T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

RANK METRİĞİ VE KODLAR

İLHAMİ KALKAN

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
DOÇ. DR. GÜRSEL YEŞİLOT

İSTANBUL, 2012

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

RANK METRİĞİ VE KODLAR

İlhami KALKAN tarafından hazırlanan tez çalışması 04.07.2012 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Doç. Dr. Gürsel YEŞİLOT
Yıldız Teknik Üniversitesi

Prof. Dr. İrfan ŞİAP
Yıldız Teknik Üniversitesi

Yard. Doç. Dr. Tevfik BİLGİN
Fatih Üniversitesi

ÖNSÖZ

Bu tez, rank metriği ve rank metriği üzerinde oluşturulan kodları incelemeye yönelik bir çalışmadır.

Başta tez çalışmam boyunca beni yönlendiren, fikirleriyle bana yol gösteren ve çalışmanın daha anlaşılır hale gelmesini sağlayan danışman hocam Doç. Dr. Gürsel YEŞİLOT'a teşekkürlerimi sunarım. Ayrıca bu konu ile tanışmamı sağlayan Prof. Dr. İrfan ŞİAP'a teşekkürü bir borç bilirim.

Son olarak bugünlere gelmemi sağlayan, beni her konuda destekleyen, bana güvenen ve her zaman yanımda olan aileme sonsuz teşekkürlerimi sunarım.

Mayıs, 2012

İlhami KALKAN

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

$\delta(C)$	C kodunun bağıl uzaklığı
$C^{\perp}$	C kodunun duali
$\Re(C)$	C kodunun iletim hızı
$d(C)$	C kodunun minimum uzaklığı
$d_R(C)$	C kodunun rank uzaklığı
$\lvert\mathbb{F}\rvert$	$\mathbb{F}$ cisminin eleman sayısı
$\mathbb{F}[x]$	$\mathbb{F}$ cismi üzerindeki polinom halkası
α	İlkel eleman
$\Re$	Halka
$Ham(r,2)$	Hamming kodu
$H_q(x)$	Hilbert entropi fonksiyonu
$\Re/(m)$	Kalan sınıfı
H	Kontrol matrisi
$S(x,t)$	Merkezinde x kodsözü olan ve t yarıçaplı küre
$B(x,t)$	Merkezinde x kodsözü olan ve t yarıçaplı yuvar
$\mathbb{F}^n$	n boyutlu vektör uzayı
(n, M)-kod	n uzunluğunda M büyüklüğünde blok kod
$[n, k, d]$-kodu	n uzunluğunda k boyutunda ve d minimum uzaklığında lineer kod
$A_q(n,d)$	Optimal kod
$B_q(n,d)$	Optimal lineer kod
$GF(q)$	q elemanlı Galois cismi
$\mathbb{F}_q$	q elemanlı sonlu cisim
$\mathbb{F}^*$	Sonlu cismin sıfırdan başka elemanlarının oluşturduğu küme
$S^{\perp}$	S kümesinin ortogonel tümleyeni
$\mathbb{B}$	Taban
$\langle S \rangle$	Üreteç
G	Üreteç matrisi
$wt(x)$	x kodsözünün Hamming ağırlığı
$S(x)$	x kodsözünün sendromu
$r(x)$	x vektörünün rank normu
$d(x,y)$	x ve y kodsözleri arasındaki Hamming uzaklığı

V	Vektör uzayı
$\dim(V)$	V vektör uzayının boyutu

KISALTMA LİSTESİ

BCH	BCH kodu (Bose-Chaudhuri-Hochquenghem Kodu)
BSC	İkili Simetrik Kanal (Binary Symmetric Channel)
MLD	Maksimum Olasılıkla Dekodlama (Maximum Likelihood Decoding)
MDS	Maksimum Uzaklıklı Ayrılabilir (Maximum Distance Separable)
MRD	Maksimum Rank Uzaklığı (Maximum Rank Distance)

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

ÖZET

RANK METRİĞİ VE KODLAR

İLHAMİ KALKAN

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Doç. Dr. Gürsel YEŞİLOT

Rank metriği, 1985 yılında E. M. Gabidulin tarafından tanımlanan ve hata – düzeltmede kullanılan yeni bir metriktir. Hata – düzeltme kapasitesi, kodlar arasındaki uzaklığa bağlı olduğu için uygun bir metrik seçmek oldukça önemlidir. Cebirsel kodlama teorisinin büyük kısmı Hamming metriği ile ilgilidir. Ancak bu metrik her zaman kanal karakteristiği ile uyumlu olmayabiliyor. Özellikle de kod sembolleri büyük boyutlu Galois cisimlerinin elemanları ise bu uyumsuzluk daha da çok beliriyor. Hamming uzaklığı kod alfabesinin çeşitli sinyalleri arasında lineer bağımlılığı fark edemediğinden çapraz – hata (criss – cross) oluşumuna uygunsuz olmaktadır. Rank metrik birçok hata çeşidini etkili bir şekilde düzeltme kapasitesinden dolayı ideal bir metriktir.

Bu çalışmada rank metriğinin incelenmesi için öncelikle sonlu cisimler anlatılmıştır. Sonraki kısımda kodlama teorisi ayrıntılı bir şekilde anlatılmıştır. Son bölümde ise rank metriği anlatılmış ve bu metrik üzerindeki kodlar kısaca incelenmiştir.

Anahtar Kelimeler: Rank metrik, Galois cismi, kodlama teorisi, Hamming metriği, hata – düzelten kodlar.

ABSTRACT

RANK METRIC AND CODES

İlhami KALKAN

Department of Mathematic

MSc. Thesis

Advisor: Assoc. Prof. Dr. Gürsel YEŞİLOT

Rank metric which was introduced by E. M. Gabidulin in 1985, is a new metric that have found applications in error – correcting. Since error – correcting capability of a code depends on the distance between codewords, choosing a convenient metric is considerably important. Most studies in algebraic coding theory are relative to Hamming metric. However this metric is not always suitable for characteristic of channel. Especially if code symbols are elements of higher dimensional Galois field, this incompatiblity is more significant. As Hamming distance cannot distinguish the linear dependency among the various signals of alphabet, it is inappropriate to criss – cross errors occurrence. Because of the fact that rank metric capacity of handling varied error patterns efficiently, it is an ideal metric.

In this context, firstly finite fields are represented for research in rank metric. In the following part, coding theory is represented in detailed. In the last part, rank metric is represented and codes on the rank metric are researched.

Key words: Rank metric, Galois field, coding theory, Hamming metric, error – correcting codes.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Önceleri rank, bir metrik olarak bilinmesine rağmen rank metrik ilk olarak Delsarte'nin 1978 yılında yayınladığı makalede hata kontrol kodları için ortaya atılmıştır. Ancak bilgi iletiminde rank hatalarının düzeltilmesi amacıyla kullanılan, sonlu cisimler üzerinde oluşturulmuş rank metriği ilk olarak E. M. Gabidulin tarafından 1985 yılında tanımlanmıştır. Bu n uzunluğundaki metrik kodlar, $GF(q^m)$ cisim genişlemesi üzerinde vektör kümeleri veya $GF(q)$ taban cismi üzerinde $m \times n$ matrisleri olarak düşünülebilirler. Kodsözlerin rankı, bilinen matris rankına karşılık gelir ve bu metrik hata düzeltmeler için uygundur. Aynı makalede E. M. Gabidulin Frobenious otomorfizma özelliklerini kullanarak lineer kodların optimal ailesini inşa etmiştir. Bu aile Reed – Solomon kodlarının rank metriği için eşdeğer olarak düşünülebilir.1991 yılında R. M. Roth, verilen ranka uygun $GF(2)$ üzerinde matrissel kod ailesini oluşturdu. Bu kodlar bant kaydı gibi matris kolonu veya satırında oluşan hata düzeltilerine uygundur. Diğer kod aileleri, örneğin RRC kodları [1], bu kodların alt cismi, alt uzayı veya kodların direk çarpım yapısına matris ekleme şeklinde dizayn edilmişlerdir.

Yapılan çalışmaların çoğunda rank uzaklık özellikleri, kod inşası ve rank metrik kodların verimli dekodlaması üzerine odaklanılmıştır [2], [3], [4]. Bu makalelerde minimum rank uzaklığı üzerinde Teklik sınırı (Singleton bound) oluşturulmuş ve bu sınırı sağlayan kod sınıfları inşa edilmiştir. Bu sınıflara Gabidulin kodları denilecektir. [2] ve [4]'te Teklik sınırı sağlayan lineer kodların ağırlık dağılımlarını (weight distribution) hesaplamak için analitik tanımlamalar yapılmıştır. [5]'de Gabidulin

kodların çapraz hata düzeltmede (crisscross error correcting) optimal olduğu gösterilmiştir. Gabidulin kodlar için, Sırasıyla genişlemiş (extended) Öklit algoritması ve Peterson-Gornstein-Zierler algoritmasına paralel dekodlama algoritması tanımlanmıştır, [4], [3]. [2]'da MacWilliams özdeşliği rank uzaklık kodları için oluşturulmuştur. [4]'te oluşturulan rank metrik yapısı genişletilmiş [6] ve alt uzaydaki altkodlar (subcodes) ile alt cisimdeki altkodlar çalışılmıştır [7], [8]. Welch-Berlekamp algoritması ve Berlekamp-Massey algoritması sırasıyla [9] ve [10]'te Gabidulin kodlar için çalışılmıştır. Gabidulin kodların hata performansları [11], [12], [13]'da incelenmiştir. [14]'de lineer devirli kodlarda rank uzaklık özellikleri çalışılmıştır. [15]'de kodlarda rank örtü yarıçapı (rank covering radius) ve rank metrik için küre – örtü sınırı (sphere – covering bound) tanımlanmıştır.

1.2 Tezin Amacı

Bu tez, Kodlama Teorisi alanında çalışan veya yeni çalışmaya başlayan herkesin yararlanması için hazırlanmıştır. Bunun için öncelikle Sonlu Cisimler kısaca anlatılmış ve Kodlama Teorisi ayrıntılı bir şekilde incelenerek çok sayıda örnek verilmiştir. Ayrıca son zamanlarda üzerinde çokça durulan rank metriğine dikkat çekilmiş ve bu konu ile ilgilenenlerin tek kaynakta gerekli tüm bilgileri bulabilmeleri amaçlanmıştır.

1.3 Hipotez

Bir (n,M,d)-kodu için minimum uzaklık, d Hamming uzaklığıdır. Rank uzaklığı d_R ve Hamming uzaklığı d_H olmak üzere $d_R \leq d_H$'dir. Ayrıca Hamming metriğinde mükemmel kod tanımlanmasına rağmen rank metriğinde mükemmel kod yoktur.

BÖLÜM 2

SONLU CİSİMLER

2.1 Giriş

Sonlu cisimler teorisi geçmişi, özel sonlu cisimlerin yapıları üzerinde çalışmalar yapan Pierre de Fermat (1601-1665) ve Leonhard Gauss (1707-1783) gibi ünlü matematikçilerin yaşadığı 17. ve 18. yüzyıla dayanır. Genel sonlu cisimler teorisi Carl Friedrich Gauss (1777-1855) ve Evariste Galois (1811-1832)'in çalışması ile başlamıştır. Ancak cisimler teorisi matematik, bilgisayar bilimleri ve iletişim teorisi uygulamalarından dolayı matematikçilerin ve mühendislerin son yıllarda daha çok ilgisini çekmiştir. Bu günlerde sonlu cisimler teorisi oldukça zengindir. Bu bölümde Kodlama Teorisi'nde kullanılacak olan sonlu cisimlerin küçük bir bölümünden bahsedilecektir [16].

Tanım 2.1 $\mathbb{F}$, üzerinde çarpma $(\cdot)$ ve toplama $(+)$ tanımlı bir küme olsun. $\mathbb{F}$, aşağıdaki özellikleri sağlıyorsa toplama ve çarpmaya göre bir **cisimdir** denir:

- $(\mathbb{F},+)$ bir abelian gruptur.
- 0, $(\mathbb{F},+)$ grubunun sıfırı ve $\mathbb{F}^* = \mathbb{F}\setminus\{0\}$ olmak üzere $(\mathbb{F}^*,\square)$ bir abelian gruptur.
- Tüm $a,b,c \in \mathbb{F}$ için $a(b+c) = ab + ac$

$(\mathbb{F},+,\square)$ cisim olarak isimlendirilir. $(\mathbb{F},+)$ toplamsal grup ve $(\mathbb{F}^*,\square)$ çarpımsal grup olarak adlandırılır.

Tanım 2.2 $\mathbb{F}$ bir cisim olsun. Herhangi $a,b \in \mathbb{F}$ için $a+b$'ye a ve b'nin toplamı, ab'ye a ve b'nin çarpımı denir. $(\mathbb{F},+)$ grubunun sıfırına $\mathbb{F}$'nin sıfırı denir. Herhangi bir $a \in \mathbb{F}$ elemanının $(\mathbb{F},+)$ toplamsal grubundaki tersi negatifidir ve $-a$ ile gösterilir.

$(\mathbb{F}^*, \square)$ çarpımsal grubunun birim elemanı e ile tanımlanır ve $\mathbb{F}$'nin de birim elemanıdır. Herhangi bir $a \in \mathbb{F}^*$ için $(\mathbb{F}^*, \square)$ çarpımsal grubunun tersi a^{-1} ile gösterilir ve a'nın tersi olarak isimlendirilir [17].

Cisimlere örnek olarak rasyonel sayılar $\square$, reel sayılar $\square$ ve karmaşık sayılar $\square$ verilebilir.

Lemma 2.1 $\mathbb{F}$ cisim olmak üzere $a, b \in \mathbb{F}$ olsun. Aşağıdakiler sağlanır:

- $(-1) \cdot a = -a$
- $ab = 0$ ise $a = 0$ veya $b = 0$.

Tanım 2.3 Bir cisim sonlu sayıda elemana sahipse **sonlu cisim veya Galois cismi** olarak isimlendirilir.

Tanım 2.4 a, b ve $m > 1$ tam sayı olsunlar. Eğer $m \mid (a-b)$ ise a modül m ye göre b'ye denktir denir ve şöyle gösterilir,

$a \equiv b (\mathrm{mod}\, m)$.

Teorem 2.2 p asal ve $\mathbb{F} = \{0, 1, ..., p-1\}$ olsun. Modül p'ye göre $+$ ve $\square$ sırasıyla toplama ve çarpma olsun. $(\mathbb{F}, +, \cdot, 0, 1)$, eleman sayısı p olan sonlu cisimdir ve $\mathbb{F}_p$ ile gösterilir.

Tanım 2.5 $\mathbb{F}$, q elemanlı sonlu bir cisim ve $a \in \mathbb{F} \setminus \{0\}$ olsun. $a^k = 1$ olacak şekilde en küçük k pozitif tamsayısına a'nın **derecesi** denir ve $ord(a)$ ile gösterilir.

$\{a^i \mid i = 1, 2, ...\}$ kümesi $\mathbb{F}$ kümesinin alt kümesidir ve sonlu olmak zorundadır. Böylece öyle bir i_1 ve i_2 vardır ki $a^{i_1} = a^{i_2}$ sağlar ve böylece $a^{i_1 - i_2} = 1$ olur. Yani $a^i = 1$ olacak şekilde bir i vardır ve en küçüktür. Buradan da derece iyi tanımlıdır denir.

Lemma 2.3 $\mathbb{F}$, q elemanlı sonlu bir cisim ve $a, b \in \mathbb{F} \setminus \{0\}$ olsun. Aşağıdakiler sağlanır:

1. $ord(a) = s \Rightarrow a, a^2, ..., a^s$ farklı elemanlardır.
2. $a^j = 1 \Leftrightarrow ord(a) \mid j$.
3. $ord(a^j) = \dfrac{ord(a)}{\gcd(ord(a), j)}$

4. $ord(a)=s, ord(b)=j, \gcd(s,j)=1 \Rightarrow ord(ab)=sj$ **.**

Teorem 2.4 $\mathbb{F}$, q elemanlı sonlu bir cisim olsun. Sıfırdan farklı elemanlarının derecesi $q-1$'yi böler.

Teorem 2.5 $\mathbb{F}$, q elemanlı sonlu bir cisim olsun. $\mathbb{F}$'nin herhangi bir a elemanı için $a^q - a = 0$ sağlanır [18].

Tanım 2.6 $\mathbb{F}$ bir cisim ve e birim elemanı olsun. Eğer her bir m pozitif tamsayısı için $me \neq 0$ ise $\mathbb{F}$'nin karakteristiği 0'dır denir. Eğer $me = 0$ olacak şekilde bir m pozitif tamsayısı varsa ve bu pozitif tamsayıların en küçüğü p ise $\mathbb{F}$'nin karakteristiği p'dir denir.

Örnek 2.1 $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ karakteristiği 0 olan cisimlerdir. $\mathbb{Z}_p$ ise karakteristiği p olan cisimdir.

Teorem 2.6 Bir cismin karakteristiği ya 0 ya da p asal tam sayısıdır.

Teorem 2.7 Eğer $\mathbb{F}$ bir sonlu cisim ise $\mathbb{F}$'nin karakteristiği 0'a eşit değildir.

Teorem 2.8 $\mathbb{F}$ bir cisim ve karakteristiği p olsun. $n \geq 1$ için $\mathbb{F}$, p^n eleman içerir [16].

Teorem 2.9 $\mathbb{F}$ bir cisim, karakteristiği p , $p \neq 0$ ve $a, b \in \mathbb{F}$ olsun. Aşağıdaki denklik sağlanır:

$(a \pm b)^p = a^p \pm b^p$.

Tanım 2.7 $\mathbb{F}$ bir cisim olsun.

