T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL MODÜLLER ÜZERİNDE TOPLAMSAL KODLAR

İSMAİL AYDOĞDU

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
PROF. DR. İRFAN ŞİAP

İSTANBUL, 2014

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL MODÜLLER ÜZERİNDE TOPLAMSAL KODLAR

İsmail AYDOĞDU tarafından hazırlanan tez çalışması 16.09.2014 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. İrfan ŞİAP

Yıldız Teknik Üniversitesi

Eş Danışman

Prof. Dr. Taher ABUALRUB

Sharjah Amerikan Üniversitesi

Jüri Üyeleri

Prof. Dr. İrfan ŞİAP

Yıldız Teknik Üniversitesi _____

Prof. Dr. Ahmet Göksel AĞARGÜN

Yıldız Teknik Üniversitesi _____

Prof. Dr. Ünsal TEKİR

Marmara Üniversitesi _____

Doç. Dr. Kürşat Hakan ORAL

Yıldız Teknik Üniversitesi _____

Doç. Dr. Bahattin YILDIZ

Fatih Üniversitesi _____

ÖNSÖZ

Bilim ve teknolojinin olabildiğince geliştiği günümüz şartlarında bilimsel olarak yeni çalışmalar yapmak ve dünya standartlarında bilim insanlarıyla rekabet etmek başlı başına çok zor bir iştir. Eğer uğraştınız çalışma alanı matematik ve yazdığınız da bir doktora tezi ise iyi bir rehberiniz olmadan bu yükün altından kalkmanız çok da mümkün değildir.

Bu noktada kendimi gerçekten çok şanslı hissediyorum. Sadece bilimsel olarak değil, insani yönden de kendisinden çok fazla şey öğrendiğim, bilgi ve tecrübesiyle yolumu aydınlatan, sevgi, hoşgörü ve alçakgönüllülüğü ile her şeyin maddiyattan ibaret olmadığını gösteren, bir danışmanın ötesinde bir ağabey gibi her zaman yanımda olan, bilim insanı çok değerli hocam Prof. Dr. İrfan ŞİAP'a teşekkürü bir borç bilirim.

Yanında kaldığım süre boyunca benden hiçbir yardımı esirgemeyen, kendisinden çok şey öğrendiğim ve bu tezin ortaya çıkmasında ciddi katkıları olan Prof. Dr. Taher ABUALRUB'a teşekkür ederim.

Tez çalışmalarım sırasında bilgi ve deneyimleriyle bana yol gösteren, her altı ayda bir çeşitli sıkıntılara katlanarak beni dinlemeye gelen çok değerli hocalarım Prof. Dr. Ahmet Göksel AĞARGÜN ve Prof. Dr. Ünsal TEKİR'e çok teşekkür ederim.

Kendisinden programlama konusunda çok fazla yardım aldığım ve bilgi paylaşımı konusunda çok cömert davranan değerli arkadaşım Elif Segah ÖZTAŞ'a ve bu tezi okuma zahmetine katlanan kıymetli dostum Fatih TEMİZ'e çok teşekkür ederim.

Eğitim hayatım boyunca beni hiç yalnız bırakmayan, maddi ve manevi desteklerini her zaman yanımda hissettiğim canım annem ve sevgili babam başta olmak üzere bütün aileme sevgilerimi sunarım.

Eylül, 2014

İsmail AYDOĞDU

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

C	Lineer kod
C	İkili lineer kod
$C^{\perp}$	Bir C kodunun dual kodu
G	Bir kodun üreteç matrisi
H	Bir kodun kontrol matrisi
R	Sonlu halka
γ	R halkasının maksimal ideali
ν	R halkasının nilpotentlik indeksi
$\|C\|$	C kodunun eleman sayısı
ϕ, Φ	Gray dönüşümü
ψ	Modülo dönüşümü
ι	Özdeşlik dönüşümü
$wt(C)$	C kodunun minimum ağırlığı
$d(C)$	C kodunun minimum uzaklığı
(n, M, d)	Uzunluğu n, boyutu M ve uzaklığı d olan bir kod
$[n, M, d]$	Uzunluğu n, boyutu M ve uzaklığı d olan lineer bir kod
GF	Galois cismi
$\mathbb{Z}_2\mathbb{Z}_2[u]$	$\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2) -$ lineer kod
$\hat{f}$	Hadamard fonksiyonu

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖZET

BAZI ÖZEL MODÜLLER ÜZERİNDE TOPLAMSAL KODLAR

İsmail AYDOĞDU

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Prof. Dr. İrfan ŞİAP

Eş Danışman: Prof. Dr. Taher ABUALRUB

Teknoloji çağı olan günümüzde haberleşme araçlarının çok fazla önemi vardır. Her gün cep telefonu, internet, televizyon ve benzeri iletişim araçlarıyla iç içeyiz ve daha farklı modern iletişim araçlarını kullanıyoruz. Bu araçlar yardımıyla farklı şehir veya ülkelerden insanlarla irtibata geçiyor televizyon ve internet vasıtasıyla dünyanın herhangi bir yerinde meydana gelen bir olaydan çok kısa süre içerisinde haberdar olabiliyoruz. E-posta ve diğer sosyal iletişim araçlarını kullanarak arkadaşlarımızla ya da ailemizle mesajlaşabiliyor hatta görüntülü olarak konuşabiliyoruz. Bu iletişim araçları olmadan bir dünya hayal edemesek de iletişim dünyasındaki bu yeni teknolojilerin büyük bir kısmının çok eski bir geçmişi yoktur.

1870'de telefonun hayatımıza girmesiyle beraber iletişim teknolojisi her geçen gün gelişmiş ve bugünkü halini almıştır. İletişim araçlarının yaygınlaşması, daha kaliteli ve güvenli iletişim ihtiyacını ortaya çıkarmış ve bu ihtiyaca bilgi ve kodlama teorisi denilen bilim dalı çözüm aramaya başlamıştır.

Bilgi ve kodlama teorisi ile ilgili en önemli gelişme 1948 yılında Shannon tarafından yayımlanan bir makale olmuştur [1]. Shannon bu makalesinde, iletişim sistemi için genel bir mekanizma tanımlamış, bilgi ve kodlama teorisinin temellerini oluşturmuştur.

1990'lı yıllarda kodlama teorisiyle ilgili çalışmalar halkalar üzerine aktarılmaya başlanmıştır. Özellikle $\mathbb{Z}_4$ halkası üzerinde yapılan çalışmalar ve bu halka üzerindeki kodların özel bir Gray dönüşümü tanımlanarak, önceden tanımlanmış ve mükemmel

denilen ikili kodlara çevrilmesi halkalar üzerindeki kodlar için bir dönüm noktası olmuştur.

2010 yılında $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodlar tanımlanmış ve bu kodların yapısı incelenmiştir. Bu kodlar bünyelerinde hem ikili hem de dörtlü kodları barındırdıklarından kodlama teorisinin ilginç ve araştırmaya açık bir alanı haline gelmiştir.

Bu tez, toplamsal kodlarla ilgili bugüne kadar yapılan çalışmaları genellemektedir. Giriş bölümü olan birinci bölümde literatürde toplamsal kodlarla ilgili yapılan çalışmalardan bahsedilmiş, tezin amacı ve orijinalliği hakkında bilgi verilmiştir. İkinci bölüm ise kodlama teorisiyle alakalı temel bilgi ve tanımların verildiği Kodlama Teorisine Giriş bölümüdür.

Üçüncü ve dördüncü bölümlerde; $1\le r<s$ tamsayılar ve p asal bir sayı olmak üzere, $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodların doğal birer genelleştirilmesi olan $\mathbb{Z}_2\mathbb{Z}_{2^s}-$toplamsal ve $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$toplamsal kodlar tanımlanmış ve bu kodların cebirsel yapısı hakkında bilgi veren üreteç ve kontrol matrislerinin standart formları belirlenmiştir. Ayrıca bu iki kod ailesi üzerinde bazı sınırlar verilmiş ve bu sınırları sağlayan bazı örnekler elde edilmiştir.

Beşinci bölümde; $u^2=0$ ve $\mathbb{Z}_2+u\mathbb{Z}_2=\{0,1,u,1+u\}$ olmak üzere $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$lineer kodlar tanımlanmıştır. Bu kodlar yapısal olarak $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodlara benzemelerine karşın bazı özellikleri itibariyle bu kodlardan daha avantajlıdırlar. Ayrıca, $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$lineer kodların üreteç matrislerinin standart formları belirlenmiş, bu kodlar için dual uzay tanımlanarak dual uzay için üreteç matrisi olan kontrol matrisin standart formu da verilmiştir. Son kısımda ise bu kodlardan ikili görüntüleri optimal parametrelere sahip olanlara örnekler verilmiştir. Ayrıca, MacWilliams özdeşliği elde edilerek bir C, $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$lineer kodunun ağırlık dağılımıyla dual kodunun ağırlık dağılımları arasındaki bağıntı da verilmiştir.

Tezin son bölümü olan altıncı bölüm ise sonuç bölümüdür.

Anahtar Kelimeler: Lineer kod, üreteç matris, kontrol matris, $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kod, $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$toplamsal kod, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod.

ABSTRACT

ADDITIVE CODES ON SOME SPECIAL MODULES

İsmail AYDOĞDU

Department of Mathematics

PhD Thesis

Adviser: Prof. Dr. İrfan ŞİAP

Co-Adviser: Prof. Dr. Taher ABUALRUB

Today, which is the age of technology; communication devices are very important. Every day, we come in contact with mobile phones, internet, television etc. and use other various modern communication systems. Using these media, we instantly come in contact with people in different cities and countries and also we are instantly informed about events that occur around the world through television and internet. By using e-mail and other social media we can send messages to our friends and family we even can chat with video call. Although we cannot imagine a world without these means of communications, a large part of these important technologies do not have a very ancient history.

Together with the phone came into our lives in 1870, the communication technology has advanced day by day and reached to today's status. Dissemination of the communication devices brought about a need for a securer and quality communication and a branch of mathematics called information and coding theory began to seek a solution for this need.

The most important initial development in information theory and coding theory was in 1948, when Shannon published a remarkable paper [1]. In this paper, Shannon identified a general mechanism for a communication system and set a base for information and coding theory.

In 1990's the study of coding theory began to transfer onto the rings. In particular, studies about the ring $\mathbb{Z}_4$ and finding the binary images of these codes by defining a special Gray map was an initial point for studies on finite rings.

In 2010, $\mathbb{Z}_2\mathbb{Z}_4-$additive codes were introduced and the structures of these codes were determined. These families of codes are interesting and have become an open research area of coding theory since they are related with both binary and quaternary codes.

This thesis generalizes the results related to additive codes which have been introduced so far. In the first chapter of the thesis, which is the introduction part, we mention about studies on additive codes covered in the literature and we state the goal of this thesis. The second chapter covers the basics of coding theory where we give general information and definition about coding theory.

In chapter three and four, we define $\mathbb{Z}_2\mathbb{Z}_{2^s}-$additive and $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$additive codes for $1\le r<s$ and a prime p, which are natural generalizations of $\mathbb{Z}_2\mathbb{Z}_4-$additive codes respectively. We determine the standard form of the generator and parity-check matrices of these codes and also we give some bounds on these codes and give examples that attain these bounds.

In chapter five, we define $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$linear codes where $u^2=0$ and $\mathbb{Z}_2+u\mathbb{Z}_2=\{0,1,u,1+u\}$ is a ring with four elements. Although the structure of these codes and $\mathbb{Z}_2\mathbb{Z}_4-$additive codes are similar, $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$linear codes have advantages in some cases. We also give standard form of the generator matrix of these codes and define the dual space for a $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$linear code and further we determine the generator matrix of the dual code which is actually a parity-check matrix of the code. In the last part of this chapter, we give some examples of these codes which are optimal binary codes under the Gray image. We also establish a MacWilliams-type identity between the weight distribution of a code and the weight distribution of a dual code.

The last part which is the sixth chapter of the thesis is the conclusion part.

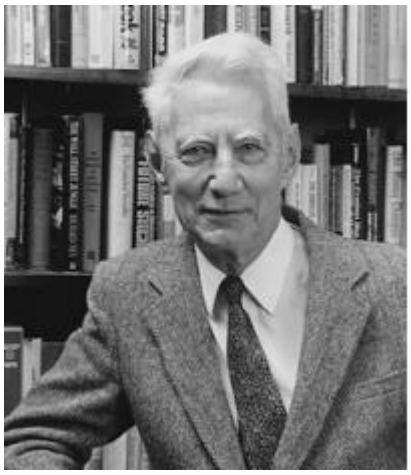
Keywords: Linear code, generator matrix, parity-check matrix, $\mathbb{Z}_2\mathbb{Z}_4-$additive codes, $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$additive codes, $\mathbb{Z}_2\mathbb{Z}_2[u]-$linear code.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Kodlama teorisi ile ilgili ilk çalışmalar 1940'lı yıllarda Hamming, Golay ve Shannon tarafından yapılmıştır. Ancak kodlama teorisi için başlangıç noktası diyebileceğimiz ve bu teorinin temellerinin atıldığı çalışma 1948 yılında Shannon tarafından yayımlanan "A mathematical theory of communication" adlı makaledir [1]. Shannon bu makale ile bilgi aktarımının gerçekleştiği bir kanal için kanal kapasitesi denilen bir sayı tanımlamış ve bu kanal kapasitesinin altındaki bir oran için güvenilir bilgi iletişiminin gerçekleştirilebileceğini ispatlamıştır. Shannon'un verdiği bu sonuçlar, bilginin gönderilmeden önce, kanalda değişime uğrayacak bilginin özel bir doğruluk değeriyle dekodlanmasını sağlayacak şekilde, kodlanabilmesini garanti altına almıştır. Bu sonuçlar günümüzde cep telefonlarında, CD'lerde ve bilgi depolama aygıtlarında kullanılmaktadır.



Şekil 1.1 Claude E. Shannon (1916-2001)

Kodlama teorisi içinde iletişim için en yaygın olarak kullanılan kodlar ikili kodlardır. n uzunluğunda ikili bir söz $\mathbb{Z}_2^n$ in bir alt kümesidir. Lineer kodlar, cebirsel yapıları ve lineer olmayan kodlara göre kodlama ve dekodlama işleminin daha kolay yapılabilmesi açısından kodlama teorisinde en çok kullanılan kodlardır. Lineer bir kod için kodsözleri üretecek olan bir üreteç matrisinden söz edilebilir.

Kodlama teorisiyle ilgili cisimler üzerinde yapılan çalışmalar çoğunlukta olsa da 1994 yılında Hammons ve arkadaşları $\mathbb{Z}_4$ halkası üzerinde bir çalışma yaptılar ve bu çalışma sonlu halkalar üzerindeki kodların araştırılması için bir başlangıç oldu [2]. Daha sonra bazı özel halkalar üzerindeki kodlar da çalışılmaya başlanmıştır.

Toplamsal kodlar ilk defa 1973 yılında Delsarte tarafından birleşim şemaları esas alınarak tanımlanmıştır [3], [4]. Genel olarak toplamsal kod, ötelenmiş birleşim şemasındaki değişmeli grubun bir alt grubu olarak tanımlanır. Daha sonra 1997 yılında ötelenme ile değişmeyen propelineer kodlar tanımlanmış ve bu ikili kodların, $\mathbb{Q}_8$ sekiz elemanlı değişmeli olmayan quaterniyon grubu göstermek üzere, $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \times \mathbb{Q}_8^\sigma$ in alt gruplarına izomorf oldukları ispatlanmıştır [5].

Birleşim şemasının Hamming şeması olduğu durumda, yani değişmeli grubun mertebesinin 2^n olduğu durumda, toplamsal kodlar değişmeli ötelenme ile değişmeyen propelineer kodlarla çakışırlar. Böylece, bu tip değişmeli gruplar, $\alpha + 2\beta = n$ olmak üzere, sadece $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ formunda olacaktır [5]. Buradan, ikili Hamming şemasındaki toplamsal kodlar yalnızca $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ nın C alt grupları olarak incelenir.

α ve β birer pozitif tamsayı olmak üzere $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ nın bir C alt grubuna $\mathbb{Z}_2\mathbb{Z}_4 -$ toplamsal kod denir. $\mathbb{Z}_2\mathbb{Z}_4 -$ toplamsal kodların cebirsel yapısı 2010 yılında Borges ve arkadaşları tarafından "$\mathbb{Z}_2\mathbb{Z}_4 -$ linear codes: Generator Matrices and Duality" adlı makale ile incelenmiş ve bu makalede $\mathbb{Z}_2\mathbb{Z}_4 -$ toplamsal kodların standart haldeki üreteç ve kontrol matrisleri belirlenmiştir [6]. Çok yeni diyebileceğimiz bu çalışmayla beraber $\mathbb{Z}_2\mathbb{Z}_4 -$ toplamsal kodlar birçok matematikçinin ilgisini çekmiş ve bugüne kadar bu konuyla ilgili olarak çeşitli çalışmalar yapılmıştır [7], [8], [9]. Ayrıca, bu

kodların uygulama alanları araştırılmış ve Steganografi üzerindeki bazı uygulamaları [10], [11] makaleleri ile verilmiştir.

1.2 Tezin Amacı

Birleşim şemasının ikili Hamming şeması olduğu durum için toplamsal kodlar $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ toplamsal grubunun ($\mathbb{Z}-$alt modülünün) birer alt grubudurlar (alt modülüdürler). Bu tezde amaçlanan ise daha genel halkalardan oluşan, $s>1$ olmak üzere $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ ve hatta daha genel olarak $1 \le r < s$ ve p asal sayısı için $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ üzerinde tanımlı alt gruplar ($\mathbb{Z}-$alt modüller) olan toplamsal kodların cebirsel yapılarının incelenmesidir. Bunların dışında $\mathbb{Z}_2^{\alpha} \times \left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)^{\beta}$ nın alt modülleri olan kodların üreteç ve kontrol matrislerinin standart formlarının belirlenmesi amaçlanmıştır. Ayrıca bu kodların özel bir Gray dönüşümü altındaki ikili ya da $p-$li görüntülerinin hangi parametrelere sahip olduğunun belirlenmesi de hedeflenmiştir.

1.3 Orijinal Katkı

Bu tezle beraber toplamsal kodlarla ilgili bugüne kadar yapılan birçok çalışma genelleştirilmiştir. Yeni toplamsal kod aileleri tanımlanmış, bu kod ailelerin yapıları incelenmiştir. Ayrıca, bu kodlardan Gray dönüşümü yardımıyla iyi parametreli ikili kodlar elde edilmiştir.

BÖLÜM 2

KODLAMA TEORİSİNE GİRİŞ

2.1 Genel Bilgiler

Kodlama teorisi, bilginin bir kaynaktan diğerine verimli ve doğru bir şekilde aktarılmasını sağlayacak metotları belirleyen çalışma alanıdır. Bilgilerin iletildiği fiziksel ortam ***kanal*** olarak adlandırılır. Telefon hatları ve atmosfer birer kanal örnekleridir. Bilgiler iletilirken meydana gelebilecek hatalar kaçınılmazdır. Bilgi kanala girdiği anda farklı nedenlerden dolayı, mesela telefon hatlarındaki kablonun küçük bir yerinde kırık olması, bozulmaya ya da kanal kirliliğine maruz kalabilir. Bu yüzden gönderilen bilginin kanalda maruz kaldığı kirlilikten dolayı oluşan hatayı belirlemek ve hatta mümkünse bu hatayı düzeltmek için sistematik bir yöntem kullanılması akıllıca olacaktır. Kodlama teorisinin asıl amacı da budur. Bilgi gönderilmeden önce kodlama dediğimiz ve bilginin sayılara dönüştürüldüğü ve bu dönüşüme cebirsel bir yapı giydirildiği bir yöntemle değiştirilir ve kanaldan çıktıktan sonra da dekodlama dediğimiz bir yöntemle sayılar tekrar bilgi haline dönüştürülür. Genel olarak zor olan kodlama değil dekodlama işlemidir. Çünkü çoğu zaman, bilginin iletimi esnasında arzu edilmeyen durumlarla karşılaşılabilir. Bu durumlar iletilen bilginin bozulmasına neden olabilir ve bu bozukluklar ***gürültü*** olarak adlandırılır. Kodlama teorisi, bilgi iletimi esnasında kanaldaki gürültü nedeniyle meydana gelen hataları tespit etme ve bu hataları düzeltme problemi üzerinde çalışır. Kodlama teorisinin temel olarak beş amacı vardır. Bunlar,

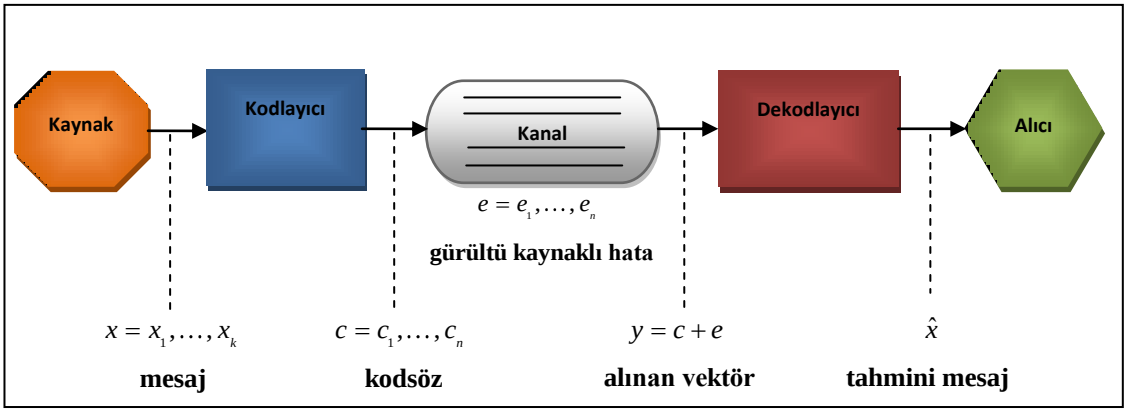
1. Bilginin hızlı kodlanması
2. Kodlanmış mesajların kolay taşınması

3. Alınan mesajların hızlı dekodlanması

4. Kanalda oluşan hataların düzeltilmesi

5. Birim zamanda maksimum bilgi transferi.

Bilgi transfer şeması genel olarak aşağıdaki gibi verilir.



Şekil 2.1 Gauss iletişim kanalı şeması

Aşağıda kodlama teorisi ile ilgili temel tanım ve teoremler verilecektir. Bu bilgiler, Ling ve Xing'in "Coding Theory: A First Course " adlı kitabı esas alınarak yazılmıştır.

Tanım 2.1 [12] q elemanlı $A=\{a_1,a_2,\ldots,a_q\}$ kümesine kod alfabesi ve bu kümenin elemanlarına da ***kod sembolleri*** denir.

i) A kümesi üzerindeki n uzunluğundaki ***söz*** diye her i için $w_i \in A$ olmak üzere $w=w_1w_2\cdots w_n$ dizisine denir. Buna denk olarak w, $(w_1,\ldots,w_n)$ vektörü ile de ifade edilebilir.

ii) A nın aynı n uzunluğuna sahip sözlerinden oluşan boştan farklı C alt kümesine A üzerinde n uzunluklu ***kod*** denir.

iii) C nin herhangi bir elemanına ***kodsöz*** denir.

iv) C nin kodsözlerinin sayısına C ***nin eleman sayısı*** denir ve $|C|$ ile gösterilir.

v) n uzunluğunda ve M boyutundaki koda $(n,M)-$***kod*** denir.

Not 2.2

1. Çoğu zaman kod alfabesi olarak q elemanlı $\mathbb{F}_q$ cismi seçilir.

2. Kod alfabesi olarak $\mathbb{Z}_2 = \mathbb{F}_2 = \{0,1\}$ alınırsa bu alfabe üzerindeki koda ***ikili kod*** denir.

3. $\mathbb{F}_3 = \{0,1,2\}$ alfabesi üzerindeki bir koda ***üçlü kod*** ve $\mathbb{F}_4 = \{0,1,2,3\}$ üzerindeki bir koda da ***dörtlü kod*** denir. Ayrıca $\mathbb{Z}_4$ halkası üzerindeki koda da dörtlü kod denmektedir.

2.2 Hamming Uzaklık

x ve y, A alfabesi üzerinde n uzunluğundaki sözler olsunlar. x ten y ye ***(Hamming) uzaklık*** $d(x,y)$ ile gösterilir ve x ve y nin birbirlerinden farklı olan koordinatlarının sayısıdır [12]. Eğer $x = x_1,\ldots,x_n$ ve $y = y_1,\ldots,y_n$ ise $d(x,y) = d(x_1,y_1)+\cdots+d(x_n,y_n)$ ve $x_i,\ y_i \in A$ bir uzunluklu sözleri göstermek üzere $d(x_i,y_i) = \begin{cases} 1, & x_i \neq y_i \\ 0, & x_i = y_i \end{cases}$ biçiminde tanımlanmıştır.

Örnek 2.3

i) $A = \{0,1\}$ olmak üzere $x = 10101,\ y = 11011$ ve $z = 00110$ olsun. Böylece,

$d(x,y) = 3,\ d(x,z) = 3$ ve $d(y,z) = 4$ dür.

ii) $A = \{0,1,2,3,4\}$ olsun. Eğer $x = 0134, y = 1243$ ve $z = 1034$ ise

$d(x,y) = 4,\ d(x,z) = 2$ ve $d(y,z) = 3$ olacaktır.

Önerme 2.4 [12] x, y ve z, A alfabesi üzerinde n uzunluğundaki sözler olsunlar. Bu durumda aşağıdaki ifadeler sağlanır.

i) $0 \le d(x,y) \le n$

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

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

iv) $d(x,z) \le d(x,y) + d(y,z)$ (Üçgen eşitsizliği)

Bu önerme d fonksiyonunun A^n üzerinde bir metrik olduğunu göstermektedir. d nin metrik olması Gauss kanalında meydana gelebilecek değişimlerin fark edilebilmesine olanak sağlar.

2.3 Bir Kodun Uzaklığı

C, en az iki adet söz içeren bir kod olsun. C nin ***minimum uzaklığı*** $d(C)$ ile gösterilir ve $d(C)=\min\{d(x,y): x,y\in C, x\neq y\}$ şeklinde tanımlanır [12].

Tanım 2.5 [12] Uzunluğu n, boyutu M ve uzaklığı d olan bir kod $(n,M,d)-$***kod*** olarak adlandırılır. Buradaki n,M ve d sayılarına C kodunun ***parametreleri*** denir.

Örnek 2.6

i) $C=\{0000,1100,1111\}$ ikili kodu için,

$d(0000,1100)=2,\ d(0000,1111)=4,\ d(1100,1111)=2$ olduğundan $d(C)=2$ ve C, ikili $(4,3,2)-$koddur.

ii) $C=\{00000,00111,22211\}$ üçlü kodu için $d(C)=3$ tür. Çünkü,

$d(00000,00111)=3,\ d(00000,22211)=5$ ve $d(00111,22211)=3$ biçimindedir ve böylece C üçlü kodu $(5,3,3)-$koddur.

