümdeki bütün hesaplamalar MAGMA (bkz. [42]) ile yapılmıştır. Çizelgelerde "*" ile işaretlenen parametrelere sahip kodlar MDS dir.

Örnek 5.3 $\mathbb{F}_{11}$ karakteristiği 11 olan sonlu cisim ve $G=2\mathbb{Z}_{10}^{*}=\{2,4,6,8\}\subset\mathbb{Z}_{10}$ olsun. Ayrıca $u=7+5g+g^2$ ve $v=7+6g+g^2$ $\mathbb{F}_{11}G$ grup halkasında iki sıfır bölen olsun. Bu durumda $rank(u)+rank(v)=4$ şartı sağlanır. $(\mathbb{F}_{11}G)u=\{xu\,|\,x\in\mathbb{F}_{11}G\}$ kümesi $\mathbb{F}_{11}G$ nin iki taraflı bir idealidir. Dolayısıyla $\theta\left((\mathbb{F}_{11}G)u\right)$ de $\mathbb{F}_{11}^4$ vektör uzayının 2 boyutlu bir alt vektör uzayı olur. Magma programı yardımıyla $\theta\left((\mathbb{F}_{11}G)u\right)$ kümesinin $\overline{G}=\begin{pmatrix}1&0&3&10\\0&1&7&8\end{pmatrix}$ matrisi tarafından üretilen ve $[4,2,3]_{11}$ parametrelerine sahip bir 6-sabit devirli lineer kod olduğu görülebilir. Bu kodun dual kodu ise $(\mathbb{F}_{11}G)v^T=\{xv^T\,|\,x\in\mathbb{F}_{11}G\}$ kümesi ile verilen $\mathbb{F}_{11}G$ grup halkasının iki taraflı idealidir. Aynı zamanda $\theta\left((\mathbb{F}_{11}G)v^T\right)$ kümesi de $H=\begin{pmatrix}1&0&4&2\\0&1&6&7\end{pmatrix}$ matrisi tarafından üretilen ve $[4,2,3]_{11}$ parametrelerine sahip bir 2-sabit devirli lineer koddur. Bu kodların her ikisi de Singleton sınırını eşitlik hali için sağladıklarından birer MDS kod belirler.

Çizelge 5. 2 $\mathbb{F}_{11}$ cismi üzerinde 12-uzunluklu bazı 3-sabit devirli kodlar ve dual kodları

u	v	C	$C^{\perp}$
$g^{10}+8g^9+6g^8+2g^7+9g^6$ $+6g^4+4g^3+3g^2+g+10$	g^2+3g+3	$[12,2,10]$	$[16,10,2]$
$g^9+9g^8+5g^7+6g^6+g^5$ $+6g^4+9g^3+6g^2+6g+2$	$g^3+2g^2+10g+4$	$^*[12,3,10]$	$^*[12,9,4]$
$g^8+9g^7+2g^6+5g^5$ $+7g^3+4g^2+10g+7$	$g^4+2g^3+2g^2+6g+9$	$[12,4,8]$	$[12,8,3]$
$g^8+6g^7+8g^6+8g^5$ $+9g^3+5g^2+3g+7$	$g^4+5g^3+6g^2+4g+9$	$[16,4,6]$	$[16,8,4]$
$g^9+g^8+6g^7+7g^6$ $+5g^3+5g^2+8g+2$	g^3+10g^2+6g+4	$[12,3,8]$	$[12,9,2]$
$g^8+8g^7+3g^6$ $+6g^2+4g+7$	$g^4+3g^3+6g^2+9g+9$	$[12,4,6]$	$[12,8,2]$
$g^6+5g^5+3g^4$ $+2g^2+10g+6$	$g^6+6g^5+4g^3+10g+5$	$[12,6,4]$	$[12,6,4]$
$g^7+9g^6+9g^5+8g^4$ $+4g^3+8g^2+2g+8$	$g^5+2g^4+6g^3+8g^2+8g+1$	$^*[12,5,8]$	$^*[12,7,6]$
$g^6+2g^5+10g^4$ $+3g^2+4g+6$	$g^6+9g^5+5g^4+$ $10g^3+4g^2+4g+5$	$[12,6,6]$	$[12,6,4]$

Örnek 5.4 $\mathbb{F}_{11}$ karakteristiği 11 olan sonlu cisim ve $G=2\mathbb{Z}_{14}^*=\{2,4,6,8,10,12\}\subset\mathbb{Z}_{14}$ olsun. Ayrıca $u=4+3g+7g^2+4g^3+g^4$ ve $v=9+7g+g^2$ $\mathbb{F}_{11}G$ grup halkasında iki sıfır bölen olsun. Bu durumda $rank(u)+rank(v)=6$ şartı sağlanır. $(\mathbb{F}_{11}G)u=\{xu\,|\,x\in\mathbb{F}_{11}G\}$ kümesi $\mathbb{F}_{11}G$ nin iki taraflı bir idealidir. Dolayısıyla $\theta((\mathbb{F}_{11}G)u)$ de $\mathbb{F}_{11}^6$ vektör uzayının 3 boyutlu bir alt vektör uzayı olur. Magma programı yardımıyla $\theta((\mathbb{F}_{11}G)u)$ kümesinin $G=\begin{pmatrix}1&0&6&10&5&6\\0&1&9&10&1&3\end{pmatrix}$ matrisi tarafından üretilen ve $[6,2,5]_{11}$ parametrelerine sahip bir 8-sabit devirli lineer kod olduğu görülebilir. Bu kodun dual kodu ise $(\mathbb{F}_{11}G)v^T=\{xv^T\,|\,x\in\mathbb{F}_{11}G\}$ kümesi ile verilen $\mathbb{F}_{11}G$ grup halkasının iki taraflı idealidir. Aynı zamanda $\theta((\mathbb{F}_{11}G)v^T)$ kümesi de

$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 8 & 5 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 5 \end{pmatrix}$ matrisi tarafından üretilen ve $[6,4,3]_{11}$ parametrelerine sahip bir 7-sabit devirli lineer koddur. Bu kodların her ikisi de Singleton sınırını eşitlik hali için sağladıklarından birer MDS kod belirler.

Çizelge 5. 3 $\mathbb{F}_7$ cismi üzerinde 16-uzunluklu bazı 4-sabit devirli kodlar ve dual kodları

u	v	C	$C^{\perp}$
g^2+2g+5	$g^{14}+5g^{13}+6g^{12}+5g^{11}+2g^{10}$ $+6g^9+6g^8+5g^6+4g^5$ $+2g^4+4g^3+3g^2+2g+2$	$[16,14,2]$	$[16,2,14]$
g^3+3g+1	$g^{13}+4g^{11}+6g^{10}+2g^9$ $+6g^8+2g^7+g^6+2g^5$ $+2g^4+6g^2+5g+3$	$[16,13,3]$	$[16,3,12]$
g^4+3g^3+6g+3	$g^{12}+4g^{11}+2g^{10}+2g^9$ $+2g^8+5g^7+2g^6+4g^5$ $+g^4+5g^3+4g^2+5g+1$	$[16,12,4]$	$[16,4,8]$
$g^5+4g^4+3g^3$ $+6g^2+5$	$g^{11}+3g^{10}+6g^9+3g^8$ $+g^7+2g^6+5g^5+g^4$ $+3g^3+6g^2+2$	$[16,11,4]$	$[16,5,10]$
$g^6+5g^4+g^3$ $+2g^2+2g+6$	$g^{10}+2g^8+6g^7+$ $2g^6+g^5+2g^4+$ $5g^3+3g^2+g+4$	$[16,10,5]$	$[16,6,8]$
$g^7+g^6+3g^5+$ g^4+2g^3+g+4	$g^9+6g^8+5g^7+$ $4g^6+g^5+5g^4+$ $5g^3+3g^2+2g+6$	$[16,9,6]$	$[16,7,8]$
$g^8+5g^7+g^6$ $+2g^5+3g^3+$ $3g^2+2g+5$	$g^8+2g^7+3g^6+$ $2g^5+4g^4+4g^3$ $+5g^2+2g+2$	$[16,8,6]$	$[16,8,6]$

5.4 $\mathbb{F}_q G$ Grup Cebirinde Kendine Dik ve Kendine Dual Sabit Devirli Kodların Yapısı

Bu başlık altında $\mathbb{F}_q G$ grup cebiri üzerinde tanımladığımız sabit devirli kodların kendine dik ve kendine dual olabilmesi için gerek ve yeter koşullar verilmiştir.