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in \mathbb{F}, n \geq 0 \right\} \tag{2.1}$$

kümesine $\mathbb{F}$ üzerinde tanımlı **polinom halkası** denir. $\mathbb{F}[x]$'in elemanlarına da **polinom** denir. $f(x) = \sum_{i=0}^{n} a_i x^i$ polinomu için $a_n \neq 0$ olmak koşuluyla n'ye $f(x)$'in **derecesi** denir ve $\deg(f(x))$ ile gösterilir. Eğer $f(x)$ polinomunda $a_n = 1$ ise $f(x)$'e **monik polinom** denir. $\mathbb{F}$'nin sıfırdan farklı elemanları $\mathbb{F}[x]$'te derecesi 0 olan elemanlardır. Eğer $f(x)$'in tüm katsayıları sıfırsa $f(x)$'e **sıfır polinom** denir ve $\deg(f(x)) = -\infty$'dir. $\mathbb{F}$'nin sıfırı ve birim elemanı $\mathbb{F}[x]$'inde sırasıyla sıfırı ve birim elemanıdır [18].

Tanım 2.8 $\mathbb{F}$ bir cisim olsun $h(x), g(x) \in \mathbb{F}[x]$ olsun. $\deg(g(x)) < \deg(f(x))$, $\deg(h(x)) < \deg(f(x))$ olmak üzere $f(x) = g(x)h(x)$ şeklinde yazılabiliyorsa $f(x)$'e **indirgenebilir** denir. Eğer yazılamıyorsa $f(x)$'e **indirgenemez** denir [16].

Örnek 2.2 $f(x) = x^4 + 2x^6 \in \mathbb{Z}_3[x]$ polinomunun derecesi 6'dır. $f(x) = x^4(1+2x^2)$ olarak yazılabildiğinden indirgenebilirdir.

Örnek 2.3 $g(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$ derecesi 2 olan indirgenemez bir polinomdur.

Tanım 2.9 $f(x) = \sum_{i=0}^{n} a_i x^i$ ve $g(x) = \sum_{i=0}^{n} b_i x^i$, $\mathbb{F}$ üzerinde tanımlı iki polinom olsunlar. Bu iki polinomun toplamı ve farkı

$$f(x) \pm g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \tag{2.2}$$

çarpımları ise

$$h(x) = \sum_{i=0}^{2n} c_i x^i \tag{2.3}$$

ile tanımlıdır. Burada katsayılar $c_i = \sum_{j=0}^{i} a_j b_{i-j}, 0 \le i \le 2n$ şeklindedir [19].

Tanım 2.10 $f(x) \in \mathbb{F}[x]$ derecesi $n \ge 1$ olan bir polinom olsun. Herhangi bir $g(x) \in \mathbb{F}[x]$ polinomu için $\deg(r(x)) < \deg(f(x))$ veya $\deg(r(x)) = 0$ olacak şekilde $g(x) = s(x)f(x) + r(x)$ eşitliğini sağlayan $s(x), r(x)$ polinom çifti vardır ve buradaki $r(x)$ polinomuna **kalan** denir.

Tanım 2.11 $f(x), g(x) \in \mathbb{F}[x]$ sıfırdan farklı iki polinom olsunlar. Bu iki polinomu bölen derecesi en büyük monik polinoma **en büyük ortak bölen** denir ve $ebob(f(x), g(x))$ olarak gösterilir. Özel olarak $ebob(f(x), g(x)) = 1$ ise bu iki polinoma aralarında asal denir. $f(x), g(x)$ polinomlarının katı olan en küçük dereceli monik polinoma **en küçük ortak kat** denir ve $ekok(f(x), g(x))$ ile gösterilir [16].

Teorem 2.10 $f(x), g(x)$ ve $h(x)$, $\mathbb{F}$ üzerinde tanımlı polinomlar olsun. $h(x) \neq 0$ ve $ebob(f(x), h(x)) = 1$ sağlansın. O halde aşağıdaki sağlanır:

$h(x) \mid f(x) \cdot g(x) \Rightarrow h(x) \mid g(x).$

Önerme 2.11 $p(x)$, $\mathbb{F}$ üzerinde tanımlı indirgenemez bir polinom olsun. $a(x), b(x) \in \mathbb{F}[x]$ olsun.

$p(x) \mid a(x) \cdot b(x) \Rightarrow p(x) \mid a(x)$ veya $p(x) \mid b(x).$

Teorem 2.12 $\mathbb{F}$ cismi üzerinde tanımlı sıfırdan farklı bir polinomun indirgenemez polinomların çarpımı şeklinde yazılışı tek türlüdür [19].

Tanım 2.12 R bir halka ve m asal olmayan bir elemanı olsun. Herhangi iki $a, b \in R$ için

$a \equiv b (\mathrm{mod}\, m) \Leftrightarrow m \mid (a-b)$

eşitliği a ile b $\mathrm{mod}\, m$'ye göre **denktir** diye okunur. Bu işlem R üzerinde denklik bağıntısını sağlar. R'deki her bir denklik sınıfı modülo m'ye göre **kalan sınıfı** olarak isimlendirilir. R'deki modülo m'ye göre kalan sınıfları $R/(m)$ ile gösterilirler.

Tanım 2.13 $\mathbb{F}$ bir cisim, $\mathbb{F}[x]$ bu cisim üzerinde tanımlı bir polinom halkası ve $f(x) \in \mathbb{F}[x]$ bir polinom olsun. $\mathbb{F}[x]/(f(x))$ halkası $\mathbb{F}[x]$ polinom halkasının modülo $f(x)$ polinomuna göre kalan sınıf halkası olarak isimlendirilir. Eğer $f(x)$ indirgenemez polinom ise $\mathbb{F}[x]/(f(x))$ cismi $\mathbb{F}[x]$ polinom halkasının modülo $f(x)$ polinomuna göre kalan sınıf cismi olarak isimlendirilir [17].

Tanım 2.14 $\mathbb{F}$ bir cisim ve $\mathbb{S} \subset \mathbb{F}$ olsun. $\mathbb{S}$ kendi başına $\mathbb{F}$ cismindeki işlemlere göre bir cisim ise $\mathbb{S}$'ye $\mathbb{F}$'nin **alt cismi** denir.

Tanım 2.15 $\mathbb{E}$ ve $\mathbb{F}$ cisim olsunlar. Eğer $\mathbb{F}$, $\mathbb{E}$'nin bir alt cismi ise $\mathbb{E}$'ye $\mathbb{F}$'nin bir **genişlemesi** denir.

Eğer $p(x)$, $\mathbb{F}$ üzerinde derecesi h olan indirgenemez polinom ise $\mathbb{F}[x]/(p(x))$ cismi derecesi h olan $\mathbb{F}$'nin genişlemesidir [19].

Örnek 2.4 $\mathbb{F}$, $\mathbb{R}$ reel sayılar cismi ve $P(x)$ indirgenemez polinomu da x^2+1 olsun. $\mathbb{R}[x]/(x^2+1)$ cismi derecesi 2 olan, $\mathbb{R}$ cisminin genişlemesidir. Bu cisimden alınan $a+bx$ ve $c+dx$ iki elemanın toplamı,

$(a+bx)+(c+dx) = (a+c)+(b+d)x$

biçiminde ve çarpımları da

$$(a+bx)(c+dx) = ac + (ad+bc)x + bdx^2 \equiv (ac-bd) + (ad+bc)x^2 \pmod{(x^2+1)}$$

biçimindedir.

Lemma 2.13 $\mathbb{F}$ bir cisim ve eleman sayısı q olsun. Her $\beta \in \mathbb{F}$ elemanı için $\beta^q = \beta$ sağlanır.

Sonuç 2.14 $|\mathbb{F}| = q$ olmak üzere $\mathbb{F}$, $\mathbb{E}$ cisminin alt cismi olsun. Bir $\beta \in \mathbb{E}$ elemanının $\mathbb{F}$'de olması için gerek ve yeter koşul $\beta^q = \beta$ olmasıdır.

Tanım 2.16 $\mathbb{F}$ bir cisim ve $\mathbb{E}$ de bir genişlemesi olsun. $f(\beta) = 0$ olacak şekilde $\beta \in \mathbb{E}$ elemanına $f(x) \in \mathbb{F}[x]$ polinomunun **kökü** denir.

Önerme 2.15 $f(x) \in \mathbb{F}[x]$ ve $\mathbb{E}$, $\mathbb{F}$'nin bir genişlemesi olmak üzere $\beta \in \mathbb{E}$ olsun. $f(\beta) = 0$ olması için gerek ve yeter koşul $x - \beta \mid f(x)$ olmasıdır.

Önerme 2.16 $\mathbb{F}$ sonlu bir cisim olsun. Aşağıdaki eşitlik sağlanır:

$$\prod_{\beta \in \mathbb{F}} (x - \beta) = x^{|\mathbb{F}|} - x. \tag{2.4}$$

Teorem 2.17 $\mathbb{F}$ bir cisim olsun. $\mathbb{F}$ üzerinde tanımlı derecesi $n \geq 0$ olan polinomun, $\mathbb{F}$'nin her bir genişlemesinde en fazla n kökü vardır [19].

Bundan sonra q elemanlı sonlu bir cisim $\mathbb{F}_q$ veya $GF(q)$ biçiminde gösterilecektir.

Tanım 2.17 $\mathbb{F}_q$ sonlu bir cisim ve $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ olsun. $\mathbb{F}_q^*$ çarpımsal grubunun üretecine **ilkel eleman** (primitive element) denir. Yani $\alpha \in \mathbb{F}_q$ elemanı için $\mathbb{F}_q = \{0, \alpha, \alpha^2, ..., \alpha^{q-1}\}$ ise α'ya ilkel eleman denir.

Örnek 2.5 (i) $\mathbb{Z}_5$ kümesinin ilkel elemanları 2 ve 3'tür.

(ii) α, $1 + x + x^2 \in \mathbb{F}_2[x]$ polinomunun kökü olmak üzere $\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \mathbb{F}_2[x]/(x^2 + x + 1)$ kümesi ele alınsın.

$$\alpha^2 + \alpha + 1 = 0 \Rightarrow \alpha^2 = -(1+\alpha) = 1 + \alpha \qquad \alpha^3 = \alpha(\alpha^2) = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1$$

Böylece $\mathbb{F}_4 = \{0, \alpha, 1+\alpha, 1\} = \{0, \alpha, \alpha^2, \alpha^3\}$ olur. Yani α ilkel elemandır. Benzer şekilde $\alpha+1$'inde ilkel eleman olduğu görülebilir.

Teorem 2.18 Her sonlu cisim bir ilkel eleman içerir. Yani, sonlu cismin çarpımsal grubu devirlidir.

Teorem 2.19 $\mathbb{F}_q$'da bir elemanın ilkel olması için gerek ve yeter koşul derecesinin $q-1$ olmasıdır.

Tanım 2.18 $f(x) \in \mathbb{F}_q[x]$ derecesi en küçük monik polinom ve $\alpha \in \mathbb{F}_{q^m}$ olsun. Eğer $f(\alpha) = 0$ ise $f(x)$'e **minimal polinom** denir.

Örnek 2.6 α, $1+x+x^2 \in \mathbb{F}_2[x]$ polinomunun kökü olsun.

$$1+(1+\alpha)+(1+\alpha)^2 = 1+1+\alpha+1+\alpha^2 = 1+\alpha+\alpha^2 = 0$$

ve $1+\alpha$, x ve $1+x$'nin kökü olmadığından $1+x+x^2$, $1+\alpha$'nın minimal polinomudur. Benzer şekilde $1+x+x^2$, α'nın da minimal polinomudur.

Teorem 2.20 (i) $\mathbb{F}_{q^m}$'nın her elemanının minimal polinomu vardır ve tektir. Bu polinom $\mathbb{F}_q$ üzerinde indirgenemezdir.

(ii) Eğer monik indirgenemez bir $M(x) \in \mathbb{F}_q[x]$ polinomunun $\alpha \in \mathbb{F}_{q^m}$ kökü varsa bu polinom α'nın minimal polinomudur.

Tanım 2.19 n ve q aralarında asal olsunlar. q'nun modülo n'ye göre **dairesel koseti** (cyclotomic coset) aşağıdaki şekilde tanımlanır:

$$C_i = \{(i \cdot q^j \pmod n) \in \mathbb{Z}_n : j = 0,1,\ldots\}. \tag{2.5}$$

Eğer $C_{i_1},\ldots,C_{i_t}$'ler faklı ve $\bigcup_{j=1}^{t} C_{i_j} = \mathbb{Z}_n$ ise $\{i_1,\ldots,i_t\} \subset \mathbb{Z}_n$ alt kümesi, q'nun modülo n'ye göre dairesel kosetlerinin tüm küme gösterimi olarak isimlendirilir.

Örnek 2.7 Modülo 15'e göre 2'nin dairesel kosetleri bulunsun.

$C_0 = \{0\}$ $C_1 = \{1,2,4,8\}$ $C_3 = \{3,6,9,12\}$ $C_5 = \{5,10\}$ $C_7 = \{7,11,13,14\}$

$C_1 = C_2 = C_4 = C_8$'dir. Benzer şekilde diğer eşitliklerde söylenebilir. Buradan $\{0,1,3,5,7\}$ kümesi 2'nin modülo 15'e göre dairesel kosetlerinin tüm küme gösterimidir.

Teorem 2.21 α, $\mathbb{F}_{q^m}$ 'nin ilkel elemanı olsun. α^i'nin minimal polinomu

$$M^{(i)}(x) = \prod_{j \in C_i} (x - \alpha^j) \tag{2.6}$$

şeklindedir. Burada C_i, q'nun modülo $q^m - 1$'e göre tek dairesel kosetidir.

Örnek 2.8 α, $2 + x + x^2 \in \mathbb{F}_3[x]$ polinomunun kökü olsun. Buradan,

$$2 + \alpha + \alpha^2 = 0$$

yazılır. Hem α'nın minimal polinomu hem de α^3'ün minimal polinomu $2 + x + x^2$'dir. Çünkü

$$\begin{aligned} 2 + \alpha^3 + \alpha^6 &= 2 + \alpha(\alpha^2) + (\alpha^3)^2 = 2 + \alpha(1 + 2\alpha) + (\alpha^3)^2 = 2 + \alpha + 2\alpha^2 + (\alpha^3)^2 \\ &= 2 + \alpha + 2(1 + 2\alpha) + (\alpha^3)^2 = 2 + \alpha + 2 + \alpha + (\alpha^3)^2 = 2 + (2 + 2\alpha) + (2 + 2\alpha)^2 \\ &= 2 + 2 + 2\alpha + 1 + 2\alpha + \alpha^2 = 2 + \alpha + \alpha^2 = 0 \end{aligned}$$

α^2'nin minimal polinomuna bakılırsa,

$$M^{(2)}(x) = \prod_{j \in C_2} (x - \alpha^j) = (x - \alpha^2)(x - \alpha^6) = \alpha^8 - (\alpha^2 + \alpha^6)x + x^2$$

$\alpha^8 = 1$ 'dir. $M^{(2)}(x)$'i bulmak için $\alpha^2 + \alpha^6$ bulmak yeterlidir. $2 + \alpha + \alpha^2 = 0$ eşitliği kullanılırsa,

$$\alpha^2 + \alpha^6 = (1 - \alpha\ ) + (1 - \alpha)^3 = 2 - \alpha - \alpha^3 = 2 - \alpha - \alpha(1 - \alpha) = 2 - 2\alpha + \alpha^2 = 0$$

Buradan α^2'nin minimal polinomu $1 + x^2$ olduğu çıkar. Benzer şekilde α^5'in minimal polinomu $2 + 2x + x^2$ olduğu elde edilir.

Teorem 2.22 n pozitif bir tamsayı olmak üzere $ebob(q,n)=1$ olsun. m, $n|(q^m-1)$ sağlayacak şekilde pozitif bir tamsayı olsun. α, $\mathbb{F}_{q^m}$'in ilkel elemanı ve $M^{(j)}(x)$ α^j'nin minimal polinomu olsun. $\{s_1,...,s_t\}$ modülo n'ye göre q'nun dairesel kosetlerinin tüm küme gösterimi olsun. O halde x^n-1 polinomunun, $\mathbb{F}_q$ üzerinde monik indirgenemez polinomların çarpımı şeklinde yazılışı vardır:

$$x^n-1=\prod_{i=1}^{t} M^{((q^m-1)s_i/n)}(x). \tag{2.7}$$

Sonuç 2.23 n pozitif bir tamsayı olmak üzere $ebob(q,n)=1$ olsun. x^n-1'in monik indirgenemez çarpanlarının sayısı modülo n'ye göre q'nun dairesel kosetlerinin sayısına eşittir [16].

2.2 Sonlu Cisimler Üzerindeki Vektör Uzayları

Tanım 2.20 $\mathbb{F}_q$ sonlu bir cisim olsun. $\mathbb{F}_q$ üzerinde tanımlı V kümesi boştan farklı ve elemanları arasında toplama ve çarpma işlemi sağlansın. Eğer V kümesi aşağıdaki özellikleri sağlarsa $\mathbb{F}_q$ üzerinde **vektör uzayı** olarak isimlendirilir [16].

Tüm $u,v,w\in V$ ve $\lambda,\mu\in\mathbb{F}_q$ olmak üzere,

- **i.** $u+v\in V$
- **ii.** $(u+v)+w=u+(v+w)$
- **iii.** Tüm $v\in V$ için $0+v=v+0=v$ olacak şekilde $0\in\mathbb{F}$ var,
- **iv.** Tüm $u\in V$ için $u+(-u)=(-u)+u=0$ olacak şekilde $-u\in V$ var,
- **v.** $u+v=v+u$
- **vi.** $\lambda v\in V$
- **vii.** $\lambda(u+v)=\lambda u+\lambda v,(\lambda+\mu)u=\lambda u+\mu u$
- **viii.** $(\lambda\mu)u=\lambda(\mu u)$
- **ix.** 1, $\mathbb{F}_q$'nun çarpımsal birimseli ise $1u=u$.