Tanım 2.7 [12] m pozitif bir tamsayı olsun. Eğer bir kodsöz en az bir ve en fazla m hataya maruz kaldığında oluşan yeni söz bir kodsöz değilse C ye $m-$***hata tespit eden kod*** denir. Bir C kodu eğer $m-$hata tespit eder $(m+1)-$hata tespit edemezse C ye ***tam olarak*** $m-$***hata tespit eden kod*** denir.

Örnek 2.8 $C=\{00000,11100,11111\}$ ikili kodu $1-$hata tespit eden bir koddur. Çünkü, herhangi bir kodsöz bir koordinatının değişmesi ile diğer bir kodsöze dönüşmez. Diğer bir deyişle,

$00000\rightarrow 11100$, üç koordinatın değişmesi gerekli

$00000\rightarrow 11111$, beş koordinatın değişmesi gerekli

$11100\rightarrow 11111$, iki koordinatın değişmesi gerekli

Daha doğru bir ifadeyle C kodu tam olarak $1-$hata tespit eder denebilir. Çünkü 11100 kodsözünde iki koordinatın değişmesiyle 11111 kodsözü elde edilir. Yani C, $2-$hata tespit edemez.

Teorem 2.9 [12] Bir C kodunun $m-$hata tespit edebilmesi için gerekli ve yeterli şart $d(C) \geq m+1$ olmasıdır. Yani d uzaklığa sahip bir C kodu tam olarak $(d-1)$ hata tespit edebilir.

Tanım 2.10 [12] Pozitif bir t tamsayısı için eğer C kodu minimum uzaklık dekodlamasıyla t veya daha az hata düzeltebiliyorsa, C koduna ***tam olarak*** $t-$***hata düzelten kod*** denir.

Buradaki ***minimum uzaklık dekodlaması*** şöyle tanımlanır. Bir iletişim kanalından bir C kodunun kodsözlerinin gönderildiğini varsayalım. Eğer x sözü alıcı tarafından alınmışsa, en yakın komşuluk dekodlama kuralı veya minimum uzaklık dekodlama kuralı; x i c_x olarak dekodlayacaktır ki $d(x,c_x)$, C nin kodsözleri arasında en küçüğüdür. Yani, $d(x,c_x) = \min_{c \in C} d(x,c)$ biçimindedir.

Eğer bir C kodu t hata düzetebiliyor ancak $(t+1)$ hatayı düzeltemiyorsa C ye ***tam olarak*** $t-$***hata düzelten kod*** denir.

Örnek 2.11 $C = \{000, 111\}$ ikili kodu verilsin. C, tam olarak $1-$hata düzelten bir koddur. Gerçekten de minimum uzaklık dekodlama kuralı kullanılırsa;

i) Eğer kanaldan 000 gönderilmiş ve bir hata meydana gelmişse alınacak söz $(100, 010 \text{ veya } 001)$ olup bunlara en yakın 000 olarak dekodlanacaktır.

ii) Eğer kanaldan 111 gönderilmiş ve bir hata meydana gelmişse alınacak söz $(101, 110 \text{ veya } 011)$ olacak ve bunlara en yakın 111 olarak dekodlanacaktır.

olduğu görülür.

Teorem 2.12 [12] Bir C kodunun $t-$hata düzeltebilmesi için gerekli ve yeterli şart $d(C) \geq 2t+1$ olmasıdır. Yani d uzaklığa sahip bir C kodu tam olarak $\left\lfloor \frac{d-1}{2} \right\rfloor$ hata düzeltir. Buradaki $\lfloor x \rfloor$; x e eşit ya da x ten küçük olan en büyük tamsayıdır.

2.4 Lineer Kodlar

$\mathbb{F}_q^n$ nin bir C alt uzayına $\mathbb{F}_q$ üzerinde n uzunluklu ***lineer kod*** denir [12].

Örnek 2.13 Aşağıdaki kodlar lineerdir.

i) $C=\{(\lambda,\lambda,\ldots,\lambda):\lambda\in\mathbb{F}_q\}$ bir tekrarlı koddur.

ii) $C=\{000,001,022,002,003,023,020,021\}$ bir dörtlü koddur.

iii) $C=\{0000,1001,1011,0110,0010,1111,1101,0100\}$ bir ikili koddur.

Tanım 2.14 [12] C, $\mathbb{F}_q^n$ üzerinde lineer bir kod olsun.

i) C nin ***dual kodu*** $C^{\perp}$ ile gösterilir ve $\mathbb{F}_q^n$ nin C alt uzayının ortogonal tümleyenidir.

Daha açık bir ifadeyle, $C^{\perp}$, C nin bütün elemanlarına ortogonal olan elemanların kümesidir. Yani, $x=(x_1,x_2,\ldots,x_n), y=(y_1,y_2,\ldots,y_n)\in\mathbb{F}_q^n$ için $\langle x,y\rangle=\sum_{i=1}^{n}x_iy_i$, $\mathbb{F}_q$ üzerindeki elemanların standart iç çarpımını göstermek üzere, $C^{\perp}=\{y\in\mathbb{F}_q^n\mid\langle x,y\rangle=0,\ \forall x\in C\}$ biçimindedir.

ii) C lineer kodunun ***boyutu*** $\dim(C)$ ile gösterilir ve $\mathbb{F}_q$ üzerinde C nin vektör uzayı olarak boyutudur.

Teorem 2.15 [12] C, $\mathbb{F}_q$ üzerinde n uzunluğunda lineer bir kod olsun. Bu durumda,

i) $|C|=q^{\dim(C)}$ yani $\dim(C)=\log_q|C|$,

ii) $C^{\perp}$ lineer bir koddur ve $\dim(C)+\dim(C^{\perp})=n$,

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

Tanım 2.16 [12] C lineer bir kod olsun.

i) Eğer $C\subseteq C^{\perp}$ ise C ye ***kendine dik***,

ii) Eğer $C=C^{\perp}$ ise C ye ***kendine dual***

kod denir.

2.5 Hamming Ağırlık

x, $\mathbb{F}_q^n$ üzerinde bir söz olsun. x in ***(Hamming) ağırlığı*** $wt(x)$ ile gösterilir ve x deki sıfırdan farklı koordinatların sayısı olarak tanımlanır [12]. Yani 0, sıfır sözünü göstermek üzere $wt(x) = d(x,0)$ dir.

Her $x \in \mathbb{F}_q$ için Hamming ağırlığı aşağıdaki gibi tanımlanabilir.

$$wt(x) = d(x,0) = \begin{cases} 1, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Önerme 2.17 [12] $x, y \in \mathbb{F}_q^n$ olmak üzere $d(x,y) = wt(x-y)$ dir.

Tanım 2.18 [12] Herhangi bir C kodu için ***minimum (Hamming)ağırlık*** $wt(C)$ ile gösterilir ve C nin sıfırdan farklı kodsözlerinden en küçük ağırlığa sahip olanın ağırlığına eşittir.

Teorem 2.19 [12] C, $\mathbb{F}_q$ üzerinde lineer bir kod olsun. Bu durumda, $d(C) = wt(C)$ dir.

Not 2.20 Lineer kodların lineer olmayan kodlara göre bazı avantajları aşağıdaki gibi sıralanabilir.

1. $d(C) = wt(C)$ olduğundan lineer kodun minimum uzaklığını bulmak daha kolaydır.
2. Lineer kodlarla kodlama yapmak daha hızlıdır ve daha az hafıza gerektirir.
3. Hangi hataların düzeltilebileceğini ya da tespit edilebileceğini belirlemek daha kolaydır.
4. Lineer kodlar için çok verimli dekodlama yöntemleri mevcuttur.
5. Lineer kodlar vektör uzayı olduklarından bazlar cinsinden ifade edilebilirler.

2.6 Lineer Kodların Bazları

Lineer kodlar vektör uzayı olduklarından bütün elemanları bazlar cinsinden ifade edilebilir.

Tanım 2.21 [12] A, $\mathbb{F}_q$ üzerinde bir matris olsun. A üzerindeki elementer satır işlemleri aşağıdaki üç işlemden birisiyle yapılır.

i) Herhangi iki satırı yer değiştirme,

ii) Herhangi bir satırı sıfırdan farklı bir skaler ile çarpma,

iii) Bir satırı diğer bir satırın skaler çarpımı ve kendisinin toplamıyla yer değiştirme.

2.7 Üreteç Matrisi ve Kontrol Matrisi

Lineer bir kod için bazının bilinmesi kodsözlerinin tam olarak belirlenebilmesini sağlar. Kodlama teorisinde, lineer bir kodun bazı genel olarak matris formunda verilir ve bu matrise üreteç matrisi denir. Dual kodun bazını ifade eden matrise de kontrol matrisi denir. Bu matrisler kodlama teorisinde büyük öneme sahiptirler. Çünkü bu matrisler yardımıyla kodun bazı önemli parametreleri ve özellikleri hakkında bir şeyler söylenebilir.

Tanım 2.22 [12]

i) Satırları C lineer kodunun bütün kodsözlerini üreten, yani C lineer kodu için baz olan G matrisine C nin ***üreteç matrisi*** denir.

ii) $C^{\perp}$ dual kodunun H üreteç matrisine de C lineer kodunun ***kontrol matrisi*** denir.

Not 2.23

1. Eğer C bir $[n,k]-$lineer kod ise C nin üreteç matrisi $k \times n$ boyutunda ve kontrol matrisi de $(n-k) \times n$ boyutunda olacaktır.
2. Bir vektör uzayı birden fazla baza sahip olabilir. Dolayısıyla, lineer bir kodun da birden fazla üreteç matrisi olabilir. Eğer sabit bir baz seçilirse, bu bazla ifade edilen üreteç matrisin satırlarının permütasyonu ile farklı üreteç matrisleri elde edilebilir.
3. Üreteç matrisinin satırları lineer bağımsızdır. Aynı şekilde kontrol matrisinin satırları da lineer bağımsızdır. $k \times n$ boyutundaki bir G matrisinin verilen bir

$[n,k]-$lineer kodunun üreteç matrisi olduğunu göstermek için G nin satırlarının C nin kodsözleri olması ve lineer bağımsız olmaları yeterlidir.

Tanım 2.24 [12] Lineer bir C kodu için verilen G üreteç matrisi elementer satır işlemleri kullanılarak özel bir forma getirilebilir. Bu forma üreteç matrisin ***standart formu*** denir. Özel olarak eğer C sonlu bir cisim üzerinde bir $[n,k]-$lineer kod ise,

i) Üreteç matrisin standart formu $\left(I_k \mid X\right)$ biçiminde ve

ii) Kontrol matrisin standart formu ise $\left(Y \mid I_{n-k}\right)$ biçimindedir.

Önerme 2.25 [12] $\mathbb{F}_q$ üzerindeki C, $[n,k]-$lineer kodu G üreteç matrisiyle verilmiş olsun. $v \in \mathbb{F}_q^n$ elemanının $C^{\perp}$ in bir elemanı olması için gerekli ve yeterli şart; v nin G deki her satıra dik olmasıdır. Yani, $v \in C^{\perp}$ olması için gerekli ve yeterli şart $vG^t = 0$ olmasıdır. Özel olarak, $(n-k)\times n$ boyutlu H matrisinin C lineer kodunun kontrol matrisi olabilmesi için gerek ve yeterli şart; H nin satırlarının lineer bağımsız olması ve $HG^t = 0$ olmasıdır.

Teorem 2.26 [12] C bir lineer kod ve C nin kontrol matrisi de H olsun. Buradan,

i) C nin uzaklığının d ye eşit veya d den büyük olması için gerekli ve yeterli şart; H nin bütün $d-1$ sütunlu kümelerinin lineer bağımsız olmasıdır.

ii) C nin uzaklığının d ye eşit veya d den küçük olması için gerekli ve yeterli şart; H nin d sütundan oluşan bir sütun kümesinin lineer bağımlı olmasıdır.

Sonuç 2.27 [12] C bir lineer kod ve H, C nin kontrol matrisi olsun. Aşağıdaki ifadeler denktirler.

i) C, d uzaklığına sahiptir.

ii) H nin herhangi $d-1$ sütunu lineer bağımsızdır ve H, d adet lineer bağımlı sütuna sahiptir.

Teorem 2.28 [12] Eğer C, $[n,k]-$lineer kodunun standart formdaki üreteç matrisi $G=\left(I_k \mid X\right)$ ise C nin kontrol matrisi $H=\left(-X^t \mid I_{n-k}\right)$ formundadır.

Örnek 2.29 $\mathbb{F}_5$ üzerindeki C lineer kodu, $G=\begin{bmatrix}2&3&0&1&4\\1&2&0&4&3\\2&2&1&1&0\end{bmatrix}$ üreteç matrisiyle verilsin. G matrisinin standart formu aşağıdaki gibi elde edilir.

$$\begin{bmatrix}2&3&0&1&4\\1&2&0&4&3\\2&2&1&1&0\end{bmatrix}\sim\begin{bmatrix}1&2&0&4&3\\2&3&0&1&4\\2&2&1&1&0\end{bmatrix}\underset{H_{31}(-2)}{\overset{H_{21}(-2)}{\sim}}\begin{bmatrix}1&2&0&4&3\\0&4&0&3&3\\0&3&1&3&4\end{bmatrix}\overset{H_3(2)}{\sim}$$

$$\begin{bmatrix}1&2&0&4&3\\0&4&0&3&3\\0&1&2&1&3\end{bmatrix}\underset{H_{23}(1)}{\overset{H_{13}(-2)}{\sim}}\begin{bmatrix}1&0&1&2&2\\0&0&2&4&1\\0&1&2&1&3\end{bmatrix}\overset{H_2(3)}{\sim}\begin{bmatrix}1&0&1&2&2\\0&0&1&2&3\\0&1&2&1&3\end{bmatrix}\underset{H_{32}(-2)}{\overset{H_{12}(-1)}{\sim}}$$

$$\begin{bmatrix}1&0&0&0&4\\0&0&1&2&3\\0&1&0&2&2\end{bmatrix}\overset{H_{12}}{\sim}\left[\underbrace{\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}}_{I_3}\underbrace{\begin{bmatrix}0&4\\2&2\\2&3\end{bmatrix}}_{X}\right]$$

Bu matris G üreteç matrisinin standart formudur. Bu matris yardımıyla,

- $k=3$ ve dolayısıyla $|C|=q^k=5^3=125$ dir.
- $wt(C)=d(C)=2$ dir.
- C, bir $[5,3,2]-$koddur.

Ayrıca C kodunun kontrol matrisi de bulunabilir. Yukarıda verilen teoremden $G=\left[I_k\mid X\right]$ üreteç matrisiyle verilen bir kodun kontrol matrisinin

$H=\left[-X^t\mid I_{n-k}\right]$ formunda olduğu biliniyor. O halde C kodunun kontrol matrisi

$H=\left[-X^t\mid I_{n-k}\right]=\begin{bmatrix}0&3&3&1&0\\1&3&2&0&1\end{bmatrix}$ formundadır.

2.8 Lineer Kodların Denkliği

Bazı kodların üreteç matrisleri standart formda olmayabilir. Ancak kodsözlerin koordinatlarında yapılacak uygun permütasyonlarla bu matris standart forma getirilebilir ve standart haldeki bu matris yeni bir kodun üreteç matrisidir.

Tanım 2.30 [12] $\mathbb{F}_q$ üzerinde verilen iki $(n, M)-$koddan birisi diğerinin aşağıdaki işlemlerden birisine maruz kalmasıyla elde edilebiliyorsa bu iki koda ***denk*** ya da ***permütasyon denk*** kodlar denir.

i) Kodsözlerin n bileşenlerinin permütasyonu.

ii) Sabit bir koordinattaki tüm elemanların sıfırdan farklı sabit bir skalerle çarpılması.

Örnek 2.31

i) Beş uzunluğundaki ikili

$C = \{00000, 10010, 01011, 11101, 11001, 01111, 10110, 00100\}$ kodunun koordinatlarına $\tau = (24153)$ permütasyonu uygulanırsa

$C' = \{00000, 01100, 11010, 10111, 10110, 11011, 01101, 00001\}$ kodu elde edilir. Bu kod C koduna denk olan bir koddur.

ii) $C = \{0000, 0231, 2020, 2211, 2002, 2033, 0022, 0213\}$ dörtlü

kodunun ikinci ve üçüncü koordinatları yer değiştirilip, dördüncü koordinat 3 ile çarpılırsa, $C' = \{0000, 0323, 2200, 2123, 2002, 2301, 0202, 0121\}$ denk kodu bulunur.

Not 2.32 Denk kodların tüm parametreleri aynıdır. Kodlama açısından aralarında hiçbir fark yoktur ancak uygulama esnasında bazı özel durumlar (mesela standart formda üreteç matrisine sahip lineer kodlar) tercih edilebilir.

Teorem 2.33 [12] Herhangi bir lineer C kodu standart formda üreteç matrisine sahip bir C' lineer koduna denktir.

Yukarıdaki teoremden, bir lineer kod için üreteç matrisin standart formda seçilmesi genelliği bozmayacağından genel olarak üreteç matrisin standart formda olduğu düşünülür.

2.9 Kodlama Teorisinde Bazı Sınırlar

n sabit bir sayı olmak üzere $q-$lu bir alfabe üzerinde verilen (n,M,d) kodu için; M sayısı kodun verimliliğinin ölçüsünü ve d sayısı da kodun hata düzeltebilme kapasitesini gösterir. M ve d den her ikisinin de mümkün olduğunca büyük olması bir kod için çok iyi bir özellik olacaktır ancak bu pek mümkün değildir.

Literatürde, verilen q,n ve d parametreleri için M nin alabileceği mümkün en büyük değeri veren bazı alt ve üst sınırlar belirlenmiştir. Bu sınırlardan bazıları, küre paketleme sınırı, Gilbert-Varshamov sınırı, Hamming sınırı, Singleton sınırı ve Plotkin sınırıdır. Tezin bu bölümünde ileride kullanılmak üzere sadece Singleton sınırından bahsedilecektir.

Tanım 2.34 [12] $q>1$ olmak üzere q boyutlu A alfabesi ve verilen n, d parametreleri için $A_q(n,d)$, A üzerinde bir $(n,M,d)-$kod var olacak biçimdeki en büyük M değerini göstersin. Buradan

$A_q(n,d)=\max\{M:\ A \text{ üzerinde bir } (n,M,d)-\text{kod vardır}\}$ dir.

Herhangi bir C, $(n,M,d)-$kodu maksimum boyuta sahipse, yani $M=A_q(n,d)$ ise C koduna ***optimal kod*** denir.

Not 2.35

1. $A_q(n,d)$ sadece A nın boyutuna, n ve d ye bağlıdır. A dan bağımsızdır.
2. $A_q(n,d)$ sayısının hesaplanması kodlama teorisi açısından çok önemlidir. Bu değerin hesaplanabilmesi için çok sayıda çalışma yapılmaktadır. Aslında, $A_q(n,d)$ değerini hesaplama problemi ***Kodlama Teorisinin Temel Problemi*** olarak da bilinir.

2.9.1 Singleton Sınırı

Bu bölümde 1964'de Singleton tarafından belirlenen ve $A_q(n,d)$ için bir üst sınır olan Singleton sınırı verilecektir.

Teorem 2.36 [13] $q>1$ herhangi bir tamsayı, n pozitif bir tamsayı ve d, $1\le d\le n$ olacak biçimdeki bir tamsayı olmak üzere

$$A_q(n,d)\le q^{n-d+1} \tag{2.1}$$

dir. Eğer özel olarak q bir asalın kuvveti ve C kodu da $\mathbb{F}_q$ üzerinde $[n,k,d]$ parametrelerine sahip lineer bir kod ise $k+d\le n+1$ dir.

Tanım 2.37 [12] $[n,k,d]$ parametrelerine sahip lineer bir C kodu için $k+d=n+1$ eşitliği sağlanıyorsa, C koduna ***MDS (Maximum Distance Separable)*** kod denir.

BÖLÜM 3

$\mathbb{Z}_2\mathbb{Z}_{2^s}$ – TOPLAMSAL KODLAR

Tezin bu bölümünde $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodların bir yönden genelleştirmesi olan $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodlar tanımlanacak ve bu kodların cebirsel yapısı incelenecektir. Ayrıca bu bölümdeki bazı teorem ve ispatları, bir sonraki bölümde verilecek olan ve $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodları da kapsayan $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – toplamsal kodların daha kolay anlaşılmasını sağlamak için ayrıntılı olarak verilecektir.

3.1 Sonlu Zincir Halkaları Üzerinde Kodlar

Sonlu halkalar üzerindeki kodlar yıllardır birçok araştırmacının ilgisini çekmiş ve bu konuyla ilgili çok sayıda çalışma yapılmıştır. Bu çalışmalar arasında en fazla dikkat çeken Hammons ve arkadaşlarının 1994 yılında yayımladıkları "The $\mathbb{Z}_4$ – linearity of Kerdock, Preparata, Goethals and related codes" adlı makaledir [2]. Bu makalede Nordstrom-Robinson, Kerdock, Preparata, Goethals ve Delsarte-Goethals gibi lineer olmayan ikili kodların aslında $\mathbb{Z}_4$ üzerindeki bazı önemli lineer kodların Gray görüntüsü oldukları ispatlanmıştır. Daha sonra bu Gray dönüşüm 1998 de Carlet tarafından genişletilerek $\mathbb{Z}_{2^s}$ üzerindeki kodlar için tanımlanmıştır [14].

Gray dönüşümün $\mathbb{Z}_{2^s}$ üzerine genişletilmesiyle beraber $\mathbb{Z}_{2^s}$ üzerindeki lineer kodların ve hatta daha genel olarak $\mathbb{Z}_{p^s}$ üzerindeki lineer kodların yapıları da incelenmiştir [15],[16],[17].

Sonlu halkalar içerisinde bulunan sonlu zincir halkaları üzerindeki kodların kodlama teorisinde özel bir yeri vardır. Çünkü;

- Özellikleri ve yapıları belirlenebilmektedir. Sonlu zincir halkaları tek maksimal ideal içerdiklerinden bu halkaların bölüm halkaları cisimlere izomorf olacaktır. Ayrıca bu halkalar Gray fonksiyonu yardımıyla sonlu cisimlere resmedilebilirler. Yani sonlu zincir halkaları üzerindeki lineer kodlar teorisi sonlu cisimler üzerindeki lineer kodlar teorisiyle benzer özelliktedir.
- $\mathbb{Z}_{p^s}$ ve Galois gibi özel halka aileleri de sonlu zincir halkalarıdır.

Tezin bu bölümünde $\mathbb{Z}_2$ ve $\mathbb{Z}_{2^s}$ sonlu zincir halkasının elemanlarıyla oluşturulan ve $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodların doğal bir genişlemesi olan $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodların yapısı incelenecektir. Bu kodların tanımı verilmeden önce $\mathbb{Z}_{2^s}$ sonlu zincir halkası üzerindeki lineer kodlar ve bunların cebirsel yapılarından kısaca bahsedilecek, sonlu zincir halkası ve Galois halkalarının tanımları verilecektir.

3.2 Sonlu Zincir Halkası ve Galois Halkası

R sonlu ve birimli bir halka olsun. [18]'den;

i) Eğer R halkasının bir I ideali bir tek eleman tarafından üretiliyorsa I ya ***temel(esas) ideal*** denir.

ii) R halkasının bütün idealleri temel ideal ise R ye ***temel ideal halkası*** denir.

iii) Eğer R halkası bir tek maksimal sol (sağ) ideale sahipse R ye ***lokal halka*** denir.

Tanım 3.1 [18] Eğer R halkasının bütün sol (sağ) ideallerinden oluşan kümesi kümelerdeki alt küme olma (kapsama) bağıntısı altında lineer sıralı ise R ye ***sonlu zincir halkası*** denir.

R halkasının maksimal idealinin üretecine γ diyelim. R nin idealleri

$\langle 0\rangle = \langle \gamma^s \rangle \subset \langle \gamma^{s-1} \rangle \subset \cdots \subset \langle \gamma \rangle \subset \langle 1\rangle = R$ formunda olacaktır. Buradaki s pozitif tamsayısı $\langle \gamma^s \rangle = \{0\}$ olacak biçimdeki en küçük sayıdır ve s ye R nin ***nilpotentlik indeksi*** denir. $\mathbb{F} = R/\langle \gamma \rangle$ cismi için eğer $\mathbb{F} \cong \mathbb{F}_q$ ise $|R| = q^s$ dir.

Tanım 3.2 [20] Eğer bir $f(x) \in \mathbb{Z}_{p^s}[x]$ polinomu $\mathbb{Z}_p[x]$ üzerinde indirgenemez bir polinom ise bu $f(x)$ polinomuna ***temel indirgenemez polinom*** denir.

Karakteristiği p^s, boyutu m olan ***Galois halkası*** $GR\left(p^s, m\right)$ ile gösterilir ve $\mathbb{Z}_{p^s}$ halkasının $m.$ dereceden Galois genişlemesidir. Ya da buna denk olarak,

$GR\left(p^s, m\right) = \mathbb{Z}_{p^s}[u] \Big/ \langle h(u) \rangle$ dır. Burada, $h(u)$ polinomu $\mathbb{Z}_{p^s}[u]$ üzerinde m dereceli monik temel indirgenemez polinomdur.

Galois halkası tanımında eğer;

- $s = 1$ ise $GR(p, m) = GF(p^m)$ ve
- $m = 1$ ise $GR(p^s, 1) = \mathbb{Z}_{p^s}$ biçiminde olacaktır.

Yani $\mathbb{Z}_{p^s}$ sonlu zincir halkası Galois halkasının özel bir halidir.

Sonlu zincir halkalarına örnek olarak, $\mathbb{Z}_{p^s}$ halkası, $GR(p^s, m)$ Galois halkası, p asal bir sayı ve $s \geq 2$, $m, s \in \mathbb{Z}^+$ ve $u^s = 0$ olmak üzere $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{s-1}\mathbb{F}_{p^m}$ halkası verilebilir.

Not 3.3

1. $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{s-1}\mathbb{F}_{p^m}$ halkası $\mathbb{F}_{p^m}[u] \Big/ \langle u^s \rangle$ ye izomorftur ve karakteristiği p, nilpotentlik indeksi s olan tek sonlu zincir halkasıdır.
2. Her sonlu zincir halkasının değişmeli olması gerekmez. Değişmeli olmayan en küçük sonlu zincir halkası 16 mertebelidir ve $R = GF(4) \oplus GF(4)$ biçiminde ifade edilebilir [19]. Burada toplama ve çarpma işlemleri

$$\left(a_1, b_1\right) + \left(a_2, b_2\right) = \left(a_1 + a_2, b_1 + b_2\right)$$

$$\left(a_1, b_1\right)\left(a_2, b_2\right) = \left(a_1 a_2, a_1 b_2 + b_1 a_2^2\right)$$

biçiminde tanımlanmışlardır. Ayrıca $GF(4)=\mathbb{Z}_2[x]/\langle x^2+x+1\rangle=\{0,1,\beta,\delta\}$, $\delta=\beta+1$ ve β, (x^2+x+1) in kökü olmak üzere dört elemanlı $GF(4)$ Galois cisminin elemanları için toplama ve çarpma tabloları aşağıdaki gibidir.