Lemma 5.5 $C = \theta\left(\left(\mathbb{F}_q G\right)u\right)$ Teorem 5.2'de verilen sabit devirli bir kod olsun. Eğer C kodu kendine dual bir kod ise dual kodu $C^{\perp} = \theta\left(\left(\mathbb{F}_q G\right)v^T\right)$ da bir $\left(p^k + 1\right)$-sabit devirli koddur.

İspat: Kendine dual kodun tanımının bir sonucudur.

Teorem 5.3 $C = \theta\left(\left(\mathbb{F}_q G\right)u\right)$ Teorem 5.2'de verilen $\varphi\left(p^k\right)$-uzunluğunda ve dual kodu $C^{\perp} = \theta\left(\left(\mathbb{F}_q G\right)v^T\right)$ olan $\left(p^k + 1\right)$-sabit devirli kod olsun. Bu durumda C kendine dualdir ancak ve ancak $e^2 = 1\left(mod\ q\right)$ ve $u = v^T$ olmasıdır.

İspat: Açık bir şekilde $C = \theta\left(\left(\mathbb{F}_q G\right)u\right) = \theta\left(\left(\mathbb{F}_q G\right)v^T\right) = C^{\perp}$ ise $u = v^T$ ve $e = e^{-1}\left(mod\ q\right)$ olduğundan $e^2 = 1\left(mod\ q\right)$ sağlanır.

Tersine, eğer $e^2 = 1\left(mod\ q\right)$ ve $u = v^T$ ise $C = \theta\left(\left(\mathbb{F}_q G\right)u\right) = \theta\left(\left(\mathbb{F}_q G\right)v^T\right) = C^{\perp}$ dir.

Sonuç 5.6 $C = \theta\left(\left(\mathbb{F}_q G\right)u\right)$ Teorem 5.2'de verilen $\varphi\left(p^k\right)$-uzunluğunda ve dual kodu $C^{\perp} = \theta\left(\left(\mathbb{F}_q G\right)v^T\right)$ olan $\left(p^k + 1\right)$-sabit devirli kod olsun. Bu durumda $p^k \equiv -2\left(mod\ q\right)$ denkliği sağlanır.

İspat: Teorem 5.3'ten $\left(p^k + 1\right)^2 = p^{2k} + 2p^k + 1 = 1\left(mod\ q\right)$ dir. Buradan $p^k = 0\left(mod\ q\right)$ veya $p^k = -2\left(mod\ q\right)$ yazılır.

Teorem 5.4 $C = \theta\left(\left(\mathbb{F}_q G\right)u\right)$ Teorem 5.2'de verilen $\varphi\left(p^k\right)$-uzunluğunda ve dual kodu $C^{\perp} = \theta\left(\left(\mathbb{F}_q G\right)v^T\right)$ olan $\left(p^k + 1\right)$-sabit devirli kod olsun. Bu durumda C kendine diktir ancak ve ancak $e^2 = 1\left(mod\ q\right)$ ve en az bir $w \in \mathbb{F}_q G$ için $u = wv^T$ olmasıdır.

İspat: Açık bir şekilde $C=\theta\left(\left(\mathbb{F}_qG\right)u\right)\subset\theta\left(\left(\mathbb{F}_qG\right)v^T\right)=C^{\perp}$ ise en az bir $w\in\mathbb{F}_qG$ için $u=wv^T$ ve $e=e^{-1}\left(mod\ q\right)$ olduğundan $e^2=1\left(mod\ q\right)$ sağlanır.

Tersine, eğer $e^2=1\left(mod\ q\right)$ ve en az bir $w\in\mathbb{F}_qG$ için $u=wv^T$ ise $C=\theta\left(\left(\mathbb{F}_qG\right)u\right)\subset\theta\left(\left(\mathbb{F}_qG\right)v^T\right)=C^{\perp}$ olduğundan $C=\theta\left(\left(\mathbb{F}_qG\right)u\right)$ kendine diktir.

5.5 $\mathbb{F}_qG$ Grup Cebirinde Kendine Dik ve Kendine Dual Sabit Devirli Kodlardan Elde Edilen Kuantum Kodlar

$\mathbb{F}_2$ cismi üzerindeki klasik kodlardan kuantum kodların elde edilmesi ilk olarak 1996 yılında Calderbank ve Shor [43] ve Steane [44] tarafından verilmiştir. Daha sonra bu yöntem Ketkar v.d. tarafından [45]'te $\mathbb{F}_q$ cismine genelleştirilmiştir.

Tanım 5.2 $\mathbb{C}^{q^n}$ Hilbert uzayının q^k boyutlu alt uzayına $\left[\left[n,k,d\right]\right]_q$ parametrelerine sahip bir Q kuantum kod denir ve bu kod $\left\lfloor\frac{d-1}{2}\right\rfloor$ tane hata düzeltebilir.

Lemma 5.6 (CSS Kod İnşası) [45] C_1 ve C_2 sırasıyla $\left[n,k_1,d_1\right]_q$ ve $\left[n,k_2,d_2\right]_q$ parametrelerine sahip lineer kodlar olsun. Ayrıca $C_2^{\perp}\subseteq C_1$ olsun. Bu durumda $d=min\{wt(c)\,|\,c\in(C_1\setminus C_2^{\perp})\cup(C_2\setminus C_1^{\perp})\}$ olacak şekilde $\left[\left[n,k_1+k_2-n,d\right]\right]_q$ parametrelerine sahip bir kuantum stabilizer kodu vardır.

Sonuç 5.7 [45] Eğer $\left[n,k,d\right]_q$ parametrelerine sahip C lineer kodu $C^{\perp}\subseteq C$ şartını sağlıyorsa $\left[\left[n,2k-n,d\right]\right]_q$ parametrelerine sahip bir kuantum stabilizer kodu vardır.

Sonuç 5.7 yardımıyla Teorem 5.3 ve Teorem 5.4'te elde edilen kendine dual ve kendine dik kodlardan kuantum kod parametreleri elde edeceğiz. Hesaplamalar Magma ([42]) programı ile yapılmıştır.

Çizelge 5. 4 $\mathbb{F}_5$ cismi üzerindeki 12-uzunluklu 4-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

u	v^T	C	$C^{\perp}$	Q
$g^6+2g^5+4g^3$ $+2g^2+4g+3$	$g^6+2g^5+4g^3$ $+2g^2+4g+3$	$[12,6,5]$	$[12,6,5]$	$\left[[12,0,\geq 5]\right]_5$
$g^8+4g^7+g^6$ $+g^5+g^4+2g^3$ $+4g^2+2g+1$	g^4+3g^3+g+1	$[12,4,6]$	$[12,8,4]$	$\left[[12,4,\geq 4]\right]_5$
$g^{10}+3g^9+g^8+$ $4g^7+4g^6+3g^4+$ $4g^3+3g^2+2g+2$	$3g^2+2g+1$	$[12,2,10]$	$[12,10,2]$	$\left[[12,8,\geq 2]\right]_5$

Örnek 5.5 $\mathbb{F}_5$ karakteristiği 5 olan sonlu cisim ve

$$G=2\mathbb{Z}_{26}^{*}=\{2,4,6,8,10,12,14,16,18,20,22,24\}\subset\mathbb{Z}_{26}$$ olsun.