$\mathbb{F}_q^n$, elemanları $\mathbb{F}_q$'de olan n uzunluğunda tüm vektörlerin kümesi olmak üzere aşağıdaki şekilde tanımlanır:

$$\mathbb{F}_q^n = \{(v_1, v_2, ..., v_n) : v_i \in \mathbb{F}_q\}.$$

$\mathbb{F}_q^n$ için **vektör toplamı** $v = (v_1, v_2, ..., v_n) \in \mathbb{F}_q^n$ ve $w = (w_1, w_2, ..., w_n) \in \mathbb{F}_q^n$ olmak üzere

$$v + w = (v_1 + w_2, ..., v_n + w_n) \in \mathbb{F}_q^n$$

şeklinde tanımlanır. $\mathbb{F}_q^n$ için **skaler çarpım** ise $v = (v_1, v_2, ..., v_n) \in \mathbb{F}_q^n$ ve $\lambda \in \mathbb{F}_q$ olmak üzere

$$\lambda v = (\lambda v_1, ..., \lambda v_n) \in \mathbb{F}_q^n$$

olarak tanımlanır.

$0 = (0, 0, ..., 0) \in \mathbb{F}_q^n$'de **sıfır vektör** olarak tanımlansın.

Örnek 2.9 Aşağıdakiler $\mathbb{F}_q$ üzerinde tanımlı vektör uzaylarıdır.

(i) $C_1 = \mathbb{F}_q^n$ ve $C_2 = \{0\}$.

(ii) $(q = 2)$ $\quad C_3 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$.

(iii) $(q = 3)$ $\quad C_4 = \{(0,0,0), (0,1,2), (0,2,1)\}$.

Bundan sonra $(v_1, v_2, ..., v_n)$ vektörü $v_1 v_2 ... v_n$ olarak yazılacaktır.

Tanım 2.21 C, vektör uzayı V'nin bir alt kümesi olsun. Eğer C, V'deki toplama ve çarpma işlemine göre kendi başına bir vektör uzayı ise C'ye V'nin **alt uzayı** denir.

Önerme 2.24 C, $\mathbb{F}_q$ üzerinde tanımlı V vektör uzayının alt kümesi olsun. Aşağıdaki denklik sağlanır:

C alt uzaydır $\Leftrightarrow$ $x, y \in C$ ve $\lambda, \mu \in \mathbb{F}_q$ için $\lambda x + \mu y \in C$.

Tanım 2.22 V , $\mathbb{F}_q$ üzerinde tanımlı vektör uzay olsun. $\lambda_1,...,\lambda_r \in \mathbb{F}_q$ skalerler olmak üzere $v_1, v_2, ..., v_r \in V$ vektörlerinin **lineer kombinasyonu** $\lambda_1 v_1 + ... + \lambda_r v_r$ şeklindedir.

Tanım 2.23 V , $\mathbb{F}_q$ üzerinde tanımlı vektör uzay olsun. Eğer

$$\lambda_1 v_1 + ... + \lambda_r v_r = 0 \Rightarrow \lambda_1 = \cdots = \lambda_r = 0$$

ise $(v_1, v_2, ..., v_r)$ vektör kümesine **lineer bağımsız** denir.

Eğer küme lineer bağımsız değilse **lineer bağımlı** olarak isimlendirilir. Yani $\lambda_1,...,\lambda_r \in \mathbb{F}_q$ skalerlerden en az bir tanesi sıfırdan farklı olmak üzere

$$\lambda_1 v_1 + ... + \lambda_r v_r = 0$$

sağlanıyorsa $(v_1, v_2, ..., v_r)$ vektör kümesi lineer bağımlıdır denir.

Örnek 2.10 (i) $\{(0,0,0,1),(0,0,1,0),(0,1,0,0)\}$ kümesi lineer bağımsızdır.

(ii) $\{(0,0,0,1),(1,0,0,0),(1,0,0,1)\}$ kümesi lineer bağımlıdır.

Tanım 2.24 V , $\mathbb{F}_q$ üzerinde tanımlı vektör uzay olsun ve $S = \{v_1,...,v_k\}$, V 'nin boştan farklı bir alt kümesi olsun. S 'nin **(lineer) üreteci**

$$\langle S \rangle = \{\lambda_1 v_1 + ... + \lambda_k v_k : \lambda_i \in \mathbb{F}_q\}$$

şeklinde tanımlanır. Eğer $S = \varnothing$ ise $\langle S \rangle = \{0\}$ ile tanımlanır. $\langle S \rangle$, V 'nin alt uzayıdır ve S tarafından üretilmiş alt uzay olarak isimlendirilir.

Örnek 2.11 $q = 2$ ve $S = \{0001, 0010, 0100\}$ olmak üzere

$$\langle S \rangle = \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\}.$$

Tanım 2.25 V , $\mathbb{F}_q$ üzerinde tanımlı vektör uzay ve $B = \{v_1,...,v_k\}$, V 'nin alt kümesi olsun. Eğer $V = \langle B \rangle$ ve B lineer bağımsız ise B 'ye V için **taban** denir.

Tanım 2.26 $B=\{v_1,...,v_k\}$, V'nin tabanı olsun. Herhangi bir vektör $v\in V$ B'deki vektörlerin lineer kombinasyonu olarak tek türlü şekilde yazılır. Yani, $\lambda_1,...,\lambda_r\in\mathbb{F}_q$ için

$v=\lambda_1 v_1+\lambda_2 v_2...+\lambda_k v_k$.

Tanım 2.27 V, $\mathbb{F}_q$ üzerinde tanımlı vektör uzay olsun. V birden fazla tabana sahip olabilir. Ancak tüm tabanlar aynı sayıda eleman sayısına sahiptir. Bu sayı V'nin **boyutu** olarak isimlendirilir ve $\dim(V)$ ile gösterilir.

Teorem 2.25 V, $\mathbb{F}_q$ üzerinde tanımlı vektör uzay olsun. Eğer $\dim(V)=k$ ise aşağıdakiler sağlanır:

(i) V, q^k elemana sahiptir.

(ii) V'nin $\frac{1}{k!}\prod_{i=0}^{k-1}(q^k-q^i)$ faklı tabanı vardır.

Örnek 2.12 $q=2$, $S=\{0001,0010,0100\}$ ve $V=\langle S\rangle$ olsun. O halde,

$V=\{0000,0001,0010,0100,0011,0101,0110,0111\}$

S lineer bağımsızdır ve $\dim(V)=3$. V için farklı taban sayısı,

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k-2^i)=\frac{1}{3!}(2^3-1)(2^3-2\ )(2^3-2^2)=28.$$

Tanım 2.28 $v=(v_1,v_2,...,v_n), w=(w_1,w_2,...,w_n)\in\mathbb{F}_q^n$ olsun.

(i) v ve w'nin **skaler çarpımı (iç çarpım)** aşağıdaki şekilde tanımlanır:

$v\cdot w=v_1w_1+\cdots+v_nw_n\in\mathbb{F}_q^n$.

(ii) Eğer $v\cdot w=0$ ise v ve w vektörleri **diktir (orthogonal)** denir.

(iii) S, $\mathbb{F}_q^n$'nin boştan farklı alt kümesi olsun. S'nin **ortoganal tümleyeni**

$S^{\perp}=\{v\in\mathbb{F}_q^n : v\cdot s=0, \forall s\in S\}$

olarak tanımlanır. Eğer $S = \varnothing$ ise $S^{\perp} = \mathbb{F}_q^n$.

Örnek 2.13 $q = 2$ ve $n = 4$ olsun. $u = (1,1,1,1)$, $v = (1,1,1,0)$ ve $w = (1,0,0,1)$ için

$$u \cdot v = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 1$$
$$u \cdot w = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 = 0$$
$$v \cdot w = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 = 1$$

u ve w ortogonaldir.

Teorem 2.26 S, $\mathbb{F}_q^n$'nin alt kümesi olsun. Aşağıdaki sağlanır:

$$\dim\left(\langle S \rangle\right) + \dim\left(\left\langle S^{\perp} \right\rangle\right) = n.$$

BÖLÜM 3

KODLAMA TEORİSİ

3.1 Giriş

Haberleşme sistemleri ve veri depolama aygıtları gibi bilgi araçları, parazitler yüzünden çok güvenilir değildir [16]. Bilginin parazitli kanallar boyunca güvenilir şekilde iletimi dijital bilgi ve haberleşme araçlarının temel gereksinimidir. Buradaki iletim, hem boşlukta iletim (mobil radyo kanalları gibi) hem de zaman içinde iletim (herhangi bir anda depolanmış bilginin bir süre sonra alınması) olarak anlaşılmalıdır. Bu gereksinimden dolayı modern haberleşme sistemleri çok güçlü kanal kodlama metodolojilerine bağlı durumdadır. Pratik uygulamalarda bu kodlama teknikleri yalnızca kanalda tanımlanan hataları bulma veya düzeltme kapasitelerine göre iyi kodlama karakteristiğine sahip olması yetmez. Hızlı bir şekilde uygulanabilir olmalıdır. Örneğin; dijital donanımlardaki birleşik devrelerde (integrated circuit) olduğu gibi. Kanal kodlarının uygulamaları boşluk ve uydu haberleşmesi, veri iletimi, dijital ses ve video yayımları ve mobil haberleşmeleri içerir. Bunlara ek olarak bilgisayar hafızaları veya yoğun (compact) disk gibi depolama sistemleri de sayılabilir [20].

3.2 Veri – İletim Kodlarının Tarihi

Veri-iletim kodlarının tarihi, 1948'de Claude Shannon tarafından yazılan meşhur makale ile başladı. Shannon'un gösterdiği herhangi bir iletişim kanalı veya depo kanalı ile ilişkilendirilmiş ve bu kanalın *kapasitesi* olarak adlandırılan bir C sayısı (bit/saniye olarak ölçülür) aşağıda belirtilen öneme sahiptir. İletişim ve depolama sistemleri için gerekli olan bilgi iletim hızı (oranı) R'nin (bit/saniye) C'den az olduğu durumlarda data-iletim kodları kullanılarak, çıkış hataları ihtimalinin istenilen kadar küçük olduğu kanallar için iletişim sistemleri tasarlamak mümkündür. Aslında, Shannon'un bilgi

teorisinin en önemli sonuçlarından biri kodlanmamış modülatör-demodülatör kullanarak ham hata oranını (the raw error rate) çok iyi yapmaya çalışmanın gereksiz olduğudur. Güçlü data-iletim kodlarının kullanımı hem daha ucuz hem de sonuç olarak daha verimlidir.

Ne var ki, Shannon, uygun kodların nasıl bulunacağını bize söylemiyor. Shannon'un katkısı bu kodların var olduğunu ispatlamak ve onların rollerini tanımlamak olmuştur. 1950'ler boyunca istenilen rastgele hata olasılıklarını üretecek kodların elde edilebilmesi için gereken belirgin yapıların bulunması için büyük çaba sarf edildi. Fakat ilerlemeler yetersiz kaldı. 1960'larda bu iddialı hedefi gerçekleştirmek için daha az çaba sarf edildi. Bunun yerine kodlama çalışmaları daha geniş zamana yayılarak iki ana yola bölünmüştür.

İlk yol daha cebirseldir ve öncelikli olarak blok kodlarla alakalıdır. İlk blok kodlar 1950 yılında Hamming tek-hata-düzelten blok kod sınıflarını tanımlamasıyla ortaya çıkmıştır. Bundan kısa bir süre sonra, Muller (1954) çoklu-hata-düzelten kod sınıflarını tanımlamıştır ve Reed de aynı yıl bu kodları dekodlayan (çözümleyen) algoritmaları vermiştir. Hamming kodları ve Reed-Muller kodları ne yazık ki Shannon tarafından vaat edilen çok güçlü kodlara nazaran zayıftılar. Yürütülen titiz araştırmalara rağmen 1960'ların sonuna kadar daha iyi bir kod sınıfı bulunamamıştır. Bu süreçte kısa blok-uzunlukta kodlar bulunmuş fakat genel bir teori oluşturulamamıştır. Büyük ilerlemeler Bose ve Ray-Chaudhuri'nin (1960) ve Hocquenghem'in (1959) büyük bir çoklu-hata-düzelten kod sınıfı (BCH kodları) ve Reed ve Solomon'un (1960), aynı zamanda bu çalışmalardan bağımsız olarak Arimoto'nun (1961) bu kod sınıfı ile bağlantılı iki elemanlı olmayan (nonbinary) kanallar için bir kod sınıfı geliştirmesi ile gerçekleşmiştir. Geliştirilen bu kod sınıfları en önemli kodlar arasında yer almakla birlikte, konunun teorisi o zamandan beri sürekli güçlendirilmektedir ve yeni kodlar keşfedilmeye devam etmektedir.

BCH kodlarının keşfi kodlayıcı (encoder) ve dekoder yapabilmek için gereken donanım ve yazılım geliştirilmesi için pratik metotların araştırılmasına sebep olmuştur. İlk iyi algoritma Peterson (1960) tarafından bulunmuştur. Sonra, Berlekamp (1968) ve Massey (1969) tarafından dekodlama için güçlü birer algoritma geliştirilmiştir ve bu algoritmanın gerçekleştirilmesi yeni dijital teknolojinin ortaya çıkmasıyla mümkün olmuştur. Şimdi değişik kod ve uygulamalara uyan birçok çeşit algoritma vardır.

Kodlama araştırmalarında ikinci yol daha çok olasılıkla ilgilidir. En iyi kodlar bilinmemesine rağmen ilk araştırmalar en iyi blok kod ailelerinin hata olasılıklarının tahmin edilmesine yönlendirildi. Bu çalışmalarla ilişkili olarak olasılık bakış açısından kodlama ve dekodlma işlemleri anlaşılmaya çalışıldı ve bu çabalar sıralı dekodlama (sequential decoding) kavramını ortaya çıkardı. Sıralı dekolama, bir ağaçla gösterilen ve bu ağacı araştıran algoritmalarla dekodlanan sonsuz uzunluktaki non-blok kod sınıflarını gerektirmiştir. En kullanışlı ağaç kodları *konvolüsyonel kodlar (convolutional codes)* olarak adlandırılan oldukça yapılandırılmış kodlardır. Bu kodlar, data dizisinde konvolüsyon işlemi gerçekleştiren lineer değiştir-kaydol (shift-register) devreleri tarafından oluşturulur. Konvolüsyonel kodlar 1950'li yılların sonlarında başarıyla sıralı dekodlama kodları tarafından dekodlanmıştır. Bu kodları dekodlayan ve daha basit bir algoritma olan Viterbi algoritmasının 1967 senesine kadar geliştirilememiş olması oldukça şaşırtıcıdır. Viterbi algoritması orta karışıklıktaki konvolüsyonel kodlar için geniş bir popülarite kazandı fakat daha güçlü konvolüsyonel kodlar için kullanışsızdır.

1970'ler boyunca, bu iki araştırma yolu bazı noktalarda birleşirken bazı noktalarda birbirlerinden ayrılmışlardır. Konvolüsyonel kodların cebirsel teorilerinin geliştirilmesine konuya yeni bir bakış açısı getiren Massey ve Forney tarafından başlandı. Blok kodlar teorisinde, uzun blok-uzunluklu iyi kodlar (good codes) oluşturabilmek için şemaların kullanılması önerildi. Bağlantılı kodlar (Concatenated codes) Forney (1966) tarafından tanımlandı ve Justesen bağlantılı kod fikrini iyi performanslı ve tamamen yapısal uzun blok kod sınıflarının oluşturulması için kullandı. Aynı zamanda, Goppa 1970 yılında, iyi kodların nasıl tanımlanacağını söylememesine rağmen kesinlikle iyi kodlar içeren bir kod sınıfı tanımladı.

1980'ler yeni dizayn edilmiş dijital iletişim ve depolama sistemlerini sıklıkla kullanan kodlayıcı (encoder) ve dekodlayıcının (decoder) varlığına şahitlik etti. Bu konuda en iyi örnek, çifte bayt hatalarını düzeltmek için basit Reed-Solomon kodlarını kullanan kompakt disklerdir. Reed-Solomon kodları aynı zamanda sıklıkla manyetik teyp sürücüleri, net modemleri ve şimdi de dijital video disklerinde kullanılmaktadır. Telefon-hatlı modem gibi diğer uygulamalarda, cebirsel kodların rollerini, Ungerboeck'in (1982) trelis-kodlu (trellis-coded) modülasyonu gibi Öklid-uzay kodları almıştır. Bu metotların başarısı, Öklid uzaklık tabanlı cebirsel olmayan kodların dizaynı üzerine daha fazla çalışma yapılmasına sebep olmuştur. 1980'ler bilgi-iletim kodlarının geniş bir alanda kullanımları ile sona ermiştir. Aynı zamanda, matematikçiler, cebirsel

geometri konusunun Hamming uzaklığını temel alan iyi kodları araştırmaya başladılar ve bu noktada git gide daha da büyüyen teoriksel bir gelişim dalgası başlamış oldu.

1990'lar kodlama, sinyal işleme ve dijital iletişim arasındaki duvarların giderek kaybolduğu yıllar oldu. Turbo dekodlama kavramının gelişmesi ve buna eşlik eden Berrou (1993) kodları bu dönemin ana olayları olarak görülebilir. Bu olanlar, geniş bant kanalları üzerinden iletişim için en az Ungerboeck'in bir önceki on yılda limitli bant kanalları üzerinden iletişim için yaptıkları kadar etkili olmuştur. Büyük ikili kodların kolay-karar verme (soft-decision) dekodlaması için kullanılan "İki-Yol Algoritması" gibi pratik tekrarlayan algoritmalar, Shannon tarafından vaat edilen performansın yakalanmasına artık olanak sağlamaktadır. Ungerboeck ve Berrou kodları, onların Öklid-uzay dekodlama algoritmaları ile birlikte, halen hızlı bir gelişim içerisinde olan ve modülasyon teorisi ile bilgi-iletim kodları konuları arasında yer alan bir kısım teknikleri oluşturmuştur. Shannon'un vaat ettiği kodlar için halen çalışmalar gerekmektedir.