Çizelge 3.1 $GF(4)$ Galois cisminin elemanları için toplama ve çarpma tablosu

$+$	0	1	β	δ
0	0	1	β	δ
1	1	0	δ	β
β	β	δ	0	1
δ	β	δ	1	0

$\times$	0	1	β	δ
0	0	0	0	0
1	0	1	β	δ
β	0	β	δ	1
δ	0	δ	1	β

Önerme 3.4 [18] R sonlu değişmeli bir halka olsun. Bu durumda aşağıdaki ifadeler denktirler.

i) R bir lokal halkadır ve R nin M maksimal ideali temel idealdir.

ii) R lokal temel ideal halkasıdır.

iii) R zincir halkasıdır.

3.3 Bir Modül Olarak R^n

Genel olarak R halkası üzerindeki n uzunluğundaki lineer bir kod, R^n nin bir $R-$alt modülü olarak tanımlanır. Bu bölümde modül ve alt modül tanımları verilecektir.

Tanım 3.5 [21] R birimli ve değişmeli bir halka ve $(M,+)$ değişmeli bir grup olsun. Eğer $R\times M\to M$ işlemi aşağıdaki koşulları sağlıyor ise M ye R üzerinde ***modül*** ya da $R-$***modül*** denir. Her $r,s\in R$ ve $x,y\in M$ için;

i) $r(x+y)=rx+ry$

ii) $(r+s)x=rx+sx$

iii) $(rs)x=r(sx)$

iv) $1_R x = x$.

Burada M modülü üzerindeki işleme skaler çarpma işlemi denir.

Tanım 3.6 [21] R bir halka ve M, $R-$modül olsun. M nin boştan farklı bir N alt kümesi de bir $R-$modül ise, N ye M nin ***alt modülü*** veya $R-$***alt modülü*** denir.

Örnek 3.7

i) Bir R cismi üzerindeki M vektör uzayı $R-$modüldür.

ii) Herhangi bir halka kendi üzerinde modüldür.

iii) R bir halka olmak üzere, R^n elemanları R den olan bütün $n-$lilerin kümesi olsun. R^n kümesi bilinen toplama ve skalerle çarpma işlemi altında bir $R-$modüldür.

iv) Her değişmeli grup bir $\mathbb{Z}-$modüldür.

3.4 $\mathbb{Z}_{2^s}$ Halkası Üzerinde Lineer Kodlar

$\mathbb{Z}_{2^s}$, modülo 2^s ye göre tamsayıların kümesi olmak üzere [22]'den;

i) $\mathbb{Z}_{2^s}^n$ nin bir C alt kümesine $\mathbb{Z}_{2^s}$ üzerinde n uzunluklu kod denir. Eğer C kodu $\mathbb{Z}_{2^s}$ nin bir alt modülü ise C ye lineer kod denir.

ii) Eğer C, $\mathbb{Z}_{2^s}$ üzerinde bir kod ise $\langle C \rangle$, $\mathbb{Z}_{2^s}$ üzerinde C nin elemanlarının gerdiği bir koddur.

iii) $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}_{2^s}^n$ vektörleri için standart iç çarpım $\langle u, v \rangle_{2^s} = \sum_{i=1}^{n} u_i v_i \pmod{2^s}$ biçiminde tanımlanır. Bu iç çarpım yardımıyla C nin ortogonal tümleyeni $C^{\perp} = \{u \mid \langle u, v \rangle_{2^s} = 0,\ \forall v \in C\}$ şeklinde tanımlanır. Ayrıca eğer C kodu lineer değilse $C^{\perp} = \langle C \rangle^{\perp}$ dir.

iv) $\mathbb{Z}_{2^s}$ üzerinde Lee ağırlığı, $wt_L : \mathbb{Z}_{2^s} \to \mathbb{Z}_{2^s}$, $wt_L(i) = \min\{i, 2^s - i\}$ biçiminde tanımlanır. C kodunun minimum Lee ağırlığı $d_L(C)$ ile gösterilir.

Örneğin, $s=2$ alınırsa $\mathbb{Z}_4$ halkası üzerindeki kodlar elde edilir. $\mathbb{Z}_4$ üzerindeki kodlar için Lee ağırlığı,

$x=(x_1,x_2,\ldots,x_n)\in\mathbb{Z}_4^n$ için $wt_L(x)=\sum_{i=1}^{n} wt_L(x_i)$ şeklinde tanımlanır. Buradaki $x_i\in\mathbb{Z}_4$ elemanlarının Lee ağırlıkları da; $wt_L(0)=0, wt_L(1)=1, wt_L(2)=2$ ve $wt_L(3)=1$ biçimindedir [23].

3.4.1 Gray Dönüşümü

$\mathbb{Z}_4$ halkası üzerindeki kodlar özel bir dönüşüm altında ikili kodlara dönüştürülebilir. Bu dönüşüme Gray dönüşümü denir ve $\phi:\mathbb{Z}_4\to\mathbb{Z}_2^2$ olmak üzere, $\phi(0)=(00),\phi(1)=(01),\phi(2)=(11)$ ve $\phi(3)=(10)$ biçiminde tanımlanır [2].

1998 yılında Carlet bu Gray dönüşümü $\mathbb{Z}_{2^s}$ üzerinde aşağıdaki gibi genelleştirmiştir [14].

$$\phi:\mathbb{Z}_{2^s}\to\mathbb{Z}_2^{2^{s-1}},\ \phi(i)=\begin{cases}0_{2^{s-1}-i}1_i, & 0\le i\le 2^{s-1}\\ 1_{2^{s-1}}+\phi(i-2^{s-1}), & i>2^{s-1}\end{cases} \tag{3.1}$$

Burada 0_i, bütün bileşenleri 0 olan i uzunluklu vektörü ve 1_i de bütün bileşenleri 1 olan i uzunluklu vektörü göstermektedir. Bu Gray dönüşüm bir izometridir ve $\mathbb{Z}_{2^s}$ üzerindeki Lee uzaklığını $n=2^{s-1}$ olmak üzere $\mathbb{Z}_2^n$ üzerindeki Hamming uzaklıklarına dönüştürür. Gray dönüşümünü daha iyi anlamak için, bir örnek üzerinde $\mathbb{Z}_8$ in elemanlarının $\mathbb{Z}_2$ ye nasıl resmedildiğini inceleyelim.

$\phi : \mathbb{Z}_8 \to \mathbb{Z}_2^4$

$0 \to (0000)$

$1 \to (0001)$

$2 \to (0011)$

$3 \to (0111)$

$4 \to (1111)$

$5 \to (1110)$

$6 \to (1100)$

$7 \to (1000)$

şeklindedir.

3.4.2 $R = \mathbb{Z}_{p^s}$ Halkası Üzerindeki Lineer Kodların Üreteç ve Kontrol Matrisleri

Cisimler birer vektör uzayı olduklarından, cisimler üzerindeki lineer kodlar birer baza sahiptirler. Ancak bir sonlu zincir halkası üzerindeki lineer kod için bazdan söz edilemez. Bunun yerine en küçük üreteç kümesinden bahsedilebilir. Bu üreteç kümesine kodun üreteç matrisi gözüyle de bakılabilir. $\mathbb{Z}_{p^s}$ üzerindeki n uzunluğundaki bir C kodunun üreteç matrisi aşağıda standart formla verilen üreteç matrise permütasyon denktir [16].

$$G = \begin{bmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,s} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \cdots & \cdots & pA_{1,s} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \cdots & \cdots & p^2 A_{2,s} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & p^{s-1} I_{k_{s-1}} & p^{s-1} A_{s-1,s} \end{bmatrix}. \tag{3.2}$$

Bu matriste özel olarak $p = 2$ yazılarak $\mathbb{Z}_{2^s}$ üzerindeki lineer bir kodun üreteç matrisinin standart formu elde edilir. Böylece G matrisi yardımıyla, C kodu için $\{k_0, k_1, \ldots, k_{s-1}\}$ tipindedir ve $\prod_{i=0}^{s-1} \left(p^{s-i}\right)^{k_i}$ kodsöze sahiptir denir.

- $i > 0$ için eğer $k_i = 0$ ise C koduna ***serbest kod*** denir.

- Eğer C, $\mathbb{Z}_4$ üzerinde $\{k_0, k_1\}$ tipinde bir kod ise C ye $2^{k_1}4^{k_0}$ tipinden dörtlü kod denir.

Örneğin $\mathbb{Z}_4$ üzerindeki bir C kodu için standart haldeki üreteç matrisi

$G = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} \\ 0 & 2I_{k_1} & 2A_{12} \end{bmatrix}$ formundadır.

Tanım 3.8 [22] $\mathbb{Z}_{2^s}$ zincir halkası üzerinde eğer $\sum_{i=1}^{k} \alpha_i v_i = 0$ iken her i için $\alpha_i \in \langle 2 \rangle$ oluyorsa $\{v_1, v_2, \ldots, v_k\}$ vektör kümesine ***modüler bağımsız küme*** denir. Burada $\langle 2 \rangle$, $\mathbb{Z}_{2^s}$ nin 2 tarafından üretilen maksimal idealidir.

$\mathbb{Z}_{2^s}$ üzerindeki kodlar için modüler bağımsız üreteç kümesi en küçük üreteç kümesidir [24]. Böylece standart formda verilen üreteç matrisindeki satırlar modüler bağımsızdırlar.

Not 3.9 $\mathbb{Z}_m$ üzerindeki kodlar için eğer m bir asalın kuvveti biçiminde değilse durum farklıdır. $\mathbb{Z}_{2^s}$ bir zincir halkası olduğundan standart formda bir üreteç matrise sahiptir ve modüler bağımsızlık bu üreteç matrisin en küçük üreteç küme olmasını garanti altına alır. Diğer taraftan m bir asalın kuvveti değilken $\mathbb{Z}_m$ bir zincir halkası değildir ve modüler bağımsızlık en küçük üreteç küme olmasını garanti etmeye yeterli değildir. Böylece üreteç matrisin standart formu mevcut değildir [24].

- Modüler bağımsız vektörlerin Gray dönüşümü altındaki görüntülerinin lineer bağımsız olması gerekmez. Yani Gray dönüşümü her zaman lineer bir uzay vermez. Örneğin, $\mathbb{Z}_4$ üzerindeki modüler bağımsız $(1,1,2,2), (1,0,1,3)$ ve $(0,1,3,1)$ vektörlerini düşünelim. Bu vektörlerin Gray dönüşümü altındaki görüntüleri olan $(0,1,0,1,1,1,1,1), (0,1,0,0,0,1,1,0)$ ve $(0,0,0,1,1,0,0,1)$ vektörleri lineer bağımsız değildirler.

Önerme 3.10 [15] $\mathbb{Z}_{p^s}$ üzerindeki herhangi bir C lineer kodu (3.2) ile verilen standart forma getirilebilir.

İspat: Bir C kodu için üreteçlerin kümesi rastgele verilmiş olsun. Bu küme içerisinden birbirlerinin lineer kombinasyonu şeklinde yazılabilenleri ayırt ederek C kodu için G üreteç matrisi yazılabilir. Son olarak G matrisi, satır ve sütun işlemleri yapılarak standart forma getirilebilir. ■

Tanım 3.11 [15] R, nilpotentlik indeksi ν ve maksimal ideali γ olan sonlu zincir halkası olsun. C, R üzerindeki herhangi bir kod ve $r \in R$ için $(C:r)=\{e \in R^n \mid re \in C\}$ kümesi C nin bölüm alt modülünü göstersin. C ye $C=(C:\gamma^0)\subseteq\cdots\subseteq(C:\gamma^i)\subseteq\cdots(C:\gamma^{\nu-1})$ kod zinciri ve C nin $\mathbb{F}=R/\langle\gamma\rangle$ cismi üzerine izdüşümü olan $\bar{C}$ ye de $\bar{C}=(\overline{C:\gamma^0})\subseteq\cdots\subseteq(\overline{C:\gamma^i})\subseteq\cdots(\overline{C:\gamma^{\nu-1}})$ kod zinciri karşılık gelir.

Tanım 3.12 [15] C, $\mathbb{Z}_{p^s}$ üzerinde lineer bir kod olsun. C nin standart formdaki üreteç matrisinin satır sayısı $k(C)$ ile gösterilsin. Ayrıca $i=0,1,\ldots,s-1$ için $k_i(C)$, G üreteç matrisinde p^i ile bölünüp p^{i+1} ile bölünemeyen satırların sayısını göstersin. (Buna denk olarak $k_0(C)=\dim(\bar{C})$ ve $k_i(C)=\dim\left((\overline{C:p^i})\right)-\dim\left((\overline{C:p^{i-1}})\right)$, $1\le i\le s-1$ biçiminde tanımlanabilir.) Böylece, $k(C)=\sum_{i=0}^{s-1}k_i(C)$ dir.

Sonuç 3.13 [15] C ve D, $\mathbb{Z}_{p^s}$ üzerinde n uzunluğundaki lineer kodlar olsunlar. Bu durumda eğer $C\subseteq D$ ve $i=0,1,\ldots,s-1$ için $k_i(C)=k_i(D)$ ise $C=D$ dir.

Teorem 3.14 [15] $\mathbb{Z}_{p^s}$ üzerindeki C lineer kodu standart formdaki (3.2) üreteç matrisiyle verilsin. Buradan,

i) $0\le i<j<s$ için $B_{i,j}=-\sum_{k=i+1}^{j-1}B_{i,k}A^t_{s-j,s-k}-A^t_{s-j,s-i}$ olmak üzere,

$$H=\begin{bmatrix} B_{0,s} & \cdots & \cdots & B_{0,3} & B_{0,2} & B_{0,1} & I_{n-k(C)} \\ pB_{1,s} & \cdots & \cdots & pB_{1,3} & pB_{1,2} & pI_{k_{s-1}(C)} & 0 \\ p^2B_{2,s} & \cdots & \cdots & p^2B_{2,3} & p^2I_{k_{s-2}(C)} & 0 & 0 \\ \vdots & \iddots & & \iddots & 0 & \vdots & \vdots \\ \vdots & & \iddots & \iddots & \vdots & \vdots & \vdots \\ p^{s-1}B_{s-1,s} & p^{s-1}I_{k_1(C)} & 0 & \cdots & 0 & 0 & 0 \end{bmatrix} \tag{3.3}$$

matrisi $C^{\perp}$ dual kodunun üreteç matrisi ve C kodunun kontrol matrisidir.

ii) $i=0,1,\ldots,s-1$ için $\left(\overline{C^{\perp}:p^i}\right)=\left(\overline{C:p^{s-i-1}}\right)^{\perp}$ ve $i=1,\ldots,s-1$ için

$k_0(C^{\perp})=n-k(C)$ ve $k_i(C^{\perp})=k_{s-i}(C)$ dir.

İspat:

i) Doğrudan $HG^t=0$ olduğu gösterilebilir. Şimdi, D, H tarafından üretilen $\mathbb{Z}_{p^s}-$modül olsun. Böylece, $k_0(D)=n-k(C)$, $i=1,\ldots,s-1$ için $k_i(D)=k_{s-1}(C)$ ve D, C ye dik olacağından $D\subseteq C^{\perp}$ dir. $C^{\perp}\subseteq D$ olduğu Sonuç 3.13 ve ii) den $i=0,1,\ldots,s-1$ için $k_i(C^{\perp})=k_i(D)$ olduğu ispatlanarak gösterilebilir. Sonuç olarak, $D=C^{\perp}$ dir.

ii) Öncelikle $\left(\overline{C^{\perp}:p^i}\right)\perp\left(\overline{C:p^{s-i-1}}\right)$ olduğunu gösterelim. $b\in\left(C^{\perp}:p^i\right)$ ve $e\in\left(C:p^{s-i-1}\right)$ olsun. Böylece, $p^ib\in C^{\perp}$ ve $p^{s-i-1}e\in C$ olur. Buradan da $p^{s-1}be^t=0$ yani $\bar{b}\bar{e}^t=0$ elde edilir.

Vektör uzayları için birbirine dik iki alt uzayın boyutları toplamı tüm uzayın boyutunu geçemez. $D\subseteq C^{\perp}$ olduğundan her i için $\left(\overline{D:p^i}\right)\subseteq\left(\overline{C^{\perp}:p^i}\right)$ dir. Buradan da

$$\begin{aligned} n &\geq \dim\left(\left(\overline{C:p^{s-i-1}}\right)\right)+\dim\left(\left(\overline{C^{\perp}:p^i}\right)\right) \\ &\geq \dim\left(\left(\overline{C:p^{s-i-1}}\right)\right)+\dim\left(\left(\overline{D:p^i}\right)\right) \\ &= k_0(C)+\cdots+k_{s-i-1}(C)+k_0(D)+\cdots+k_i(D) \\ &= k_0(C)+\cdots+k_{s-i-1}(C)+n-k(C)+k_{s-i}(C)+\cdots+k_{s-1}(C)=n \end{aligned}$$

elde edilir. Böylece, $\dim\left(\left(\overline{C^{\perp}:p^{i}}\right)\right)=\dim\left(\overline{D:p^{i}}\right)=n-\dim\left(\left(\overline{C:p^{s-i-1}}\right)\right)$ ve buradan da

$i=0,\ldots,s-1$ için $\left(\overline{C^{\perp}:p^{i}}\right)=\left(\overline{C:p^{s-i-1}}\right)^{\perp}$ ve $k_i(C^{\perp})=k_i(D)$ bulunur. ■

Örnek 3.15 Yukarıda verilen teoremlere dayanılarak $\mathbb{Z}_8$ üzerindeki bir C lineer kodunun standart haldeki üreteç ve kontrol matrisleri aşağıdaki gibi yazılabilir.

$$G=\begin{bmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} \\ 0 & 2I_{k_1} & 2A_{12} & 2A_{13} \\ 0 & 0 & 4I_{k_2} & 4A_{23} \end{bmatrix} \text{ ve}$$

$$H=\begin{bmatrix} -A_{03}^t+A_{13}^tA_{01}^t+A_{23}^tA_{02}^t-A_{23}^tA_{12}^tA_{01}^t & -A_{13}^t+A_{23}^tA_{12}^t & -A_{23}^t & I_{n-k_0-k_1-k_2} \\ -2A_{02}^t+2A_{12}^tA_{01}^t & -2A_{12}^t & 2I_{k_2} & 0 \\ -4A_{01}^t & 4I_{k_1} & 0 & 0 \end{bmatrix}.$$

3.5 $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – Toplamsal Kodlar

Birleşim şemasının ikili Hamming şeması olduğu durumda toplamsal kodların $\mathbb{Z}_2^{\alpha}\times\mathbb{Z}_4^{\beta}$ nın alt gruplarına karşılık geldiği bilinmektedir [5]. Borges ve arkadaşları 2010 yılında yayımlanan [6] makalesinde $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodları tanımladılar ve bu kodların cebirsel yapısını incelediler. $\mathbb{Z}_2^{\alpha}\times\mathbb{Z}_4^{\beta}$ nın bir C alt grubuna $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kod denir ve $(\alpha,\beta;\gamma,\delta;\kappa)$ tipindeki bir C, $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodunun standart formdaki üreteç ve kontrol matrisleri aşağıdaki gibi verilir [6].

$$G=\begin{bmatrix} I_{\kappa} & T_b & 2T_2 & 0 & 0 \\ 0 & 0 & 2T_1 & 2I_{\gamma-\kappa} & 0 \\ 0 & S_b & S_q & R & I_{\delta} \end{bmatrix} \text{ ve} \qquad (3.4)$$

$$H=\begin{bmatrix} T_b^t & I_{\alpha-\kappa} & 0 & 0 & 2S_b^t \\ 0 & 0 & 0 & 2I_{\gamma-\kappa} & 2R^t \\ T_2^t & 0 & I_{\beta+\kappa-\gamma-\delta} & T_1^t & -\left(S_q+RT_1\right)^t \end{bmatrix}. \qquad (3.5)$$

Bu matrislerdeki T_1, T_2, T_b, S_b ve R bileşenleri $\mathbb{Z}_2$ nin elemanlarından oluşan matrisler ve S_q ise bileşenleri $\mathbb{Z}_4$ ün elemanlarından oluşan bir matristir.

Tezin bu bölümünde $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodların bir yönden genelleştirilmesi olan $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodlar tanımlanıp bu kodlar için standart formdaki üreteç ve kontrol matrisleri belirlenecektir. Ayrıca $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodlar için iki tane sınır belirlenip bu sınırları sağlayan örnekler verilecektir.

Tanım 3.16 s, 1 den büyük bir tamsayı olsun. $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ grubunun bir C alt grubuna $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – ***toplamsal kod*** denir.

C toplamsal kodu $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ nın bir alt grubu olduğundan sonlu değişmeli grupların temel teoreminden $\mathbb{Z}_2^{k_0} \times \mathbb{Z}_{2^s}^{k_1} \times \mathbb{Z}_{2^{s-1}}^{k_2} \times \cdots \times \mathbb{Z}_4^{k_{s-1}} \times \mathbb{Z}_2^{k_s}$ gibi değişmeli bir gruba izomorftur. Buradan,

- C toplamsal kodunun $|C| = 2^{k_0} 2^{sk_1} 2^{(s-1)k_2} \ldots 2^{k_s}$ tane kodsözü vardır.

X, $\mathbb{Z}_2$ nin koordinatlarının kümesini ve Y de $\mathbb{Z}_{2^s}$ nin koordinatlarının kümesini göstersin. Buradan $|X| = \alpha$ ve $|Y| = \beta$ dır. Bütün bu parametreler düşünülerek C, $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal koduna $(\alpha, \beta; k_0; k_1, k_2, \ldots, k_{s-1}, k_s)$ tipindedir denir.

Örnek 3.17 C bir $\mathbb{Z}_2\mathbb{Z}_8$ – toplamsal kod olsun ve C nin üreteç matrisi

$$G = \left[\begin{array}{cc|cccc} \boxed{1} & 0 & 0 & 0 & 0 & 4 \\ \hline 0 & 1 & \boxed{1} & 1 & 0 & 7 \\ 0 & 1 & 0 & \boxed{2} & 2 & 3 \\ 0 & 0 & 0 & 0 & \boxed{4} & 4 \end{array}\right] \text{ ile verilsin.}$$

- C nin mertebesi $2^1 8^1 4^1 2^1$ dir. Böylece, $k_0 = k_1 = k_2 = k_3 = 1$ dir.
- $X = \{1, 2\}$ ve $Y = \{1, 2, 3, 4\}$ olarak verildiğinden $\alpha = 2$ ve $\beta = 4$ tür.
- C, $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodu $(2, 4; 1; 1, 1, 1)$ tipindedir.

Tanım 3.18 $x = (x_1, x_2, ..., x_{\alpha}) \in \mathbb{Z}_2^{\alpha}$ ve $y = (y_1, y_2, ..., y_{\beta}) \in \mathbb{Z}_{2^s}^{\beta}$ için,

$$\Phi : \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta} \to \mathbb{Z}_2^n$$

$$\Phi(x, y) = \left(x_1, x_2, ..., x_{\alpha}, \phi(y_1), \phi(y_2), ..., \phi(y_{\beta})\right)$$

dönüşümü tanımlansın. Bu dönüşüm altında bir C, $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodunun $\Phi(C) = \mathrm{C}$ ikili görüntüsüne $n = \alpha + 2^{s-1}\beta$ uzunluğunda $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – ***lineer kod*** denir. Burada, $\phi : \mathbb{Z}_{2^s} \to \mathbb{Z}_2^{2^{s-1}}$ dönüşümü (3.1) de tanımlanan Gray dönüşümün genel halidir.

3.6 $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – Toplamsal Kodların Üreteç Matrisleri

Teorem 3.19 C, $(\alpha, \beta; k_0; k_1, k_2, ..., k_s)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kod olsun. C kodu standart formdaki üreteç matrisi aşağıdaki gibi olan $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal koda permütasyon denktir.

$$G_s = \begin{bmatrix} \bar{A} & T \\ S & A \end{bmatrix} \tag{3.6}$$

Burada,

$$\bar{A} = \begin{bmatrix} I_{k_0} & \bar{A}_{01} \end{bmatrix}, T = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 2^{s-1}T_{0,s} \end{bmatrix}, S = \begin{bmatrix} 0 & S_1 \\ 0 & S_2 \\ \vdots & \vdots \\ 0 & S_{s-1} \\ 0 & 0 \end{bmatrix},$$

$$A = \begin{bmatrix} I_{k_1} & A_{01} & A_{02} & A_{03} & \cdots & A_{0,s-2} & A_{0,s-1} & A_{0,s} \\ 0 & 2I_{k_2} & 2A_{12} & 2A_{13} & \cdots & 2A_{1,s-2} & 2A_{1,s-1} & 2A_{1,s} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2^{s-2}I_{k_{s-1}} & 2^{s-2}A_{s-2,s-1} & 2^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 2^{s-1}I_{k_s} & 2^{s-1}A_{s-1,s} \end{bmatrix}$$

biçimindedir. $\bar{A}_{01}$, bileşenleri $\mathbb{Z}_2$ nin elemanlarından oluşan matris ve $0 \le k < l \le s$ için A_{kl} matrisleri ise $\mathbb{Z}_{2^s}$ nin elemanlarından oluşan matrislerdir. Ayrıca, I_{k_m} matrisleri $0 \le m \in \mathbb{Z}$ için $k_m \times k_m$ boyutlu birim matrislerdir. $1 \le i \le s-1$ olmak üzere S_i ler $\mathbb{Z}_2$ bileşenli matrisler ve $T_{0,s}$ de $\mathbb{Z}_{2^s}$ bileşenli matristir.

İspat: Bu teoremin ispatı 4 adımda yapılacaktır.

1. Adım: İlk α koordinattaki en az bir bileşen sıfırdan farklı olmak üzere, C_1, C kodunun 2 mertebeli elemanlarından oluşsun. $C_0 = C \setminus C_1$ diyelim. Buradan $C = C_0 \cup C_1$ ve $C_0 \cap C_1 = \varnothing$ olduğu açıktır. C_1, k_0 mertebeli alt grup ise gerekli permütasyonların ardından C nin üreteç matrisi,

$\begin{bmatrix} I_{k_0} & \bar{A}_{01} & 2^{s-1}D \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \end{bmatrix}$ formunda olacaktır. Buradaki $\bar{A}_{01}$ matrisi $\mathbb{Z}_2$ bileşenli ve D matrisi de $\mathbb{Z}_{2^s}$ bileşenli matrislerdir.

2. Adım: C_0 kodunu oluşturan ilk k_0 elemanın sıfır olduğunu farz edelim. Gerekli işlemlerin uygulanmasının ardından üreteç matrisi, $\begin{bmatrix} I_{k_0} & \bar{A}_{01} & 2^{s-1}D \\ 0 & \vdots & \vdots \\ 0 & \vdots & \vdots \end{bmatrix}$ biçiminde olacaktır.