Ayrıca $u=g^8+2g^7+4g^6+2g^5+g^4+g^3+g^2+4g+1$ ve $v^T=g^4+g^3+3g+1$ $\mathbb{F}_5G$ grup halkasında iki sıfır bölen olsun. Bu durumda $rank(u)=4$ ve $rank(v)=8$ şartı sağlanır. $(\mathbb{F}_5G)u=\{xu\,|\,x\in\mathbb{F}_5G\}$ kümesi $\mathbb{F}_5G$ nin iki taraflı bir idealidir. Dolayısıyla $\theta((\mathbb{F}_5G)u)$ da $\mathbb{F}_5^{12}$ vektör uzayının 4 boyutlu bir alt vektör uzayı olur. Magma yardımıyla $\theta((\mathbb{F}_5G)u)$ kümesinin

$$\bar{G}=\begin{pmatrix}1&0&0&0&4&1&4&4&4&3&1&3\\0&1&0&0&2&2&3&1&1&3&1&0\\0&0&1&0&0&2&2&3&1&1&3&1\\0&0&0&1&4&1&1&1&2&4&2&1\end{pmatrix}$$

matrisi tarafından üretilen ve $[12,4,6]_5$ parametrelerine sahip bir 4-sabit devirli lineer kod olduğu görülebilir. Bu kodun dual kodu ise $(\mathbb{F}_5G)v^T=\{xv^T\,|\,x\in\mathbb{F}_5G\}$ kümesi ile verilen $\mathbb{F}_5G$ grup halkasının iki taraflı idealidir. Aynı zamanda $\theta((\mathbb{F}_5G)v^T)$ kümesi de

$$H=\begin{pmatrix}1&0&0&0&0&0&0&0&4&2&0&4\\0&1&0&0&0&0&0&0&1&2&2&1\\0&0&1&0&0&0&0&0&4&3&2&1\\0&0&0&1&0&0&0&0&4&1&3&1\\0&0&0&0&1&0&0&0&4&1&1&2\\0&0&0&0&0&1&0&0&3&3&1&4\\0&0&0&0&0&0&1&0&1&1&3&2\\0&0&0&0&0&0&0&1&3&0&1&1\end{pmatrix}$$

matrisi tarafından üretilen ve $[12,8,4]_5$ parametrelerine sahip bir 4-sabit devirli lineer koddur.

Çizelge 5. 5 $\mathbb{F}_5$ cismi üzerindeki 22-uzunluklu 4-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

u	v^T	C	$C^{\perp}$	Q
$g^{11}+3g^{10}+3g^9+$ $4g^8+4g^7+2g^6$ $+4g^5+2g^4+g^3$ $+3g^2+g+3$	$g^{11}+3g^{10}+3g^9+$ $4g^8+4g^7+2g^6$ $+4g^5+2g^4+g^3$ $+3g^2+g+3$	$[22,11,6]$	$[22,11,6]$	$[[22,0,\geq 6]]_5$
$g^{16}+g^{15}+2g^{14}+3g^{13}$ $+3g^{12}+4g^{11}+2g^{10}$ $+4g^9+3g^8+g^7+$ $2g^6+g^5+3g^2+1$	g^6+2g^4+ $4g^2+4g+1$	$[22,6,12]$	$[22,16,4]$	$[[22,10,\geq 4]]_5$
$g^{12}+2g^{10}+3g^6$ $+2g^4+4g^2+1$	$g^{10}+g^8+4g^6$ $+4g^4+3g^2+1$	$[22,10,6]$	$[22,12,5]$	$[[22,2,\geq 5]]_5$
$g^{17}+g^{16}+g^{14}+$ $2g^{13}+2g^{12}+4g^{11}$ $+3g^6+3g^5+3g^3$ $+g^2+g+2$	$3g^5+g^4+3g^3$ $+g^2+4g+1$	$[22,5,12]$	$[22,17,2]$	$[[22,12,\geq 2]]_5$

Sonuç 5.7'den $[[12,4,\geq 4]]_5$ parametrelerine sahip bir kuantum kod vardır. Bu kod kuantum MDS sınırına sadece 1 birim uzaklıktadır.

Çizelge 5. 6 $\mathbb{F}_5$ cismi üzerindeki 42-uzunluklu 4-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

C	$C^{\perp}$	Q
$[52,26,14]$	$[52,26,14]$	$[[52,0,\geq 14]]_5$
$[52,24,14]$	$[52,28,10]$	$[[52,4,\geq 10]]_5$
$[52,22,18]$	$[52,30,12]$	$[[52,8,\geq 12]]_5$
$[52,20,18]$	$[52,32,10]$	$[[52,12,\geq 10]]_5$
$[52,18,20]$	$[52,34,10]$	$[[52,16,\geq 10]]_5$
$[52,16,22]$	$[52,36,8]$	$[[52,20,\geq 8]]_5$
$[52,14,25]$	$[52,38,8]$	$[[52,24,\geq 8]]_5$
$[52,12,26]$	$[52,40,7]$	$[[52,28,\geq 7]]_5$
$[52,10,26]$	$[52,42,6]$	$[[52,32,\geq 6]]_5$

Çizelge 5. 7 $\mathbb{F}_7$ cismi üzerindeki 18-uzunluklu 6-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

u	v^T	C	$C^{\perp}$	Q
$g^{10}+5g^8+4g^6$ $+2g^4+3g^2+1$	$g^8+4g^6+2g^2+1$	$[18,8,3]$	$[18,10,3]$	$[[18,2,\geq 3]]_7$
$g^{16}+3g^{14}+2g^{12}+6g^{10}+$ $4g^8+5g^6+g^4+3g^2+2$	$4g^2+1$	$[18,2,9]$	$[18,16,2]$	$[[18,14,\geq 2]]_7$
$g^{12}+3g^6+2$	$4g^6+1$	$[18,6,3]$	$[18,12,2]$	$[[18,6,\geq 2]]_7$

Çizelge 5. 8 $\mathbb{F}_5$ cismi üzerindeki 42-uzunluklu 4-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

C	$C^{\perp}$	Q
$[42,21,12]$	$[42,21,12]$	$[[42,21,\geq 12]]_5$
$[42,20,12]$	$[42,22,6]$	$[[42,2,\geq 6]]_5$
$[42,19,12]$	$[42,23,10]$	$[[42,4,\geq 10]]_5$
$[42,18,12]$	$[42,24,6]$	$[[42,6,\geq 6]]_5$
$[42,15,12]$	$[42,27,8]$	$[[42,12,\geq 8]]_5$
$[42,14,12]$	$[42,28,6]$	$[[42,14,\geq 6]]_5$
$[42,13,16]$	$[42,29,6]$	$[[42,16,\geq 6]]_5$
$[42,12,12]$	$[42,30,4]$	$[[42,18,\geq 4]]_5$
$[42,9,22]$	$[42,33,4]$	$[[42,24,\geq 4]]_5$
$[42,8,12]$	$[42,34,4]$	$[[42,26,\geq 4]]_5$
$[42,7,24]$	$[42,25,4]$	$[[42,28,\geq 4]]_5$
$[42,6,24]$	$[42,36,2]$	$[[42,30,\geq 2]]_5$
$[42,3,28]$	$[42,39,2]$	$[[42,36,\geq 2]]_5$
$[42,2,28]$	$[42,40,2]$	$[[42,38,\geq 2]]_5$

Çizelge 5. 9 $\mathbb{F}_{11}$ cismi üzerindeki 52-uzunluklu 10-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

C	$C^{\perp}$	Q
$[52,26,10]$	$[52,26,10]$	$[[52,0,\geq 10]]_{11}$
$[52,24,10]$	$[52,28,8]$	$[[52,4,\geq 8]]_{11}$
$[52,14,24]$	$[52,38,6]$	$[[52,24,\geq 6]]_{11}$
$[52,12,24]$	$[52,40,3]$	$[[52,28,\geq 3]]_{11}$
$[52,2,39]$	$[52,50,2]$	$[[52,48,\geq 2]]_{11}$

5.6 $\left(\mathbb{F}_q + v\mathbb{F}_q\right)G$ Grup Halkası üzerinde Kuantum Kodlar

Karakteristiği q olan $R = \mathbb{F}_q + v\mathbb{F}_q$ değişmeli halkası $v^2 = v$ olacak şekilde $\mathbb{F}_q[v] \Big/ \langle v^2 - v \rangle$ bölüm halkasına izomorftur. p tek asal sayı ve k pozitif tam sayısı için $n = 2p^k$ olmak üzere $G = 2\mathbb{Z}_n^*$ grubunun mertebesi $p^k - p^{k-1}$ ve birim elemanı $p^k + 1$ olan devirli bir grup olduğunu Teorem 5.1'de göstermiştik. Bu başlık altında RG grup halkasında elde edilen kendine dik ve kendine dual kodlar dikliği koruyan bir dönüşüm yardımıyla $\mathbb{F}_q^{\,p^k - p^{k-1}}$ sonlu cismine taşınarak elde edilen kodların minimum uzaklıkları iki katına çıkarılmıştır.