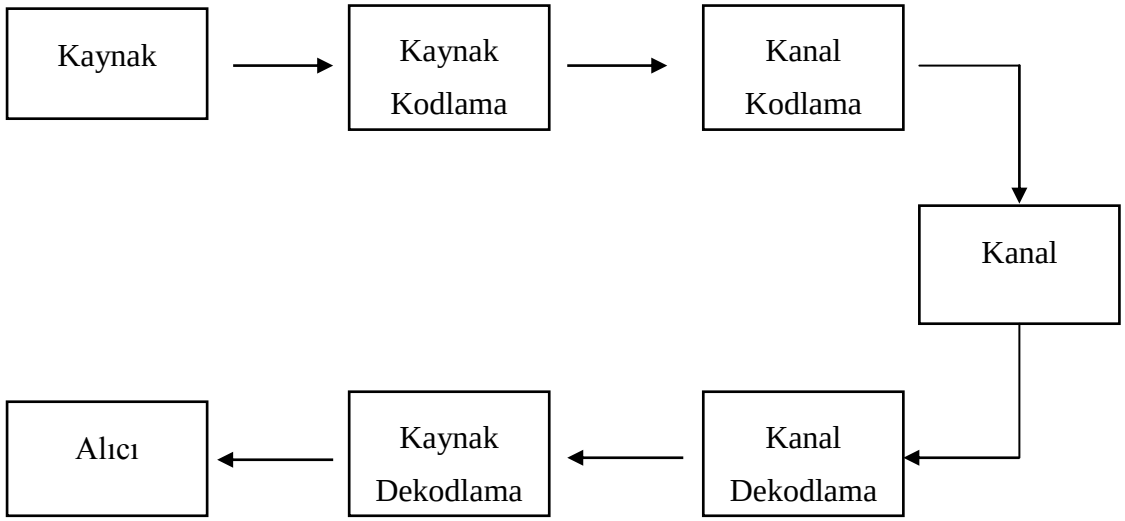
Bu on yıl ayrıca cebirsel eğriler üzerinde tanımlanan büyük ikili-olmayan kodların zor-karar verme (hard-decision) dekodlaması için kullanılan algoritmaların geliştirilmesine de şahitlik etmiştir. Hermityen kodlar olarak bilinen kodların dekoderleri artık mevcuttur ve bu kodlar yakında ticari ürün olarak temin edilebilecektir. Aynı zamanda, konunun kökleri zengin matematik toprağının derinliklerine doğru büyümeye devam etmektedir [21].

3.3 Haberleşme Sistemleri

Haberleşme sistemleri, veri kaynağını veri kullanıcısına bir kanal yoluyla bağlar. Mikrodalga bağlantılar, eş eksenli (coaxial) kablolar, telefon devreleri, manyetik ve optik diskler kanallara örnektir [21]. Şekil 3.1 bir haberleşme sisteminde bilginin kaynaktan (source) alıcıya (receiver) kanal vasıtasıyla iletimini göstermektedir [19].

Kodlama Teorisi genel olarak *kaynak kodlama (source coding)* ve *kanal kodlama (channel coding)* olarak tanımlanır [16]. Kaynak kodlamanın iki rolü vardır. Birincisi, kaynak çıktısı ile kanal girdisi arasında dönüştürücü vazifesi görmektedir. Yani kaynak mesajı, kanala uygun koda çevirmektedir. Örneğin, kaynaktan alıcıya iletilecek bilgi analog sinyallerden oluşuyor iken kanal dijital verileri alıyor olsun. Kodlama safhasında analogdan-dijitale dönüşüm gerçekleşecektir. Ve dekodlama safhasında da tersine

dijitalden-analoğa dönüşüm gerçekleşecektir. İkincisi, kaynak kodlama, iletim uzunluğunun ekonomik olması için kaynak çıktısını (output) *sıkıştırır (compress).* Kanalın diğer ucunda kaynak dekodlamasında ise alınan sinyal veya dizi genişletilir. Bazı uygulamalarda çözücü (dekoder) alınan veriyi orijinali ile eşleşmesi için onarır ve sıkıştırma *kayıpsız (lossless)* olarak nitelendirilir. Ses ve görüntü iletimi gibi bazı uygulamalarda ise, orijinal ve onarılmış veri arasında bazı farklılıklara -bozulmalara- izin verir ve sıkıştırma *kayıplı (lossy)* olarak nitelendirilir [19].



Şekil 2. 1 Haberleşme Sistemi

Örnek 3.1: Kaynak kodlamaya örnek ASCII kodlardır. Her bir karakteri 8 bitlik byte'a çevirir.

Örnek 3.2: Elma, muz, kiraz ve üzüm aşağıdaki şekilde kaynak kodlansın:

$$\text{elma} \rightarrow 00, \quad \text{muz} \rightarrow 01, \quad \text{kiraz} \rightarrow 10, \quad \text{üzüm} \rightarrow 11$$

00 olarak kodlanan 'elma' mesajı parazitli bir kanaldan iletilsin. Mesaj bu kanalda bozulsun ve 01 alınsın. Alıcı mesajın bozulduğunu fark edemeyebilir ve bu haberleşme başarısız olur.

Fiziksel ve mühendislik kısıtlamalardan dolayı kanallar mükemmel değillerdir. Parazitler veya noksanlıktan dolayı kanallara giren mesaj ile çıkan mesaj arasında farklılıklar olabilir. Kanal kodlamanın esas görevi bu kısıtlamaların üstesinden gelmektir ve kaynak ile alıcı arasında olabildiğince saydam olmaktır [19].

Kanal kodlama, mesajı kaynak kodlamadan sonra tekrar kodlayarak yapılmaktadır. Bu şekilde hatanın bulunması ve düzeltilmesi sağlanır [16].

Örnek 3.3: Örnek 3.2 deki mesajlara 1 bit eklenerek kanal kodlama aşağıdaki şekilde yapılsın:

$$00 \rightarrow 000, \quad 01 \rightarrow 011, \quad 10 \rightarrow 101, \quad 11 \rightarrow 110$$

Kaynak ve kanal kodlamasından sonra 000 şeklinde kodlanan 'elma' mesajı, 1 hata oluşturan kanaldan iletilsin. Alıcıya 100, 010, 001 kodlarından birisini ulaşacaktır. Bu kodlardan hiçbiri yukarıda tanımlanan elma, muz, kiraz, üzüm mesajlarından birine ait olmadığı için hata bulunmuş olur.

Kanal kodlamadaki amaçlar şu şekilde sıralanabilir [16]:

1. Mesajları hızlı kodlama,
2. Kodlanmış mesajları kolay şekilde iletme,
3. Alınan mesajları hızlı şekilde dekodlama,
4. Her bir saniyede maksimum bilgi transferi,
5. Azami hata bulma ve hata düzeltme kapasitesi.

Tanım 3.1 $A = \{a_1, a_2, ..., a_q\}$ kümesi sonlu bir küme olsun. A kümesi **kod alfabesi** olarak isimlendirilir. $C \subseteq A$ kümesine ***q*'lu kod** denir. C'nin elemanlarına da **kodsözler** denir [22].

Örnek 3.4: $\mathbb{Z}_2 = \{0,1\}$ kümesi bir kod alfabesidir. $C = \{00, 01, 10, 11\}$ ise ikili koddur. $10 \in C$ bir kodsözdür.

En çok kullanılan alfabe $\mathbb{Z}_2$ alfabesidir. $\mathbb{Z}_2$ üzerinde oluşturulan kodlara **ikili kodlar** (binary codes) denir. $\mathbb{Z}_3$ alfabesi üzerindeki kodlara da **üçlü kodlar** (ternary codes) denir.

Tanım 3.2 $S = \{s_1, s_2, ..., s_q\}$ sonlu bir küme olsun. S kümesine **kaynak alfabesi** (source alphabet) denir. C bir kod olsun. $f : S \rightarrow C$ bijektif fonksiyonuna **kodlama fonksiyonu** denir.

Kodlama fonksiyonu bijektif (birebir, örten) olduğundan kaynak alfabedeki her sembol (source symbol) yalnızca bir kodsöze gider. Yani her bir kod söz kaynak sembollerle ilgilidir. Bu da kodsöz dizilerini çözmede (decode) olanak sağlar [22].

Örnek 3.5: Alfabedeki 26 harf şu şekilde kodlansın; Kaynak alfabesi $S=\{a,b,...,z\}$, kod alfabesi $A=\{0,1,...,9\}$ ve kod $C=\{00,01,01,...,25\}$ olsun. $f:S\to C$ şöyle tanımlansın:

$f(a) = 00$ $f(b) = 01$ $f(c) = 02$ $f(d) = 03$ $f(e) = 04$

$f(f) = 05$ $f(g) = 06$ $f(h) = 07$ $f(i) = 08$ $f(j) = 09$

$f(k) = 10$ $f(l) = 11$ $f(m) = 12$ $f(n) = 13$ $f(o) = 14$

$f(p) = 15$ $f(q) = 16$ $f(r) = 17$ $f(s) = 18$ $f(t) = 19$

$f(u) = 20$ $f(v) = 21$ $f(v) = 22$ $f(x) = 23$ $f(y) = 24$

$f(z) = 25$

Bu kodlama fonksiyonu herhangi bir mesajı kodlamada kullanılabilir. Örneğin;

math is fun → 120019070818032013

Her bir kodsöz için iki rakamlı sayılar kullanılmasının özel bir amacı var. Eğer kod $C'=\{0,1,2,...,9,10,11,...,25\}$ kullanılmış olsaydı teklik problemi oluşurdu. Örneğin 1019 kodu birkaç farklı mesaj şeklinde sonuçlanırdı;

bat → 1019 babj → 1019 kt → 1019

Tanım 3.3 $A=\{a_1,a_2,...,a_q\}$ kod alfabesi olsun. $i=1,..,q$ ve $w_i\in A$ olmak üzere $w=w_1w_2...w_n$ dizisine ***n* uzunluğunda *q*'lu söz** denir. Burada ***w***, $(w_1,...,w_n)$ vektörü olarak düşünülmelidir [16].

Tanım 3.4 *C* bir kod olmak üzere tüm kodsözleri *n* uzunluğunda ise *C*'ye ***n* uzunluğunda blok kod** (block code) denir.

Örnek 3.6: Günlük hayatta çokça karşılaşılan uluslararası kitap numarası (ISBN) 10 uzunluğunda bir blok koddur. (Sembollerin arasındaki kısa çizgiler optik yönlendirme olduğundan okunmamaktadır) Kod alfabesi 11 sembolden oluşmaktadır: 0, 1, 2, …, 9 ve X (okunuşu: on). Örneğin; Lin ve Costello' nun (1983) kitap numarası aşağıdaki gibidir:

ISBN 0-13-283796-X

İlk numara 0 ülkeyi (ABD), 13 yayımcıyı (Prentice-Hall) ve sonraki altı basamakta yayımcı tarafından verilen kitap numarasını göstermektedir. Son sembol ise kontrol sembolüdür ve seçilişi ISBN kodsözleri $a_1a_2...a_{10}$ olmak üzere

$$\sum_{i=0}^{10} ia_{11-i} = 10a_1 + 9a_2 + 8a_3 + ... + 2a_9 + a_{10}$$

toplamını 11'in katı yapacak şekildedir. Örneğin yukarıdaki ISBN ele alınırsa ,

$$10\times0+9\times1+8\times3+7\times2+6\times8+5\times3+4\times7+3\times9+2\times6+1\times10=132=11\times12.$$

Tanım 3.5 *C* deki kodsözlerin sayısına ***C*'nin büyüklüğü** denir ve $|C|$ olarak gösterilir.

Tanım 3.6 *n* uzunluğundaki bir *C* kodunun iletim oranı (information rate) $\left(\log_q |C|\right)/n$ olarak hesaplanır.

Tanım 3.7 Uzunluğu *n*, büyüklüğü *M* olan kod **(*n*, *M*)-kod** olarak isimlendirilir [16].

Örnek 3.7 $\mathbb{F}_2 = \{0,1\}$ kod alfabesi olsun ($q = 2$).

(i) $C_1 = \{00, 01, 10, 11\}$ kodu (2,4)-koddur. İletim oranı $\log_2 4/2 = 1$'dir.

(ii) $C_2 = \{000, 011, 101, 110\}$ kodu (3,4)-koddur. İletim oranı 2/3'tür.

(iii) $C_3 = \{000, 111\}$ kodu (repetition code) (3,2)-koddur. İletim oranı 1/2'dir.

$A = \{a_1, a_2, ..., a_q\}$ kümesi bir haberleşme kanalının kod alfabesi olsun. Bu kümeden alınan herhangi bir a_i sembolü kanaldan a_j olarak çıkabilir. Farklı bir zamanda ise a_i girdisi a_k olarak da kanaldan çıkabilir. Haberleşme kanalının bu özelliği, şartlı olasılıklar kümesi P(a_j alınan $\mid a_i$ gönderilen)'dir (Burada a_i gönderilen, a_j alınan mesaj). Bu olasılıklara *kanal olasılıkları* denir [22].

Tanım 3.8 Haberleşme (iletişim) kanalı, sonlu bir $A = \{a_1, a_2, ..., a_q\}$ kanal alfabesi ve aşağıdaki denklemi sağlayan iletilen kanal olasılıklarından oluşan yapıdır.

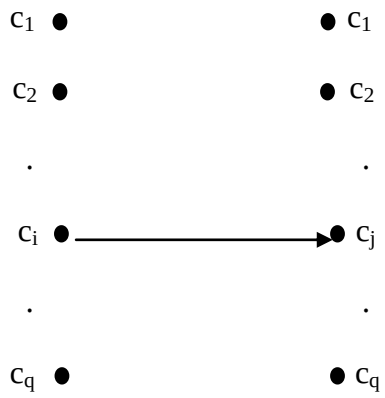
$$\sum_{j=1}^{q} P(a_j \text{ alınan} \mid a_i \text{ gönderilen}) = 1. \qquad (3.1)$$

Tanım 3.9 Bir haberleşme kanalında bir iletişim çıktısı, bir önceki çıktıdan bağımsız ise bu kanala **hafızasız** (memoryless) denir. Yani $\mathbf{x} = x_1x_2...x_n$ ve $\mathbf{c} = c_1c_2...c_n$, n uzunluğunda sözler olsunlar. Gönderilen **c** ve alınan **x**'in olasılığı

$$P(\mathbf{x} \text{ alınan} \mid \mathbf{c} \text{ gönderilen}) = \prod_{i=1}^{n} P(x_i \text{ alınan} \mid c_i \text{ gönderilen}). \tag{3.2}$$

çarpımından oluşur.

Haberleşme kanalları birçok yolla tanımlanabilir. Bunlardan bir tanesi de graf inşa etmektir (Şekil 3.2). Şekilde, sağ ve sol tarafta her bir kod sembolü için birer düğüm gösterilmiştir. Sol taraftaki her bir düğüm bir kenar ile sağdaki düğümlere bağlanmaktadır [22].



Şekil 3. 2 Graf Örneği

Tanım 3.10 Kanal alfabesinin büyüklüğü q olan hafızasız q-lu simetrik kanal şu şekilde tanımlanır:

(i) Gönderilen her bir sembolün olasılığı p $(<1/2)$, hata olarak alınan sembol ile aynıdır,

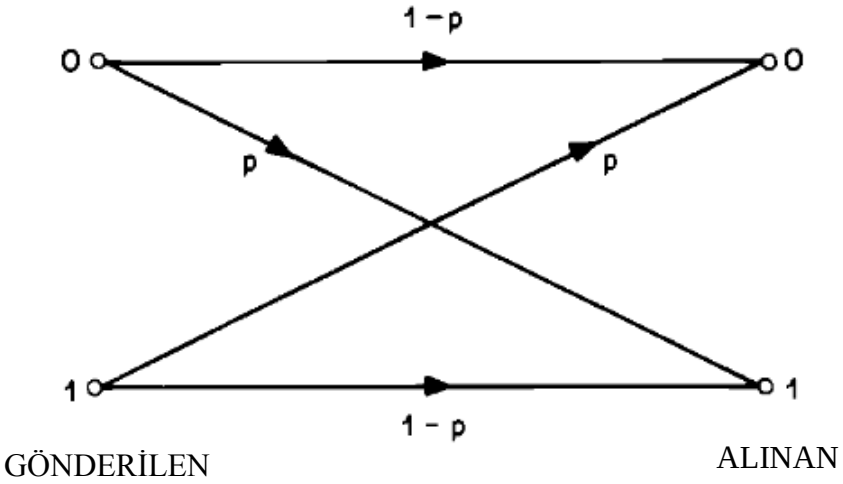
(ii) Eğer alınan sembol hatalı ise, $q-1$ sembolün her biri aynı hata olasılığına sahiptir.

Özel olarak *ikili simetrik kanal (BSC)*, kod alfabesi $\{0,1\}$ olan hafızasız kanaldır ve kanal olasılıkları

$$P(1 \text{ alınan} \mid 0 \text{ gönderilen}) = P(0 \text{ alınan} \mid 1 \text{ gönderilen}) = p, \tag{3.3}$$

$$P(1 \text{ alınan} \mid 1 \text{ gönderilen}) = P(0 \text{ alınan} \mid 1 \text{ gönderilen}) = 1-p\,. \tag{3.4}$$

BSC de her bit hatanın olasılığı p'dir ve **geçiş olasılığı** (crossover probability) ismini alır [16] (Şekil 3.3).