3. Adım: C_0 ın son β elemanlarından oluşan $\mathbb{Z}_{2^s}$ nin alt grubuna C_0^R diyelim. C_0^R, $\mathbb{Z}_{2^s}$ nin bir alt grubu olduğundan (3.2) matrisinde $p = 2$ yazılırsa, C_0^R yi üreten matris aşağıdaki formda olacaktır.

$$A = \begin{bmatrix} I_{k_1} & A_{01} & A_{02} & A_{03} & \cdots & A_{0,s-2} & A_{0,s-1} & A_{0,s} \\ 0 & 2I_{k_2} & 2A_{12} & 2A_{13} & \cdots & 2A_{1,s-2} & 2A_{1,s-1} & 2A_{1,s} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2^{s-2}I_{k_{s-1}} & 2^{s-2}A_{s-2,s-1} & 2^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 2^{s-1}I_{k_s} & 2^{s-1}A_{s-1,s} \end{bmatrix}$$ Buradan C kodunun üreteç matrisi

$\begin{bmatrix} I_{k_0} & \bar{A}_{01} & 2^{s-1}D_1 & \cdots & 2^{s-1}D_s \\ 0 & S_1 & & & \\ \vdots & \vdots & & A & \\ 0 & S_{s-1} & & & \\ 0 & 0 & & & \end{bmatrix}$ formuna gelir.

4. Adım: $\left[2^{s-1}D_1 \quad \cdots \quad 2^{s-1}D_s \right]$ matrisine G_0 diyelim. Gerekli satır işlemleri yardımıyla G_0 ın ilk k_1 bileşeni olan $2^{s-1}D_1$ alt matrisi sıfır yapılabilir. Benzer biçimde, $2^{s-1}D_2,\ldots,2^{s-1}D_{s-1}$ alt matrisleri de sıfır yapılabilir. Böylece C kodunun standart haldeki üreteç matrisi elde edilir. Buradaki $S_1, S_2,\ldots,S_{s-1}$ matrisleri $\mathbb{Z}_2$ bileşenli matrislerdir. ■

Sonuç 3.20 C, $(\alpha,\beta;k_0;k_1,k_2)$ tipindeki $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodu olsun. Bu durumda C nin üreteç matrisi,

$$G=\begin{bmatrix} I_{k_0} & \bar{A}_{01} & 0 & 0 & 2T_{02} \\ 0 & S_1 & I_{k_1} & A_{01} & A_{02} \\ 0 & 0 & 0 & 2I_{k_2} & 2A_{12} \end{bmatrix} \tag{3.7}$$

formundadır. Bu matris (3.4) formundaki üreteç matrise permütasyon denktir.

Örnek 3.21 C, $(\alpha,\beta;k_0;k_1,k_2,k_3)$ tipindeki $\mathbb{Z}_2\mathbb{Z}_8-$toplamsal kodunu alalım. Bu durumda $s=3$ tür. Teorem 3.19 yardımıyla, C kodunun standart haldeki üreteç matrisi

$$G=\begin{bmatrix} I_{k_0} & \bar{A}_{01} & 0 & 0 & 0 & 4T_{03} \\ 0 & S_1 & I_{k_1} & A_{01} & A_{02} & A_{03} \\ 0 & S_2 & 0 & 2I_{k_2} & 2A_{12} & 2A_{13} \\ 0 & 0 & 0 & 0 & 4I_{k_3} & 4A_{23} \end{bmatrix} \tag{3.8}$$

formunda olacaktır.

Örnek 3.22 $(3,3;1;3,0,0)$ tipinde ve $\begin{bmatrix} 1 & 1 & 0 & 2 & 4 & 6 \\ 0 & 1 & 1 & 0 & 4 & 5 \\ 0 & 0 & 1 & 1 & 3 & 7 \\ 1 & 0 & 1 & 0 & 5 & 4 \end{bmatrix}$ üreteç matrisiyle verilen $\mathbb{Z}_2\mathbb{Z}_8-$toplamsal kodunun üreteç matrisinin standart formu $G=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ biçimindedir.

3.7 $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – Toplamsal Kodların Dual Uzayı

Sonlu cisimler ve halkalar üzerindeki lineer kodlar için bilinen standart iç çarpımla beraber ortogonallik kolayca tanımlanabilir. Bununla beraber, $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodlar için ortogonallik kavramı farklı bir şekilde verilmiştir [6]. Bu bölümde $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodlar için verilen ortogonallik kavramı $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodlar üzerine genelleştirilip bu kodlar üzerindeki dualite incelenecektir.

Tanım 3.23 Herhangi iki $u, v \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ elemanı için iç çarpım

$$\langle , \rangle : \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta} \to \mathbb{Z}_{2^s}$$

$$\langle u, v \rangle = 2^{s-1}\left(\sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j$$

biçiminde tanımlanır.

Tanım 3.24 C bir $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kod olsun. C nin toplamsal duali, $C^{\perp}$ sembolüyle gösterilir ve

$$C^{\perp} = \left\{ v \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta} \mid \langle u, v \rangle = 0 \, , \forall u \in C \right\}$$

biçiminde tanımlanır. $C^{\perp}$ toplamsal dual kodunun $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ nın bir alt grubu olduğu kolayca görülebilir. Dolayısıyla $C^{\perp}$ de bir $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal koddur.

Tanım 3.25 Şimdi bir C, $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodunun dualinin yapısını incelemede yardımcı olacak bazı dönüşümler tanımlanacaktır.

$$\psi : \mathbb{Z}_{2^s} \to \mathbb{Z}_2$$

bilinen modülo 2 dönüşümü $\forall x \in \mathbb{Z}_{2^s}$ ve $0 \le k \in \mathbb{Z}$ için $\psi(x) = \begin{cases} 0, & x = 2k \\ 1, & x = 2k+1 \end{cases}$ şeklinde tanımlansın.

$$\iota : \mathbb{Z}_2 \to \mathbb{Z}_{2^s}$$

dönüşümü $\iota(0) = 0$ ve $\iota(1) = 1$ şeklinde tanımlı özdeşlik dönüşümü olsun. Son olarak,

$$\chi : \mathbb{Z}_2 \to \mathbb{Z}_{2^s}$$

dönüşümü $\chi(0)=0$ ve $\chi(1)=2^{s-1}$ biçiminde tanımlansın. Bu dönüşümlerin genelleştirilmiş halleri de aynı sembollerle gösterilirse,

$(\psi, I_d): \mathbb{Z}_{2^s}^{\alpha} \times \mathbb{Z}_{2^s}^{\beta} \to \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$, $(\iota, I_d): \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta} \to \mathbb{Z}_{2^s}^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$, $(\chi, I_d): \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta} \to \mathbb{Z}_{2^s}^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ yazılabilir.

Bu dönüşümler kullanılarak aşağıdaki önermeler verilecektir. Bu önermeler yardımıyla bir C, $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodunun kontrol matrisi belirlenecektir.

Önerme 3.26 $u \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ ve $v \in \mathbb{Z}_{2^s}^{\alpha+\beta}$ olmak üzere $\langle \chi(u), v \rangle_{2^s} = \langle u, \psi(v) \rangle$ dir. Burada $\langle , \rangle_{2^s}$, $\mathbb{Z}_{2^s}$ üzerindeki standart iç çarpımı göstermektedir.

İspat: $u \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ ve $v \in \mathbb{Z}_{2^s}^{\alpha+\beta}$ olsun.

$$\langle \chi(u), v \rangle_{2^s} = \sum_{i=1}^{\alpha} (2^{s-1}u_i)v_i + \sum_{j=i+1}^{\alpha+\beta} u_j v_j = \sum_{i=1}^{\alpha} (2^{s-1}u_i)(v_i \bmod 2) + \sum_{j=i+1}^{\alpha+\beta} u_j v_j = \langle u, \psi(v) \rangle. \blacksquare$$

Sonuç 3.27 Eğer $u, v \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta}$ ise $\langle \chi(u), \iota(v) \rangle_{2^s} = \langle u, v \rangle$ dir.

İspat: Önerme 3.26 yardımıyla, $\langle \chi(u), \iota(v) \rangle_{2^s} = \langle u, \psi(\iota(v)) \rangle = \langle u, v \rangle$ elde edilir. $\blacksquare$

Önerme 3.28 C, $(\alpha, \beta; k_0; k_1, \ldots, k_s)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kod olsun. Bu durumda $C^{\perp} = \psi\left(\chi(C)^{\perp}\right)$ dir.

İspat: $v \in C^{\perp}$ alalım. Buradan $\forall u \in C$ için $\langle u, v \rangle = 0$ olacaktır. Sonuç 3.27 kullanılırsa, $\langle u, v \rangle = \langle \chi(u), \iota(v) \rangle_{2^s}$ yazılabilir. Böylece, $\psi(\iota(v)) = v \in \psi\left(\chi(C^{\perp})\right)$ ve

$$C^{\perp} \subseteq \psi\left(\chi(C)^{\perp}\right) \quad (1)$$

elde edilir. Diğer taraftan, eğer $v \in \chi(C)^{\perp}$ ise $\forall u \in C$ için $\langle \chi(u), v \rangle_{2^s} = 0$ dır. Önerme 3.26 yardımıyla, $\langle \chi(u), v \rangle_{2^s} = \langle u, \psi(v) \rangle = 0$ olur ve buradan da

$$\psi\left(\chi(C)^{\perp}\right) \subseteq C^{\perp} \quad (2)$$

bulunur. (1) ve (2) den $C^{\perp} = \psi\left(\chi(C)^{\perp}\right)$ elde edilir. $\blacksquare$

3.8 $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – Toplamsal Kodların Kontrol Matrisleri

Bu bölümde $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodların kontrol matrislerinin standart formu belirlenecektir.

$k(A)$, A matrisinin satır sayısı olsun. $i=1,...,s$ için $k_i(A)$; A matrisinin satırlarından 2^{i-1} ile bölünüp 2^i ile bölünemeyenlerinin sayısını göstersin. Böylece,

$k(A)=\sum_{i=1}^{s} k_i(A)$ yazılabilir.

Teorem 3.29 C, standart haldeki üreteç matrisi (3.6) ile verilen $(\alpha,\beta;k_0;k_1,...,k_s)$ tipindeki $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kod olsun. Buradan $C^{\perp}$ toplamsal dual kodunun üreteç matrisi (C kodunun kontrol matrisi) standart formdaki aşağıdaki matrisle belirlidir.

$$H_s=\begin{bmatrix} A_1 & U \\ T_1 & B \end{bmatrix}$$

Burada, $A_1=\begin{bmatrix} -\bar{A}_{01}^t & I_{\alpha-k_0} \end{bmatrix}$, $U=\begin{bmatrix} U_{s-1} & U_{s-2} & \cdots & U_1 & 0 & 0 \end{bmatrix}$, $T_1=\begin{bmatrix} -T_{0,s}^t & 0 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix}$,

$B=\begin{bmatrix} B_{0,s} & B_{0,s-1} & \cdots & B_{0,2} & B_{0,1} & I_{\beta-k(A)} \\ 2B_{1,s} & 2B_{1,s-1} & \cdots & 2B_{1,2} & 2I_{k_s(A)} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 2^{s-1}B_{s-1,s} & 2^{s-1}I_{k_2(A)} & \cdots & 0 & 0 & 0 \end{bmatrix}$ formunda matrislerdir ve

$0\le i<j\le s$ için $B_{ij}=-\sum_{k=i+1}^{j-1} B_{i,k}A_{s-j,s-k}^t-A_{s-j,s-i}^t$ ve $1\le j\le s-1$ için

$U_j=-\sum_{k=1}^{j-1} U_k A_{s-j-1,s-k-1}^t-2^j S_{s-j}^t$ biçiminde tanımlanmışlardır.

İspat: Direkt olarak $H_sG_s^t=0$ olduğu görülebilir. Şimdi, C bir $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kod olsun ve C nin standart formdaki üreteç matrisi (3.6) ile verilsin. Buradan, $\chi(C)$ kodunun üreteç matrisi aşağıdaki formda olacaktır.

$$\tilde{G}_s = \begin{bmatrix} 2^{s-1}\bar{A} & T \\ 2^{s-1}S & A \end{bmatrix}. \tag{3.9}$$

$\chi(C)$ kodu $\mathbb{Z}_{2^s}$ üzerinde bir kod olduğundan (3.2) matrisine denk aşağıdaki $\tilde{G}$ üreteç matrisine sahip olacaktır.

$$\tilde{G} = \begin{bmatrix} I_{k_1} & \tilde{A}_{01} & \tilde{A}_{02} & \tilde{A}_{03} & \cdots & \tilde{A}_{0,s-2} & \tilde{A}_{0,s-1} & \tilde{A}_{0,s} \\ 0 & 2I_{k_2} & 2\tilde{A}_{12} & 2\tilde{A}_{13} & \cdots & 2\tilde{A}_{1,s-2} & 2\tilde{A}_{1,s-1} & 2\tilde{A}_{1,s} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2^{s-2}I_{k_{s-1}} & 2^{s-2}\tilde{A}_{s-2,s-1} & 2^{s-2}\tilde{A}_{s-2,s} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 2^{s-1}\tilde{I}_{k_s} & 2^{s-1}\tilde{A}_{s-1,s} \end{bmatrix}.$$

$\tilde{G}$ matrisi; (3.9) matrisinde, ilk k_0 satır son satıra taşındıktan sonra ilk α sütunun son $s-1$ ile s blokları arasına taşınmasıyla elde edilmiştir. Ayrıca, bu matriste $0 \le i \le s-3$ ve $1 \le j \le s-2$ için $\tilde{A}_{i,j} = A_{i,j}$ ve $\tilde{I}_{k_s} = \begin{bmatrix} I_{k_s} & 0 \\ 0 & I_{k_0} \end{bmatrix}$, $\tilde{A}_{s-1,s} = \begin{bmatrix} 0 & A_{s-1,s} \\ \bar{A}_{01} & T_{0,s} \end{bmatrix}$ formunda ve $0 \le i \le s-2$ için ise $\tilde{A}_{i,s-1} = \begin{bmatrix} A_{i,s-1} & 0 \end{bmatrix}$, $\tilde{A}_{i,s} = \begin{bmatrix} 2^{s-i-1}S_{i+1} & A_{i,s} \end{bmatrix}$ formunda matrislerdir.

Ayrıca [16]'dan $\chi(C)^{\perp}$ dual kodunun üreteç matrisinin

$$\tilde{H} = \begin{bmatrix} \tilde{B}_{0,s} & \tilde{B}_{0,s-1} & \cdots & \tilde{B}_{0,2} & \tilde{B}_{0,1} & I_{\alpha+\beta-k(\tilde{G})} \\ 2\tilde{B}_{1,s} & 2\tilde{B}_{1,s-1} & \cdots & 2\tilde{B}_{1,2} & 2\tilde{I}_{k_s(\tilde{G})} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 2^{s-1}\tilde{B}_{s-1,s} & 2^{s-1}I_{k_2(\tilde{G})} & \cdots & 0 & 0 & 0 \end{bmatrix}$$

formundaki matrise permütasyon denk olduğu biliniyor. Burada, $0 \le i < j \le s$ için $\tilde{B}_{i,j} = -\sum_{k=i+1}^{j-1} \tilde{B}_{i,k}\tilde{A}^t_{s-j,s-k} - \tilde{A}^t_{s-j-s-i}$ şeklindedir. Yukarıdaki $\tilde{H}$ matrisi düzenlenerek

$$\tilde{H} = \begin{bmatrix} \tilde{B}_{0,s} & \tilde{B}_{0,s-1} & \cdots & \tilde{B}_{0,2} & \tilde{B}_{0,1} & I_{\alpha-k_0} & 0 \\ 2\tilde{B}_{1,s} & 2\tilde{B}_{1,s-1} & \cdots & 2\tilde{B}_{1,2} & 2\tilde{I}_{k_s(\tilde{G})} & 0 & I_{\beta-k(A)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 2^{s-1}\tilde{B}_{s-1,s} & 2^{s-1}I_{k_2(\tilde{G})} & \cdots & 0 & 0 & 0 & 0 \end{bmatrix}$$ şeklinde yazılabilir.

Böylece, daha önce uygulanan sütun permütasyonları geri alınarak $\chi(C)^{\perp}$ kodunun üreteç matrisi, $\tilde{H}_s = \begin{bmatrix} -\bar{A}_{01}^t & I_{\alpha-k_0} & U \\ \tilde{T} & 0 & B \\ 2I_{k_0} & 0 & 0 \end{bmatrix}$ formunda elde edilir. Burada ise,

$$B = \begin{bmatrix} B_{0,s} & B_{0,s-1} & \cdots & B_{0,2} & B_{0,1} & I_{\beta-k(A)} \\ 2B_{1,s} & 2B_{1,s-1} & \cdots & 2B_{1,2} & 2I_{k_s(A)} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 2^{s-1}B_{s-1,s} & 2^{s-1}I_{k_2(A)} & \cdots & 0 & 0 & 0 \end{bmatrix},$$

$U = \begin{bmatrix} U_{s-1} & U_{s-2} & \cdots & U_1 & 0 & 0 \end{bmatrix}$, $\tilde{T} = \begin{bmatrix} -T_{0,s}^t \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ biçiminde matrislerdir ve $0 \le i < j \le s$ olmak üzere $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A_{s-j,s-k}^t - A_{s-j,s-i}^t$ şeklinde tanımlanmış ve $1 \le j \le s-1$ için $U_j = -\sum_{k=1}^{j-1} U_k A_{s-j-1,s-k-1}^t - 2^j S_{s-j}^t$ şeklinde tanımlanmıştır. Son olarak Önerme 3.28 kullanılarak $\psi(\tilde{H}_s) = H_s$, $C^{\perp}$ toplamsal dual kodunun üreteç matrisidir. ■

Bu teoremin daha iyi anlaşılması için aşağıda, [6]'da elde edilen bir sonuç verilip bu sonucun ispatı yapılacaktır.

Sonuç 3.30 $(\alpha, \beta; k_0; k_1, k_2)$ tipindeki bir C, $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodunun üreteç matrisi (3.7) ile verilsin. C nin kontrol matrisi aşağıda verilen matrise permütasyon denktir.

$$\begin{bmatrix} -\bar{A}_{01}^t & I_{\alpha-k_0} & -2S_1^t & 0 & 0 \\ -T_{02}^t & 0 & -A_{02}^t + A_{12}^t A_{01}^t & -A_{12}^t & I_{\beta-k_1-k_2} \\ 0 & 0 & -2A_{01}^t & 2I_{k_2} & 0 \end{bmatrix}.$$

İspat: C, $(\alpha, \beta; k_0; k_1, k_2)$ tipinde, bir $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kod olsun. Böylece C nin üreteç matrisi $\begin{bmatrix} I_{k_0} & \bar{A}_{01} & 0 & 0 & 2T_{02} \\ 0 & S_1 & I_{k_1} & A_{01} & A_{02} \\ 0 & 0 & 0 & 2I_{k_2} & 2A_{12} \end{bmatrix}$ formunda ve buradan $\chi(C)$ kodunun

üreteç matrisi $\begin{bmatrix} 2I_{k_0} & 2\bar{A}_{01} & 0 & 0 & 2T_{02} \\ 0 & 2S_1 & I_{k_1} & A_{01} & A_{02} \\ 0 & 0 & 0 & 2I_{k_2} & 2A_{12} \end{bmatrix}$ formunda olacaktır. Bu matriste birinci satır ikinci satırla ve daha sonra ikinci satır üçüncü satırla yer değiştirir ve (12345) sütunları için $(13)(24)$ permütasyonu uygulanırsa $\begin{bmatrix} I_{k_1} & A_{01} & 0 & 2S_1 & A_{02} \\ 0 & 2I_{k_2} & 0 & 0 & 2A_{12} \\ 0 & 0 & 2I_{k_0} & 2\bar{A}_{01} & 2T_{02} \end{bmatrix}$ matrisi elde edilir. Buradan $\chi(C)^{\perp}$ kodunun üreteç matrisi $\begin{bmatrix} -2S_1^t & 0 & -\bar{A}_{01}^t & I_{\alpha-k_0} & 0 \\ -A_{02}^t + A_{12}^t A_{01}^t & -A_{12}^t & -T_{02}^t & 0 & I_{\beta-k_1-k_2} \\ -2A_{01}^t & 2I_{k_2} & 0 & 0 & 0 \\ 0 & 0 & 2I_{k_0} & 0 & 0 \end{bmatrix}$ formunda yazılabilir. Daha önce uygulanan sütun permütasyonları geri alınırsa bu matris $\tilde{H}_s = \begin{bmatrix} -\bar{A}_{01}^t & I_{\alpha-k_0} & -2S_1^t & 0 & 0 \\ -T_{02}^t & 0 & -A_{02}^t + A_{12}^t A_{01}^t & -A_{12}^t & I_{\beta-k_1-k_2} \\ 0 & 0 & -2A_{01}^t & 2I_{k_2} & 0 \\ 2I_{k_0} & 0 & 0 & 0 & 0 \end{bmatrix}$ haline gelir. Son olarak, ψ dönüşümünü $\tilde{H}_s$ matrisine uygulayarak $C^{\perp}$ toplamsal dual kodunun üreteç matrisi;

$H_s = \psi\left(\tilde{H}_s\right) = \begin{bmatrix} -\bar{A}_{01}^t & I_{\alpha-k_0} & -2S_1^t & 0 & 0 \\ -T_{02}^t & 0 & -A_{02}^t + A_{12}^t A_{01}^t & -A_{12}^t & I_{\beta-k_1-k_2} \\ 0 & 0 & -2A_{01}^t & 2I_{k_2} & 0 \end{bmatrix}$ formunda elde edilir. ■

Örnek 3.31 Standart haldeki üreteç matrisi (3.8) ile verilen $(\alpha, \beta; k_0; k_1, k_2, k_3)$ tipindeki C, $\mathbb{Z}_2\mathbb{Z}_8 -$ toplamsal kodunun kontrol matrisi;

$\begin{bmatrix} -\bar{A}_{01}^t & I_{\alpha-k_0} & & -2S_2^t & 0 & 0 \\ -T_{03}^t & 0 & P & -A_{13}^t + A_{23}^t A_{12}^t & -A_{23}^t & I_{\beta-k_1-k_2-k_3} \\ 0 & 0 & & -2A_{12}^t & 2I_{k_3} & 0 \\ 0 & 0 & & 4I_{k_2} & 0 & 0 \end{bmatrix}$ formundadır. Buradaki P

$P = \begin{bmatrix} -4S_1^t + 2S_2^t A_{01}^t \\ -A_{03}^t + A_{13}^t A_{01}^t + A_{23}^t A_{02}^t - A_{23}^t A_{12}^t A_{01}^t \\ -2A_{02}^t + 2A_{12}^t A_{01}^t \\ -4A_{01}^t \end{bmatrix}$ biçimindedir.

Örnek 3.32 Standart haldeki üreteç matrisi $\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ ile verilen $(3,3;1;3,0,0)$ tipindeki C, $\mathbb{Z}_2\mathbb{Z}_8$ – toplamsal kodunun kontrol matrisi $\begin{bmatrix} 1 & 1 & 0 & 0 & 4 & 4 \\ 0 & 0 & 1 & 4 & 4 & 4 \end{bmatrix}$ dir.

3.9 $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – Toplamsal Kodlar Üzerinde Bazı Sınırlar

Bu bölümde $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodlar üzerinde iki tane sınır verilip bu sınırlar karşılaştırılacaktır.

Tanım 3.33 $v_1 \in \mathbb{Z}_2^\alpha$ nın Hamming ağırlığı $wt_H(v_1)$ ve $v_2 \in \mathbb{Z}_{2^s}^\beta$ nın Lee ağırlığı da $wt_L(v_2)$ ile gösterilsin.

$v = (v_1, v_2) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_{2^s}^\beta$ elemanının ağırlığı $wt(v) = wt_H(v_1) + wt_L(v_2)$ biçiminde tanımlanır. Bu tanım kullanılarak herhangi iki $u, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_{2^s}^\beta$ elemanı arasındaki uzaklık da $d(u,v) = wt(u-v)$ şeklinde tanımlanabilir. C kodunun kodsözleri arasındaki minimum uzaklık $d(C)$ ile gösterilecektir. Burada tanımlanan d uzaklığının bir metrik olduğu kolayca gösterilebilir.

Teorem 3.34 C, $(\alpha, \beta; k_0; k_1, k_2, \ldots, k_s)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kod ise;

$$\frac{d(C)-1}{2^{s-1}} \le \frac{\alpha}{2^{s-1}} + \beta - \frac{\left[k_0 + sk_1 + (s-1)k_2 + \cdots + k_s\right]}{2^{s-1}} \tag{3.10}$$

$$\left\lfloor \frac{d(C)-1}{2^{s-1}} \right\rfloor \le \alpha + \beta - \left(k_0 + k_1 + k_2 + \cdots + k_s\right) \tag{3.11}$$

sınırları geçerlidir.

İspat: (3.10) sınırı (2.1)'de verilen $d(C) \le n - \log_q |C| + 1$ Singleton sınırı kullanılarak kolayca elde edilebilir. Yani,

$d(C) \le n - \log_q |C| + 1 \Rightarrow d(C) \le \alpha + 2^{s-1}\beta - \left[k_0 + sk_1 + (s-1)k_2 + \cdots + k_s\right] + 1$ ve buradan

$\frac{d(C)-1}{2^{s-1}} \le \frac{\alpha}{2^{s-1}} + \beta - \frac{\left[k_0 + sk_1 + (s-1)k_2 + \cdots + k_s\right]}{2^{s-1}}$ bulunur.

(3.11) sınırını elde etmek için $(\chi, I_d) : \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_{2^s}^{\beta} \to \mathbb{Z}_{2^s}^{\alpha+\beta}$ dönüşümü kullanılırsa, $d(C) \le d(\chi(C))$ yazılabilir. Ayrıca, [25]'deki Teorem 4.3 den $\left\lfloor \frac{d(C)-1}{2^{s-1}} \right\rfloor \le n - rank(C)$ olduğu bilinen bir sonuçtur. Burada $rank(C)$, C nin standart haldeki üreteç matrisinin satır sayısıdır. Böylece, $\left\lfloor \frac{d(C)-1}{2^{s-1}} \right\rfloor \le \alpha + \beta - \left(k_0 + k_1 + k_2 + \cdots + k_s\right)$ elde edilir. ■

Önerme 3.35 $(\alpha, \beta; k_0; k_1, k_2, \ldots, k_s)$ tipindeki C, $\mathbb{Z}_2\mathbb{Z}_{2^s}$ − toplamsal kodu için; $1 < a \in \mathbb{Z}$ ve $1 < b < 2^{s-1}$, $b \in \mathbb{Z}$ olmak üzere,

(3.10) sınırının (3.11) sınırından daha kuvvetli olması için gerekli ve yeterli şart,

i) $d(C) = 2^{s-1}a + 1$ ise

$k_0 + k_s + \frac{2^{s-1}\left(k_1 + k_2 + \cdots + k_{s-1}\right) - \left[sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}\right]}{2^{s-1} - 1} < \alpha$ olmasıdır.

ii) $d(C) = 2^{s-1}a$ ise

$k_0 + k_s + \frac{2^{s-1}\left(k_1 + k_2 + \cdots + k_{s-1}\right) - \left[sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}\right]}{2^{s-1} - 1} \le \alpha$ olmasıdır.

iii) $d(C) = 2^{s-1}a + b$ ise

$k_0 + k_s + \frac{2^{s-1}\left(k_1 + k_2 + \cdots + k_{s-1}\right) - \left[sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}\right]}{2^{s-1} - 1} < \alpha + \frac{b-1}{2^{s-1} - 1}$ olmasıdır.