$\alpha = \sum_{g \in G} \alpha_g g \in RG$ olmak üzere $supp(\alpha) = \{g \in G | \alpha_g \neq 0\}$ kümesine α elemanının supportu denir. α elemanının Hamming ağırlığı $w(\alpha) = |supp(\alpha)|$ ile tanımlanır. RG grup halkasının bir M alt modülünün minimum ağırlığı $w(M)$ ile gösterilir ve $w(M) = \min\{|supp(\alpha)| \, \| \, 0 \neq \alpha \in M\}$ şeklinde tanımlanır. w_L ve w_H sırasıyla $R = \mathbb{F}_q + v\mathbb{F}_q$ üzerindeki kodlar için minimum Lee ve Hamming ağırlığını göstersin ve $w_L(a + bv) = w_H(a, a + b)$ olsun. Bunun sonucu olarak $\phi : R \to \mathbb{F}_q^2,\ \phi(a + bv) = (a, a + b)$ olacak şekilde bir Gray dönüşümü tanımlanır. Bu şekilde tanımlanan dönüşüm R den $\mathbb{F}_q^2$ ye ağırlık koruyan bir dönüşümdür. Bu dönüşüm $s > 0$ tam sayı olacak şekilde kolaylıkla $R^s = \left(\mathbb{F}_q + v\mathbb{F}_q\right)^s$ halkasına genelleştirilebilir. $x = \sum_{g \in G} \alpha_g g$ ve $y = \sum_{g \in G} \beta_g g \in RG$ elemanlarının iç çarpımı $\langle x, y \rangle = \sum_{g \in G} \alpha_g \beta_g$ olarak tanımlanır.

$a_1 + b_1 v$ ve $a_2 + b_2 v \in R$ elemanları için

$$(a_1 + b_1 v)(a_2 + b_2 v) = a_1 a_2 + (a_1 b_2 + b_1 a_2 + b_1 b_2) v = 0$$

$$\Leftrightarrow a_1 a_2 = 0 \text{ ve } a_1 b_2 + b_1 a_2 + b_1 b_2 = 0.$$

Çizelge 5. 10 $\mathbb{F}_5$ cismi üzerindeki 44 -uzunluklu 4 -sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

$\phi(C^{\perp})$	$\phi(C)$	Q
[44,22,6]	[44,22,6]	$\left[\left[44,0,6\right]\right]_5$
[44,12,12]	[44,32,4]	$\left[\left[44,20,\geq 4\right]\right]_5$
[44,20,6]	[44,24,5]	$\left[\left[44,4,\geq 5\right]\right]_5$
[44,10,12]	[44,34,2]	$\left[\left[44,24,\geq 2\right]\right]_5$

Dolayısıyla aşağıdaki eşitlik sağlanır.

$$\left(a_1,a_1+b_1\right)\left(a_2,a_2+b_2\right)=a_1a_2+a_1a_2+a_1b_2+b_1a_2+b_1b_2=0.$$

Bunun sonucu olarak ϕ dönüşümü aynı zamanda dikliği de korur.

$\theta:RG\to R^n,\ \theta\left(\sum_{i=1}^{n}\alpha_i g_i\right)=\left(\alpha_1,\alpha_2,\ldots,\alpha_n\right)$ dönüşümünün bir izomorfizma olduğunu daha önce ifade etmiştik.

Teorem 5.5 $C=\theta\left(\left(RG\right)u\right)\subset RG,\ \left[p^k-p^{k-1},rank\left(u\right),d\right]_q$ parametrelerine sahip bir $\left(p^k+1\right)-$sabit devirli kod ise $\phi\left(C\right)$ de $\mathbb{F}_q$ üzerinde $\left[2\left(p^k-p^{k-1}\right),2rank\left(u\right),d\right]_q$ parametrelerine sahip bir $\left(p^k+1\right)$-sabit devirli kod belirler.

İspat: Yukarıda tanımladığımız Gray dönüşümünün doğrudan sonucudur.

Grup cebirleri üzerindeki kodlar için verilen kendine dik ve kendine duallik koşulları $\left(\mathbb{F}_q+v\mathbb{F}_q\right)G$ grup halkası için de sağlanır. Dolayısıyla CSS inşası yardımıyla kuantum kod parametreleri elde edebiliriz.

Çizelge 5. 11 $\mathbb{F}_7$ cismi üzerindeki 36-uzunluklu 6-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri

$\phi(C^{\perp})$	$\phi(C)$	Q
$[36,16,3]$	$[36,20,3]$	$[[36,4,\geq 3]]_7$
$[36,4,9]$	$[36,32,2]$	$[[36,28,\geq 2]]_7$
$[36,12,3]$	$[36,24,2]$	$[[36,12,\geq 2]]_7$

Örnek 5.6 $R=\mathbb{F}_3+v\mathbb{F}_3$ ve

$$G=\{2,4,6,8,12,14,16,18,22,24,26,28,32,34,36,38,42,44,46,48\}\subset\mathbb{Z}_{50}$$

olsun. Ayrıca $rank(u)=2$ ve $rank(v)=18$ olacak şekilde

$u=g^{18}+g^{17}+2g^{16}+2g^{14}+2g^{13}+g^{12}+g^{10}+g^9+2g^8+2g^6+2g^5+g^4+g^2+g+2$ ve $v^T=2g^2+2g+1$ esas sıfır bölen elemanlarını alalım. Bu durumda $(RG)u=\{xu|x\in RG\}\subset RG$ iki taraflı ideali $[20,2,15]$ parametrelerine sahip bir 2-sabit devirli kod belirler. Dolayısıyla $\phi(\theta((RG)u))$, $[40,4,15]_3$ parametrelerine sahip bir 2-sabit devirli koddur. Bu kodun duali de $(RG)v^T=\{xv^T|x\in RG\}\subset RG$ iki taraflı idealinin belirlediği $[20,18,2]_3$ parametrelerine sahip 2-sabit devirli koddur. Benzer şekilde $\phi(\theta((RG)v^T))$ de $[40,36,2]_3$ parametrelerine sahip 2-sabit devirli kod olur. Sonuç 5.7'den $[[40,32,\geq 2]]_3$ parametrelerine sahip bir kuantum kod vardır.

Çizelge 5.12 $\mathbb{F}_3$ cismi üzerindeki 40-uzunluklu 2-sabit devirli kodlardan elde edilen bazı kuantum kod parametreleri.

$\phi(C^{\perp})$	$\phi(C)$	Q
$[40,20,6]$	$[40,20,6]$	$[[40,0,\geq 6]]_3$
$[40,16,6]$	$[40,24,4]$	$[[40,8,\geq 4]]_3$
$[40,12,9]$	$[40,28,4]$	$[[40,16,\geq 4]]_3$
$[40,8,12]$	$[40,32,3]$	$[[40,24,\geq 3]]_3$
$[40,4,15]$	$[40,36,2]$	$[[40,32,\geq 2]]_3$

BÖLÜM 6

GRUP HALKALARINDA LCD KODLAR

Bu bölümde grup halkaları üzerinde LCD kodların varlığı araştırılacaktır. Bunun için ilk olarak grup halkalarının bir direkt toplamı yardımıyla LCD kodlar elde edilecektir. Daha sonra grup halkalarında birimsel elemanlar tarafından üretilen kodların LCD olması için gerek ve yeter koşul verilecektir.

LCD kod kavramı ilk olarak Massey tarafından [44]'te verilmiştir. LCD kodlar verimli bir şekilde dekodlanabildiklerinden iki kullanıcılı kanallar için uygun kodlardır. Bu bölümde grup halkalarında LCD kodların yapısı irdelenecektir.

Tanım 6.1 $C,\ \mathbb{F}_q$ üzerinde n-uzunluklu bir lineer kod olsun. Eğer $C \cap C^{\perp} = \{0\}$ veya $\mathbb{F}_q^n = C \oplus C^{\perp}$ oluyorsa C koduna tamamlayıcı duali olan lineer kod (linear code with complemantary dual) denir [46].

6.1 Grup Halkalarında LCD Kodların Yapısı

Tanım 6.2 RG grup halkası verilsin. $\alpha = \sum_{g \in G} \alpha_g g$ olmak üzere $\alpha = \sum_{g \in G} \alpha_g g$ elemanının involutü $\alpha^* = \sum_{g \in G} \overline{\alpha}_g g^{-1}$ şeklinde tanımlanır.