Şekil 3. 3 İkili simetrik kanal (binary symmetric channel (BSC))

Örnek 3.8: {000,111} kodundan alınan kod sözler, geçiş olasılığı $p = 0.05$ olan BSC üzerinden gönderilsin. Alınan mesaj 110 olsun. Gönderilen kodsözün hangisi olduğu bulunmak istenirse:

$$P(\text{110 alınan} \mid \text{000 gönderilen}) = P(\text{1 alınan} \mid \text{0 gönd.})^2 \times P(\text{0 alınan} \mid \text{0 gönd.})$$

$$= (0.05)^2 \times (0.95) = 0.002375$$

$$P(\text{110 alınan} \mid \text{111 gönderilen}) = P(\text{1 alınan} \mid \text{1 gönd.})^2 \times P(\text{0 alınan} \mid \text{1 gönd.})$$

$$= (0.95)^2 \times (0.05) = 0.045125$$

İkinci olasılık birincisinden daha büyük olduğu için 111 büyük olasılıkla gönderilen mesajdır.

3.4 Dekodlama

3.4.1 Dekoder

C, F alfabesi üzerinde bir (n, M)-kod olsun. D: $F^n \rightarrow C$ fonksiyonuna **dekoder (kod çözücü)** denir. D fonksiyonunun *dekodlama hata olasılığı* P_{err} ile gösterilir ve

$$P_{err}(c) = \sum_{y:D(y)\neq c} P\,(y \text{ alınan} \mid c \text{ gönderilen})$$

olmak üzere

$$P_{err} = \max_{c \in C} P_{err}(c) \tag{3.5}$$

dır. Burada $P_{err}(c)$, c kodunun hatalı dekodlanma olasılığını göstermektedir [19].

Örnek 3.9: C kodu ikili (3,2) tekrarlı kodu olsun ve geçiş olasılığı p olan bir BSC'den gönderilsin. D: $\{0,1\}^3 \rightarrow C$ dekoderi şöyle tanımlanır:

$D(000) = D(001) = D(010) = D(100) = 000$

$D(011) = D(101) = D(110) = D(111) = 111$

P_{err} olasılığı, iki ve daha fazla hatanın olasılıklarına eşittir:

$$P_{err} = P_{err}(000) = P_{err}(111) = \binom{3}{2} p^2(1-p) + \binom{3}{3} p^3$$

$$= 3p^2 - 3p^3 + p^3$$
$$= p(2p-1)(1-p) + p.$$

3.4.2 Maksimum Olasılıkla Dekodlama

Bir C kodunun kodsözleri bir haberleşme kanalından gönderilsin. Eğer bir **x** kodu alınmış ise $c \in C$ için kanal olasılığı

$P(\mathbf{x}$ alınan $\mid \mathbf{c}$ gönderilen$)$

hesaplanabilir. Maksimim olasılıkla dekodlamada (*maximum likelihood decoding (MLD)*) kural, dekodlanan mesajın maksimum olasılıklı $c \in C$ koduna eşit olmasıdır. Yani $\mathbf{c_x}$ büyük olasılıkla gönderilen kodsözü göstermek üzere [16];

$$\mathrm{P}(\mathbf{x} \text{ alınan} \mid \mathbf{c_x} \text{ gönderilen}) = \max_{c \in C} P(\mathbf{x} \text{ alınan} \mid \mathbf{c} \text{ gönderilen}). \tag{3.6}$$

Örnek 3.10: {000, 111} kodunun kodsözleri, geçiş olasılığı p = 0.01 olan ikili simetrik kanaldan gönderilsin. Mesajın doğru alınma olasılığı 1-p = 0.99 olur. Kanal çıktısı 100 olsun. Kanal olasılıkları;

$$P(100 \text{ alınan} \mid 000) = P(1 \text{ alınan} \mid 0 \text{ gönderilen}) \times P(0 \text{ alınan} \mid 0 \text{ gönderilen})^2$$

$$= (0.01)(0.99)^2 = 0.009801.$$

$P(100 \text{ alınan} \mid 111) = P(1 \text{ alınan} \mid 1 \text{ gönderilen}) \times P(0 \text{ alınan} \mid 1 \text{ gönderilen})^2$

$= (0.99)(0.01)^2 = 0.000099.$

İlk olasılık ikincisinden daha büyük olduğu için maksimum olasılıkla dekodlama kuralına göre 100 kodsözü, 000 olarak dekodlanır.

Maksimum olasılıkla dekodlama iki çeşittir [16]:

(i) *Tam Maksimum Olasılıkla Dekodlama*. Alınan **x** sözüne karşılık en büyük olasılıklı kodsöz bulunur. Eğer bu kodsözden birden fazla varsa keyfi olarak birisi seçilir.

(ii) *Eksik Maksimum Olasılıkla Dekodlama*. Alınan **x** sözüne karşılık en büyük olasılıklı kodsöz bulunur. Eğer bu kodsözden birden fazla varsa tekrar iletim istenir.

3.4.3 Hamming Uzaklığı

$x = x_1x_2...x_n$ ve $y = y_1y_2...y_n$, bir A alfabesinin n uzunluklu iki sözü olsun. **x** ve **y** sözlerinin birbirinden farklı bileşen sayısına **Hamming uzaklığı** denir ve d(**x**, **y**) ile gösterilir [16]. Yani;

$$d(x_i, y_i) = \begin{cases} 1, x_i \neq y_i \\ 0, x_i = y_i \end{cases}$$

olmak üzere

$$d(x, y) = d(x_1, y_1) + d(x_2, y_2) + \cdots + d(x_n, y_n) \tag{3.7}$$

biçimindedir.

Örnek 3.11: (i) A = {0, 1}, **x** = 01010, **y** = 01101, **z** = 11101 olsun.

d(**x**, **y**) = 3, d(**y**, **z**) = 1, d(**z**, **x**) = 4

(ii) A = {1, 2, 3, 4}, **x** = 1234, **y** = 1423, **z** = 3214 olsun.

d(**x**, **y**) = 3, d(**y**, **z**) = 4, d(**z**, **x**) = 2

Önerme 3.1 **x, y, z** n uzunluğunda sözler olsun [16].

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

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

(iii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$

(iv) $d(\mathbf{x}, \mathbf{z}) \le d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

İspat: **(i)**, **(ii)**, **(iii)** Hamming uzaklığı tanımından açıktır. Formül (3.7)'de $n = 1$ için

$\mathbf{x} = \mathbf{z}$ alınırsa $d(\mathbf{x}, \mathbf{z}) = 0$ olduğundan **(iv)** sağlanır. Eğer $\mathbf{x} \neq \mathbf{z}$ alınırsa $\mathbf{y} \neq \mathbf{x}$ ve $\mathbf{y} \neq \mathbf{z}$ olduğundan **(iv)** sağlanır.

3.4.4 En Yakın Komşu Dekodlaması

C kodunun sözleri bir iletişim kanalından gönderilsin ve bir $\mathbf{x}$ sözü alınsın. En yakın komşu dekodlamasında (*Nearest Neighbor Decoding*) kural, $\mathbf{c_x}$, $\mathbf{x}$ kodunun dekodu olmak üzere $d(\mathbf{x}, \mathbf{c_x})$'in minimum olmasıdır [16]. Yani $c \in C$ olmak üzere,

$$d(\mathbf{x}, \mathbf{c_x}) = \min_{c \in C} d(\mathbf{x}, \mathbf{c}). \tag{3.8}$$

Örnek 3.12: C = {0000, 0011, 1000, 1100, 0001, 1001} kodu ele alınsın. C kodundan alınan kodsözler BSC üzerinden gönderilsin. $\mathbf{x}$ = 0111 sözü alınsın.

$d(0111, 0000) = 3$, $d(0111, 0011) = 1$, $d(0111, 1000) = 4$, $d(0111, 1100) = 3$

$d(0111, 0001) = 2$, $d(0111, 1001) = 3$.

En yakın komşu dekodlaması uygulanırsa $\mathbf{x}$, 0011 kodsözü olarak dekodlanır.

3.5 Kod Uzaklığı

Tanım 3.11 C kodu en az iki kodsöz içersin. C'nin **minimum uzaklığı** $d(C)$ olarak gösterilir ve $d(C)$

$$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : x, y \in C, \mathbf{x} \neq \mathbf{y}\} \tag{3.9}$$

ile verilir.

Tanım 3.12 Bir kodun uzunluğu n, büyüklüğü M ve minimum uzaklığı d **ise (*n, M, d*) kod** olarak ifade edilir [16].

Örnek 3.13: (i) C = {00000, 00111, 11111} ikili (binary) kodu ele alınsın.

d(00000, 00111) = 3, d(00000, 11111) = 5, d(00111, 11111) = 2

$d(C)$ = 2 ve C kodu (5, 3, 2)-koddur.

(ii) C = {000000, 000111, 111222} üçlü (ternary) kodu ele alınsın.

d(000000, 000111) = 3, d(000000, 111222) = 6, d(000111, 111222) = 6

$d(C)$ = 3 ve C üçlü kodu (6, 3, 3)-koddur.

Tanım 3.13 C bir kod ve u bir pozitif tamsayı olsun. C'deki bir kodsözde en az 1, en fazla u tane hata oluşsun. Hata sonrası oluşan söz C'de yoksa C'ye **u-hata-bulan** denir. Eğer u hata bulunurken (u+1) hata bulunamazsa C'ye **tam-u-hata bulan** denir [22].

Örnek 3.14: (i) C = {00000, 00111, 11111} ikili kodu 1-hata-bulan koddur. Çünkü herhangi bir kodsözün bir bileşeni değiştirilince başka bir kodsöze dönüşmemektedir. Yani,

00000 → 00111 üç bitin değişmesi gerekmektedir.

00000 → 11111 beş bitin değişmesi gerekmektedir.

00111 → 11111 iki bitin değişmesi gerekmektedir.

C kodu tam-1-hata-bulandır. Eğer 00111 kodsözünün ilk iki biti değiştirilirse 11111 kodsözüne dönüşmektedir.

(ii) C = {000000, 000111, 111222} üçlü kodu 2-hata-bulandır.

000000 → 000111 üç bitin değişmesi gerekmektedir.

000000 → 111222 altı bitin değişmesi gerekmektedir.

000111 → 111222 altı bitin değişmesi gerekmektedir.

C kodu tam-2-hata-bulandır. Eğer 000000 kodsözünün son üç biti değiştirilirse 000111 kodsözüne dönüşmektedir.

Teorem 3.2 C bir kod olsun. C, u-hata-bulandır $\Leftrightarrow d(C) \geq u + 1$. Yani bir kodun uzaklığı d ise tam (d-1)-hata-bulandır [16].

İspat: ($\Leftarrow$): $d(C) \geq u + 1$ olsun. Eğer $c \in C$ ve bir x için $1 \leq d(c, x) \leq u < d(C)$ sağlanırsa $x \notin C$ olur. Böylece C, u-hata-bulandır.

$(\Rightarrow)$: C u-hata-bulan olsun. $d(C) < u + 1$ alalım. Buradan $d(C) \leq u$ ve $c_1, c_2 \in C$ için $1 \leq d(c_1, c_2) = d(C) \leq u$ olur. c_1 kodu gönderilir ve $d(C)$ hata oluşursa ($1 \leq d(C) \leq u$) alınan söz c_2 olur ki C'ye ait olan bir kodsözdür. Böylece C u-hata-bulan olmaz. Çelişkidir.

Örnek 3.15: (i) C = {00000, 00111, 11111} ikili kodu 1-hata-bulan koddur. u = 1 ve $d(C)=2 \geq u + 1$.

(ii) C = {000000, 000111, 111222} üçlü kodu 2-hata-bulandır. u = 1 ve $d(C) = 3 \geq u + 1$.

Tanım 3.14 v bir pozitif tamsayı olsun. Eğer C'de en yakın komşu dekodlaması, v veya daha az hatayı düzeltmeye olanak sağlıyorsa C' ye ***v*-hata-düzeltir** denir. Eğer kod v hata düzeltirken v+1 hata düzeltemiyorsa koda **tam *v*-hata-düzeltir** denir [22].

Örnek 3.16: C = {000,111} ikili kodu ele alınsın. En yakın komşu dekodlaması uygulansın.

- Eğer 000 kodsözü gönderilir ve bir hata oluşursa, (001, 010, 100) sözlerinden birisi alınır ve 000 olarak dekodlanır.
- Eğer 111 kodsözü gönderilir ve bir hata oluşursa, (110, 101, 011) sözlerinden birisi alınır ve 111 olarak dekodlanır.

Yani bir hata düzeltilmiş olur. Böylece C, 1-hata-düzeltendir.

Eğer en az iki hata oluşsaydı dekodlama kuralı yanlış kodsözü üretebilirdi. Örneğin, 000 gönderilip 011 alınsaydı, en yakın komşu dekodlama kuralı 011 sözünü 111 olarak dekodlayacaktı. Bu yüzden C tam 1-hata-düzeltendir.

Teorem 3.3 C bir kod olsun. C, v-hata-düzeltendir $\Leftrightarrow d(C) \geq 2v + 1$. Yani bir kodun minimum uzaklığı d ise tam $\lfloor (d-1)/2 \rfloor$-hata-düzeltir. Burada $\lfloor x \rfloor$, x'e eşit veya x'ten küçük en büyük tam sayıdır [16].

İspat: $(\Leftarrow)$: $d(C) \geq 2v + 1$ olsun. Eğer gönderilen bir c kodsözü için en az 1 en fazla v hata oluşuyorsa alınan bir x sözü için $1 \leq d(c, x) \leq v$ sağlanır. Bu ise x'in c'ye herhangi bir kodsözden daha yakın olduğunu gösterir. Eğer herhangi bir $d \neq c$ kodsözü için $d(x, d) \leq v$ ise üçgen eşitsizliğinden

$d(c, d) \leq d(c, x) + d(x, d) \leq v + v = 2v$

olur. Bu ise çelişkidir. Çünkü $d(C) = 2v + 1 > 2v$. Böylece en yakın komşu dekodlaması v veya daha az hata düzeltir.

$(\Rightarrow)$: C v-hata-düzeltsin. $d(C) < 2v + 1$ olsun. $d, c \in C$ için $d(c, d) = d(C) \leq 2v$ olur. c gönderilmiş olsun ve en fazla v hata oluşsun.

Eğer $d(c, d) \leq v + 1$ olsa c kodsözü oluşan v hata ile d kodsözüne dönüşebilir. $d \in C$ olduğundan hata düzeltilmez. Bu ise C'nin v-hata-düzelten olmasıyla çelişir. O halde $d(c, d) \geq v + 1$'dir. $v + 1 \leq k \leq 2v$ olmak üzere c ile d arasında ilk $k = d(C)$ koordinatı farklı olsun. Alınan x sözü, c ile ilk $k - v$ koordinatı, d ile son v koordinatı, hem c hem de d ile son $n - k$ koordinatı uygun olsun.

$$x = \underbrace{x_1 \ldots x_{k-v}}_{c} \underbrace{x_{k-v+1} \ldots x_k}_{d} \underbrace{x_{k+1} \ldots x_n}_{c,d}$$

$d(c, x) = v$ ve $d(d, x) = k - v \leq v$ olduğundan ya $d(c, x) = d(d, x)$ olur ki dekodlanan hata bildirilir ya da $d(c, x) \geq d(d, x)$ olur ki x düzeltilmeden d olarak dekodlanır. Bu ise C'nin v-hata-düzelten olması ile çelişir. Böylece $d(C) \geq 2v + 1$.

Örnek 3.17: İkili $(n, 2, n)$ tekrarlı kodu 00...0 ve 11…1 kodsözlerinden oluşur. En yakın komşu dekodlaması $\lfloor (n-1)/2 \rfloor$ hata düzeltir.

3.6 Lineer Kodlar

$GF(q)$, büyüklüğü (eleman sayısı) q olan sonlu cisim (Galois cismi) olarak tanımlansın. Eğer q asal tam sayı ise modulo q'ya göre kalan sınıfı ile çakışır ve $\mathbb{Z}_q$ ile belirtilir.

Tanım 3.15 C, $\mathbb{F}_q = GF(q)$ cismi üzerinde tanımlı bir (n, M, d)-kodu olsun. Eğer C, $\mathbb{F}_q$ üzerinde tanımlı $\mathbb{F}_q^n$'in bir alt uzayı ise C bir **lineer kod** denir. Yani, iki kodsöz $c_1, c_2 \in C$ ve iki skaler $a_1, a_2 \in \mathbb{F}_q$ olmak üzere $a_1 c_1 + a_2 c_2 \in C$ olmasıdır [19].

Tanım 3.16 Lineer bir (n, M, d)-kod C'nin **boyutu**, $\mathbb{F}_q^n$'in lineer alt uzayı olarak C'nin boyutudur. Eğer C'nin boyutu k ise C'ye $\mathbb{F}_q$ üzerinde bir **lineer [n, k, d]-kodu** denir (Minimum uzaklık çıkarılarak $[n, k]$-kod olarak da gösterilmektedir). n, k, d sayıları lineer kodun **parametreleri** olarak isimlendirilir.

$n-k$ farkı C'nin **artıklığı (redundancy)** olarak isimlendirilir. Eğer k = 0 ise trivial lineer koddur ve yalnızca **0** = 00…0 sözünden oluşur.

$\mathbb{F}_q$ = $GF(q)$ üzerinde tanımlı lineer [n, k, d]-kodu C'nin tüm tabanları k kodsöz içerir ve tüm C kümesini üretir. Böylece C'nin eleman sayısı $|C| = M = q^k$ ve kod oranı $R = (\log_q M)/n = k/n$'dir [19].