İspat: $1 < a \in \mathbb{Z}$ ve $1 < b < 2^{s-1}$, $b \in \mathbb{Z}$ olmak üzere,

i) $d(C) = 2^{s-1}a + 1$ olsun.

(3.10) sınırının (3.11) sınırından daha kuvvetli olması için gerekli ve yeterli şart,

$$\alpha + 2^{s-1}\beta - [k_0 + sk_1 + (s-1)k_2 + \cdots + k_s] + 1 < 2^{s-1}\alpha + 2^{s-1}\beta - 2^{s-1}(k_0 + k_1 + \cdots + k_s) + 1$$

$$(k_0 + k_s)(2^{s-1} - 1) + 2^{s-1}(k_1 + k_2 + \cdots + k_{s-1}) - \left[sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}\right] < (2^{s-1} - 1)\alpha$$

$$k_0 + k_s + \frac{2^{s-1}\left(k_1 + k_2 + \cdots + k_{s-1}\right) - \left[sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}\right]}{2^{s-1} - 1} < \alpha \text{ olmasıdır.}$$

ii) $d(C) = 2^{s-1}a$ olsun.

(3.10) sınırının (3.11) sınırından daha kuvvetli olması için gerekli ve yeterli şart,

$$\alpha + 2^{s-1}\beta - [k_0 + sk_1 + (s-1)k_2 + \cdots + k_s] + 1 < 2^{s-1}[\alpha + \beta - (k_0 + k_1 + \cdots + k_s) + 1]$$

$$(k_0 + k_s)(2^{s-1} - 1) + 2^{s-1}(k_1 + k_2 + \cdots + k_{s-1}) - \left[sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}\right] < (2^{s-1} - 1)(\alpha + 1)$$

$$k_0 + k_s + \frac{2^{s-1}(k_1 + k_2 + \cdots + k_{s-1}) - [sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}]}{2^{s-1} - 1} < \alpha + 1$$

$$k_0 + k_s + \frac{2^{s-1}(k_1 + k_2 + \cdots + k_{s-1}) - [sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}]}{2^{s-1} - 1} \le \alpha \text{ olmasıdır.}$$

iii) $d(C) = 2^{s-1}a + b$ olsun.

(3.10) sınırının (3.11) sınırından daha kuvvetli olması için gerekli ve yeterli şart,

$$\alpha + 2^{s-1}\beta - \left[k_0 + sk_1 + (s-1)k_2 + \cdots + k_s\right] + 1 < 2^{s-1}\left[\alpha + \beta - (k_0 + k_1 + \cdots + k_s)\right] + b$$

$$k_0 + k_s + \frac{2^{s-1}(k_1 + k_2 + \cdots + k_{s-1}) - \left[sk_1 + (s-1)k_2 + \cdots + 2k_{s-1}\right]}{2^{s-1} - 1} < \alpha + \frac{b-1}{2^{s-1} - 1} \text{ olmasıdır.}$$

Aşağıda sınırlar ile ilgili verilen iki örnekte bu tezde elde edilen yeni sınırların sağlandığı görülecektir. Yani, verilen bu yeni sınırlar olası en iyi sınırlardır.

Örnek 3.36 C, $(1,1;1;0,0,0,0)$ tipinde ve $G = \begin{bmatrix} 1 & 8 \end{bmatrix}$ üreteç matrisine sahip $\mathbb{Z}_2\mathbb{Z}_{16}$ – toplamsal kod olsun. Buradan, $s = 4$ ve $C = \{(0,0),(1,8)\}$ ve $d(C) = 9$ dur. (3.10) sınırı kullanılırsa,

$$\frac{d(C)-1}{8} \le \frac{\alpha}{8} + \beta - \frac{k_0 + 4k_1 + 3k_2 + 2k_3 + k_4}{8} \Rightarrow \frac{9-1}{8} \le \frac{1}{8} + 1 - \frac{1}{8} \Rightarrow 1 \le 1 \text{ elde edilir.}$$

Örnek 3.37 C, $\mathbb{Z}_2\mathbb{Z}_8-$toplamsal kodu $G=\begin{bmatrix}1 & 0 & 0 & 4\\ 0 & 4 & 0 & 4\\ 0 & 0 & 4 & 4\end{bmatrix}$ standart haldeki üreteç matrisiyle verilsin. Böylece, C, $(1,3;1;0,0,2)$ tipindedir ve C nin kodsözleri;

$C=\{(0,0,0,0),(1,0,0,4),(0,4,0,4),(0,0,4,4),(1,4,0,0),(1,0,4,0),(0,4,4,0),(1,4,4,4)\}$

biçimindedir. Ayrıca $d(C)=5$ olduğu açıktır. Buradan (3.11) sınırını uygulayarak,

$\left\lfloor \frac{d(C)-1}{4} \right\rfloor \le \alpha+\beta-(k_0+k_1+k_2+k_3) \Rightarrow \left\lfloor \frac{5-1}{4} \right\rfloor \le 1+3-(1+0+0+2) \Rightarrow 1\le 1$ bulunur.

BÖLÜM 4

$\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – TOPLAMSAL KODLAR

Bu bölümde $\mathbb{Z}_2\mathbb{Z}_4$ – toplamsal kodların en genel hali olan $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – toplamsal kodlar incelenecektir. Bu toplamsal kodlar $p=2$ ve $r=1$ için $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodlara karşılık geleceklerinden, bu bölümde verilecek olan bazı teoremler $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – toplamsal kodlar bölümünde verilen teoremlerin ispatlarıyla benzer yöntemler kullanılarak ispatlanabilir. Dolayısıyla bazı teoremlerin ispatları yapılmayacaktır.

Tanım 4.1 p, asal bir sayı ve $1 \le r < s$ tamsayılar olmak üzere $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ nın bir C alt grubuna $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – ***toplamsal kod*** denir.

Tanımdan görüldüğü üzere C, $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – toplamsal kodu $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ nın bir alt grubudur. Buradan, sonlu değişmeli grupların temel teoremi kullanılarak C toplamsal kodunun $\mathbb{Z}_{p^r}^{k_0} \times \mathbb{Z}_{p^{r-1}}^{k_1} \times \cdots \times \mathbb{Z}_{p}^{k_{r-1}} \times \mathbb{Z}_{p^s}^{l_0} \times \mathbb{Z}_{p^{s-1}}^{l_1} \times \cdots \times \mathbb{Z}_{p}^{l_{s-1}}$ değişmeli grubuna izomorf olduğu söylenebilir. Bu yapıyla ilişkili olarak böyle bir toplamsal kod için $(\alpha, \beta; k_0, k_1, \ldots, k_{r-1}; l_0, l_1, \ldots, l_{s-1})$ tipindedir denir.

$\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – toplamsal kodların hem $\mathbb{Z}_{p^r}$ üzerindeki hem de $\mathbb{Z}_{p^s}$ üzerindeki kodlarla ilişkili olduğu aşikârdır. O halde $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – toplamsal kodlarla bu kodlar arasında bir bağıntı kurmak için özel bir dönüşüm tanımlanabilir. “A Generalization of the Lee Weight to

$\mathbb{Z}_{p^k}$" adlı makalelerinde Yıldız ve Ö. Özger, Lee ağırlığını $\mathbb{Z}_{p^s}$ üzerine genişlettiler [26]. Ayrıca, bu ağırlık yardımıyla mesafeleri de koruyan aşağıdaki Gray dönüşümünü elde ettiler.

$\phi : \mathbb{Z}_{p^s} \to \mathbb{Z}_p^{p^{s-1}}$

$$
\begin{aligned}
0 &\to (000\cdots000),\\
1 &\to (100\cdots000),\\
2 &\to (110\cdots000),\\
&\vdots\\
p^{s-1} &\to (111\cdots111),\\
p^{s-1}+1 &\to (211\cdots111),\\
&\vdots\\
2p^{s-1} &\to (222\cdots222),\\
2p^{s-1}+1 &\to (322\cdots222),\\
&\vdots\\
(p-1)p^{s-1} &\to ((p-1)(p-1)(p-1)\cdots(p-1)(p-1)(p-1)),\\
(p-1)p^{s-1}+1 &\to (0(p-1)(p-1)\cdots(p-1)(p-1)(p-1)),\\
&\vdots\\
p^s-2 &\to (000\cdots0(p-1)(p-1)),\\
p^s-1 &\to (000\cdots00(p-1)).
\end{aligned}
$$

Diğer bir ifadeyle bu Gray dönüşümü; $x \le p^{s-1}$ iken ilk x koordinatı 1 e ve geri kalan koordinatları sıfıra götürür. $x = qp^{s-1} + r > p^{s-1}$ durumunda ise, $\overline{q} = (qqq\cdots qqq)$ olmak üzere x i $\phi(x) = \overline{q} + \phi(r)$ e taşır. Bu dönüşümün nasıl çalıştığı bir örnek yardımıyla aşağıdaki gibi gösterilebilir.

Örnek 4.2 ϕ Gray dönüşümü $\mathbb{Z}_9$ un elemanlarını $\mathbb{Z}_3$ ün elemanlarına resmetsin. $\phi : \mathbb{Z}_{3^2} \to \mathbb{Z}_3^{3^{2-1}}$ olmak üzere

$\phi : \mathbb{Z}_9 \to \mathbb{Z}_3^3$

$0 \to (000)$

$1 \to (100)$

$2 \to (110)$

$3 \to (111)$

$4 \to (211)$

$5 \to (221)$

$6 \to (222)$

$7 \to (022)$

$8 \to (002)$

biçimindedir.

Tanım 4.3 $\Phi : \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta} \to \mathbb{Z}_p^n$ dönüşümü

$x = (x_1, x_2, ..., x_\alpha) \in \mathbb{Z}_{p^r}^{\alpha}$, $y = (y_1, y_2, ..., y_\beta) \in \mathbb{Z}_{p^s}^{\beta}$ ve $n = p^{r-1}\alpha + p^{s-1}\beta$ olmak üzere,

$$\Phi(x, y) = \left(\phi(x_1), \phi(x_2), ..., \phi(x_\alpha), \phi(y_1), \phi(y_2), ..., \phi(y_\beta)\right) \quad (4.1)$$

biçiminde tanımlanır.

Bu durumda $\Phi(C) = \mathrm{C}$ Gray görüntüsüne $n = p^{r-1}\alpha + p^{s-1}\beta$ uzunluğunda $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – ***lineer kod*** denir.

4.1 Üreteç Matrisin Standart Formu

Teorem 4.4 C, $(\alpha, \beta; k_0, k_1, \ldots, k_{r-1}; l_0, l_1, \ldots, l_{s-1})$ tipinde bir $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – toplamsal kod olsun. C kodu aşağıda standart formla verilen G_p üreteç matrisinin ürettiği $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ – toplamsal koda denktir ve

$$G_p = \begin{bmatrix} B_p & T_p \\ S_p & A_p \end{bmatrix} \quad (4.2)$$

$$B_p=\begin{bmatrix} I_{k_0} & B_{0,1} & B_{0,2} & B_{0,3} & \cdots & B_{0,r-2} & B_{0,r-1} & B_{0,r} \\ 0 & pI_{k_1} & pB_{1,2} & pB_{1,3} & \cdots & pB_{1,r-2} & pB_{1,r-1} & pB_{1,r} \\ 0 & 0 & p^2I_{k_2} & p^2B_{2,3} & \cdots & p^2B_{2,r-2} & p^2B_{2,r-1} & p^2B_{2,r} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{r-2}I_{k_{r-2}} & p^{r-2}B_{r-2,r-1} & p^{r-2}B_{r-2,r} \\ 0 & 0 & 0 & 0 & \cdots & 0 & p^{r-1}I_{k_{r-1}} & p^{r-1}B_{r-1,r} \end{bmatrix},$$

$$T_p=\begin{bmatrix} 0 & 0 & \cdots & p^{s-r}T_{0,1} & p^{s-r}T_{0,2} & \cdots & p^{s-r}T_{0,r-2} & p^{s-r}T_{0,r-1} & p^{s-r}T_{0,r} \\ 0 & 0 & \cdots & 0 & p^{s-r+1}T_{1,2} & \cdots & p^{s-r+1}T_{1,r-2} & p^{s-r+1}T_{1,r-1} & p^{s-r+1}T_{1,r} \\ 0 & 0 & \cdots & 0 & 0 & \cdots & p^{s-r+2}T_{2,r-2} & p^{s-r+2}T_{2,r-1} & p^{s-r+2}T_{2,r} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & p^{s-2}T_{r-2,r-1} & p^{s-2}T_{r-2,r} \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & p^{s-1}T_{r-1,r} \end{bmatrix},$$

$$S_p=\begin{bmatrix} 0 & S_{0,1} & S_{0,2} & S_{0,3} & \cdots & S_{0,r-2} & S_{0,r-1} & S_{0,r} \\ 0 & S_{1,1} & S_{1,2} & S_{1,3} & \cdots & S_{1,r-2} & S_{1,r-1} & S_{1,r} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & S_{s-r-1,1} & S_{s-r-1,2} & S_{s-r-1,3} & \cdots & S_{s-r-1,r-2} & S_{s-r-1,r-1} & S_{s-r-1,r} \\ 0 & 0 & pS_{s-r,2} & pS_{s-r,3} & \cdots & pS_{s-r,r-2} & pS_{s-r,r-1} & pS_{s-r,r} \\ 0 & 0 & 0 & p^2S_{s-r+1,3} & \cdots & p^2S_{s-r+1,r-2} & p^2S_{s-r+1,r-1} & p^2S_{s-r+1,r} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & p^{r-1}S_{s-2,r} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$ ve

$$A_p=\begin{bmatrix} I_{l_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,s-2} & A_{0,s-1} & A_{0,s} \\ 0 & pI_{l_1} & pA_{1,2} & pA_{1,3} & \cdots & pA_{1,s-2} & pA_{1,s-1} & pA_{1,s} \\ 0 & 0 & p^2I_{l_2} & p^2A_{2,3} & \cdots & p^2A_{2,s-2} & p^2A_{2,s-1} & p^2A_{2,s} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{s-2}I_{l_{s-2}} & p^{s-2}A_{s-2,s-1} & p^{s-2}A_{s-2,s} \\ 0 & 0 & 0 & 0 & \cdots & 0 & p^{s-1}I_{l_{s-1}} & p^{s-1}A_{s-1,s} \end{bmatrix}$$ biçiminde

matrislerdir. Ayrıca, $0\le i<r,\ 0<j\le r$ için B_{ij} ler $\mathbb{Z}_{p^r}$ üzerinde ve T_{ij} ler de $\mathbb{Z}_{p^s}$ üzerinde matrisler; $0\le m<s-1,\ 0\le t<s,\ 0<q\le s$ için S_{mj} ve A_{tq} ler $\mathbb{Z}_{p^s}$ üzerinde matrislerdir. Son olarak $0\le w\le r-1$ ve $0\le y\le s-1$ olmak üzere, I_{k_w} ve I_{l_y} sırasıyla $k_w\times k_w$ ve $l_y\times l_y$ boyutlu birim matrislerdir.

Örnek 4.5 $p=3$ olmak üzere C, $(2,3;1;2,0)$ tipindeki $\mathbb{Z}_3\mathbb{Z}_9-$toplamsal kodu $\begin{bmatrix}1&2&3&4&5\\0&1&6&7&8\\1&1&1&4&6\end{bmatrix}$ üreteç matrisi ile verilsin. Bu matriste gerekli satır işlemleri yapılırsa C, $\mathbb{Z}_3\mathbb{Z}_9-$toplamsal kodunun üreteç matrisinin standart formu,

$$G=\begin{bmatrix}1&1&0&0&6\\0&2&1&0&4\\0&1&0&1&8\end{bmatrix} \tag{4.3}$$

şeklinde elde edilir.

Örnek 4.6 $(3,2;1;0,1)$ tipindeki C, $\mathbb{Z}_3\mathbb{Z}_9-$toplamsal kodu $\begin{bmatrix}1&1&1&0&3\\0&0&0&3&6\end{bmatrix}$ üreteç matrisiyle verilsin. Böylece,

$$C=\{(0,0,0,0,0),(1,1,1,0,3),(0,0,0,3,6),(1,1,1,3,0),(2,2,2,0,6),(0,0,0,6,3),$$
$$(2,2,2,3,3),(1,1,1,6,6),(2,2,2,6,0)\}$$

biçimindedir.

Örnek 4.7 C, $(\alpha,\beta;k_0,k_1;l_0,l_1,l_2)$ tipindeki $\mathbb{Z}_4\mathbb{Z}_8-$toplamsal kodu olsun. Böylece, $p=r=2$ ve $s=3$ tür. C toplamsal kodunun üreteç matrisi;

$$G=\begin{bmatrix}I_{k_0}&B_{01}&B_{02}&0&0&2T_{01}&2T_{02}\\0&2I_{k_1}&2B_{12}&0&0&0&4T_{12}\\0&S_{01}&S_{02}&I_{l_0}&A_{01}&A_{02}&A_{03}\\0&0&2S_{12}&0&2I_{l_1}&2A_{12}&2A_{13}\\0&0&0&0&0&4I_{l_2}&4A_{23}\end{bmatrix} \tag{4.4}$$

formundadır.

Örnek 4.8 C, $\mathbb{Z}_{16}\mathbb{Z}_{32}-$toplamsal kodu $\alpha=7$ ve $\beta=11$ olmak üzere

$$G=\left[\begin{array}{ccccccc|ccccccccccc}
\boxed{1} & 0 & 1 & 1 & 6 & 3 & 14 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 14 & 10 & 10 & 22 \\
0 & \boxed{2} & 0 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 8 & 8 & 8 & 4 & 28 \\
0 & \boxed{0} & \boxed{2} & 2 & 0 & 2 & 10 & 0 & 0 & 0 & 0 & 4 & 0 & 4 & 4 & 12 & 4 & 12 \\
0 & 0 & 0 & \boxed{4} & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 8 & 24 \\
0 & 0 & 0 & 0 & \boxed{8} & \boxed{0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 \\
0 & 0 & 0 & 0 & \boxed{0} & \boxed{8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 \\
\hline
0 & 1 & 1 & 2 & 4 & 5 & 8 & \boxed{1} & 0 & 0 & 1 & 0 & 1 & 14 & 9 & 11 & 24 & 31 \\
0 & 0 & 0 & 2 & 4 & 0 & 4 & 0 & \boxed{2} & \boxed{0} & 0 & 6 & 4 & 10 & 6 & 14 & 4 & 10 \\
0 & 0 & 0 & 0 & 4 & 4 & 4 & 0 & \boxed{0} & \boxed{2} & 2 & 2 & 2 & 0 & 12 & 10 & 12 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & \boxed{4} & 0 & 0 & 12 & 12 & 8 & 24 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \boxed{8} & \boxed{0} & 0 & 0 & 0 & 0 & 16 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \boxed{0} & \boxed{8} & 8 & 8 & 0 & 16 & 16 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \boxed{16} & \boxed{0} & \boxed{0} & 0 & 16 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 16 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \boxed{0} & \boxed{0} & \boxed{16} & 0 & 0
\end{array}\right] \tag{4.5}$$

standart formdaki üreteç matrisiyle verilsin. Buradan C kodu $(7,11;1,2,1,2;1,2,1,2,3)$ tipindedir.

Sonuç 4.9 Eğer $p=2, r=1$ ve $s=2$ alınırsa $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodu elde edilir. $(\alpha,\beta;k_0;l_0,l_1)$ tipindeki bir C, $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodunun üreteç matrisi (3.7) matrisine permütasyon denktir. Ayrıca, $p=2$ ve $r=1$ için $\mathbb{Z}_2\mathbb{Z}_{2^s}-$toplamsal kod elde edilir ve $(\alpha,\beta;k_0;l_0,l_1,\ldots,l_{s-1})$ tipindeki bir C, $\mathbb{Z}_2\mathbb{Z}_{2^s}-$toplamsal kodunun standart formdaki üreteç matrisi yukarıdaki teorem kullanılarak (3.6) matrisi olarak elde edilir.

4.2 Dual Uzay ve Kontrol Matrisin Standart Formu

Bu bölümde $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$toplamsal kodların dual uzayı incelenip bu kodların kontrol matrislerinin standart formu verilecektir.

Tanım 4.10 $u,v\in\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ elemanlarının iç çarpımı,

$$u\cdot v=p^{s-r}\left(\sum_{i=1}^{\alpha}u_iv_i\right)+\sum_{j=\alpha+1}^{\alpha+\beta}u_jv_j$$

biçiminde tanımlanır. $\mathbb{Z}_2\mathbb{Z}_{2^s}$ −toplamsal kodlara benzer olarak bir C, $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ −toplamsal kodunun toplamsal duali,

$$C^{\perp}=\left\{v\in\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}\mid u\cdot v=0,\ \forall u\in C\right\}$$

şeklindedir.

$k(B)$ ve $l(A)$ sırasıyla B ve A matrislerinin satır sayıları olsun. $i=0,1,...,r-1(s-1)$ için $B\ (A)$ matrisinin satırlarından p^i ile bölünüp p^{i+1} ile bölünemeyenlerin (toplamsal mertebeleri p^{i+1} olanların) sayısı $k_i(B)\ (l_i(A))$ ile gösterilsin.

Teorem 4.11 C, (4.2) formundaki üreteç matrisiyle verilen $(\alpha,\beta;k_0,k_1,...,k_{r-1};l_0,l_1,...,l_{s-1})$ tipindeki $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ −toplamsal kodu olsun. C nin kontrol matrisi

$$H_p=\begin{bmatrix}\bar{B}_p+F & U\\ V & \bar{A}_p+E\end{bmatrix}$$

formundadır. Buradaki $\bar{B}_p, F, U, V, \bar{A}_p$ ve E matrisleri sırasıyla

$$\bar{B}_p=\begin{bmatrix}\bar{B}_{0,r} & \bar{B}_{0,r-1} & \bar{B}_{0,r-2} & \cdots & \bar{B}_{0,3} & \bar{B}_{0,2} & \bar{B}_{0,1} & I_{\alpha-k(B)}\\ p\bar{B}_{1,r} & p\bar{B}_{1,r-1} & p\bar{B}_{1,r-2} & \cdots & p\bar{B}_{1,3} & p\bar{B}_{1,2} & pI_{k_{r-1}(B)} & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ p^{r-2}\bar{B}_{r-2,r} & p^{r-2}\bar{B}_{r-2,r-1} & p^{r-2}I_{k_2(B)} & \cdots & 0 & 0 & 0 & 0\\ p^{r-1}\bar{B}_{r-1,r} & p^{r-1}I_{k_1(B)} & 0 & \cdots & 0 & 0 & 0 & 0\end{bmatrix},$$

$$F=\begin{bmatrix}F_{0,r-2} & F_{0,r-3} & \cdots & F_{0,2} & F_{0,1} & 0 & 0 & 0\\ pF_{1,r-2} & pF_{1,r-3} & \cdots & pF_{1,2} & 0 & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ p^{r-4}F_{r-4,r-2} & p^{r-4}F_{r-4,r-3} & \cdots & 0 & 0 & 0 & 0 & 0\\ p^{r-3}F_{r-3,r-2} & 0 & \cdots & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0\end{bmatrix},$$

$$U=\begin{bmatrix} U_{0,s-1} & U_{0,s-2} & \cdots & U_{0,3} & U_{0,2} & U_{0,1} & 0 & 0 \\ pU_{1,s-1} & pU_{1,s-2} & \cdots & pU_{1,3} & pU_{1,2} & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p^{r-2}U_{r-2,s-1} & p^{r-2}U_{r-2,s-2} & \cdots & 0 & 0 & 0 & 0 & 0 \\ p^{r-1}U_{r-1,s-1} & p^{r-1}U_{r-1,s-2} & \cdots & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$V=\begin{bmatrix} V_{0,r} & V_{0,r-1} & V_{0,r-2} & \cdots & V_{0,3} & V_{0,2} & V_{0,1} & 0 \\ pV_{1,r} & pV_{1,r-1} & pV_{1,r-2} & \cdots & pV_{1,3} & pV_{1,2} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p^{r-1}V_{r-1,r} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\bar{A}_p=\begin{bmatrix} \bar{A}_{0,s} & \bar{A}_{0,s-1} & \bar{A}_{0,s-2} & \cdots & \bar{A}_{0,3} & \bar{A}_{0,2} & \bar{A}_{0,1} & I_{\beta-l(A)} \\ p\bar{A}_{1,s} & p\bar{A}_{1,s-1} & p\bar{A}_{1,s-2} & \cdots & p\bar{A}_{1,3} & p\bar{A}_{1,2} & pI_{l_{s-1}(A)} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p^{s-2}\bar{A}_{s-2,s} & p^{s-2}\bar{A}_{s-2,s-1} & p^{s-2}I_{l_2(A)} & \cdots & 0 & 0 & 0 & 0 \\ p^{s-1}\bar{A}_{s-1,s} & p^{s-1}I_{l_1(A)} & 0 & \cdots & 0 & 0 & 0 & 0 \end{bmatrix} \text{ ve}$$

$$E=\begin{bmatrix} E_{0,s-2} & E_{0,s-3} & E_{0,s-4} & \cdots & E_{0,2} & E_{0,1} & 0 & 0 & 0 \\ pE_{1,s-2} & pE_{1,s-3} & pE_{1,s-4} & \cdots & pE_{1,2} & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p^{r-2}E_{r-2,s-2} & p^{r-2}E_{r-2,s-3} & p^{r-2}E_{r-2,s-4} & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ biçimindedir.}$$

Ayrıca bu matrislerin bileşenleri;

$$\bar{B}_{i,j}=-\sum_{k=i+1}^{j-1}\bar{B}_{i,k}B^t_{r-j,r-k}-B^t_{r-j,r-i},\ 0\le i<j\le r,$$

$$\bar{A}_{i,j}=-\sum_{k=i+1}^{j-1}\bar{A}_{i,k}A^t_{s-j,s-k}-A^t_{s-j,s-i},\ 0\le i<j\le s,$$

$$U_{i,j}=-\sum_{k=i+1}^{j-1}U_{i,k}A^t_{s-j-1,s-k-1}-q_1\left(\sum_{l=i+1}^{j-1}\bar{B}_{i,l}S^t_{s-j-1,r-l}+\sum_{m=i+1}^{j-3}F_{i,m}S^t_{s-j-1,r-m-2}+S^t_{s-j-1,r-i}\right),$$

$l \le r-1,\ m \le r-3$ ve $q_1 = \begin{cases} p, & j < r \\ p^{j-r+1}, & j \ge r \end{cases}$

$$V_{i,j} = -\sum_{k=i+1}^{j-1} V_{i,k} B^t_{r-j,r-k} - \sum_{k=i+1}^{j-1} \bar{A}_{i,k} T^t_{r-j,r-k} - \sum_{k=i+1}^{j-3} E_{i,i+j-k-2} T^t_{r-j,r+k-i-j} - T^t_{r-j,r-i},$$

$$E_{i,j} = -\sum_{k=i+1}^{j-1} E_{i,k} A^t_{s-j-2,s-k-2} - q_2 \sum_{l=i+1}^{j} V_{i,l} S^t_{s-j-2,r-l},$$

$l \le r-1$ ve $q_2 = \begin{cases} p, & j < r \\ p^{j-r+2}, & j \ge r \end{cases}$,

$$F_{i,j} = -\sum_{k=i+1}^{j-1} F_{i,k} B^t_{r-j-2,r-k-2} - \sum_{k=i+1}^{j} U_{i,k} T^t_{r-j-2,r-k-1}$$

biçiminde tanımlanmışlardır.