Teorem 6.1 RG grup halkası verilsin. $RG^{+}=\left\{\alpha=\sum_{g\in G}\alpha_g g \,\middle|\, \alpha^{*}=\alpha\right\}$ ve $RG^{-}=\left\{\alpha=\sum_{g\in G}\alpha_g g \,\middle|\, \alpha^{*}=-\alpha\right\}$ kümelerini tanımlayalım. $RG=RG^{+}\oplus RG^{-}$ ve $RG^{+}\cap RG^{-}=\{0\}$. Ayrıca her $x\in RG^{+}$ ve her $y\in RG^{-}$ için $\langle x,y\rangle=0$ dır.

İspat: Her $\alpha=\sum_{g\in G}\alpha_g g$ ve $\beta=\sum_{g\in G}\beta_g g\in RG^{+}$ için $(\alpha+\beta)^{*}=\alpha^{*}+\beta^{*}=\alpha+\beta$ olduğundan $\alpha+\beta\in RG^{+}$ ve $(\alpha\beta)^{*}=\alpha^{*}\beta^{*}=\alpha\beta\in RG^{+}$ dir. Bu durumda RG^{+} kümesi RG nin bir alt halkası olur.

Ayrıca, $\alpha=\sum_{g\in G}\alpha_g g\in RG^{+}\cap RG^{-}$ ise $\alpha^{*}=\alpha=-\alpha$ olur. Yani $\sum_{g\in G}\alpha_g g=-\sum_{g\in G}\alpha_g g$ $\Rightarrow \alpha_g=-\alpha_g\ (\forall g\in G)$. Bu da ancak $\alpha=\sum_{g\in G}\alpha_g g=0$ ile mümkündür. O halde $RG^{+}\cap RG^{-}=\{0\}$.

Buna ek olarak $x\in RG^{+}$ ve $y\in RG^{-}$ alalım. Bu durumda $RG=RG^{+}\oplus RG^{-}$ ve $RG^{+}\cap RG^{-}=\{0\}$ olduğundan $\langle x,y\rangle=0$ elde ederiz.

Sonuç 6.1 $C=RG^{+}$ dual kodu $C^{\perp}=RG^{-}$ olan bir LCD koddur.

Örnek 6.1 $R=\mathbb{F}_3=\{0,1,2\}$ üç elemanlı sonlu cisim ve g elemanı tarafından üretilen $G=C_3=\{1,g,g^2\}$ devirli grubu iken

$$RG=\left\{\begin{matrix}0,1,2,g,2g,g^2,2g^2,1+g,2+g,1+2g,2+2g,1+g^2,2+g^2,g+g^2,\\1+g+g^2,2+g+g^2,2g+g^2,1+2g+g^2,2+2g+g^2,1+2g^2,2+2g^2,\\g+2g^2,1+g+2g^2,2+g+2g^2,2g+2g^2,1+2g+2g^2,2+2g+2g^2\end{matrix}\right\}.$$

Teorem 6.1'den aşağıda verilen $[3,2,1]_3$ parametrelerine sahip LCD kod elde edilir.

$RG^{+}=\{0,1,2,1+g+g^2,2+g+g^2,2g+2g^2,1+2g+2g^2,2+2g+2g^2\}$ ve

$RG^{-}=\{0,2g+g^2,g+2g^2\}$ dir.

$\theta(RG^{+})=\{000,100,200,111,211,022,122,222\}$

$\theta(RG^{-})=\{000,021,012\}$.

6.2 Birimsel Elemanlardan Elde Edilen Kodlar

Bu alt başlık altında [2]'de verilen grup halkasının birimsel elemanları ile kod elde etme metodu hatırlatıldıktan sonra bu kodların LCD olması için gerek ve yeter şartlar verilecektir.

R bir halka ve $G=\{g_1,g_2,\ldots,g_n\}$ iken $u\in RG$ birim eleman olsun. Bu durumda $uu^{-1}=1$ olacak şekilde $u^{-1}\in RG$ vardır. O halde, $\varphi: RG\to M_n(R)$ matris temsili için $\varphi(u)\varphi(u^{-1})=I_n$ dir. $\varphi(u)=U=\begin{pmatrix}A\\B\end{pmatrix}$ ve $\varphi(u^{-1})=U^{-1}=\begin{pmatrix}E & D\end{pmatrix}$ olsun. Burada A,B,E,D sırasıyla $r\times n,\ (n-r)\times n,\ n\times r$ ve $n\times(n-r)$ tipinde matrislerdir. $\varphi(u)\varphi(u^{-1})=I_n$ olduğundan $\begin{pmatrix}A\\B\end{pmatrix}\begin{pmatrix}E & D\end{pmatrix}=\begin{pmatrix}AE & AD\\BE & BD\end{pmatrix}=I_n$ dir. Buradan $AD=0$ ve $BE=0$ elde edilir. A matrisi tarafından üretilen r boyutlu C koduna $u\in RG$ birimsel elemanı tarafından üretilen lineer kod diyeceğiz. Dolayısıyla $C^{\perp}$, D^T tarafından üretilen $(n-r)$ boyutlu bir lineer koddur.

Birim eleman tarafından üretilen kodları aşağıdaki şekilde de tanımlayabiliriz:

Tanım 6.2 [2] $S\subseteq G$ olmak üzere $W=\langle S\rangle$, RG grup halkasının bir R alt modülü ve $u\in RG$ birim eleman olsun. $C=\{ux \mid x\in W\}$ kümesine u birimsel elemanı tarafından üretilen grup halkası kod denir. C kodunun duali ise $C^{\perp}=\left\{\left(u^{-1}\right)^T y \,\middle|\, y\in W^{\perp}\right\}$ şeklindedir. Burada $W^{\perp}=\langle G-S\rangle$ dir.

Örnek 6.2 $C_4=\langle g\rangle=\{1,g,g^2,g^3\}$ mertebesi 4 olan devirli grup ve $\mathbb{F}_2=\{0,1\}$ ikili sonlu cisim iken

$$\mathbb{F}_2C_4=\begin{Bmatrix}0,1,g,g^2,g^3,1+g,1+g^2,g+g^2,1+g+g^2,1+g^3,g+g^3,\\1+g+g^3,g^2+g^3,1+g^2+g^3,g+g^2+g^3,1+g+g^2+g^3\end{Bmatrix}$$

dir. $\mathbb{F}_2C_4$ grup cebirinin birimsel elemanlarının kümesi $U(\mathbb{F}_2C_4)$ olmak üzere $U(\mathbb{F}_2C_4)=\{1,g,g^2,g^3,1+g+g^2,1+g+g^3,1+g^2+g^3,g+g^2+g^3\}$ olarak bulunur.

$u_1 = 1 + g + g^2$ olarak alırsak u_1 elemanının tersi ve tersinin transpozu sırasıyla $u_1^{-1} = 1 + g^2 + g^3$ ve $\left(u_1^{-1}\right)^T = 1 + g + g^2$ olarak hesaplanır. Bu durumda

$$U_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \text{ ve } U_1^{-1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}. \; A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \Rightarrow D = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

$C = \langle A \rangle = \{0000, 1110, 0111, 1001\}$ bir $[4,2,2]_2$ koddur. Bu kodun duali ise $C^{\perp} = \langle D^T \rangle = \{0000, 1011, 1101, 0110\}$ bir $[4,2,2]_2$ koddur.

Ayrıca $W_1 = \langle \{1, g\} \rangle = \{0, 1, g, 1+g\}$ olarak alınırsa

$C = \{u_1 x \mid x \in W_1\} = \{0, 1+g+g^2, g+g^2+g^3, 1+g^3\}$ ve

$\theta(C) = \{0000, 1110, 0111, 1001\}$ olarak bulunur.

$W_1^{\perp} = \langle \{g^2, g^3\} \rangle = \{0, g^2, g^3, g^2+g^3\}$ olmak üzere

$C^{\perp} = \left\{ \left(u_1^{-1}\right)^T x \,\middle|\, x \in W_1^{\perp} \right\} = \{0, 1+g^2+g^3, 1+g+g^3, g+g^2\}$ ve

$\theta(C^{\perp}) = \{0000, 1011, 1101, 0110\}$.