Örnek 3.18: İkili C = {0000,1011, 0110, 1101} kodu $\mathbb{Z}_2^4$'nin alt uzayıdır ve bir lineer koddur. $\mathbb{B}$ = {1011, 0110} kümesi C için tabandır. Boyutu $dim(C)$ = 2'dir. Böylece C bir [4, 2]-koddur.

Örnek 3.19: 0121 ve 2210 sözleri $\mathbb{Z}_3$ üzerinde lineer bağımsız olduğundan üçlü [4, 2]-lineer kodunu üretebilirler.

$C = \langle 0121, 2210 \rangle = \{a(0121) + b(2210) : a, b \in \mathbb{Z}_3\}$.

3.6.1 Hamming Ağırlığı

Tanım 3.17 x, $\mathbb{F}_q^n$'de bir söz olsun. x'in **Hamming ağırlığı**, x'in sıfırdan farklı koordinatlarının sayısı olarak tanımlanır ve $wt(x)$ olarak gösterilir. $0 = 00...0$ olmak üzere

$$wt(x) = d(x, 0). \tag{3.10}$$

Her bir $x \in \mathbb{F}_q$ için Hamming ağırlığı şu şekilde tanımlanır;

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

Buradan $x \in \mathbb{F}_q^n$ olmak üzere $x = x_1...x_n$ için x'in Hamming ağırlığı

$$wt(x) = wt(x_1) + wt(x_2) + \cdots + wt(x_n). \tag{3.11}$$

olarak tanımlanır [16].

Örnek 3.20: C = {0000, 1000, 0100, 1100} lineer kodu ele alınsın.

$wt(1000) = 1$ $\quad$ $wt(0100) = 1$ $\quad$ $wt(1100) = 2$

Örnek 3.21: $C = \langle 0121, 2210 \rangle = \{a(0121) + b(2210) : a, b \in \mathbb{Z}_3\}$ kodu ele alınsın.

$wt(0121) = 3$ $wt(2001) = 2$ $wt(1211) = 4$

Teorem 3.4 Eğer $a = -a$ ise $d(x, y) = wt(x - y)$.

İspat:

$$\begin{aligned} d(x, y) &= d(x_1, y_1) + \cdots + d(x_n, y_n) \\ &= d(x_1 - y_1, 0) + \cdots + d(x_n - y_n, 0) \\ &= wt(x_1 - y_1) + \cdots + wt(x_n - y_n) \\ &= wt(x - y) \end{aligned}$$

Örnek 3.22: **x** = 1100 ve **y** = 1000 olsun.

d(1100, 1000) = 1

$wt(1100 - 1000) = wt(0100) = 1.$

Sonuç 3.5 q çift tamsayı olmak üzere her $a \in GF(q)$ için $a = -a$ 'dır. q çift tamsayı olsun. $x, y \in GF(q)^n (= \mathbb{F}_q^n)$ için $d(x, y) = wt(x + y)$.

Örnek 3.23: $x, y \in GF(2)$ için **x** = 1100 ve **y** = 1000 olsun.

d(1100, 1000) = 1
wt(1100+1000) = wt(0100) = 1 $\Big\}\ d(x, y) = wt(x + y)$

$x = (x_1 x_2 ... x_n)$, $y = (y_1 y_2 ... y_n) \in GF(2)^n$ olsun. $x * y = (x_1 y_1, ..., x_n y_n)$ olarak tanımlansın.

Lemma 3.6 $x, y \in \mathbb{F}_2^n$ olmak üzere aşağıdaki eşitlik sağlanır:

$$wt(x + y) = wt(x) + wt(y) - 2wt(x * y). \tag{3.12}$$

Örnek 3.24: $x = (11101011)$, $y = (10100110) \in \mathbb{F}_2^8$ olsun.

wt(x+y) = wt(01001101) = 4
wt(x) = 6 wt(y) = 4
wt(x*y) = wt(10100010) = 3 $\Big\}\ \underbrace{\text{wt(x+y)}}_{4} = \underset{6}{\text{wt(x)}} + \underset{4}{\text{wt(y)}} - \underbrace{\text{2wt(x*y)}}_{6}.$

Tanım 3.18 C lineer olması gerekmeyen bir kod olsun. C'nin minimum (Hamming) ağırlığı, C'deki sıfırdan farklı kodsözlerden, ağırlığı minimum olanına eşittir ve $wt(C)$ olarak gösterilir [16].

Teorem 3.7 C bir lineer kod ise $d(C) = wt(C)$.

İspat: $d(C) = min\{d(x,y) : x, y \in C, x \neq y\}$

$= min\{wt(x-y) : x, y \in C, x \neq y\}$

$= min\{wt(c) : c \in C, c \neq 0\}$.

Örnek 3.25: C = {0000, 1000, 0100, 1100} lineer kodu ele alınsın.

$wt(C) = 1 = d(C)$.

3.6.2 Lineer Kodlar için Tabanlar

Bir lineer kod, vektör uzayı olduğundan kodun her elemanı taban ile belirtilebilir. Bu bölümde, verilen lineer bir kodun tabanını bulmak için iki algoritma tanımlanacaktır.

Tanım 3.19 A, $\mathbb{F}_q$ üzerinde tanımlı bir matris olsun. Aşağıdakilerin herhangi birisi A üzerinde gerçekleştirilen *temel satır işlemleri* (*elemantary row operation*) olarak isimlendirilir:

(i) İki satırın yerini değiştirmek,

(ii) Bir satırı sıfırdan farklı bir skaler ile çarpmak,

(iii) Bir satırın sıfırdan farklı bir skaler ile çarpılıp diğer bir satıra eklenmesi.

Tanım 3.20 Bir matris temel satır işlemleri ile başka bir matristen oluşuyor ise bu iki matrise *satır eşdeğer (row equivalent) matrisler* denir.

3.6.2.1 Algoritma 1

Tanım 3.21 $0 \neq S \subset \mathbb{F}_q^n$ olsun. $C = \langle S \rangle$, S tarafından üretilen kod olsun. S'nin sözleri satırlar olacak şekilde A matrisi oluşturulsun. Temel satır işlemleri ile A matrisinin satır eşdeğer olduğu matris bulunur. Bu matrisin sıfırdan farklı satırları C kodu için tabandır [16].

Örnek 3.26: q = 3 ve S = {12101, 20110, 01122, 11010} olsun. $C = \langle S \rangle$ kodu için taban bulalım.

$$A = \begin{bmatrix} 12110 \\ 20110 \\ 01122 \\ 11010 \end{bmatrix} \rightarrow \begin{bmatrix} 12110 \\ 02211 \\ 01122 \\ 02212 \end{bmatrix} \rightarrow \begin{bmatrix} 12101 \\ 01122 \\ 00001 \\ 00000 \end{bmatrix}.$$

Son matris A'nın satır eşdeğer matrisidir. {12101, 01122, 00001} kümesi C kodu için tabandır.

3.6.2.2 Algoritma 2

Tanım 3.22 $0 \neq S \subset \mathbb{F}_q^n$ olsun. $C = \langle S \rangle$, S tarafından üretilen kod olsun. S'nin sözleri, sütunları olacak şekilde A matrisi oluşturulsun. Temel satır işlemleri ile A matrisinin satır eşdeğer olduğu matris bulunur. Bu matriste sütunların ilk elemanı 0'dan farklı olanlar tespit edilir. Bu sütunların A matrisinde karşılık geldiği orijinal sütunlar C için taban oluşturur [16].

Örnek 3.27: q = 2 ve S = {11101, 10110, 01011, 11010} olsun. $C = \langle S \rangle$ kodu için taban bulalım.

$$A = \begin{bmatrix} 1101 \\ 1011 \\ 1100 \\ 0111 \\ 1010 \end{bmatrix} \rightarrow \begin{bmatrix} 1101 \\ 0110 \\ 0001 \\ 0111 \\ 0111 \end{bmatrix} \rightarrow \begin{bmatrix} 1101 \\ 0110 \\ 0001 \\ 0000 \\ 0000 \end{bmatrix}.$$

Son matris A'nın satır eşdeğer matrisidir. Bu matriste 1., 2. ve 4. sütunlardaki ilk elemanlar sıfırdan farklı olduğu için A matrisindeki 1, 2 ve 4. sütun elemanları {11101, 10110, 11010} C için taban oluşturur.

3.6.3 Üreteç Matrisi

Tanım 3.23 C bir lineer [n, k, d]-kod olsun. $\mathbb{B} = \{b_1, b_2, ..., b_k\}$ C'nin tabanı olsun. $\mathbb{B}$ 'nin elemanlarını satır olarak kabul eden $k \times n$'lik matrise **üreteç matris** denir ve G ile gösterilir. Yani,

$b_1 = b_{11}b_{12}...b_{1n}$
$b_2 = b_{21}b_{22}...b_{2n}$
$\vdots$
$b_k = b_{k1}b_{k2}...b_{kn}$

olmak üzere

$$G = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ & & \vdots & \\ b_{k1} & b_{k2} & \dots & b_{kn} \end{bmatrix}$$

matrisi C için üreteç matristir [22].

Çoğunlukla lineer bir kodun üreteç matrisi tek değildir. Vektör uzayları için birden fazla taban olabildiğinden üreteç matrisi de birden fazla olabilir. Üreteç matrisin satırları lineer bağımsızdır. Ayrıca lineer bir C kodun G üreteç matrisinin rankı C'nin boyutuna eşittir [19].

Örnek 3.28: (i) İkili C = {0000,1011, 0110, 1101} kodunun tabanı $\mathbb{B}$ = {1011, 0110}'tır. C'nin üreteç matrisi

$$G = \begin{bmatrix} 1011 \\ 0110 \end{bmatrix}.$$

(ii) $C = \langle 0121, 2210 \rangle = \{a(0121) + b(2210) : a, b \in \mathbb{Z}_3\}$

kodunun üreteç matrisi

$$G = \begin{bmatrix} 0121 \\ 2210 \end{bmatrix}.$$

Tanım 3.24 Üreteç bir matrisin $\left[I_k \,|\, X \right]$ formuna **standart form** denir.

Örnek 3.29: Aşağıdaki üçlü (ternary) üreteç matrisinin standart formunu bulalım.

$$G = \begin{bmatrix} 12200 \\ 10111 \\ 01121 \end{bmatrix}$$

$$\begin{bmatrix}12200\\10111\\01121\end{bmatrix}\to\begin{bmatrix}21200\\01111\\10121\end{bmatrix}\to\begin{bmatrix}12100\\01111\\10121\end{bmatrix}\to\begin{bmatrix}12100\\01111\\01021\end{bmatrix}\to\begin{bmatrix}10222\\01111\\00210\end{bmatrix}\to\begin{bmatrix}10222\\01111\\00120\end{bmatrix}\to\begin{bmatrix}10012\\01021\\00120\end{bmatrix}.$$

3.6.4 Lineer Kodun Duali ve Kontrol Matrisi

Tanım 3.25 C, $\mathbb{F}_q$ üzerinde bir lineer [n, k, d]-kod olsun. Tüm $c \in C$ için $x \cdot c^T = 0$ sağlayan bütün $x \in \mathbb{F}_q^n$'lerden oluşan kümeye C'nin **duali** denir ve $C^\perp$ ile gösterilir. $C^\perp$'nin kodsözleri C'ye ortogonaldir (diktir) [19]. G, C kodunun üreteç matrisi olmak üzere dual kodun tanımı

$$C^\perp = \{x \in \mathbb{F}_q^n : xG^T = 0\} \tag{3.13}$$

şeklindedir.

Teorem 3.8 C, $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda lineer kod olsun.

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

(ii) $C^\perp$ lineer koddur ve $\dim(C) + \dim(C^\perp) = n$.

(iii) $(C^\perp)^\perp = C$.

İspat: (i) $\dim(C) = k$ olsun. C'nin tabanı $\{b_1, b_2, ..., b_k\}$ olacak şekilde k elemandan oluşur. C bir vektör uzayı olduğu için

$$C = \{\lambda_1 v_1 + ... + \lambda_k v_k : \lambda_1, .., \lambda_k \in \mathbb{F}_q\}$$

olur. $|\mathbb{F}_q| = q$ olduğundan her bir $\lambda_1, .., \lambda_k$ için q seçim yapılabilir. Böylece $|C| = q^{\dim(C)}$'dir.

(ii) $x = x_1...x_n$, $y = y_1...y_n \in C^\perp$ ve $c = c_1...c_n \in C$ olsun. O halde $c \cdot x = 0$ ve $c \cdot y = 0$'dir. Teorem 2.26'dan

$$c \cdot (x + y) = c \cdot x + c \cdot y = 0$$

ve $a \in \mathbb{F}_q$ için

$$c \cdot (ax) = a(c \cdot x) = a0 = 0$$

olur. Bu ise $C^{\perp}$'nin toplama ve çarpma işlemine göre kapalı olduğunu dolayısıyla $\mathbb{F}_q^n$'in alt uzayı olduğunu gösterir.

$x = x_1 ... x_n$ ve $y = y_1 ... y_n$ olmak üzere iki vektörün iç çarpımı

$$x \cdot y = x_1 y_1 + ... + x_n y_n$$

şeklindedir. Eğer $x \in C^{\perp}$ ise

$$x_1 y_1 + ... + x_n y_n = 0 \tag{3.14}$$

eşitliği sağlanır. Bu eşitliğe $C^{\perp}$ için *parite kontrol eşitliği* (*parity check equation*) denir.

$\mathbb{B} = \{b_1, b_2, ..., b_k\}$ C için taban olsun. Çözümleri $C^{\perp}$ deki kodsözler olan parite kontrol eşitlikleri

$$\begin{aligned}
&b_{11}x_1 + b_{12}x_2 + ... + b_{1n}x_n = 0 \\
&b_{21}x_1 + b_{22}x_2 + ... + b_{2n}x_n = 0 \\
&\vdots \\
&b_{k1}x_1 + b_{k2}x_2 + ... + b_{kn}x_n = 0
\end{aligned}$$

ele alınsın. $\{b_1, b_2, ..., b_k\}$ lineer bağımsız olduğundan bir $x_{i_1}, ..., x_{i_k}$ k koordinat kümesi vardır ki yukarıdaki sistem, her bir x_{i_j} sıfırdan farklı katsayılı tam bir tane eşitliği belirten sisteme eşdeğerdir ve bu eşitlikte x_{i_j}'in katsayısı 1'dir. Örneğin, eğer koordinatlar $x_1, ..., x_k$ olsa eşdeğer sistem, katsayılar $d_{i,j} \in \mathbb{F}_q$ olmak üzere

$$\begin{array}{ccccccccccc}
x_1 & & & + & d_{1,k+1}x_{k+1} & + & \dots & + & d_{1,n}x_n & = & 0 \\
& x_2 & & + & d_{2,k+1}x_{k+1} & + & \cdots & + & d_{2,n}x_n & = & 0 \\
& & \ddots & & & & & & & & \vdots \\
& & & x_n & + & d_{k,k+1}x_{k+1} & + & \dots & + & d_{k,n}x_n & = & 0
\end{array}$$

formundadır. Bu sistemlerde $x_{k+1}, ..., x_n$ koordinatlarına keyfi değerler vererek $x_1, ..., x_k$ değerleri hesaplanır. $n-k$ tane değişken $x_{k+1}, ..., x_n$ için p tane seçim yapılabildiğinden p^{n-k} çözüm vardır. Böylece $C^{\perp}$'nin büyüklüğü p^{n-k} olur ve boyutu $n-k$'dır.

(iii) $c \in C$ olsun. $c \in (C^{\perp})^{\perp}$ olduğunu göstermek için tüm $x \in C^{\perp}$ olmak üzere $c \cdot x = 0$ göstermek yeterlidir. $c \in C$ ve $x \in C^{\perp}$ olduğundan, $C^{\perp}$ tanımından $c \cdot x = 0$ sağlanır. Buradan $C \subseteq (C^{\perp})^{\perp}$'dir. **(ii)**'den

$$\dim((C^{\perp})^{\perp}) = n - \dim(C^{\perp}) = n - (n - \dim(C)) = \dim(C)$$

olur. Eğer bir *D* kodu bir *E* kodunun alt uzayı ve dim(*D*) = dim(*E*) ise *D* = *E*'dir. Buradan $C = (C^{\perp})^{\perp}$.

Örnek 3.30: (i) *C* = {0000, 1011, 0110, 1101} ikili kodu ele alınsın. Tabanı $\mathbb{B}$ = {1011, 0110}'dir. Üreteç matrisi

$$G = \begin{bmatrix} 1011 \\ 0110 \end{bmatrix}$$

olur. C'nin dual kodu

$$\begin{array}{ccccccc} x_1 & & + & x_3 & + & x_4 & = & 0 \\ & x_2 & + & x_3 & & & = & 0 \end{array}$$

parite kontrol eşitliğinden bulunabilir. Yukarıdaki sistemde x_3 ve x_4'e keyfi değerler verilerek x_1 ve x_2 çözümleri bulunur. Örneğin, $x_3 = 1$ ve $x_4 = 0$ için $x_1 = 1$ ve $x_2 = 1$ olur ki $1110 \in C^{\perp}$ olur. Bu şekilde devam edilirse

$$C^{\perp} = \{0000, 1110, 1001, 0111\} = \langle 1110, 1001 \rangle$$

dual kodu elde edilir. *C*'nin tüm kodsözleri $C^{\perp}$'deki kodsözlere ortogonaldir. Örneğin, $c = 1011 \in C$ ve $x = 1110 \in C^{\perp}$ alınsın.

$$c \cdot x = 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 0$$

olur. *C*'nin boyutu

$$\dim(C) = \log_2 |C| = \log_2 4 = 2$$

buradan $\dim(C^{\perp}) = 2$ olur.