İspat: $G_p H_p{}^t = 0$ olduğu kontrol edilebilir. Bunun yanında H_p matrisinden faydalanarak

$$|C||C^\perp| = p^{rk_0}.p^{(r-1)k_1} \dots p^{k_{r-1}}.p^{sl_0}.p^{(s-1)l_1} \dots p^{l_{s-1}}.p^{r(\alpha-k_0-k_1-\cdots-k_{r-1})}.p^{(r-1)k_{r-1}} \dots p^{k_1}.p^{s(\beta-l_0-l_1-\cdots-l_{s-1})}.$$
$$p^{(s-1)l_{s-1}} \dots p^{l_1} = p^{r\alpha}.p^{s\beta}$$

yazılabilir. Böylece H_p matrisinin satırları G_p matrisinin satırlarına dik ve aynı zamanda H_p, $C^\perp$ dual kodunun tümünü üretmektedir. Yani H_p, $C^\perp$ kodunun üreteç matrisidir. ■

Örnek 4.12 C, üreteç matrisi (4.3) ile verilen $\mathbb{Z}_3\mathbb{Z}_9$ – toplamsal kodu olsun. C nin kontrol matrisi

$$\begin{bmatrix} 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 7 & 1 \\ 0 & 0 & 0 & 3 & 0 \end{bmatrix}$$ biçimindedir. Bu matris yardımıyla, $C^\perp$ in tipi $(3,2;2;1,1)$ olarak belirlenir.

Örnek 4.13 C, (4.4) üreteç matrisiyle verilen $(\alpha,\beta;k_0,k_1;l_0,l_1,l_2)$ tipindeki $\mathbb{Z}_4\mathbb{Z}_8$ – toplamsal kod olsun. $C^\perp$ toplamsal dual kodunun üreteç matrisi aşağıdaki gibi hesaplanabilir.

$H_p = \begin{bmatrix} \overline{B}_p + F & U \\ V & \overline{A}_p + E \end{bmatrix}$ formundaydı. Burada $r = 2$ olduğundan $F = 0$ dır. Diğer bileşenler de aşağıdaki gibi hesaplanırlar.

$\overline{B}_{01} = -B_{12}^t$, $\overline{B}_{02} = -\overline{B}_{01}B_{01}^t - B_{02}^t$, $\overline{B}_{12} = -B_{01}^t$ olmak üzere, $\overline{B}_2 = \begin{bmatrix} \overline{B}_{02} & \overline{B}_{01} & I_{\alpha-k_0-k_1} \\ 2\overline{B}_{12} & 2I_{k_1} & 0 \end{bmatrix}$ ve

$V_{01} = -T_{12}^t$, $V_{02} = -V_{01}B_{01}^t - \overline{A}_{01}T_{01}^t - T_{02}^t$, $V_{12} = -T_{01}^t$ olmak üzere, $V = \begin{bmatrix} V_{02} & V_{01} & 0 \\ 2V_{12} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ ve

$U_{01} = -2S_{12}^t$, $U_{02} = -U_{01}A_{01}^t - 2\left(\overline{B}_{01}S_{01}^t + S_{02}^t\right)$, $U_{12} = -2S_{01}^t$ olmak üzere,

$U = \begin{bmatrix} U_{02} & U_{01} & 0 & 0 \\ 2U_{12} & 0 & 0 & 0 \end{bmatrix}$ ve $E_{01} = -2V_{01}S_{01}^t$ olmak üzere $E = \begin{bmatrix} E_{01} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ dır.

Ayrıca, $\overline{A}_2$ matrisinin bileşenleri;

$\overline{A}_{01} = -A_{23}^t$, $\overline{A}_{02} = -\overline{A}_{01}A_{12}^t - A_{13}^t$, $\overline{A}_{03} = -\left(\overline{A}_{01}A_{02}^t + \overline{A}_{02}A_{01}^t\right) - A_{03}^t$

$\overline{A}_{12} = -A_{12}^t$, $\overline{A}_{13} = -\overline{A}_{12}A_{01}^t - A_{02}^t$, $\overline{A}_{23} = -A_{01}^t$ olmak üzere,

$\overline{A}_2 = \begin{bmatrix} \overline{A}_{03} & \overline{A}_{02} & \overline{A}_{01} & I_{\beta-l_0-l_1-l_2} \\ 2\overline{A}_{13} & 2\overline{A}_{12} & 2I_{l_2} & 0 \\ 4\overline{A}_{23} & 4I_{l_1} & 0 & 0 \end{bmatrix}$ biçimindedir. Böylece,

$$H = \begin{bmatrix} \overline{B}_{02} & \overline{B}_{01} & I_{\alpha-k_0-k_1} & U_{02} & U_{01} & 0 & 0 \\ 2\overline{B}_{12} & 2I_{k_1} & 0 & 2U_{12} & 0 & 0 & 0 \\ V_{02} & V_{01} & 0 & \overline{A}_{03} + E_{01} & \overline{A}_{02} & \overline{A}_{01} & I_{\beta-l_0-l_1-l_2} \\ 2V_{12} & 0 & 0 & 2\overline{A}_{13} & 2\overline{A}_{12} & 2I_{l_2} & 0 \\ 0 & 0 & 0 & 4\overline{A}_{23} & 4I_{l_1} & 0 & 0 \end{bmatrix}$$

formundadır.

Örnek 4.14 C, $\mathbb{Z}_{16}\mathbb{Z}_{32}$ – toplamsal kodu (4.5) üreteç matrisiyle verilmiş olsun. C nin kontrol matrisi,

$$H=\begin{bmatrix}
7 & 3 & 14 & 13 & 0 & 0 & 1 & 28 & 2 & 30 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 2 & 0 & 0 & 16 & 24 & 24 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
12 & 12 & 14 & 0 & 0 & 2 & 0 & 24 & 0 & 24 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 12 & 12 & 4 & 0 & 0 & 0 & 0 & 24 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 8 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
8 & 0 & 8 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
10 & 4 & 1 & 15 & 15 & 15 & 0 & 28 & 8 & 10 & 26 & 0 & 30 & 0 & 0 & 0 & 1 & 0\\
11 & 1 & 3 & 14 & 0 & 0 & 0 & 18 & 13 & 2 & 6 & 30 & 0 & 31 & 31 & 0 & 0 & 1\\
8 & 0 & 0 & 14 & 0 & 0 & 0 & 20 & 30 & 8 & 26 & 0 & 30 & 2 & 0 & 0 & 0 & 0\\
10 & 14 & 14 & 0 & 0 & 0 & 0 & 30 & 30 & 28 & 26 & 0 & 30 & 0 & 2 & 0 & 0 & 0\\
12 & 12 & 10 & 0 & 0 & 0 & 0 & 2 & 18 & 26 & 28 & 0 & 0 & 0 & 0 & 2 & 0 & 0\\
4 & 12 & 12 & 0 & 0 & 0 & 0 & 16 & 20 & 28 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 12 & 0 & 0 & 0 & 0 & 0 & 4 & 24 & 28 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 24 & 0 & 24 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

biçimindedir ve $C^{\perp}$ toplamsal dual kodu $(7,11;1,2,1,2;2,3,2,1,2)$ tipindedir.

Sonuç 4.15 Eğer C, $(\alpha,\beta;k_0;l_0,l_1)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kod ise C nin kontrol matrisi yukarıdaki teorem yardımıyla kolaylıkla yazılabilir ve elde edilen bu matris Sonuç 3.30 ile verilen matrise permütasyon denktir. Ayrıca, $p=2$ ve $r=1$ için C, $\mathbb{Z}_2\mathbb{Z}_{2^s}-$toplamsal kod olur ve C nin kontrol matrisi Teorem 3.29 ile verilen H_s matrisine denk olacaktır.

4.3 $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$Toplamsal Kodlar Üzerinde Sınırlar

Bu bölümde $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$toplamsal kodlar üzerinde iki tane sınır verilecektir. Yukarıda tanımlanan Gray dönüşümü bir izometridir. Böylece, (4.1) de tanımlanan Φ dönüşümü, $\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ üzerindeki Lee uzaklığını $n=p^{r-1}\alpha+p^{s-1}\beta$ olmak üzere, $\mathbb{Z}_p^n$ üzerindeki Lee uzaklıklarına dönüştürür. Şimdi, $wt_L(v_1)$, $v_1\in\mathbb{Z}_{p^r}^{\alpha}$ nın Lee ağırlığını ve $wt_L(v_2)$ de $v_2\in\mathbb{Z}_{p^s}^{\beta}$ nın Lee ağırlığını göstersin. $v=(v_1,v_2)\in\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ nın ağırlığı, $wt(v)=wt_L(v_1)+wt_L(v_2)$ biçiminde tanımlanır. Ayrıca, $u,v\in\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ elemanları

arasındaki uzaklık da $d(u,v)=wt(u-v)$ olarak tanımlanır. Her zaman olduğu gibi $d(C)$, C nin kodsözleri arasındaki minimum uzaklıktır.

Teorem 4.16 Eğer C, $(\alpha,\beta;k_0,k_1,\ldots,k_{r-1};l_0,l_1,\ldots,l_{s-1})$ tipinde bir $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$toplamsal kod ise C üzerinde aşağıdaki sınırlar mevcuttur.

$$\frac{d(C)-1}{p^{r+s-2}}\le\frac{\alpha}{p^{s-1}}+\frac{\beta}{p^{r-1}}-\frac{\left[rk_0+(r-1)k_1+\cdots+k_{r-1}+sl_0+(s-1)l_1+\cdots+l_{s-1}\right]}{p^{r+s-2}} \tag{4.6}$$

$$\left\lfloor\frac{d(C)-1}{p^{r+s-2}}\right\rfloor\le\alpha+\beta-\left(k_0+k_1+\cdots+k_{r-1}+l_0+l_1+\cdots+l_{s-1}\right) \tag{4.7}$$

İspat: $\mathbb{F}_q$ cismi üzerindeki bir kod için Singleton sınırı (2.1) ile verilmişti. $\Phi(C)=\mathrm{C}$ koduna bu Singleton sınırı uygulanırsa,

$$d(C)\le n-\log_q^{|C|}+1\Rightarrow d(C)\le p^{r-1}\alpha+p^{s-1}\beta-\left[rk_0+(r-1)k_1+\cdots+k_{r-1}+sl_0+(s-1)l_1+\cdots+l_{s-1}\right]+1$$
$$\frac{d(C)-1}{p^{r+s-2}}\le\frac{\alpha}{p^{s-1}}+\frac{\beta}{p^{r-1}}-\frac{\left[rk_0+(r-1)k_1+\cdots+k_{r-1}+sl_0+(s-1)l_1+\cdots+l_{s-1}\right]}{p^{r+s-2}}$$

(4.6) sınırı elde edilir.

(4.7) sınırını elde etmek için aşağıdaki dönüşüm tanımlansın. $\forall x\in\mathbb{Z}_{p^r}^{\alpha}$ için,

$(\chi,I_d):\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}\to\mathbb{Z}_{p^s}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$, $\quad\chi(x)=p^{s-r}x$ biçiminde olsun. Buradan $d(C)\le d(\chi(C))$ olacağı açıktır. Ayrıca [25]'deki Teorem 4.3'den

$\left\lfloor\frac{d(C)-1}{p^{r+s-2}}\right\rfloor\le n-rank(C)$ dir. Bu iki sonuç kullanılarak

$\left\lfloor\frac{d(C)-1}{p^{r+s-2}}\right\rfloor\le\alpha+\beta-\left(k_0+k_1+\cdots+k_{r-1}+l_0+l_1+\cdots+l_{s-1}\right)$ bulunur. ■

Örnek 4.17 C, $(1,3;0,1;0,0,2)$ tipindeki $\mathbb{Z}_4\mathbb{Z}_8-$toplamsal kodu $G=\begin{bmatrix}2&0&0&4\\0&4&0&4\\0&0&4&4\end{bmatrix}$

üreteç matrisiyle verilsin. C kodu $2^1 2^2=8$ tane kodsöze sahiptir ve bunlar;

$\{(0,0,0,0),(2,0,0,4),(0,4,0,4),(0,0,4,4),(2,4,0,0),(2,0,4,4),(0,4,4,0),(2,4,4,4)\}$ dır. Bu kodsözler arasında sıfırdan farklı en küçük ağırlığa sahip elemanın ağırlığı 6 olduğundan $d(C)=6$ dır. Böylece C koduna (4.7)'deki sınır uygulanırsa,

$\left\lfloor \frac{6-1}{2^{2+3-2}} \right\rfloor \leq 1+3-(0+1+0+0+2) \Rightarrow 0<1$ elde edilir.

Aşağıda $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ −toplamsal kodlar içerisinde (4.6) sınırındaki eşitliği sağlayan bir kod ailesinin özelliklerini veren bir önerme verilecektir.

Önerme 4.18 C, $\left[\begin{array}{cc} p^{r-1} & p^{2r-1} \end{array}\right]$ üreteç matrisine sahip $\mathbb{Z}_{p^r}\mathbb{Z}_{p^{2r}}$ − toplamsal kod olsun. Bu durumda C toplamsal kodu (4.6) sınırındaki eşitliği sağlar.

İspat: C nin üreteç matrisi $\left[\begin{array}{cc} p^{r-1} & p^{2r-1} \end{array}\right]$ formunda olduğundan C toplamsal kodu,

$(1,1;\ 0,\ldots,0,1;0,\ldots,0)$ tipindedir. Ayrıca $d(C)=p^{r-1}+p^{2r-1}$ olduğu da açıktır. Bu koda (4.6) sınırı uygulanırsa,

$$\frac{p^{r-1}+p^{2r-1}-1}{p^{3r-2}} \leq \frac{1}{p^{2r-1}}+\frac{1}{p^{r-1}}-\frac{1}{p^{3r-2}}$$

$\frac{p^{r-1}+p^{2r-1}-1}{p^{3r-2}} = \frac{p^{r-1}+p^{2r-1}-1}{p^{3r-2}}$ eşitliği bulunur. ■

Örnek 4.19 C, $\mathbb{Z}_9\mathbb{Z}_{81}$ − toplamsal kodu için üreteç matrisi $G=\left[\begin{array}{cc} 3 & 27 \end{array}\right]$ ile verilsin. Bu durumda, $p=3, r=2, s=4$ ve $d(C)=30$ olup C toplamsal kodu (4.6) sınırındaki eşitliği sağlar.

BÖLÜM 5

$\mathbb{Z}_2\mathbb{Z}_2[u]-$LİNEER KODLAR

Bu bölümde $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodların farklı yönden bir genelleştirilmesi olan $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$lineer kodlar tanımlanıp bu kodların cebirsel yapısı hakkında bilgi veren üreteç ve kontrol matrislerinin hangi formlarda oldukları belirlenecektir. Bu lineer kod ailesi $\mathbb{Z}_2\mathbb{Z}_2[u]$ sembolüyle gösterilecektir.

$\mathbb{Z}_4$ dört elemanlı bir halkadır. $\mathbb{Z}_4$ den farklı olarak dört elemanlı önemli diğer bir halka da $u^2=0$ olmak üzere $\mathbb{Z}_2+u\mathbb{Z}_2=\{0,1,u,1+u\}$ halkasıdır. Bu halka R sembolüyle gösterilirse, $R=\mathbb{Z}_2+u\mathbb{Z}_2$ halkası ya da kısaca $R=\mathbb{Z}_2[u]$ halkası için toplama ve çarpma tablosu aşağıdaki biçimde verilebilir.

Çizelge 5.1 $\mathbb{Z}_2+u\mathbb{Z}_2$ halkası için toplama ve çarpma tablosu

$+$	0	1	u	$1+u$
0	0	1	u	$1+u$
1	1	0	$1+u$	u
u	u	$1+u$	0	1
$1+u$	$1+u$	u	1	0

$\times$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

R halkası üzerindeki bir C lineer kodunun $G=\begin{bmatrix} I_{k_1} & A & B_1+uB_2 \\ 0 & uI_{k_2} & uD \end{bmatrix}$ formunda standart haldeki üreteç matrisine sahip olduğu iyi bilinen bir sonuçtur [27]. Burada, A, B_1, B_2 ve D matrisleri $\mathbb{Z}_2$ üzerinde matrislerdir.

Örnek 5.1 R üzerindeki 4 uzunluklu C lineer kodu $G=\begin{bmatrix} 1 & u & 1+u & 0 \\ u & u & 0 & u \end{bmatrix}$ üreteç matrisiyle verilmiş olsun. G matrisinin standart formu $\begin{bmatrix} 1 & 0 & 1 & u \\ 0 & u & u & u \end{bmatrix}$ biçimindedir.

Ayrıca

$C=\{(0,0,0,0),(1,0,1,u),(u,0,u,0),(1+u,0,1+u,u),(0,u,u,u),(1,u,1+u,0),(u,u,0,u),(1+u,u,1,0)\}$ kodsözlerine sahiptir.

$\mathbb{Z}_2$ nin R halkasının bir alt halkası olduğu açıktır. Şimdi aşağıdaki kümeyi tanımlayalım;

$\mathbb{Z}_2\mathbb{Z}_2[u]=\{(a,b)\mid a\in\mathbb{Z}_2 \text{ ve } b\in R\}$.

Yukarıdaki Cayley tablosundan da görüleceği gibi bu halka bilinen çarpma işlemi altında R halkasındaki u elemanına göre kapalı değildir. Dolayısıyla standart çarpma işlemine göre bir $R-$modül değildir. Bu halkanın daha iyi bir cebirsel yapıya sahip olması ve bir $R-$modül olması için yeni bir çarpma işlemi tanımlanmalıdır.

Tanım 5.2 $\begin{matrix}\eta: R\to\mathbb{Z}_2 \\ \eta(r+uq)=r\end{matrix}$ dönüşümü, $\eta(0)=0, \eta(1)=1, \eta(u)=0$ ve $\eta(1+u)=1$ olarak tanımlansın. Bu dönüşümün bir halka homomorfizması olduğu kolaylıkla gösterilebilir. η dönüşümü yardımıyla skaler çarpma işlemi aşağıdaki gibi tanımlanır.

Herhangi bir $d\in R$ ve $v=(a_0,a_1,\ldots,a_{\alpha-1},b_0,b_1,\ldots,b_{\beta-1})\in\mathbb{Z}_2^{\alpha}\times\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)^{\beta}$ için

$$dv=\left(\eta(d)a_0,\eta(d)a_1,\ldots,\eta(d)a_{\alpha-1},db_0,db_1,\ldots,db_{\beta-1}\right). \qquad (*)$$

Önerme 5.3 $(*)$ ile tanımlanan çarpma işlemi altında $\mathbb{Z}_2^{\alpha}\times R^{\beta}$ halkası bir $R-$modüldür.

İspat: $\mathbb{Z}_2^{\alpha}\times R^{\beta}=M$ diyelim. M değişmeli bir grup olduğundan $\forall r_1, r_2\in R$ ve

$m_1 = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}), m_2 = (\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{\alpha-1}, \tilde{b}_0, \tilde{b}_1, \ldots, \tilde{b}_{\beta-1}) \in M$ için

$\mu : R \times M \to M$
$(r, m) \to rm$ dönüşümü yardımıyla M nin bir sol $R-$modül olduğunu gösterelim.

i) $r(m_1 + m_2) = r\left(a_0 + \tilde{a}_0, a_1 + \tilde{a}_1, \ldots, a_{\alpha-1} + \tilde{a}_{\alpha-1}, b_0 + \tilde{b}_0, b_1 + \tilde{b}_1, \ldots, b_{\beta-1} + \tilde{b}_{\beta-1}\right)$

$= \left(\eta(r)(a_0 + \tilde{a}_0), \eta(r)(a_1 + \tilde{a}_1), \ldots, \eta(r)(a_{\alpha-1} + \tilde{a}_{\alpha-1}), r(b_0 + \tilde{b}_0), r(b_1 + \tilde{b}_1), \ldots, r(b_{\beta-1} + \tilde{b}_{\beta-1})\right)$
$= \left(\eta(r)a_0, \eta(r)a_1, \ldots, \eta(r)a_{\alpha-1}, rb_0, rb_1, \ldots, rb_{\beta-1}\right) + \left(\eta(r)\tilde{a}_0, \eta(r)\tilde{a}_1, \ldots, \eta(r)\tilde{a}_{\alpha-1}, r\tilde{b}_0, r\tilde{b}_1, \ldots, \tilde{r}b_{\beta-1}\right)$
$= rm_1 + rm_2$

ii) $(r_1 + r_2)m_1 = \left(\eta(r_1 + r_2)a_0, \ldots, \eta(r_1 + r_2)a_{\alpha-1}, (r_1 + r_2)b_0, \ldots, (r_1 + r_2)b_{\beta-1}\right)$

η bir halka homomorfizması olduğundan $\eta(r_1 + r_2) = \eta(r_1) + \eta(r_2)$ ve buradan da

$(r_1 + r_2)m_1 = \left((\eta(r_1) + \eta(r_2))a_0, \ldots, (\eta(r_1) + \eta(r_2))a_{\alpha-1}, r_1b_0 + r_2b_0, \ldots, r_1b_{\beta-1} + r_2b_{\beta-1}\right)$

$= \left(\eta(r_1)a_0, \ldots, \eta(r_1)a_{\alpha-1}, r_1b_0, \ldots, r_1b_{\beta-1}\right) + \left(\eta(r_2)a_0, \ldots, \eta(r_2)a_{\alpha-1}, r_2b_0, \ldots, r_2b_{\beta-1}\right)$

$= r_1m_1 + r_2m_1$

iii)

$r_1(r_2m_1) = r_1\left(\eta(r_2)a_0, \ldots, \eta(r_2)a_{\alpha-1}, r_2b_0, \ldots, r_2b_{\beta-1}\right) = \left(\eta(r_1)\eta(r_2)a_0, \ldots, \eta(r_1)\eta(r_2)a_{\alpha-1}, r_1r_2b_0, \ldots, r_1r_2b_{\beta-1}\right)$
ve yine η nın bir halka homomorfizması olması kullanılarak, $\eta(r_1)\eta(r_2) = \eta(r_1r_2)$ ve böylece $r_1(r_2m_1) = \left(\eta(r_1r_2)a_0, \ldots, \eta(r_1r_2)a_{\alpha-1}, r_1r_2b_0, \ldots, r_1r_2b_{\beta-1}\right) = (r_1r_2)m_1$ bulunur.

iv) $\eta(1) = 1$ olarak tanımlandığından $1m = m$ olacağı açıktır.

Sonuç olarak M bir $R-$modüldür. ■

Tanım 5.4 Eğer bir C lineer kodu $(*)$ ile tanımlanan skaler çarpma işlemine göre $\mathbb{Z}_2^{\alpha} \times \left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)^{\beta}$ nın bir $\mathbb{Z}_2 + u\mathbb{Z}_2 -$alt modülü ise C ye $\mathbb{Z}_2\mathbb{Z}_2[u] -$ ***lineer kod*** denir.

$\mathbb{Z}_2\mathbb{Z}_4 -$toplamsal kodlar için $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ nın alt gruplarıyla $\mathbb{Z}_4 -$alt modülleri aynı olduklarından $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ nın boştan farklı bir C alt grubuna($\mathbb{Z}_4 -$alt modülüne) $\mathbb{Z}_2\mathbb{Z}_4 -$toplamsal kod denmişti. Ancak $\mathbb{Z}_2^{\alpha} \times R^{\beta}$ nın alt gruplarıyla $R -$alt modülleri birbirlerinden farklıdırlar. $\mathbb{Z}_2^{\alpha} \times R^{\beta}$ nın bütün alt grupları yalnızca toplama işlemine

göre kapalı iken R nin elemanlarıyla çarpma işlemine göre de kapalı olan alt grupları ise alt modülleridir. Bu yüzden bu kodlara $\mathbb{Z}_2\mathbb{Z}_4$ durumundaki gibi toplamsal değil de $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod denilmesi daha uygun olacaktır.

$\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodlar, eğer $\alpha=0$ ise ikili kodlara, eğer $\beta=0$ ise $R=\mathbb{Z}_2+u\mathbb{Z}_2$ üzerindeki lineer kodlara dönüşürler.

C bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod olsun. C, $\mathbb{Z}_2^{\alpha}\times R^{\beta}$ nın bir alt grubu olacağından $\mathbb{Z}_2^{k_0}\times\mathbb{Z}_2^{2k_1}\times\mathbb{Z}_2^{k_2}$ gibi değişmeli bir gruba izomorftur.

Şimdi, C nin C_{β}^{F} alt modülü, $C_{\beta}^{F}=\left\{(a,b)\in\mathbb{Z}_2^{\alpha}\times R^{\beta}\mid b,\ R \text{ üzerinde serbest}\right\}$ ve bu alt modülün boyutu da k_1 olsun. Ayrıca,

$C_0=\left\{(a,b)\in\mathbb{Z}_2^{\alpha}\times R^{\beta}\mid a\neq 0\right\}\subseteq C\setminus C_{\beta}^{F}$ ve $C_2=\left\{(a,b)\in\mathbb{Z}_2^{\alpha}\times R^{\beta}\mid a=0\right\}\subseteq C\setminus C_{\beta}^{F}$ olmak üzere $D=C\setminus C_{\beta}^{F}=C_0\oplus C_2$ olsun. C_0 ve C_2 nin boyutları sırasıyla k_0 ve k_2 ile gösterilsin.

Böylece,

- C nin eleman sayısı $2^{k_0}2^{2k_1}2^{k_2}=2^{k_0+2k_1+k_2}$ dir.

Bütün bu parametreler göz önünde bulundurulursa böyle bir C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer koduna $(\alpha,\beta;k_0,k_1,k_2)$ tipindedir denir.

Tanım 5.5 $\phi:R\to\mathbb{Z}_2^2$ dönüşümü; $\phi(0)=(0,0),\phi(1)=(0,1),\phi(u)=(1,1)$ ve $\phi(1+u)=(1,0)$ biçiminde tanımlansın. Yani ϕ fonksiyonu R üzerindeki lineer kodları $\mathbb{Z}_2$ üzerinde ikili kodlara taşısın. Bu dönüşüm $\mathbb{Z}_2^{\alpha}\times R^{\beta}$ üzerine aşağıdaki gibi genişletilebilir.