6.3 Birimsel Elemanlardan Elde Edilen Kodların LCD Olmasının Şartı

Bu başlık altında grup halkalarının birimsel elemanlarından üretilen lineer kodların LCD koşulunu sağlaması için gerek ve yeter şartlar verilecektir. Grup halkalarının birimsel elemanlarından üretilen lineer kodların LCD koşulunu vermeden önce bunu örnekler üzerinde görelim.

Örnek 6.3 $C_6 = \langle g \rangle = \{1, g, g^2, g^3, g^4, g^5\}$ mertebesi 6 olan devirli grup ve $\mathbb{F}_2 = \{0,1\}$ ikili sonlu cisim iken $\mathbb{F}_2 C_6$'nın birimsel elemanları aşağıdaki gibidir.

$$U(\mathbb{F}_2 C_6) = \left\{ \begin{array}{l} 1, g, g^2, g^3, g^4, g^5, 1+g+g^3, 1+g^2+g^3, 1+g+g^4, g+g^2+g^4, 1+g^3+g^4, \\ g+g^3+g^4, 1+g+g^2+g^3+g^4, 1+g^2+g^5, g+g^2+g^5, 1+g^3+g^5, \\ g^2+g^3+g^5, 1+g+g^2+g^3+g^5, g+g^4+g^5, g^2+g^4+g^5, 1+g+g^2+g^4+g^5, \\ 1+g+g^3+g^4+g^5, 1+g^2+g^3+g^4+g^5, g+g^2+g^3+g^4+g^5 \end{array} \right\}.$$

$u = 1+g+g^3$ olarak alırsak, $u^T = 1+g^3+g^5$, $u^{-1} = g+g^4+g^5$ ve $\left(u^{-1}\right)^T = g+g^2+g^5$ şeklindedir. $W = \langle \{1, g^2, g^4\} \rangle = \{0, 1, g^2, 1+g^2, g^4, 1+g^4, g^2+g^4, 1+g^2+g^4\}$ olsun. Bu durumda

$$C = \{ux \mid x \in W\} = \left\{ \begin{array}{l} 0, 1+g+g^3, 1+g^2+g^4, g+g^2+g^3+g^4, \\ 1+g+g^2+g^5, g^2+g^3+g^5, g+g^4+g^5, 1+g^3+g^4+g^5 \end{array} \right\}$$

$$\theta(C) = \{000000, 110100, 101010, 011110, 111001, 001101, 010011, 100111\}$$

$[6,3,3]_2$ parametrelerine sahip bir lineer koddur. Ayrıca, $W^{\perp} = \langle \{g, g^3, g^5\} \rangle = \{0, g, g^3, g+g^3, g^5, g+g^5, g^3+g^5, g+g^3+g^5\}$ dir. Bu durumda

$$C^{\perp} = \left\{ \left(u^{-1}\right)^T x \,\middle|\, x \in W^{\perp} \right\} = \left\{ \begin{array}{l} 0, 1+g^2+g^3, 1+g+g^4, g+g^2+g^3+g^4, \\ 1+g+g^2+g^5, g+g^3+g^5, g^2+g^4+g^5, 1+g^3+g^4+g^5 \end{array} \right\}$$

$$\theta(C^{\perp}) = \{000000, 101100, 110010, 011110, 111001, 010101, 001011, 100111\}$$

$[6,3,3]_2$ parametrelerine sahip bir lineer koddur. Dikkat edilirse

$$\begin{aligned} C \cap C^{\perp} &= \{0, g+g^2+g^3+g^4, 1+g+g^2+g^5, 1+g^3+g^4+g^5\} \\ &= \{000000, 011110, 111001, 100111\}. \end{aligned}$$

Örnek 6.4 $C_6 = \langle g \rangle = \{1, g, g^2, g^3, g^4, g^5\}$ mertebesi 6 olan devirli grup ve $\mathbb{F}_2 = \{0,1\}$ ikili sonlu cisim iken $u = 1 + g + g^2 + g^4 + g^5 \in \mathbb{F}_2 C_6$ olarak alırsak, $u^T = u = u^{-1}$ olur. $W = \langle \{1, g^2, g^4\} \rangle = \{0, 1, g^2, 1+g^2, g^4, 1+g^4, g^2+g^4, 1+g^2+g^4\}$ alalım. Bu durumda

$$C = \{ux \mid x \in W\} = \begin{Bmatrix} 0, g+g^3, 1+g^2+g^4, 1+g+g^2+g^3+g^4, g+g^5, \\ g^3+g^5, 1+g+g^2+g^4+g^5, 1+g^2+g^3+g^4+g^5 \end{Bmatrix}$$

$$\theta(C) = \{000000, 010100, 101010, 111110, 010001, 000101, 111011, 101111\}$$

$[6,3,2]_2$ parametrelerine sahip bir lineer koddur. Ayrıca, $W^{\perp} = \langle \{g, g^3, g^5\} \rangle = \{0, g, g^3, g+g^3, g^5, g+g^5, g^3+g^5, g+g^3+g^5\}$ dir. Bu durumda

$$C^{\perp} = \left\{ \left(u^{-1}\right)^T x \,\middle|\, x \in W^{\perp} \right\} = \begin{Bmatrix} 0, 1+g^2, 1+g^4, g^2+g^4, g+g^3+g^5, 1+g+g^2+g^3+g^5, \\ 1+g+g^3+g^4+g^5, g+g^2+g^3+g^4+g^5 \end{Bmatrix}$$

$$\theta(C^{\perp}) = \{000000, 101000, 100010, 010010, 010101, 111101, 110111, 011111\}$$

$[6,3,2]_2$ parametrelerine sahip bir lineer koddur.

Dikkat edilirse $C \cap C^{\perp} = \{000000\}$. Dolayısıyla C kodu LCD şartını sağlar.

Teorem 6.2 R bir halka, $G = \{g_1, g_2, \ldots, g_n\}$ bir grup ve $S \subseteq G$ olmak üzere $W = \langle S \rangle$, $W^{\perp} = \langle G - S \rangle$, RG grup halkasının R – alt modülleri olsun. $u \in RG$ birim elemanı için $C = \{ux \mid x \in W\}$ ve $C^{\perp} = \left\{ \left(u^{-1}\right)^T y \,\middle|\, y \in W^{\perp} \right\}$ kodlarını tanımlayalım. $C \cap C^{\perp} = \{0\}$ ancak ve ancak $u^{-1} = u^T$.

İspat: $(\Leftarrow)$ $u^{-1} = u^T$ olsun. $C \cap C^{\perp} \neq \{0\}$ olduğunu kabul edelim. Bu durumda en az bir $0 \neq z \in C \cap C^{\perp}$ vardır. Öyle ki $z = ux = \left(u^{-1}\right)^T y$ dir. $u^{-1} = u^T$ olduğundan $z = ux = \left(u^T\right)^T y \Rightarrow ux = uy$ olur. Buradan $0 \neq x = y$ elde ederiz. $W \cap W^{\perp} = \{0\}$ olduğundan bu bir çelişkidir.

$(\Rightarrow)$ $C \cap C^{\perp} = \{0\}$ ve $0 \neq x \in W, 0 \neq y \in W^{\perp}$ için $ux \in C$ ve $\left(u^{-1}\right)^{T} y \in C^{\perp}$ olsun. Eğer $ux, \left(u^{-1}\right)^{T} y \in C \cap C^{\perp}$ ise $ux = \left(u^{-1}\right)^{T} y = 0$ dır. O halde $uxy = 0$ ve $\left(u^{-1}\right)^{T} xy = 0$ yazabiliriz. Bu durumda $uxy - \left(u^{-1}\right)^{T} xy = xy\left(u - \left(u^{-1}\right)^{T}\right) = 0$ olur. Sonuç olarak $u - \left(u^{-1}\right)^{T} = 0$ ve buradan $u^{-1} = u^{T}$.

BÖLÜM 7

SONUÇ VE ÖNERİLER

Dördüncü bölümde devresel sıfır bölen kodların yapısı bir grup halkası ailesinde çalışıldı. Ayrıca elde edilen bu kodların eleman sayıları ile dual kodları verildi.