(ii) $\mathbb{F}_3$ üzerinde *C* = {000, 001, 002, 010, 020, 011, 012, 021, 022} kodu ele alınsın. Boyut,

$\dim(C) = \log_3 |C| = \log_3 9 = 2$ ve $\dim(C^\perp) = 1$ olur.

Tanım 3.26 C bir lineer kod olsun.

(i) Eğer $C \subseteq C^\perp$ ise C'ye **kendine-dik** (self-orthogonal) denir.

(ii) Eğer $C = C^\perp$ ise C'ye **kendine-dual** (self-dual) denir.

Örnek 3.31: $\mathbb{F}_q$ üzerinde tanımlı C = {0000, 1010, 0101, 1111} kodunun duali $C^\perp$ = {0000, 1010, 0101, 1111}'dir. $C = C^\perp$ olduğundan C kendine dualdir.

Tanım 3.27 C bir lineer kod ve $C^\perp$ de duali olsun. $C^\perp$'nin üreteç matrisine C kodu için **kontrol matrisi** (parity-check matrix) denir ve H ile gösterilir.

Tanım 3.28 Bir kontrol matrisinin $\left[Y | I_{n-k} \right]$ formuna **standart form** denir [16].

Örnek 3.32: C = {0000, 1011, 0110, 1101} kodunun kontrol matrisini bulalım.

C'nin duali $C^\perp = \{0000, 1110, 1001, 0111\} = \langle 1110, 1001 \rangle$'dir. C'nin kontrol matrisi

$$H = \begin{bmatrix} 1110 \\ 1001 \end{bmatrix}$$

olur ve standart formdadır.

Lemma 3.9 C, $\mathbb{F}_q$ üzerinde bir [n, k]-lineer kod ve üreteç matrisi G olsun. $v \in \mathbb{F}_q^n$ olmak üzere

$$v \in C^\perp \Leftrightarrow vG^T = 0.$$

Özel olarak H, $(n-k) \times n$'lik matris olmak üzere, C'nin kontrol matrisinin H olması için gerek ve yeter koşul H'nin satırlarının lineer bağımsız ve $HG^T = 0$ olmasıdır [16].

İspat: r_i, G'nin i. satırı olsun. $1 \le i \le k$ için $r_i \in C$ olur ve her $c \in C$ sözü $\lambda_1, ..., \lambda_k \in \mathbb{F}_q$ olmak üzere

$$c = \lambda_1 r_1 + ... + \lambda_k r_k$$

olarak ifade edilir. Eğer $v \in C^T$ ise tüm $c \in C$ için $v \cdot c = 0$ olur. Özel olarak v, r_i'ye ortogonaldir. Yani $vG^T = 0$.

Tersine, eğer $1 \le i \le k$ için $v \cdot r_i = 0$ ise açıktır ki $c = \lambda_1 r_1 + ... + \lambda_k r_k \in C$ için

$$v \cdot c = \lambda_1 (v \cdot r_1) + ... + \lambda_k (v \cdot r_k) = 0$$

sağlanır. Son kısım için, eğer *H*, *C*'nin kontrol matrisi ise tanımdan *H*'nin satırları lineer bağımsızdır. *H*'nin satırları $C^{\perp}$'nin kodsözleri olduğundan $HG^T = 0$'dir.

Tersine, eğer $HG^T = 0$ ise *H*'nin satırları $C^{\perp}$ tarafından kapsanır. *H*'nin satırları lineer bağımsız olduğundan *H*'nin satır uzayının boyutu $n - k$'dır. Böylece *H*'nin satır uzayı gerçekten $C^{\perp}$'dedir. Diğer bir deyişle *H*, *C*'nin kontrol matrisidir.

Örnek 3.33: *C* = {0000, 0121, 0212, 2210, 2001, 2122, 1120, 1211, 1002} kodunun duali $C^{\perp} = \langle 0110, 1201 \rangle$ ve üreteç matrisi

$$G = \begin{bmatrix} 0121 \\ 2210 \end{bmatrix}$$

olur. $v = 1011 \in C^{\perp}$ alınsın.

$$vG^T = [1011] \begin{bmatrix} 0 & 2 \\ 1 & 2 \\ 2 & 1 \\ 1 & 0 \end{bmatrix} = [0 \quad 0] = 0.$$

Teorem 3.10: *C* bir lineer kod ve *H*, *C*'nin kontrol matrisi olsun [16].

(i) $d(C) \ge d \Leftrightarrow$ *H*'nin $d - 1$ sütunu lineer bağımsızdır.

(ii) $d(C) \le d \Leftrightarrow$ *H*'nin $d - 1$ sütunu lineer bağımlıdır.

İspat: (i) $v = (v_1, ..., v_n) \in C$ ağırlığı $e > 0$ olan bir söz olsun. Sıfırdan farklı koordinatlar $\{i_1, ..., i_e\}$ olsun. O halde c_i ise $v_j = 0$ olur. c_i $(1 \le i \le n)$, *H*'nin *i.* sütunu olsun. Lemma 3.9'dan *C*'nin ağırlığı *e* olan sıfırdan farklı bir sözü (sıfırdan farklı koordinatlar $v_{i_1}, ..., v_{i_e}$) olması için gerek ve yeter koşul

$$0 = vH^T = v_{i_1} c_{i_1}^T + ... + v_{i_n} c_{i_e}^T$$

olmasıdır. Bu eşitliğin doğru olması da *H*'nin *e* tane kolonunun $(c_{i_1}, ..., c_{i_e})$ lineer bağımlı olması ile mümkündür.

$d(C) \geq d$ olması, C'nin ağırlığı $d-1$'den küçük kodsözü olmaması ile eşdeğerdir. Bu ise H'nin kolonlarının ağırlığı $d-1$'den küçük olanların lineer bağımsız olması demektir.

(ii) Benzer şekilde $d(C) \leq d$ olması C'nin ağırlığı d'den küçük sıfırdan farklı söz içermesi ile eşdeğerdir. Bu ise H'nin kolonlarının ağırlığı d'den küçük olanların lineer bağımlı olması demektir.

Sonuç 3.11 C bir lineer kod ve H, C'nin kontrol matrisi olsun. Aşağıdakiler denktir [16]:

(i) $d(C) = d$.

(ii) H'nin $d-1$ kolonu lineer bağımsız ve d kolonu lineer bağımlıdır.

Örnek 3.34: (i) C, $\mathbb{F}_2$ üzerinde bir [5,2]-kod olsun.

$$H = \begin{bmatrix} 10100 \\ 01010 \\ 01001 \end{bmatrix}$$

Kontrol matrisi için 1. ve 3. kolonların toplamı

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = 0$$

En az iki kolonun toplamı sıfır olduğundan $d(C) = 2$.

(ii) $\mathbb{F}_2$ üzerinde tanımlı bir kodun kontrol matrisi

$$H = \begin{bmatrix} 1000 \\ 0110 \\ 0101 \end{bmatrix}$$

olsun. 2, 3 ve 4. kolonların toplamı sıfır olduğundan $d(C) = 3$.

Teorem 3.12 C bir $[n, k]$-kod olsun. Eğer C'nin üreteç matrisinin standart formu $G = \left[I_k \middle| X \right]$ ise kontrol matrisi $H = \left[-X^T \middle| I_{n-k} \right]$ formundadır.

Örnek 3.35: (i) $\mathbb{F}_2$ üzerinde tanımlı $C = \langle 1011, 0110 \rangle$ kodu ele alınsın.

$$G = \begin{bmatrix} 1011 \\ 0110 \end{bmatrix}$$

Üreteç matris standart formdadır. Buradan,

$$X = \begin{bmatrix} 11 \\ 10 \end{bmatrix} \to -X^T = \begin{bmatrix} 11 \\ 10 \end{bmatrix} \to\to \left[-X^T \middle| I_2 \right] = \begin{bmatrix} 1110 \\ 1001 \end{bmatrix} = H.$$

(ii) Üreteç matrisi aşağıda verilen kodun kontrol matrisi bulunsun.

$$G = \begin{bmatrix} 01111 \\ 21200 \\ 10121 \end{bmatrix}$$

G'nin standart formu,

$$G = \begin{bmatrix} 10012 \\ 01021 \\ 00120 \end{bmatrix}$$

Buradan,

$$X = \begin{bmatrix} 12 \\ 21 \\ 20 \end{bmatrix} \to -X^T = \begin{bmatrix} 211 \\ 120 \end{bmatrix} \to\to \left[-X^T \middle| I_2 \right] = \begin{bmatrix} 21110 \\ 12001 \end{bmatrix} = H.$$

3.6.5 Lineer Kodların Denkliği

Tanım 3.29 C_1 ve C_2, $\mathbb{F}_q$ üzerinde tanımlı iki (*n*, *M*)-kod olsunlar. Eğer aşağıdaki yollardan herhangi biri veya ikisi ile bu kodlardan biri diğerinden elde ediliyorsa C_1 ve C_2'ye **denk kodlar** denir [16]:

(i) Kodsözlerin *n* bileşeninin (koordinatların) permütasyonu,

(ii) Belli yerdeki bileşenlerin sıfırdan farklı bir skalerle çarpımı.

Örnek 3.36 (i) $\mathbb{F}_2$ üzerinde tanımlı C_1 = {0000, 0011, 0110, 0101} kodu ele alınsın.

Bu koda (2, 1, 4, 3) permütasyonu uygulanırsa C_2 = {0000, 0011, 1001, 1010} kodu elde edilir. C_1 ve C_2 denktir.

(ii) $\mathbb{F}_3$ üzerinde tanımlı C_1 = {0000, 1220, 0112, 1002} kodu ele alınsın.

Bu koda (4, 2, 3, 1) permütasyonu uygulansın. C_2 = {0000, 0221, 2110, 2001} kodu elde edilir. C_2'nin üçüncü bileşenleri 2 ile çarpılırsa C_3 = {0000, 0211, 2120, 2001} kodu elde edilir. $C_1 \cong C_2 \cong C_3$.

Teorem 3.13 Lineer bir C kodunun üreteç matrisinde sütunlara permütasyon uygulanarak C kodu lineer bir C_1 koduna denk olur ve bu kodun üreteç matrisi G_1'dir.

Örnek 3.37: İkili bir lineer C kodun üreteç matrisi

$$G = \begin{bmatrix} 1100001 \\ 0010011 \\ 0001001 \end{bmatrix}$$

olsun. Bu matrisin sütunlarına 1, 3, 4, 2, 5, 6, 7 permütasyonu uygulanırsa

$$G_1 = \begin{bmatrix} 1001001 \\ 0100011 \\ 0010001 \end{bmatrix}$$

matrisi elde edilir. Bu matris bir C_1 lineer kodun üreteç matrisidir. C kodu C_1 koduna denktir.

3.6.6 Lineer Kodlarda Kodlama (Encode)

Tanım 3.30 C, $\mathbb{F}_q$ üzerinde tanımlı bir lineer [n, k, d]-kod olsun ve üreteç matrisi G olsun. $u \in \mathbb{F}_q^k$ vektörü için $u \to uG$ ile tanımlı $\mathbb{F}_q^k \to C$ fonksiyonu ile her bir bilgi sözü (information words) C'nin kodsözlerine kodlanabilir. $rank(G) = k$ olduğundan kodun q^k kodsözü vardır ve q^k bilgi sözü (mesaj) ile eşleşebileceğinden fonksiyon 1-1'dir [19]. $u \in \mathbb{F}_q^k$ vektörünün C'deki $c = uG$ kodsözü ile gösterim sürecine **kodlama (encoding)** denir.

Eğer $G = \left[I \middle| A \right]$ standart formda ise $u \to uG$ fonksiyonu $u \to \left[u \middle| uA \right]$ formuna dönüşecektir. $c = uG$ kodlanmış (encoded) kodsözü için ilk k bileşen bilgi sözünü belirtmektedir. Kalan $n-k$ bileşen ise kontrol sembolüdür. u mesajına eklenen kontrol sembolleri hata oluşumuna karşı mesajı korur. Eğer kodun üreteç matrisi standart

formda değilse koda permütasyon uygulanarak, üreteç matrisi standart formdaki denk kod elde edilebilir.

Kodlamada ikinci bir yol kontrol matrisi ile olur. G üreteç matrisi standart formda iken bu yol çok daha kolaylaşır. $G=\left[I_k \middle| A\right]$ için kontrol matris $H=\left[-A^T \middle| I_{n-k}\right]$ olur. $u=u_1...u_k$ mesajı $c=c_1...c_n$ olarak kodlansın. G standart formda olduğundan $c_1...c_k=x_1...x_k$'dır. $c_{k+1}...c_n$ kontrol sembolünün tanımlanması gerekmektedir. $0=Hc^T=\left[-A^T \middle| I_{n-k}\right]c^T$ olduğundan $A^T x^T=\left[c_{k+1}...c_n\right]^T$ olur [23].

Örnek 3.38: C bir [5,3]-lineer kod olsun ve üreteç matrisi

$$G=\begin{bmatrix}10110\\01011\\00101\end{bmatrix}$$

olsun. u = 101 mesajı kodlansın.

$$c=uG=\begin{bmatrix}101\end{bmatrix}\begin{bmatrix}10110\\01011\\00101\end{bmatrix}=10011$$

u mesajı c = 10011 kodsözü olarak kodlanır. Bu sözde 3 bit mesajı taşır. Eğer G standart formda olsaydı

$$c=uG=\begin{bmatrix}101\end{bmatrix}\begin{bmatrix}10011\\01011\\00101\end{bmatrix}=10110$$

u mesajı c = 10110 sözü olarak kodlanırdı ve ilk 3 bit mesajı taşırdı.

Örnek 3.39: [6, 3, 3]-lineer kodunun üreteç ve kontrol matrisi

$$G=\begin{bmatrix}100101\\010110\\001011\end{bmatrix} \quad \text{ve} \quad H=\begin{bmatrix}110100\\011010\\101001\end{bmatrix}$$

olsun. $u=u_1u_2u_3$ mesajı $c=c_1...c_6$ sözü olarak kodlansın.

$$c=uG=(u_1,u_2,u_3,u_1+u_2,u_2+u_3,u_1+u_3)$$

H kontrol matrisi kodlamada kullanılırsa $0 = Hc^T$ olduğundan

$$0 = c_1 + c_2 + c_4$$
$$0 = c_2 + c_3 + c_5$$
$$0 = c_1 + c_3 + c_6$$

sistemi elde edilir. G standart formda olduğundan $c_1c_2c_3 = u_1u_2u_3$ olur ve yukarıdaki sistemin çözümünden

$$c = uG = (u_1, u_2, u_3, u_1 + u_2, u_2 + u_3, u_1 + u_3).$$

3.6.7 Lineer Kodlarda Dekodlama

3.6.7.1 Kosetler

Tanım 3.31 C, $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda lineer bir kod ve $u \in \mathbb{F}_q^n$, n uzunluğunda bir vektör olsun. C'nin u ile belirli koseti

$$C + u = \{v + u : v \in C\} (= u + C)$$

ile tanımlanır.

Örnek 3.40: $\mathbb{F}_2$ üzerinde tanımlı C = {000, 101, 010, 111} kodu tanımlansın.

C + 000 = {000, 101, 010, 111},

C + 001 = {001, 100, 011, 110},

C + 010 = {010, 111, 000, 101},

C + 100 = {100, 001, 110, 011},

C + 011 = {011, 110, 001, 100},

C + 101 = {101, 000, 111, 010},

C + 110 = {110, 011, 100, 001},

C + 111 = {111, 010, 101, 000}.

Teorem 3.14 C, $\mathbb{F}_q$ üzerinde tanımlı [n, k, d]-lineer kod olsun.

(i) $\mathbb{F}_q^n$'in her vektörü C'nin bir kosetindedir.

(ii) Her $u \in \mathbb{F}_q^n$ için $|C+u| = |C| = q^k$.

(iii) Her $u, v \in \mathbb{F}_q^n$ için $u \in C+v \Rightarrow C+u = C+v$.

(iv) İki koset ya aynıdır ya da ayrıktır.

(v) C'nin q^{n-k} adet koseti vardır.

(vi) Her $u, v \in \mathbb{F}_q^n$ için $u-v \in C \Leftrightarrow u$ ve v C'nin aynı kosetindedirler.

İspat: (i) $u \in \mathbb{F}_q^n$ olsun. C lineer kod olduğundan $0 = 00...0$ vektörü içerir. $u+0=u$ olduğundan her $u \in \mathbb{F}_q^n$, C'nin bir kosetinde vardır.

$C+u = \{u, u+c_2, ...\}$.

(ii) $u \in \mathbb{F}_q^n$ olsun. Kosetin tanımından $C + u$ en fazla $|C| = q^k$ eleman içerir. $c_1 \neq c_2$ iken $u+c_1 \neq u+c_2$ olur. Böylece $|C+u| = |C| = q^k$ olur.

(iii) $u \in C+v \Rightarrow u+C \subseteq C+v$ olur. $|C+u| = q^k = |C+v|$ olduğundan $u+C = v+C$

(iv) $C + u$ ve $C + v$ C'nin iki koseti olsunlar.

$x \in (C+u) \cap (C+v)$

olsun. Buradan $x \in (C+u)$ ve $x \in (C+v)$ olur. **(iii)**'den $x+C = C+v$ ve $x+C = C+u$'dir. O halde $C + u = C + v$ olur.

(v) $u_1 + C = \{u_1 + c_1, u_1 + c_2 + \cdots\}$

$u_2 + C = \{u_2 + c_1, u_2 + c_2 + \cdots\}$

$\vdots$

$u_{q^n} + C = \{u_{q^n} + c_1, u_{q^n} + c_2, ...\}$

Her bir kosette q^k tane eleman var. $q^k.x = q^n \rightarrow x = q^{n-k}$ adet koset vardır.