Her $a=(a_0,a_1,\ldots,a_{\alpha-1})\in\mathbb{Z}_2^{\alpha}$ ve her $b=(b_0,b_1,\ldots,b_{\beta-1})\in R^{\beta}$ için

$\Phi:\mathbb{Z}_2^{\alpha}\times R^{\beta}\to\mathbb{Z}_2^{n}$, $\Phi(a,b)=\left(a_0,a_1,\ldots,a_{\alpha-1},\phi(b_0),\phi(b_1),\ldots,\phi(b_{\beta-1})\right)$ ve $n=\alpha+2\beta$ biçimindedir. Buradan C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodunun $\Phi(C)=\mathrm{C}$ ikili görüntüsü de lineerdir. Bölüm 5.4'de Φ altındaki ikili görüntüsü optimal kod olan $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod örnekleri verilecektir.

Örnek 5.6 C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu $G=\left[\begin{array}{cc|ccc} 1 & 0 & 0 & u & u \\ \hline 0 & 1 & 1 & u & 1+u \\ 0 & 0 & 0 & u & u \end{array}\right]$ matrisiyle üretilmiş olsun. Buradan,

$$C=\{(0,0\,|\,0,0,0),(1,0\,|\,0,u,u),(0,1|1,u,1+u),(0,0\,|\,0,u,u),(0,0\,|\,u,0,u),(0,1|1+u,u,1)$$
$$(1,1|1,0,1),(0,1|1,0,1),(1,0\,|\,0,0,0),(1,0\,|\,u,u,0),(0,0\,|\,u,u,0),(1,1|1,u,1+u),(1,1|1+u,0,1+u),$$
$$(0,1|1+u,0,1+u),(1,0\,|\,u,0,u),(1,1|1+u,u,1)\}$$

$\alpha=2,\beta=3,k_0=1,k_1=1$ ve $k_2=1$ olup

- C lineer kodu $(2,3;1,1,1)$ tipindedir.
- C nin eleman sayısı, $|C|=2^{k_0}2^{2k_1}2^{k_2}=2^{1+2+1}=16$ dır.

5.1 $\mathbb{Z}_2\mathbb{Z}_2[u]-$Lineer Kodların Üreteç Matrislerinin Standart Formu

Bu bölümde $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodların üreteç matrislerinin standart halinin hangi formda olduğu belirlenecektir. Bir C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu herhangi formda bir üreteç matrisine sahipse bu matris standart forma getirilebilir. Standart formdaki bu matris yardımıyla C kodunun tipi ve eleman sayısı kolaylıkla söylenebilir.

Teorem 5.7 C, $(\alpha,\beta;k_0,k_1,k_2)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod olsun. C kodu, üreteç matrisinin standart hali aşağıdaki gibi verilen $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer koda permütasyon denktir.

$$G_s=\begin{bmatrix} I_{k_0} & A_1 & 0 & 0 & uT \\ 0 & S & I_{k_1} & A & B_1+uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \end{bmatrix} \qquad (5.1)$$

Burada; A, A_1, B_1, B_2, D, S ve T matrisleri $\mathbb{Z}_2$ üzerindeki matrislerdir.

İspat: C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodunun $\mathbb{Z}_2$ de olmayan son β kısmı $\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)^{\beta}$ üzerinde lineer bir kod olduğundan C nin üreteç matrisi; $i\in\{1,2,3,4\}$ için S_i ler $\mathbb{Z}_2$ üzerindeki matrisler olmak üzere

$\underbrace{\begin{bmatrix} S_1 & S_2 \\ S_3 & S_4 \end{bmatrix}}_{\alpha} \underbrace{\begin{bmatrix} I_{k_1} & R & T_1+uT_2 \\ 0 & uI_k & uZ \end{bmatrix}}_{\beta}$ formunda yazılabilir. Bu matrisin serbest olmayan, yani

$\begin{bmatrix} S_3 & S_4 & 0 & uI_k & uZ \end{bmatrix}$ kısmı yeniden düzenlenerek iki satırda ifade edilirse,

$\underbrace{\begin{bmatrix} S_1 & S_2 \\ S_{31} & S_{41} \\ 0 & 0 \end{bmatrix}}_{\alpha} \underbrace{\begin{bmatrix} I_{k_1} & R & T_1+uT_2 \\ 0 & uI_r & uN \\ 0 & uI_{k_2} & uD \end{bmatrix}}_{\beta}$ matrisi bulunur. Bu matrisin ikili kısmında gerekli satır

işlemleri yapılarak I_{k_0} boyutunda bir birim matris elde edilir. Böylece,

$\underbrace{\begin{bmatrix} S_1 & S_2 \\ I_{k_0} & E_1 \\ 0 & 0 \end{bmatrix}}_{\alpha} \underbrace{\begin{bmatrix} I_{k_1} & A' & B_1'+uB_2' \\ 0 & uE_2 & uE_3 \\ 0 & uI_{k_2} & uD \end{bmatrix}}_{\beta}$ matrisi bulunur. Buradan, bu matris üzerindeki I_{k_0}

birim matrisi kullanılarak S_1 matrisi, uI_{k_2} birim matrisi kullanılarak da uE_2 matrisi sıfır yapılabilir. Sonuç olarak bulunan $\underbrace{\begin{bmatrix} 0 & S_2 \\ I_{k_0} & E_1 \\ 0 & 0 \end{bmatrix}}_{\alpha} \underbrace{\begin{bmatrix} I_{k_1} & A' & B_1'+uB_2' \\ 0 & 0 & uE_3 \\ 0 & uI_{k_2} & uD \end{bmatrix}}_{\beta}$ matrisi C,

$\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu için bir üreteç matristir ve bu matris standart formdadır. ■

Örnek 5.8 C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu $\alpha=3=\beta$ için $G=\begin{bmatrix} 1 & 0 & 1 & 1+u & 1+u & 0 \\ 1 & 1 & 0 & u & 0 & u \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & u & u & 1+u \\ 1 & 1 & 0 & 0 & u & u \end{bmatrix}$

üreteç matrisiyle verilsin. G matrisini standart hale getirip C lineer kodunun tipini belirleyelim.

$$\begin{bmatrix} 1 & 0 & 1 & 1+u & 1+u & 0 \\ 1 & 1 & 0 & u & 0 & u \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & u & u & 1+u \\ 1 & 1 & 0 & 0 & u & u \end{bmatrix} \overset{H_{13}(1+u)}{\underset{H_{43}(u)}{\sim}} \begin{bmatrix} 1 & 1 & 0 & 0 & u & u \\ 1 & 1 & 0 & u & 0 & u \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & 0 & 0 & 1+u \\ 1 & 1 & 0 & 0 & u & u \end{bmatrix} \overset{H_{52}(1)}{\sim}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & u & u \\ 1 & 1 & 0 & u & 0 & u \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & 0 & 0 & 1+u \\ 0 & 0 & 0 & u & u & 0 \end{bmatrix} \overset{H_{53}(u)}{\sim} \begin{bmatrix} 1 & 1 & 0 & 0 & u & u \\ 1 & 1 & 0 & u & 0 & u \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & 0 & 0 & 1+u \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \overset{H_{53}(u)}{\sim}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & u & u \\ 1 & 1 & 0 & u & 0 & u \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & 0 & 0 & 1+u \end{bmatrix} \overset{H_{21}(1)}{\sim} \begin{bmatrix} 1 & 1 & 0 & 0 & u & u \\ 0 & 0 & 0 & u & u & 0 \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & 0 & 0 & 1+u \end{bmatrix} \overset{H_{23}(u)}{\sim}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & u & u \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & 0 & 0 & 1+u \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 0 & u & u \\ 0 & 1 & 1 & 1 & 1+u & u \\ 0 & 1 & 0 & 0 & 0 & 1+u \end{bmatrix} \overset{\substack{H_{13}(u) \\ H_{23}(u)}}{\sim}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & u & 0 \\ 0 & 1 & 1 & 1 & 1+u & 0 \\ 0 & 1 & 0 & 0 & 0 & 1+u \end{bmatrix} \overset{H_3(1+u)}{\sim} \begin{bmatrix} 1 & 1 & 0 & 0 & u & 0 \\ 0 & 1 & 1 & 1 & 1+u & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \overset{K_5 \leftrightarrow K_6}{\sim}$$

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & u \\ 0 & 1 & 1 & 1 & 0 & 1+u \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

$$\begin{matrix} 1 & 2 & 3 & 4 & 6 & 5 \end{matrix}$$

Böylece G matrisinin standart formu;

$$G_s = \underbrace{\left[\begin{array}{c|cc|cc|c} 1 & 1 & 0 & 0 & 0 & u \\ \hline 0 & 1 & 1 & 1 & 0 & 1+u \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right]}_{3} \underbrace{\phantom{\left[\begin{array}{c|cc|cc|c} 1 & 1 & 0 & 0 & 0 & u \\ \hline 0 & 1 & 1 & 1 & 0 & 1+u \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right]}}_{3} = \begin{bmatrix} I_1 & A_1 & 0 & uT \\ 0 & S & I_2 & B_1 + uB_2 \end{bmatrix} \tag{5.2}$$

biçimindedir. Ancak bu matris C kodunun değil bu koda permütasyon denk olan başka bir C', $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodunun standart formdaki üreteç matrisidir. Denk kodların parametreleri aynı olacağından,

- $k_0 = 1, k_1 = 2$ ve $k_2 = 0$ dır.
- C lineer kodu $(3,3;1,2,0)$ tipindedir.

- C lineer kodu $|C|=2^1 2^{2.2}=32$ adet kodsöze sahiptir.

denir.

5.2 $\mathbb{Z}_2\mathbb{Z}_2[u]-$ Lineer Kodların Dual Uzayı

Bu bölümde $\mathbb{Z}_2\mathbb{Z}_2[u]-$ lineer kodların dual uzayının yapısı incelenecektir.

Tanım 5.9 $\mathbb{Z}_2^{\alpha}\times\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)^{\beta}$ üzerindeki herhangi iki v,w elemanının iç çarpımı

$$\langle v,w\rangle = u\left(\sum_{i=1}^{\alpha} v_i w_i\right)+\sum_{j=\alpha+1}^{\alpha+\beta} v_j w_j \in \mathbb{Z}_2+u\mathbb{Z}_2$$

biçiminde tanımlanır. Örneğin,

$v=(1,0\,|\,1+u,u,0), w=(1,1\,|\,1+u,1+u,u)\in\mathbb{Z}_2^2\times\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)^3$ vektörlerinin iç çarpımı,

$\langle v,w\rangle = u(1.1+0.1)+\left[(1+u)(1+u)+u(1+u)+0.u\right]=u+\left[1+u+0\right]=1$ dir.

Tanım 5.10 C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$ lineer kodunun duali, $C^{\perp}$ sembolüyle gösterilir ve

$$C^{\perp}=\left\{w\in\mathbb{Z}_2^{\alpha}\times\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)^{\beta}\,|\,\langle v,w\rangle=0\ ,\forall v\in C\right\}$$

biçiminde tanımlanır.

$C^{\perp}$ dual kodunun $\mathbb{Z}_2^{\alpha}\times\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)^{\beta}$ nın bir $\mathbb{Z}_2+u\mathbb{Z}_2-$ alt modülü olduğu kolaylıkla gösterilebilir. Böylece $C^{\perp}$ de bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$ lineer koddur.

Bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$ lineer kodun dualini oluşturmak için kullanılacak bazı dönüşümler aşağıdaki gibi tanımlanacaktır.

- $\chi:\mathbb{Z}_2\to\mathbb{Z}_2+u\mathbb{Z}_2$, $\chi(0)=0$ ve $\chi(1)=u$.
- $\psi:\mathbb{Z}_2+u\mathbb{Z}_2\to\mathbb{Z}_2$, $\forall x\in\mathbb{Z}_2+u\mathbb{Z}_2$ için $\psi(x)=\begin{cases}0, & x\in\{0,u\}\\ 1, & x\in\{1,1+u\}\end{cases}$.
- $\iota:\mathbb{Z}_2\to\mathbb{Z}_2+u\mathbb{Z}_2$, $\iota(0)=0$ ve $\iota(1)=1$.

Bu dönüşümlerin genişletilmiş halleri de aynı sembollerle gösterilirse,

$(\chi, I_d): \mathbb{Z}_2^\alpha \times R^\beta \to R^\alpha \times R^\beta$, $(\psi, I_d): R^\alpha \times R^\beta \to \mathbb{Z}_2^\alpha \times R^\beta$, $(\iota, I_d): \mathbb{Z}_2^\alpha \times R^\beta \to R^\alpha \times R^\beta$ elde edilir.

Bu dönüşümler ile ilgili olarak aşağıdaki önermeler verilecektir. Bu sonuçlar C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodunun kontrol matrisinin standart formunun belirlenmesinde kullanılacaktır.

Önerme 5.11 $v \in \mathbb{Z}_2^\alpha \times (\mathbb{Z}_2 + u\mathbb{Z}_2)^\beta$ ve $w \in (\mathbb{Z}_2 + u\mathbb{Z}_2)^{\alpha+\beta}$ için $\langle \chi(v), w \rangle_u = \langle v, \psi(w) \rangle$ dir. Buradaki $\langle , \rangle_u$ $\mathbb{Z}_2 + u\mathbb{Z}_2$ üzerindeki standart iç çarpımı göstermektedir.

İspat: $u \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_{2^s}^\beta$ ve $v \in \mathbb{Z}_{2^s}^{\alpha+\beta}$ olmak üzere

$\langle \chi(v), w \rangle_u = \sum_{i=1}^{\alpha} (uv_i) w_i + \sum_{j=i+1}^{\alpha+\beta} v_j w_j = \sum_{i=1}^{\alpha} uv_i (w_i \bmod u) + \sum_{j=i+1}^{\alpha+\beta} v_j w_j = \langle v, \psi(w) \rangle$ dir. ■

Örneğin, $v = (1,0 \mid 0,1+u,1) \in \mathbb{Z}_2^2 \times (\mathbb{Z}_2 + u\mathbb{Z}_2)^3$ ve $w = (1,1+u \mid 1+u,u,1) \in (\mathbb{Z}_2 + u\mathbb{Z}_2)^5$ için

$\langle \chi(v), w \rangle_u = \langle (u,0 \mid 0,1+u,1), (1,1+u \mid 1+u,u,1) \rangle_u = u+u+u^2+1 = 1$

$\langle v, \psi(w) \rangle = \langle (1,0 \mid 0,1+u,1), (1,1 \mid 1+u,u,1) \rangle = u(1+0)+u+u^2+1 = 1$ eşitliği bulunur.

Sonuç 5.12 Eğer $u, v \in \mathbb{Z}_2^\alpha \times (\mathbb{Z}_2 + u\mathbb{Z}_2)^\beta$ ise $\langle \chi(v), \iota(w) \rangle_u = \langle v, w \rangle$ dir.

İspat: Önerme 5.11'den $\langle \chi(v), \iota(w) \rangle_u = \langle v, \psi(\iota(w)) \rangle$ yazılabilir. Böylece, $\langle \chi(v), \iota(w) \rangle_u = \langle v, \psi(\iota(w)) \rangle = \langle v, w \rangle$ elde edilir. ■

Bu sonuca örnek olarak, $v = (1,1 \mid u,1,1+u), w = (1,0 \mid 1,0,1+u) \in \mathbb{Z}_2^2 \times (\mathbb{Z}_2 + u\mathbb{Z}_2)^3$ olsun.

$\langle \chi(v), \iota(w) \rangle_u = \langle (u,u \mid u,1,1+u), (1,0 \mid 1,0,1+u) \rangle = u+0+u+0+1+u^2 = 1$

$\langle v, w \rangle = \langle (1,1 \mid u,1,1+u), (1,0 \mid 1,0,1+u) \rangle = u(1+0)+u+0+1+u^2 = 1$

Önerme 5.13 $C, (\alpha, \beta; k_0, k_1, k_2)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod olsun. C nin duali, $C^\perp = \psi(\chi(C)^\perp)$ eşitliği ile elde edilir.

İspat: Eşitliği elde etmek için çift taraflı kapsamayı gösterelim. $w \in C^{\perp}$ olsun. O halde her $v \in C$ için $\langle v, w \rangle = 0$ olacaktır. Sonuç 5.12 yardımıyla, $\langle v, w \rangle = \langle \chi(v), \imath(w) \rangle_u$ yazılabilir. Böylece, $\langle \chi(v), \imath(w) \rangle_u = 0$ ve $\psi(\imath(w)) = w \in \psi(\chi(C^{\perp}))$ olacağından $C^{\perp} \subseteq \psi(\chi(C)^{\perp})$ dir.

Şimdi de $w \in \chi(C)^{\perp}$ alalım. Buradan her $v \in C$ için $\langle \chi(v), w \rangle_u = 0$ dır.

Önerme 5.11'den $\langle \chi(v), w \rangle_u = \langle v, \psi(w) \rangle = 0$ olur ve böylece $\psi(\chi(C)^{\perp}) \subseteq C^{\perp}$ elde edilir.

O halde $C^{\perp} = \psi(\chi(C)^{\perp})$ bulunur. ■

5.3 $\mathbb{Z}_2\mathbb{Z}_2[u]-$ Lineer Kodların Kontrol Matrislerinin Standart Formu

Bu bölümde bir C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodunun dual uzayını üreten ve C için kontrol matrisi olan matrisin standart olarak hangi formda olduğu belirlenecektir.

Teorem 5.14 $(\alpha, \beta; k_0, k_1, k_2)$ tipindeki C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu (5.1)'deki standart formdaki üreteç matrisine sahip olsun. Buradan $C^{\perp}$ lineer dual kodunun standart formdaki üreteç matrisi (C kodunun kontrol matrisi) aşağıdaki matrisle verilir.

$$H_s = \begin{bmatrix} -A_1^t & I_{\alpha-k_0} & -uS^t & 0 & 0 \\ -T^t & 0 & -(B_1 + uB_2)^t + D^t A^t & -D^t & I_{\beta-k_1-k_2} \\ 0 & 0 & -uA^t & uI_{k_2} & 0 \end{bmatrix} \tag{5.3}$$

İspat: H_s nin C kodu için kontrol matrisi olduğu, doğrudan $H_s G_s^t = 0$ olduğu ve H_s nin $C^{\perp}$ dual uzayının tümünü gerdiği gösterilerek ispatlanabilir. Ancak burada $C^{\perp} = \psi(\chi(C)^{\perp})$ olması gerçeği kullanılacaktır.

C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu $G_s = \begin{bmatrix} I_{k_0} & A_1 & 0 & 0 & uT \\ 0 & S & I_{k_1} & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \end{bmatrix}$ standart haldeki üreteç matrisine sahip olsun. Yukarıda tanımlanan χ dönüşümü yardımıyla, $\chi(C)$ kodunun

$G_{\chi(C)} = \begin{bmatrix} uI_{k_0} & uA_1 & 0 & 0 & uT \\ 0 & uS & I_{k_1} & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \end{bmatrix}$ üreteç matrisine sahip olacağı söylenebilir.

$\chi(C)$ kodu $\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)^{\alpha+\beta}$ üzerinde lineer bir koddur. Ayrıca $\mathbb{Z}_2 + u\mathbb{Z}_2$ üzerindeki lineer bir kod $\begin{bmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{bmatrix}$ standart haldeki üreteç matrisiyle verildiğinden $G_{\chi(C)}$ matrisini de bu forma getirilebilir.

$$\begin{bmatrix} uI_{k_0} & uA_1 & 0 & 0 & uT \\ 0 & uS & I_{k_1} & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \end{bmatrix} \overset{H_1 \leftrightarrow H_2}{\sim} \begin{bmatrix} 0 & uS & I_{k_1} & A & B_1 + uB_2 \\ uI_{k_0} & uA_1 & 0 & 0 & uT \\ 0 & 0 & 0 & uI_{k_2} & uD \end{bmatrix} \overset{H_2 \leftrightarrow H_3}{\sim}$$

$$\begin{bmatrix} 0 & uS & I_{k_1} & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \\ uI_{k_0} & uA_1 & 0 & 0 & uT \end{bmatrix} \overset{K_2 \leftrightarrow K_3}{\sim} \begin{bmatrix} 0 & I_{k_1} & uS & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \\ uI_{k_0} & 0 & uA_1 & 0 & uT \end{bmatrix} \overset{K_1 \leftrightarrow K_2}{\sim}$$

$$\begin{bmatrix} I_{k_1} & 0 & uS & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \\ 0 & uI_{k_0} & uA_1 & 0 & uT \end{bmatrix} \overset{K_3 \leftrightarrow K_4}{\sim} \begin{bmatrix} I_{k_1} & 0 & A & uS & B_1 + uB_2 \\ 0 & 0 & uI_{k_2} & 0 & uD \\ 0 & uI_{k_0} & 0 & uA_1 & uT \end{bmatrix} \overset{K_2 \leftrightarrow K_3}{\sim}$$

$\begin{bmatrix} I_{k_1} & A & 0 & uS & B_1 + uB_2 \\ 0 & uI_{k_2} & 0 & 0 & uD \\ 0 & 0 & uI_{k_0} & uA_1 & uT \end{bmatrix} = \tilde{G}_{\chi(C)}$ olsun. Bu matriste $u\tilde{I}_{\tilde{k}_2} = \begin{bmatrix} uI_{k_2} & 0 \\ 0 & uI_{k_0} \end{bmatrix}$,

3 4 1 2 5

$\tilde{A} = \begin{bmatrix} A & 0 \end{bmatrix}$, $\left(\tilde{B}_1 + u\tilde{B}_2\right) = \begin{bmatrix} uS & B_1 + uB_2 \end{bmatrix}$ ve $u\tilde{D} = \begin{bmatrix} 0 & uD \\ uA_1 & uT \end{bmatrix}$ diyelim. Böylece, $\tilde{G}_{\chi(C)}$ matrisi $\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)^{\alpha+\beta}$ üzerinde $\begin{bmatrix} I_{k_1} & \tilde{A} & \left(\tilde{B}_1 + u\tilde{B}_2\right) \\ 0 & u\tilde{I}_{\tilde{k}_2} & u\tilde{D} \end{bmatrix}$ standart formunda yazılmış oldu. Böyle bir matrisin kontrol matrisi aşağıdaki gibi yazılabilir.

$\begin{bmatrix} -\left(\tilde{B}_1 + u\tilde{B}_2\right)^t + \tilde{D}^t\tilde{A}^t & -\tilde{D}^t & I_{\alpha+\beta-k_1-\tilde{k}_2} \\ -u\tilde{A}^t & u\tilde{I}_{\tilde{k}_2} & 0 \end{bmatrix}$. Böylece gerekli matrisler yerlerine yazılırsa,

$\chi(C)^{\perp}$ dual kodunun üreteç matrisi

$$\begin{bmatrix} -uS^t & 0 & -A_1^t & I_{\alpha+\beta-k_0-k_1-k_2} \\ -\left(B_1 + uB_2\right)^t + D^tA^t & -D^t & -T^t & 0 \\ -uA^t & uI_{k_2} & 0 & 0 \\ 0 & 0 & uI_{k_0} & 0 \end{bmatrix}$$

formunda elde edilir. Bu matris de

$$\begin{bmatrix} -uS^t & 0 & -A_1^t & I_{\alpha-k_0} & 0 \\ -\left(B_1 + uB_2\right)^t + D^tA^t & -D^t & -T^t & 0 & I_{\beta-k_1-k_2} \\ -uA^t & uI_{k_2} & 0 & 0 & 0 \\ 0 & 0 & uI_{k_0} & 0 & 0 \end{bmatrix}$$

biçiminde düzenlenebilir. Burada

daha önce uygulanan sütun permütasyonları geri alınırsa,

$$\tilde{H} = \left[\begin{array}{cc|ccc} -A_1^t & I_{\alpha-k_0} & -uS^t & 0 & 0 \\ -T^t & 0 & -\left(B_1 + uB_2\right)^t + D^tA^t & -D^t & I_{\beta-k_1-k_2} \\ 0 & 0 & -uA^t & uI_{k_2} & 0 \\ uI_{k_0} & 0 & 0 & 0 & 0 \end{array}\right]$$

matrisi $\chi(C)^{\perp}$ dual kodunun üreteç matrisidir. Son olarak Önerme 5.13 yardımıyla,

$$\psi(\tilde{H}) = \left[\begin{array}{cc|ccc} -A_1^t & I_{\alpha-k_0} & -uS^t & 0 & 0 \\ -T^t & 0 & -\left(B_1 + uB_2\right)^t + D^tA^t & -D^t & I_{\beta-k_1-k_2} \\ 0 & 0 & -uA^t & uI_{k_2} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] = H_s$$ elde edilir. ■

Sonuç 5.15 $(\alpha, \beta; k_0, k_1, k_2)$ tipindeki bir C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu için kontrol matrisinin standart formu yukarıdaki teoremle belirlenmişti. Bu kontrol matrisine dayanarak $C^{\perp}$ lineer dual kodunun tipi de söylenebilir. Eğer C, $(\alpha, \beta; k_0, k_1, k_2)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod ise $C^{\perp}$, $\left(\alpha, \beta; \alpha - k_0, \beta - k_1 - k_2, k_2\right)$ tipindedir.

Örnek 5.16 C', üreteç matrisinin standart formu (5.2) ile verilen $(3,3;1,2,0)$ tipindeki $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod olsun. Buradan Örnek 5.8'de verilen C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodunun kontrol matrisini bulup $C^{\perp}$ in tipini belirleyelim.

$$G_s=\underbrace{\begin{bmatrix}1&1&0\\0&1&1\\0&1&0\end{bmatrix}}_{3}\underbrace{\begin{bmatrix}0&0&u\\1&0&1+u\\0&1&0\end{bmatrix}}_{3}=\begin{bmatrix}I_1&A_1&0&uT\\0&S&I_2&B_1+uB_2\end{bmatrix}$$ idi. Yani,

$A_1=\begin{bmatrix}1&0\end{bmatrix}, T=\begin{bmatrix}1\end{bmatrix}, S=\begin{bmatrix}1&1\\1&0\end{bmatrix}$ ve $B_1+uB_2=\begin{bmatrix}1+u\\0\end{bmatrix}$ formundadırlar. Böylece,

$$\begin{bmatrix}-A_1^t & I_{\alpha-k_0} & -uS^t & 0 & 0\\ -T^t & 0 & -\left(B_1+uB_2\right)^t+D^tA^t & -D^t & I_{\beta-k_1-k_2}\\ 0 & 0 & -uA^t & uI_{k_2} & 0\end{bmatrix}=\begin{bmatrix}\boxed{\begin{matrix}1\\0\end{matrix}} & \boxed{\begin{matrix}1&0\\0&1\end{matrix}} & \boxed{\begin{matrix}-u&-u\\-u&0\end{matrix}} & 0\\ \boxed{1} & 0 & 0 & \boxed{-(1+u)} & 0 & \boxed{1}\end{bmatrix}$$

$$\begin{matrix}1 & 2 & 3 & 4 & 6 & 5\end{matrix}$$

matrisi C' lineer kodunun kontrol matrisidir. Bu yüzden bu matriste standart haldeki üreteç matrisine uygulanan sütun permütasyonu geri alınmalıdır. Yani beşinci ve altıncı sütunlar yer değiştirilmelidir. O halde C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodunun kontrol matrisi,

$H=\begin{bmatrix}1&1&0&-u&0&-u\\0&0&1&-u&0&0\\1&0&0&-(1+u)&1&0\end{bmatrix}$ biçimindedir. Bu matrise dayanarak $C^{\perp}$ lineer dual kodu için aşağıdakiler kolayca söylenebilir.