Beşinci bölümde literatürde bir ilk olarak sabit devirli kodlar ile grup cebirleri arasında ilişki kuruldu ve bu kodların yapısı çalışıldı. Ayrıca grup cebirlerindeki sıfır bölenler kullanılarak sabit devirli kodlar için bir inşa yöntemi verildi. Bunlara ek olarak önerilen inşa metodu yardımıyla sabit devirli kodlar için bazı iyi kod parametreleri tablolar halinde verildi. Daha sonra bu kodlar içinde kendine dik ve kendine dual olan kodlar belirlendi. Bu kodlara bağlı olarak kuantum hata düzelten kodlar için bazı güzel kod parametreleri elde edildi. Buna ek olarak $\left(\mathbb{F}_q + v\mathbb{F}_q\right)G$ grup halkasındaki sabit devirli kodlardan kendine dik ve kendine dual olan kodlar belirlendi. Belirlenen bu kodlar için uygun bir Gray dönüşümü tanımlanarak $\mathbb{F}_q$ üzerinde birçok kuantum hata düzelten kod parametresi elde edildi.

Altıncı bölümde grup halkaları üzerinde LCD kodlar için bazı koşullar belirlendi. Son bölüm ise sonuç ve önerilere ayrılmıştır.

Bu çalışmada elde edilen kod parametreleri değişmeli grup halkalarından elde edilmiştir. Değişmeli olmayan gruplar üzerine inşa edilen grup halkaları vasıtasıyla daha ilginç sonuçların elde edilebileceğini öngörmekteyiz.

KAYNAKLAR

[1] Cayley, A., (1854). “On the theory of groups, as depending on the symbolic equation $\theta^n = 1$”, The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 7(42): 40-47.

[2] Hurley, P. ve Hurley, T., (2007). “Module codes in group rings”, In 2007 IEEE International Symposium on Information Theory, 1981-1985).

[3] Hurley, P. ve Hurley, T., (2009). “Codes from zero-divisors and units in group rings”, International Journal of Information and Coding Theory, 1(1): 57-87.

[4] Berman, S. D., (1967). "On the theory of group codes", Cybernetics and Systems Analysis, 3 (1): 25-31.

[5] Berman, S. D., (1967). "Semisimple cyclic and Abelian codes II", Cybernetics and Systems Analysis, 3 (3): 17-23.

[6] MacWilliams, F. J., (1969). “Codes and ideals in group algebras”, Combinatorial mathematics and its applications, 317-328.

[7] MacWilliams, M., (1970). “Binary codes which are ideals in the group algebra of an abelian group”, Bell System Technical Journal, 49(6): 987-1011.

[8] Miller, R. L., (1979). “Minimal codes in abelian group algebras”, Journal of Combinatorial Theory, Series A, 26(2): 166-178.

[9] Vesselin, D. ve Lakatos, P., (1989). "Monomial ideals, group algebras and error correcting codes", Applied Algebra, Algebraic Algorithms and error-correcting codes, 181-188.

[10] Sabin, R. E., (1994). “On row-cyclic codes with algebraic structure”, Designs, Codes and Cryptography, 4(2): 145-155.

[11] Sabin, R. E. ve Lomonaco, S. J., (1995). “Metacyclic error-correcting codes”, Applicable Algebra in Engineering, Communication and Computing, 6(3): 191-210.

[12] Forney, G. D. ve Trott, M. D., (2004). "The dynamics of group codes: Dual abelian group codes and systems", IEEE Transactions on Information Theory, 50 (12): 2935-2965.

[13] Forney, G. D. ve Trott, M. D., (1993). “The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders”, IEEE Transactions on Information Theory, 39 (5): 1491-1513.

[14] Biglieri, E. ve Michele E., (1995). "On the construction of group block codes", Annales des télécommunications. 50: Springer-Verlag.

[15] Pruthi, M. ve Arora, S. K., (1997). “Minimal codes of prime-power length”, Finite fields and their applications, 3(2): 99-113.

[16] Arora, S. K. ve Manju P., (1999). "Minimal cyclic codes of length $2p^n$ ", Finite fields and their applications, 5 (2): 177-187.

[17] Bakshi, G. K., Dumir, V. C. ve Raka. M., (2002). "Minimal cyclic codes of length 2^m ", Ranchi Univ. Math. J, 33: 1-18.

[18] Bakshi, G. K. ve Raka, M., (2003). "Minimal cyclic codes of length p^nq ", Finite Fields and Their Applications, 9 (4): 432-448.

[19] Dutra, F. S., Ferraz, R. A. ve Milies, C. P., (2009). "Semisimple group codes and dihedral codes", Algebra and Discrete Mathematics, 3: 28-48.

[20] Ferraz, R. A. ve Milies, C. P., (2007). "Idempotents in group algebras and minimal abelian codes", Finite Fields and Their Applications, 13 (2): 382-393.

[21] Pıllado, C. G. Gonzalez, S., Martinez, C., Markov, V. ve Nechaev, A., (2013). “Group codes over non-abelian groups”, Journal of Algebra and its Applications, 12(07): 1350037.

[22] Polcino Milies, C. ve de Melo, F. D., (2013). “On Cyclic and Abelian Codes”, IEEE Transactions on Information Theory, 59(11): 7314-7319.

[23] Chalom, G., Ferraz,R. A., Guerreiro, M. ve Milies, C. P., (2012). "Minimal Binary Abelian Codes of length p^mq^n ", arXiv preprint arXiv:1205.5699.

[24] Schäfer, A., (2012). Two Sided and Abelian Group Ring Codes (Doctoral dissertation, RWTH Aachen University).

[25] Singh, R. ve Pruthi, M., (2011). “Primitive idempotents of irreducible quadratic residue cyclic codes of length p^nq^m ”, Int. J. Algebra, 5(6): 285-294.

[26] Hurley, T., (2006). “Group rings and rings of matrices”, Int. J. Pure Appl. Math, 31(3): 319-335.

[27] Hurley, T., (2007). “Convolutional codes from units in matrix and group rings”, arXiv:0711.3629.

[28] Hurley, T., (2014). “Convolutional codes from unit schemes”, arXiv:1412.1695.

[29] Hurley, P. ve Hurley, T., (2010). Block codes from matrix and group rings, Selected Topics in Information and Coding Theory, (eds: I. Woungang, S. Misra and SC Misma) World Scientific, 159-194.

[30] OShaughnessy, J., (2014). “Convolutional codes from group rings”, International Journal of Information and Coding Theory, 2(4), 171-190.

[31] Fu, W. ve Feng, T., (2009). “On self-orthogonal group ring codes”, Designs, Codes and Cryptography, 50 (2): 203-214.

[32] McLoughlin, I., (2012). “A group ring construction of the $[48, 24, 12]$ type II linear block code”, Designs, Codes and Cryptography, 63(1): 29-41.

[33] Hurley, B. ve Hurley, T., (2014) “Systems of MDS codes from units and idempotents”, Discrete Mathematics, 335: 81-91.

[34] MacWilliams, F. J. ve Sloane, N. J. A., (1977). The theory of error correcting codes, Elsevier.

[35] Ling, S. ve Xing, C., (2004). Coding theory: A first course, Cambridge University Press.

[36] Morelos-Zaragoza, R. H., (2006). The art of error correcting coding, John Wiley & Sons.

[37] Wan, Z. X., (1997). Quaternary codes. (Vol. 8). World Scientific

[38] Milies, C. P. ve Sehgal, S. K., (2002). An introduction to group rings, (Vol. 1). Springer Science & Business Media.

[39] Passman, D. S., (2011). The algebraic structure of group rings, Courier Corporation.

[40] Berlekamp, E. R., (1968). Algebraic Coding Theory. Series in Systems Science, New York-Toronto: McGraw Hill.

[41] Grassl, M. Bounds on the minimum distance of linear codes, Available at: <http://www.codetables.de>. Accessed on 2016-02-15.

[42] Bosma, W. Cannon, J. ve Playoust, C., (1997). “The Magma algebra system I: The user language.” Journal of Symbolic Computation, 24(3): 235-265.

[43] Calderbank, A. R. ve Shor, P. W., (1996). “Good quantum error-correcting codes exist”, Physical Review A, 54(2): 1098.

[44] Steane, A. M., (1996). “Simple quantum error-correcting codes”, Physical Review A, 54(6): 4741.

[45] Ketkar, A. Klappenecker, A. Kumar, S. ve Sarvepalli, P. K., (2006). “Nonbinary stabilizer codes over finite fields”, IEEE Transactions on Information Theory, 52(11): 4892-4914.

[46] Massey, J. L., (1992). “Linear codes with complementary duals”, Discrete Mathematics, 106: 337-342.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı	:Mehmet Emin KÖROĞLU
Doğum Tarihi ve Yeri	:Gerger-1982
Yabancı Dili	:İngilizce
E-posta	:sadecesad@gmail.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Y. Lisans	Matematik	Yıldız Teknik Üniversitesi	2012
Lisans	Matematik	Atatürk Üniversitesi	2009
Lise	Fen Bilimleri	Esenler İbrahim Turhan Lisesi	1995-1997
		Açık Öğretim Lisesi	2006

İŞ TECRÜBESİ

Yıl	**Kurum**	**Görevi**
2012	Yıldız Teknik Üniversitesi	Araştırma Görevlisi

YAYINLARI

Makale

1. Köroğlu Mehmet Emin, Şiap İrfan (2017). A Class of Constacyclic Codes from Group Algebras. Filomat, 31(10), 2917-2923, Doi: 10.2298/FIL1710917K

2. Köroglu Mehmet Emin, Şiap İrfan, Akın Hasan (2016). The reversibility problem for a family of two dimensional cellular automata. Turk J Math, 3(40), 665-678., Doi: 10.3906/mat-1503-18

3. Köroglu Mehmet Emin, Şiap İrfan, Akın Hasan (2014). Error Correcting Codes via Reversible Cellular Automata Over Finite Fields. Arabian Journal for Science and Engineering, 39(3), 1881-1887. Doi: 10.1007/s13369-013-0757-0

4. Şiap İrfan, Akın Hasan, **Köroğlu Mehmet Emin** (2012). Cellular automata with Penta Cyclic Rule and ECCs. International Journal of Modern Physics C, 23(10), 0-13., Doi: 10.1142/S0129183112500660

5. Köroğlu Mehmet Emin, Özbek İbrahim, Şiap İrfan (2017). Optimal codes from Fibonacci polynomials and secret sharing schemes. Arabian Journal of Mathematics, Doi: 10.1007/s40065-017-0171-7

6. Köroğlu Mehmet Emin, Şiap İrfan (2017). Quantum Codes From A Class of Constacyclic Codes over Group Algebras. Malaysian Journal of Mathematical Sciences (MJMS), 11(2), 289-301.

7. Köroğlu Mehmet Emin, Şiap İrfan (2016). Quantum Codes From Negacyclic Codes over Group Ring $\left(\mathbb{F}_q + v\mathbb{F}_q\right)G$. Journal of Physics: Conference Series. Vol. 766. No. 1. IOP Publishing, 766(1), 12019, Doi: 10.1088/1742-6596/766/1/012019

8. Şiap İrfan, Akın Hasan, **Köroğlu Mehmet Emin** (2013). The Reversıbılıty of (2r +1)-Cyclıc Rule Cellular Automata. TWMS J. Pure Appl. Math., 4(2), 215-225.

9. Köroğlu Mehmet Emin, Şiap İrfan, Akın Hasan (2012). Cellular automata based byte error correcting codes over finite fields. American Institute of Physics, 1470, 183-186., Doi: 10.1063/1.4747670

10. Akın Hasan, Şiap İrfan, **Köroğlu Mehmet Emin** (2012). Transient and cycle

structure of elementary rule 150 with reflectiveboundary. American Institute of Physics, 1470, 156-158., Doi: 10.1063/1.4747663

11. Köroğlu Mehmet Emin, Şiap İrfan, Akın Hasan, Temiz Fatih (2012). Hybrid quadratic cellular automata and its applications to Pseudo random number generators. Global Journal on Technology, 1166-1171.

12. Temiz Fatih, Şiap İrfan, Akın Hasan, **Köroğlu Mehmet Emin** (2012). A Family of Two Dimensional Hybrid Cellular Automata and Its Applications to Pseudo Random Number Generators. Global Journal on Technology, 1, 1649-1655.

Bildiri

1. Köroğlu Mehmet Emin, Ersoy Bayram Ali (2017). On LCD codes from group rings. International Congress on Fundamental and Applied Sciences 2017 (ICFAS2017) (Özet Bildiri)

2. Köroğlu Mehmet Emin, Ersoy Bayram Ali (2017). A class of LCD codes from group rings. 13th International Conference on Algebraic Hyperstructures and its Applications (AHA2017) (Özet Bildiri)

3. Köroğlu Mehmet Emin, Sarı Mustafa (2017). Negacyclic Hermitian LCD Codes. Internatıonal Conference on Mathematıcs and Engıneerıng, 362-362. (Özet Bildiri)

4. Sarı Mustafa, **Köroğlu Mehmet Emin** (2017). On MDS Neagacyclic LCD Codes. Internatıonal Conference on Mathematıcs and Engıneerıng, 218-218. (Özet Bildiri)

5. Köroglu Mehmet Emin, Şiap İrfan (2016). On quantum codes via constacyclic codes from group algebras. International Congress on Fundamental and Applied Sciences (Özet bildiri)

6. Köroglu Mehmet Emin, Şiap İrfan (2016). Constacyclic Codes over Group Rings. Analysis, Topology and Algebra: The Theory and Applications (ATA2016), 32-32. (Özet bildiri)

7. Köroglu Mehmet Emin, Şiap İrfan (2016). Quantum Codes From A Class of Constacyclic Codes over Group Algebras. International Conference on Quantum Science and Applications (Özet bildiri)

8. Köroglu Mehmet Emin, Şiap İrfan (2015). Zero Divisor Codes From Group Rings. Mathematics Days in Tirana (Tam metin bildiri)

9. Özbek İbrahim, **Köroglu Mehmet Emin,** Şiap İrfan (2015). Secret Sharing Schemes Obtained from Some Special Codes. Non Commutative Rings and Their Applications IV (Özet bildiri)

10. Köroğlu Mehmet Emin, Şiap İrfan, Akın Hasan (2014). The Reversibility Problem for A Special Family of 2D Cellular Automata. 3rd International Eurasian Conference on Mathematical Sciences and Applications (IECMSA-2014) (Özet Bildiri)

11. Köroglu Mehmet Emin, Şiap İrfan (2014). Structure of Codes in The Group Rings $\mathbb{Z}_4 C_n$. KMD'2014 (Özet bildiri)

12. Şiap İrfan, **Köroglu Mehmet Emin** (2014). Optimal Code Families From Fibonacci Polynomials. KMD'2014 (Özet bildiri)

13. Köroglu Mehmet Emin, Şiap İrfan, Akın Hasan (2012). Transient and Cycle Structure of Elementary Rule 150 with Reflective Boundary. ICAAM-2012 (Özet bildiri)

14. Köroglu Mehmet Emin, Şiap İrfan (2012). Cellular automata based byte error correcting codes over finite fields. First International Conference on Analysis and Applied Mathematics (Özet bildiri)

15. Şiap İrfan, Akın Hasan, **Köroglu Mehmet Emin** (2012). On One Dimensional (2r+1) Cyclic Rule Cellular automata. IECMSA-2012 (Özet bildiri)

16. Köroglu Mehmet Emin, Şiap İrfan (2012). Cellular Automata Based Byte Error Correcting Codes over Ternary Fields. ICAAA-2012 (Özet bildiri)

17. Temiz Fatih, Şiap İrfan, Akın Hasan, **Köroğlu Mehmet Emin** (2011). A Family of Two Dimensional Hybrid Cellular Automata and Its Applications to Pseudo Random Number Generators. WCIT'2011 (Özet bildiri)

18. Köroğlu Mehmet Emin, Şiap İrfan, Akın Hasan, Temiz Fatih (2011). Hybrid Quadratic Cellular Automata and Its Applications to Pseudo Random Number Generators. WCIT'2011 (Özet bildiri)

Proje

1. Yıldız Teknik Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü **(2016-01-03-DOP01)** Bazı Grup Halkaları Üzerinde Tanımlı Kodların Yapıları (Araştırmacı)

2. Cisim ve Halkalar Üzerinde Tanımlı 2 Boyutlu HücreselDönüşümlerin Cebirsel Yapıları ve Davranışları, TÜBİTAK PROJESİ, 01/09/2011 - 01/09/2012 (Bursiyer)

ÖDÜLLERİ

1. TÜBİTAK Yurtiçi Doktora Bursu

2. Yıldız Teknik Üniversitesi Yayın Teşvik Ödülü (2013,2014)