- $(3,3;2,1,0)$ tipindedir.
- $|C^{\perp}|=2^2.2^{2.1}=16$ adet kodsözü vardır.

Ayrıca $HG^t=0$ olduğu da gösterilebilir. Bu iki matrisi çarparken daha önce tanımlanan iç çarpım gereği ilk $\alpha=3$ sütun u ile çarpılmalıdır. Yani,

$$\begin{bmatrix} 1 & 1 & 0 & -u & 0 & -u \\ 0 & 0 & 1 & -u & 0 & 0 \\ 1 & 0 & 0 & -(1+u) & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1+u & u & 1 & u & 0 \\ 1+u & 0 & 1+u & u & u \\ 0 & u & u & 1+u & u \end{bmatrix}$$

$$= \begin{bmatrix} u-u-u^2 & u+u-u^2-u^2 & u-u-u^2 & u-u^2-u-u^2 & u+u-u^2 \\ u-u-u^2 & -u^2 & u-u & -u^2 & 0 \\ u-1+1+u & u-u+u^2 & -(1+u)+1+u & -u-u^2+u & u+u \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ elde edilir.}$$

5.4 $\mathbb{Z}_2\mathbb{Z}_2[u]-$ Lineer Kodların İkili Görüntüleri ve İyi Parametreli Kod Örnekleri

Bir C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu, Tanım 5.5 ile verilen Φ Gray dönüşümü yardımıyla $\mathbb{Z}_2$ üzerindeki ikili koda dönüştürülebilir. Bu dönüşüm, $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodlar üzerinde tanımlanan ve $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodları ikili kodlara dönüştüren Gray dönüşümden farklı olarak lineer bir dönüşümdür.

Tezin bu bölümünde Φ lineer dönüşümü kullanılarak görüntüsü optimal (iyi parametreli) kod olan ikili kod örnekleri verilecektir.

Eğer bir kodun minimum uzaklığı verilen bir uzunluk ve boyut için alabileceği mümkün en büyük değeri almışsa bu koda optimal ya da iyi parametreli (ya da uzaklık-optimal) kod denildiği tezin ilk bölümünde söylenmişti. Örneğin, $\mathbb{Z}_2$ üzerinde $n=189$ uzunluklu ve $k=47$ boyutlu bir lineer kod için minimum uzaklığın alabileceği en büyük değer $d=67$ dir. Yani $\mathbb{Z}_2$ üzerinde $[189,47,67]$ parametrelerine sahip bir kod optimal koddur.

Aşağıdaki örneklerdeki $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodların $\mathbb{Z}_2$ görüntüleri ve parametreleri Mathematica adlı bir programla hesaplanmıştır. İkili kodların parametrelerine göre sınıflandırılması, yani optimal kod olup olmadıkları http://www.codetables.de/ internet adresindeki kod tabloları esas alınarak yapılmıştır [28].

Örnek 5.17 C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu $(9,9;6,1,0)$ tipinde ve

$$\left[\begin{array}{ccccccccc|ccccccccc}
1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1+u & 1+u & 1+u & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & u & 0 & 0 & u & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & u & 0 & 0 & u & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & u & 0 & 0 & u & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & u & 0 & 0 & u & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & u & 0 & 0 & u & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & u & 0 & 0 & u
\end{array}\right]$$

üreteç matrisiyle verilsin. C nin ikili görüntüsü olan $\Phi(C)=\mathrm{C}$ kodunun parametreleri $[27,8,10]$ dur. Bu parametrelerle birlikte C kodu optimal (iyi parametreli) bir koddur.

Örnek 5.18 C, $(9,9;0,1,0)$ tipindeki $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu

$$[1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1|\ 1+u\ \ 1+u\ \ 1+u\ \ 1+u\ \ 1+u\ \ 1+u\ \ 1+u\ \ 1+u\ \ 1+u]$$

üreteç matrisiyle verilmiş olsun. $\Phi(C)=\mathrm{C}$ ikili kodu bir $[27,2,18]-$optimal koddur.

Örnek 5.19 $(7,7;3,1,0)$ tipindeki C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu

$$\left[\begin{array}{ccccccc|ccccccc}
1 & 0 & 1 & 1 & 0 & 0 & 0 & 1+u & 1 & 1+u & 1+u & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & u & 0 & u & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & u & 0 & u & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & u & 0 & u
\end{array}\right]$$

üreteç matrisine sahipse $\Phi(C)=\mathrm{C}$ ikili kodu $[21,5,10]$ parametrelerine sahiptir ve bu parametrelerle birlikte optimal bir koddur.

5.5 $\mathbb{Z}_2\mathbb{Z}_2[u]-$Lineer Kodlar İçin MacWilliams Özdeşliği

Klasik anlamda bir lineer ikili kodun ağırlık dağılımıyla dualinin ağırlık dağılımı arasında cebirsel bir bağıntı vardır [29]. Genel olarak, eğer ağırlık dağılımı tanımlanmış ise kodların ağırlık dağılımlarıyla duallerinin ağırlık dağılımları arasında böyle bir ilişkinin kurulup kurulamayacağı akla gelebilecek doğal bir sorudur. $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodlar için bu sorunun cevabı evettir.

Bu bölümde, MacWilliams özdeşliği kullanılarak $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodlarla dualleri arasında böyle bir bağıntının var olduğu ispatlanacaktır. Bu özdeşlik verilen ağırlık

dağılımıyla bağıntılı olarak dual kodun ağırlık dağılımını cebirsel olarak belirlemekle kalmaz aynı zamanda kodların olası ağırlık dağılımları hakkında bilgi de verir. Bu bağıntının kodlama teorisinde, lineer programlama sınırları ve self-dual kodlar üzerinde bazı uygulamaları vardır [29].

Şimdi $v=\left(v_1,v_2,\ldots,v_\alpha,v_{\alpha+1},\ldots,v_{\alpha+\beta}\right)=\left(v^\alpha,v^\beta\right)\in\mathbb{Z}_2^\alpha\times\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)^\beta$ olsun. Yukarıda $R=\mathbb{Z}_2+u\mathbb{Z}_2$ halkası üzerinde tanımlanmış olan Gray dönüşümü

$\phi: R\to\mathbb{Z}_2^2,\ \phi(a+ub)=(b,a+b)$ biçiminde ve Lee ağırlığı da

$w_L(a+ub)=w_H(b,a+b)$ biçiminde ifade edilebilir.

Böylece v nin ağırlığı $w(v)=w_H(v^\alpha)+w_L(v^\beta)$ olarak tanımlanır.

Tanım 5.20 C bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod ve $N=\alpha+2\beta$ olsun. C nin ağırlık sayacı $W(x,y)=\sum_{c\in C}x^{N-w(c)}y^{w(c)}$ biçiminde tanımlanır.

$(a+ub)\in\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)$ olsun. $\chi(a+ub)=(-1)^{a+b}$ ye R ***nin karakteri*** denir ve bu karakter aşikar değildir.

Önerme 5.21 $v\in R=\mathbb{Z}_2+u\mathbb{Z}_2$ ve χ, R nin karakteri olsun. Buradan,

$$\sum_{l\in\mathbb{Z}_2^\alpha\times R^\beta}\chi\left(\langle l,v\rangle\right)x^{N-w(l)}y^{w(l)}=\left(x+y\right)^{N-w(v)}\left(x-y\right)^{w(v)}$$ dir.

İspat:

$$\sum_{l\in\mathbb{Z}_2^\alpha\times R^\beta}\chi\left(\langle l,v\rangle\right)x^{N-w(l)}y^{w(l)}=\sum_{l^\alpha\in\mathbb{Z}_2^\alpha}\sum_{l^\beta\in R^\beta}\chi\left(\left\langle v^\alpha,l^\alpha\right\rangle\right)x^{\alpha-w(l^\alpha)}y^{w(l^\alpha)}\chi\left(\left\langle v^\beta,l^\beta\right\rangle\right)x^{2\beta-w_L(l^\beta)}y^{w_L(l^\beta)}$$

$$=\left(\prod_{i=1}^{\alpha}\sum_{l_i\in\mathbb{Z}_2}(-1)^{\sum_{i=1}^{\alpha}l_iv_i}x^{1-w(l_i)}y^{w(l_i)}\right)\left(\prod_{j=1}^{\beta}\sum_{l_{j+\alpha}\in R}(i)^{\sum_{j=1}^{\beta}l_{j+\alpha}v_{j+\alpha}}x^{2-w_L(l_{j+\alpha})}y^{w_L(l_{j+\alpha})}\right)$$

$$=\left(\prod_{i=1}^{\alpha}\left(x-y\right)^{1-w_H(v_i)}\left(x+y\right)^{w_H(v_i)}\right)\left(\prod_{j=1}^{\beta}\sum_{l_{j+\alpha}^0,l_{j+\alpha}^1\in\mathbb{Z}_2}(-1)^{\sum_{j=1}^{\beta}l_{j+\alpha}^0v_{j+\alpha}^0+l_{j+\alpha}^1v_{j+\alpha}^1}x^{2-w_L(l_{j+\alpha})}y^{w_L(l_{j+\alpha})}\right)$$

$$=\left(\prod_{i=1}^{\alpha}(x-y)^{1-w_H(v_i)}(x+y)^{w_H(v_i)}\right)\left(\prod_{j=1}^{\beta}(x-y)^{2-w_L(v_i)}(x+y)^{w_L(v_i)}\right)$$

$$=(x-y)^{N-w(v)}(x+y)^{w(v)}. \blacksquare$$

Önerme 5.22 C, R üzerinde lineer bir kod ve $C^{\perp}$, C nin dual kodu ve

$\hat{f}(z)=\sum_{v\in\mathbb{Z}_2^{\alpha}\times R^{\beta}}\chi\left(\langle z,v\rangle\right)f(v)$ olsun. Buradan, $\sum_{v\in C^{\perp}}f(v)=\frac{1}{|C|}\sum_{z\in C}\hat{f}(z)$ dir.

İspat:

$$\sum_{z\in C}\hat{f}(z)=\sum_{z\in C}\sum_{v\in\mathbb{Z}_2^{\alpha}\times R^{\beta}}\chi\left(\langle z,v\rangle\right)f(v)=\sum_{z\in C}\sum_{v\in C^{\perp}}\chi\left(\langle z,v\rangle\right)f(v)+\sum_{z\in C}\sum_{v\in\mathbb{Z}_2^{\alpha}\times R^{\beta}\setminus C^{\perp}}\chi\left(\langle z,v\rangle\right)f(v)$$

$$=|C|\sum_{v\in C^{\perp}}f(v)+\sum_{v\in\mathbb{Z}_2^{\alpha}\times R^{\beta}\setminus C^{\perp}}\sum_{z\in C}\chi\left(\langle z,v\rangle\right)f(v).$$

Herhangi bir $v\in\mathbb{Z}_2^{\alpha}\times R^{\beta}\setminus C^{\perp}$ ve her $c\in C$ için $\phi_v(c)=\langle c,v\rangle$ olsun. $\phi_v(c)$ nin bir $R-$modül homomorfizması olduğu açıktır. Böylece $\phi_v(C)$, R nin sıfırdan farklı bir idealidir. [30]'daki Önerme 2.1'den $\sum_{z\in C}\chi\left(\langle z,v\rangle\right)=0$ olduğu biliniyor. Böylece son eşitlikteki çift toplam sıfır olacaktır. Buradan da $\sum_{z\in C}\hat{f}(z)=|C|\sum_{v\in C^{\perp}}f(v)$ elde edilir. $\blacksquare$

Teorem 5.23 C, bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod olsun. C nin ağırlık sayaçları ile dualinin ağırlık sayaçları arasındaki bağıntı aşağıdaki eşitlik ile verilir.

$$W_{C^{\perp}}(x,y)=\frac{1}{|C|}W_C(x+y,x-y)$$

Örnek 5.24 C, $(2,2;1,1,0)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod olsun. C nin standart formdaki üreteç matrisi $G=\begin{bmatrix}1&1&0&u\\0&0&1&u\end{bmatrix}$ ile verilsin. Buradan,

$C=\{(0,0,0,0),(1,1,0,u),(0,0,1,u),(1,1,1,0),(0,0,u,0),(1,1,u,u),(0,0,1+u,u),(1,1,1+u,0)\}$ ve $W_C(x,y)=x^6+x^2y^4+4x^3y^3+x^4y^2+y^6$ şeklindedir.

C nin standart haldeki üreteç matrisi kullanılarak $C^{\perp}$ lineer dual kodunun üreteç matrisi de $H=\begin{bmatrix}1 & 1 & 0 & 0\\ 1 & 0 & u & 1\end{bmatrix}$ olarak yazılabilir. Bu matris yardımıyla

$C^{\perp}=\{(0,0,0,0),(1,1,0,0),(1,0,u,1),(0,1,u,1),(0,0,0,u),(1,1,u,0),(1,0,u,1+u),(0,1,u,1+u)\}$ ve $C^{\perp}$, $(2,2;1,1,0)$ tipindedir. $C^{\perp}$ için ağırlık sayacı ise $W_{C^{\perp}}(x,y)=x^6+5x^2y^4+2x^4y^2$ şeklinde olacaktır. Bu örnek için yukarıda verilen teorem uygulanırsa

$$W_{C^{\perp}}(x,y)=\frac{1}{|C|}W_C(x+y,x-y)$$

$$x^6+5x^2y^4+2x^4y^2=\frac{1}{8}\left[(x+y)^6+(x+y)^2(x-y)^4+4(x+y)^3(x-y)^3+(x+y)^4(x-y)^2+(x-y)^6\right]$$

$$=\frac{1}{8}\left[8x^6+16x^4y^2+40x^2y^4\right]=x^6+5x^2y^4+2x^4y^2$$

olduğu görülür.

Örnek 5.25 $(2,3;1,2,0)$ tipindeki C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu $H=\begin{bmatrix}1 & 1 & u & 0 & 0\\ 1 & 0 & 0 & 1 & 0\end{bmatrix}$ kontrol matrisiyle verilmiş olsun. Buradan $C^{\perp}$ in kodsözleri

$$C^{\perp}=\{(0,0,0,0,0),(1,1,u,0,0),(1,0,0,1,0),(0,1,u,1,0),(0,0,0,u,0),(1,1,u,u,0),$$
$$(1,0,0,1+u,0),(0,1,u,1+u,0)\}$$

biçiminde kolaylıkla yazılabilir. Böylece $C^{\perp}$ için ağırlık sayacı

$W_{C^{\perp}}(x,y)=x^8+x^2y^6+3x^4y^4+3x^6y^2$ şeklindedir.

Ayrıca C, $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodu için ağırlık sayacı

$W_C(x,y)=x^8+2x^7y+4x^6y^2+6x^5y^3+6x^4y^4+6x^3y^5+4x^2y^6+2xy^7+y^8$ biçiminde olacaktır. Teorem 5.23 uygulanarak,

$W_C(x+y,x-y)=32x^8+32x^2y^6+96x^4y^4+96x^6y^2=32W_{C^{\perp}}(x,y)$

elde edilir.

BÖLÜM 6

SONUÇ VE ÖNERİLER

Bu çalışmayla $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodların doğal birer genelleştirilmesi olan $\mathbb{Z}_2\mathbb{Z}_{2^s}$ ve $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$toplamsal kod aileleri tanımlanmıştır. Bu kod ailelerinin cebirsel yapılarını incelemede çok önemli bir yere sahip olan üreteç ve kontrol matrislerinin standart formları belirlenmiştir. Ayrıca bu iki yeni kod ailesi üzerinde bazı sınırlar verilip bu sınırlardaki eşitlikleri tam olarak sağlayan toplamsal kod örnekleri elde edilmiştir. Bunların dışında, $\mathbb{Z}_2[u]=\mathbb{Z}_2+u\mathbb{Z}_2$ olmak üzere $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodlar tanımlanmış bu kodların standart haldeki üreteç ve kontrol matrisleri belirlenmiştir. Ayrıca bu lineer kod ailesi için MacWilliams özdeşliği elde edilerek bir $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kodla duali arasındaki bağıntı incelenmiştir. Son olarak $\mathbb{Z}_2\mathbb{Z}_2[u]-$lineer kod ailesi içinden ikili görüntüleri optimal olanlarına örnekler verilmiştir.

İleride, bu tezde tanımlanan kod aileleri için kodlama teorisinde çok iyi bilinen devirli kodlar ve kendine-duallik veya diklik gibi kavramlar incelenebilir. Ayrıca bu kod ailelerinin Steganografi üzerine veya başka alanlarda uygulamaları olup olmadığı araştırmaya açıktır.

KAYNAKLAR

[1] Shannon, C.E., (1948), "A mathematical theory of communication", The Bell System Technical Journal, 27: 379–423.

[2] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J., ve Solé, P.,(1994), "The $\mathbb{Z}_4-$linearity of Kerdock, Preparata, Goethals and related codes", IEEE Trans. Inform. Theory, 40: 301–319.

[3] Delsarte, P., (1973), "An algebraic approach to the association schemes of coding theory", Philips Research Rep. Suppl. 10, vi+97.

[4] Delsarte, P. ve Levenshtein, V., (1998), "Association schemes and coding theory" IEEE Trans. Inform. Theory, 44: 2477–2504.

[5] Pujol, J. ve Rifà, J., (1997), "Translation Invariant Propelinear Codes", IEEE Trans. Inform. Theory, 43: 590-598.

[6] Borges, J., Fernández-Córdoba, C., Pujol, J., Rifà, J. ve Villanueva, M., (2010), "$\mathbb{Z}_2\mathbb{Z}_4-$linear codes: Generator Matrices and Duality", Designs, Codes and Cryptography, 54: 167-179.

[7] Bilal, M., Borges, J., Dougherty, S.T. ve Fernández-Córdoba, C., (2011), "Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2\times\mathbb{Z}_4$", Designs, Codes and Cryptography, 61: 31-40.

[8] Bilal, M., Borges, J., Dougherty, S.T. ve Fernández-Córdoba, C., (2010), "Optimal codes over $\mathbb{Z}_2\times\mathbb{Z}_4$", VII Jornadas de Matemática Discreta y Algorítmica Castro Urdiales, Cantabria, 7–9 de julio de 2010.

[9] Fernández-Córdoba, C., Pujol, J. ve Villanueva, M., (2010), "$\mathbb{Z}_2\mathbb{Z}_4-$linear codes:rank and kernel", Designs, Codes and Cryptography, 56: 43-59.

[10] Rifa, J. ve Ronquillo, L., (2010) "Product perfect $\mathbb{Z}_2\mathbb{Z}_4-$linear codes in steganography", 2010 International Symposium on Information Theory and Its Applications (ISITA), Taichung, Taiwan, October 2010, 696–701.

[11] Rifa, H., Rifa, J. ve Ronquillo, L., (2010) "Perfect $\mathbb{Z}_2\mathbb{Z}_4-$linear codes in steganography", Comput. Res. Reposit., vol.abs/1002.0.

[12] Ling, S. ve Xing, C., (2004), Coding Theory: A First Course, Cambridge University press.

[13] Singleton, R.C., (1964), "Maximum Distance q-ary Codes", IEEE Trans. Inform. Theory, 10: 116 -118.

[14] Carlet, C., (1998), "$\mathbb{Z}_{2^k}$ – linear codes", IEEE Trans. Inform. Theory, 44: 1543–1547.

[15] Norton, G. H. ve Salagean, A., (2000), "On the structure of linear and cyclic codes over a finite chain ring", Applicable algebra in engineering, communication and computing, 10: 489–506.

[16] Calderbank, A.R. ve Sloane, N.J.A., (1995), "Modular and *p*-adic cyclic codes," Designs, Codes and Cryptography, 6: 21–35.

[17] Bannai, E., Dougherty, S.T., Harada, M. ve Oura, M., (1999), "Type II Codes, Even Unimodular Lattices, and Invariant Rings", IEEE Trans. Inform. Theory, 45(4):1194-1205.

[18] Dinh, H.Q., (2010), Advances in Ring Theory Trends in Mathematics, 131–147, Birkhauser Verlag Basel/Switzerland.

[19] Kleinfeld, E.,(1959), "Finite Hjelmslev planes", Illinois J. Math. 3: 403–407.

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

[21] Çallıalp, F. ve Tekir, Ü., (2009), Değişmeli Halkalar ve Modüller, Birsen yayınevi, İstanbul.

[22] Dougherty, S.T. ve Fernández-Córdoba, C., (2011), "Codes over $\mathbb{Z}_{2^k}$, gray map and self-dual codes", Adv. Math. Comm, 5: 571-588.

[23] Wan, Z.X., (1997), Quaternary Codes, Series on Applied Math., Vol. 8, World Scientific pub., Singapore.

[24] Park, Y.H., (2009), "Modular independence and generator matrices for codes over $\mathbb{Z}_m$", Designs, Codes and Cryptography, 50: 147-162.

[25] Dougherty, S.T. ve Shiromoto, K., (2001), "Maximum Distance Codes Over Rings of Order 4", IEEE Transaction on Information Theory, 47: 400-404.

[26] Yildiz, B. ve Odemis Ozger, Z., (2012), "A Generalization of the Lee Weight to $\mathbb{Z}_{p^k}$", TWMS J. App. Eng. Math. 2, 2: 145-153.

[27] Özen, M. ve Şiap, İ., (2006), "Linear Codes Over $\mathbb{F}_q[u]/\langle u^s \rangle$ With Respect to the Rosenbloom-Tsfasman Metric", Designs, Codes and Cryptography., 38: 17-29.

[28] Grassl, M., Code tables: Bounds on the parameters of various types of codes, Online database. Available at http://www.codetables.de/

[29] MacWilliams, F.J. ve Sloane, N.J.A., (1977), The Theory of Error Correcting Codes, North-Holland Pub. Co., Amsterdam.

[30] Şiap, İ., (2012), "An identity between m spotty weight enumerators of a linear code and its dual", Turk. J. Math., 36: 641–650.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : İsmail AYDOĞDU

Doğum Tarihi ve Yeri : 22.10.1984-Denizli

Yabancı Dili : İngilizce

E-posta : ismayilaydogdu@windowslive.com

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Matematik	Balıkesir Üniversitesi	2009
Lisans	Matematik	Balıkesir Üniversitesi	2007
Lise	Anadolu Lisesi	Denizli Türk Eğitim Vakfı Anadolu Lisesi	2003

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2009-	Yıldız Teknik Üniversitesi	Araştırma Görevlisi

YAYINLARI

Makale

1. Aydoğdu, İ. ve Şiap, İ.,(2013), "The Structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}-$Additive Codes: Bounds on the Minimum Distance", Applied Mathematics and Information Sciences (AMIS),7, (6), 2271-2278.

2. Aydoğdu, İ., Abualrub, T. ve Şiap, İ., (2013), "On $\mathbb{Z}_2\mathbb{Z}_2[u]-$additive codes", International Journal of Computer Mathematics, doi: 10.1080/00207160.2013.859854.

3. Şiap, İ. ve Aydoğdu, İ., (2013) "Counting the Generator Matrices of $\mathbb{Z}_2\mathbb{Z}_8-$Codes", Mathematical Sciences And Applications E-Notes Vol. 1 No. 2 pp. 143-149.

4. Aydoğdu, İ. ve Şiap, İ., (2014), "On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$additive codes", Linear and Multilinear Algebra, doi: 10.1080/03081087.2014.952728.

Bildiri

1. Aydoğdu, İ. ve Şiap, İ.,(11-13 Haziran, 2014), "Bounds on the minimum distance of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$additive codes", Karatekin Mathematics Days 2014, Çankırı, Türkiye.

2. Aydoğdu, İ. ve Şiap, İ.,(5-7 Mart, 2014), "On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$additive codes", International Workshop on Discrete Structures (IWODS), İslamabad, Pakistan.

3. Abualrub, T., Şiap, İ. ve Aydoğdu, İ., (12-14 Mart, 2014), "$\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)-$Linear Cyclic Codes", International MultiConference of Engineers and Computer Scientists 2014, Hong Kong.

4. Aydoğdu, İ. ve Şiap, İ.,(12-14 Eylül, 2013), "On $\mathbb{Z}_p\mathbb{Z}_{p^2}-$additive codes", The Algerian-Turkish International Days on Mathematics 2013, İstanbul, Türkiye.

5. Aydoğdu, İ., Abualrub, T. ve Şiap, İ., (24-27 Haziran, 2013), "On $\mathbb{Z}_2\mathbb{Z}_2[u]-$Additive Codes", International Conference on Computational and Mathematical Methods in Science and Engineering, CMMSE 2013, Almeria, İspanya.

6. Aydoğdu, İ. ve Şiap, İ.,(2-5 Temmuz, 2013), "Generator and Parity-check Matrices of $\mathbb{Z}_{2^r}\mathbb{Z}_{2^s}-$Additive Codes", 4th International Conference on Matrix Analysis and Applications, ICMAA, Konya, Türkiye.

7. Şiap, İ. ve Aydoğdu, İ., (2-5 Temmuz, 2013), "Counting the Generator Matrices of $\mathbb{Z}_2\mathbb{Z}_8-$Codes", 4th International Conference on Matrix Analysis and Applications, ICMAA, Konya, Türkiye.

8. Şiap, İ., Aydoğdu, İ. ve Öztaş, E.S., (26-29 Ağustos, 2013), "The Number of $\mathbb{Z}_2\mathbb{Z}_{2^s}-$Additive Codes and Some Combinatorial Relations", 2nd International

Eurasian Conference on Mathematical Sciences and Applications, Saraybosna, Bosna Hersek.

9. Abualrub, T., Aydoğdu, İ. ve Şiap, İ., (23-26 Ağustos, 2012), "The Structure of $\mathbb{Z}_2\mathbb{Z}_8$ – Additive Cyclic Codes", International Congress in Honour of Professor Hari M. Srivastava, Bursa,Türkiye.

10. Aydoğdu, İ. ve Şiap, İ., (14 Nisan, 2012), "Some Bounds on $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – Additive Codes", 10th UAE Math Day, Sharjah, Birleşik Arap Emirlikleri.

11. Aydoğdu, İ., (13-16 Haziran, 2012), "On Chaki Pseudo Symmetric Manifolds", X. Geometri Sempozyumu, Balıkesir-Burhaniye, Türkiye.

12. Aydoğdu, İ., ve Şiap, İ., (Haziran, 2011), "The Structure of $\mathbb{Z}_{2^r}\mathbb{Z}_{2^s}$ – Additive Codes", International Conference On Applied Analysis and Algebra, ICAAA 2011, İstanbul, Türkiye.