(vi) $(\Rightarrow)$: $u - v = c \in C$ olsun. Buradan

$u = c + v \in C + v$
$\Rightarrow C + u = C + v.$

$(\Leftarrow)$: $u, v \in C + x$ olsun. Buradan

$\Rightarrow u \in C + x \Rightarrow u = c_1 + x$

$v \in C + x \Rightarrow v = c_2 + x$

$\Rightarrow u - v = (c_1 + x) - (c_2 + x) = c_1 - c_2 = c_3 \in C.$

Örnek 3.41: C = {0000, 1011, 0101, 1110} ikili kodunun kosetleri $q^{n-k} = 2^{4-2} = 4$ tanedir. Bu kosetler

0000 + C = {0000, 1011, 0101, 1110}

0001 + C = {0001, 1010, 0100, 1111}

0010 + C = {0010, 1001, 0111, 1100}

1000 + C = {1000, 0011, 1101, 0110}

Tanım 3.32 Bir kosetteki en küçük ağırlıklı söze **koset lideri** denir.

Örnek 3.42: Örnek 3.41'deki kosetlerden 0010 + C kosetinde koset lideri 0010 sözüdür.

3.6.7.2 En Yakın Koset Dekodlaması (Nearest Neighbour Decoding)

C bir lineer kod olsun. v kodsözü kanaldan gönderilsin ve w sözü alınsın. Hata vektörü e olmak üzere şöyle tanımlanır:

$e = w - v \in w + C.$

Buradan $w - e = v \in C$ olur. Teorem 3.14 (vi)'den hata vektörü e ve alınan söz w aynı kosettedir. O halde alınan w sözü için $w + C$ kosetinden en küçük ağırlıklı e sözü seçilir ve gönderilen v sözü $v = w - e$ ile bulunur [16].

Örnek 3.43: $\mathbb{F}_2$ üzerinde tanımlı C = {0000, 1011, 0101, 1110} kodu ele alınsın.

C kodunun standart dizisi oluşturulursa

0000 + C :	0000	1011	0101	1110
0001 + C :	0001	1010	0100	1111
0010 + C :	0010	1001	0111	1100

$1000 + C$: 1000 0011 1101 0110.

(i) w = 1101 sözü alınsın. $w + C$ dördüncü kosettedir. Bu kosetteki en küçük ağırlıklı söz 1000'dir. Böylece, 1101 – 1000 = 0101 sözü en büyük olasılıkla gönderilen kodsözdür. Dikkat edilirse 0101 kodsözü, alınan 1101 sözünün bulunduğu sütunda en üst sıradaki kodsözdür.

(ii) w = 1111 sözü alınsın. $w + C$ ikinci kosettedir. Bu kosette en küçük ağırlıklı iki tane söz vardır: 0001 ve 0100. Eğer alınan söz için oluşturulan kosette iki tane koset lideri varsa dekodlama, dekodlama planına (tamamlanmış veya tamamlanmamış) göre yapılır. Eğer tamamlanmamış dekodlama kullanılırsa yeniden veri iletimi istenir. Eğer tamamlanmış dekodlama kullanılırsa keyfi olarak ağırlığı en küçük olan sözlerden biri seçilir. e = 0001 sözü seçilmiş olsun. 1111 – 0001 = 1110 sözü en büyük olasılıklı gönderilen kodsözdür. Dikkat edilirse 1110 kodsözü alınan 1111 sözünün bulunduğu sütunda en üst sıradaki kodsözdür.

3.6.7.3 Sendrom Dekodlaması

C, $\mathbb{F}$ üzerinde bir kod olsun. $v \in C$ kodsözü gönderilmiş ve $r = v + e$ sözü alınmış olsun. Eğer $C = \{v_1, v_2, ..., v_M\}$, M tane kodsöze sahip kod ise, E mümkün hataların kümesini göstermek üzere

$$E = \{r - v_1, r - v_2, ..., r - v_M\} = \{r - v : v \in C\} = r - C$$

olur. Alınan vektör r olmak üzere mümkün hataların kümesi ile kodsözler arasında birebir eşleme vardır. Yani $|E| = |C| = M$.

C lineer kod ise $-C = \{-v : v \in C\} = C$ olduğundan

$$E = r - C = r + C = \{r + v : v \in C\}$$

yazılabilir. Böylece alınan söz r ile eşleşen mümkün hataların kümesi $r + C$ kosetidir. Dekodlama için bu koset incelenerek hata bulur.

Tanım 3.33 C lineer bir kod olmak üzere H kontrol matrisi olsun. Alınan söz r olmak üzere r sözünün sendromu

$$S(r) = rH^T \tag{3.15}$$

ile tanımlıdır. Burada

$$S(r) = rH^T = (v+e)H^T = vH^T + eH^T = eH^T$$

olduğu görülür. Yani sendrom yanlızca e hata modeline bağlıdır ve gönderilen kodsöz v'ye bağlı değildir.

Örnek 3.44 C bir kod olmak üzere kontrol matrisi

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

olsun. Bir $x = 0111$ kodsözünün sendromu şöyle hesaplanır:

$$S(x) = xH^T = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \end{bmatrix}.$$

Teorem 3.15 $x, y \in \mathbb{F}^n$ iki vektör olmak üzere, bu iki vektörün aynı sendrom olması için gerek ve yeter koşul C'nin aynı kosetinde olmalarıdır.

İspat: x ve y, $r+C$'nin aynı kosetinde iki eleman olsun. Yani $v, w \in C$ kodsözleri için $x = r+v$ ve $y = r+w$

O halde,

$$xH^T = (r+v)H^T = rH^T + vH^T = rH^T$$

ve benzer şekilde,

$$yH^T = (r+w)H^T = rH^T + wH^T = rH^T$$

olur. Böylece x ve y aynı sendromdurlar.

Tersine, x ve y aynı sendrom olsunlar. Yani

$$xH^T = yH^T \Rightarrow (x-y)H^T = 0 \Rightarrow x-y \in C.$$

Yani bazı $v \in C$ için $x-y = v \Rightarrow x = y+v$ olur. Bu ise x'in $y+C$ kosetinin bir elemanı olduğunu gösterir.

Sendrom koset tanımladığından ve hata modeli kosetin elemanı olması gerektiğinden bu teorem, sendromun hata modeli tanımlaması için yeterli olduğunu söyler [24].

Teorem 3.15, en yakın koset dekodlamasına uygulanabilmektedir. En yakın koset dekodlamasında alınan söz x olmak üzere e hata modeli ile x aynı kosettedir ve e koset lideridir. Dekodlama da $c = x - e$ şeklinde yapılmaktadır. x'in sendromu e'nin sendromuna eşit ve koset liderlerinin sendromları farklı olduğundan x ile koset liderlerinin sendromları karşılaştırılarak e hata modeli kolaylıkla bulunabilir. Bunun için gerekli olan koset liderlerinin listesi ve bu kosetlerin sendromlarıdır ki bu tabloya **sendrom tablosu** denir.

En yakın koset dekodlaması şu şekilde uygulanabilir:

1. Alınan kodsözün sendromu $S(x)$ hesaplanır.

2. Koset liderlerinin sendromları ile karşılaştırılır. Eğer herhangi bir koset lideri x_i için $S(x) = S(x_i)$ ise x_i hata modelidir ve $c = x - x_i$ ile dekodlanır.

Örnek 3.45 $C = \{0000, 1011, 0110, 1101\}$ kodu ve kontrol matrisi

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

ele alınsın. Bu kodun standart dizisi

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

şeklindedir. Sendrom tablosu ise şöyle olur:

Çizelge 3. 1 Sendrom tablosu

Koset Lideri	Sendrom
0000	00
1000	11
0100	10
0001	01

$x = 1110$ kodsözü alınmış olsun. Bu kodsözün sendromu $S(1110) = [1110]H^T = 11$ olur. Sendrom tablosuna bakıldığında karşılık gelen koset lideri $x_i = 1000$'dir. Böylece en yakın koset dekodlaması uygulanırsa $x - x_i = 0110$ elde edilir.

3.7 Sınırlar

Hata düzelten kodların maksimum kapasitesini ve sınırlarını bilmek önemlidir. Bu bilgi, neyin pratik olarak ulaşılabilir olduğu bilgisiyle birleşirse hangi problemin hemen hemen çözüldüğünü ve hangisinin daha fazla çalışma ihtiyacı gerektirdiğini gösterir. Ayrıca sınırlar, iletişim sistemleri dizaynının ilk etaplarında kullanışlıdır. Tasarımcıya çeşitli kodların etkilerini kolaylıkla tahmin etmesine izin verir [25].

3.7.1 Kodlama Teorisinin Esas Problemi

İyi bir (n, M, d) kodunun dizaynında en önemli iki amaçtan birisi bu kodun yüksek performanslı (high efficiency) olmasıdır. Bir kodun yüksek performanslı olması şu şekilde olur:

- Küçük *n* (iletim (transmission) hızı için)
- Büyük *M* (daha çok mesaj çeşidi için)
- Büyük *d* (daha çok sayıda hata bulmak ve düzeltmek için)

Bunlar birbirleriyle çelişen amaçlardır. Bu yüzden kodlama teorisinin esas problemi iki parametreyi sabit tutarak üçüncü parametreyi optimize etmektir.

Diğer önemli amaç ise oluşturulan kodun kolaylıkla kodlanıp (encoding) dekodlanmasıdır (decoding) [22].

Bir kodun iletim hızı (transmission rate) $\Re(C)=\frac{\log_q M}{n}$ ile tanımlanmıştı. Eğer kod lineer ise iletim hızı $\Re(C)=\frac{k}{n}$ 'dir. Şimdi uzunluk ve uzaklığa bağlı benzer bir tanımlama yapılacaktır.

Tanım 3.34 $\mathbb{F}_q$ üzerinde tanımlı bir C kodunun parametreleri (n,M,d) olsun. C kodunun **bağıl uzaklığı**

$$\delta(C)=\frac{d-1}{n} \tag{3.16}$$

ile tanımlanır.

Bağıl uzaklık d/n ile de tanımlanmaktadır. Ancak $(d-1)/n$ bazı hesaplamalarda kolaylık sağlamaktadır [26].

Örnek 3.46 (i) $C=\mathbb{F}_q^n$ trivial kodu için $d(C)=1$ ve $\delta(C)=0$ 'dır.

(ii) $[n,1,n]$ tekrarlı kodu ele alınsın. $C=\{0^n,1^n\}$ 'dir. $\delta(C)=\frac{n-1}{n}\to 1$ ve $\Re(C)=\frac{1}{n}\to 1.$

Tanım 3.35 C bir q 'lu (n,M,d) kod olsun. Verilen n ve d değerleri için M 'nin en büyük değeri $A_q(n,d)$ ile tanımlansın.

$A_q(n,d)=\max\{M:\text{bir } (n,M,d) \text{ kodu var}\}.$

C maksimum büyüklüğe sahipse yani $M=A_q(n,d)$ ise C 'ye **optimal kod** denir.

$A_q(n,d)$ sayılarının kodlama teorisinde önemli bir yeri vardır ve değerlerini hesaplamak için çok çaba sarf edilmektedir. Daha doğrusu $A_q(n,d)$ değerlerini hesaplamak kodlama teorisinin temel problemidir.

$A_q(n,d)=K$ olduğunu göstermek için, bazı K sayıları için $A_q(n,d)\le K$ olduğunu göstermek ve $d(C)\ge d$ olmak şartıyla $A_q(n,d)\ge A_q(n,d(C))\ge K$ olacak şekilde bir q 'lu (n,K) özel kodu bulmak yeterlidir [22].

Örnek 3.47 $A_2(4,3)=2$ olduğunu gösterelim.

***Lemma*:** Eğer A kod alfabesi 0'ı içeriyorsa A üzerinde oluşturulan kod, $0 = 00..0$ kodsözünü içeren koda denktir.

Bu lemma kullanılarak verilen bir (n, M, d) kodu, C'nin sıfır kodsözünü içeren bir (n, M, d) kodu C''ne denk olduğu söylenebilir.

C bir $(4, M, 3)$ kod olsun. Yukarıdaki özellikten C'nin $0 = 0000$ kodsözünü içerdiği söylenebilir. $d(C) = 3$ olduğundan C'deki herhangi bir c kodsözü için $d(c, 0) \geq 3$ sağlanmalıdır. Bu ise c'nin en az üç tane 1 içermesini gerektirir. C'de beş tane olasılık vardır:

1110 , 1101 , 1011 , 0111 , 1111

Bu kodsözlerin kendi aralarındaki uzaklık 3 olmadığından sadece bir tanesi C'de bulunabilir. Böylece C, en fazla iki kodsöze sahiptir ki $A_2(4,3) \leq 2$ sağlanır. Ayrıca $C = (0000, 1110)$ bir $(4, 2, 3)$ kodu olduğundan $A_2(4,3) \geq 2$ yazılabilir. Buradan $A_2(4,3) = 2$ olur.

$n \leq 10$ ve $d \leq 7$ için $A_2(n, d)$ değerleri aşağıda verilmiştir.

Çizelge 3. 2 $A_2(n, d)$ değerleri

n	$d = 3$	$d = 5$	$d = 7$
5	4	2	–
6	8	2	–
7	16	2	2
8	20	4	2
9	40	6	2
10	72 – 79	12	2

Tanım 3.36 q asal olmak üzere $\mathbb{F}_q$ üzerinde tanımlı $[n, k, d]$ lineer kodu için q^k'nın en büyük değeri $B_q(n, d)$ ile tanımlansın.

$B_q(n, d) = \max\{q^k : \text{bir } [n, k, d] \text{ lineer kodu var}\}$

$[n, k, d]$ lineer koda **optimal lineer kod** denir.

Teorem 3.16 $q \geq 2$ bir asal olsun. Aşağıdakiler sağlanır [16]:

(i) $B_q(n,d) \le A_q(n,d) \le q^n$, $1 \le d \le n$.

(ii) $B_q(n,1) = A_q(n,1) = q^n$.

(iii) $B_q(n,n) = A_q(n,n) = q$.

İspat: (i) İlk eşitlik tanımdan açıktır. $\mathbb{F}_q$ üzerinde tanımlı bir (n,M,d) kodu $\mathbb{F}_q^n$'in bir alt kümesidir. O halde $M \le q^n$ yazılabilir. İkinci eşitlik de sağlanır.

(ii) $\mathbb{F}_q^n$ bir $[n,n,1]$-lineer koddur ve $\mathbb{F}_q$ üzerinde tanımlı $(n,q^n,1)$-kodu olarak yazılabilir. Böylece $q^n \le B_q(n,1) \le q^n$ olur ki $B_q(n,1) = A_q(n,1) = q^n$ yazılır.

(iii) C, $\mathbb{F}_q$ üzerinde bir (n,M,n) kod olsun. Tüm kodözlerin uzunlukları n ve iki farklı kodsöz arasındaki uzaklık $\ge n$ olduğundan iki kod söz arasındaki uzaklık gerçekten n'dir. Yani iki farklı kodsözün tüm koordinatları farklıdır. Her bir koordinat için tüm M tane söz farklı değer alır. Yani $M \le q$ olur. Bu da $B_q(n,d) \le A_q(n,d) \le q$ sağlar.

n uzunluğundaki bir tekrarlı kod (n,q,n) için $A_q(n,n) \ge q$ sağlanır. Buradan $B_q(n,n) = A_q(n,n) = q$ olur.

Sonuç 3.17 Aşağıdaki kodlar optimaldir:

1. $C = \mathbb{F}_q^n$.
2. Tekrarlı kod $C = \{a^q \mid a \in \mathbb{F}_q\}$.

Bu kodlar ve $|C| = 1$ olan herhangi bir kod **trivial optimal kodlar** olarak isimlendirilir [26].

Teorem 3.18 Eğer $d > 0$ çift ise $A_2(n,d) = A_2(n-1,d-1)$ sağlanır.

Örnek 3.48 $A_2(9,4) = A_2(8,3)$.

Teorem 3.17 $B_2(n,d)$ için de sağlanır.

3.7.2 Küre-Örtü Alt Sınırı (The Sphere-Covering Lower Bound)

Tanım 3.37 $q>1$ olmak üzere A, büyüklüğü q olan bir alfabe olsun. Herhangi bir $u \in A^n$ ve $r \geq 0$ tamsayısı için merkezi u ve yarıçapı r olan **küre (sphere)** $S_A(u,r)$ ile gösterilir ve aşağıdaki küme olarak tanımlanır:

$$S_A(u,r) = \{v \in A^n \mid d(u,v) \leq r\}.$$

Bu kürenin **hacmi** $V_q^n(r)$ ile gösterilir ve $|S_A(u,r)|$ ile tanımlanır [26].

Teorem 3.19 $r \geq 0$ bir doğal sayı, A $q-1$ büyüklüğünde bir alfabe ve $u \in A^n$ olsun. Aşağıdaki eşitlik sağlanır:

$$V_q^n(r) = \begin{Bmatrix} \sum_{i=0}^{r} \binom{n}{i}(q-1)^i & 0 \leq r \leq n \\ q^n & r > n \end{Bmatrix}.$$

İspat: $u \in A^n$ olsun. u'dan uzaklığı m olacak şekilde yani $d(u,v)=m$ olan $v \in A^n$ vektörleri ele alınsın. v'nin u'dan farklı m tane koordinatı $\binom{n}{m}$ farklı şekilde seçilebilir. Her bir koordinat için de $q-1$ farklı seçim yapılabilir. Böylece u'dan m uzaklığında $\binom{n}{m}(q-1)^m$ vektör vardır. Mümkün olan tüm m'lerin toplanması ile $0 \leq r \leq n$ için $\sum_{i=0}^{r} \binom{n}{i}(q-1)^i$ elde edilir. Diğer taraftan $r>n$ için uzaydaki tüm vektörlerin uzaklığı r'dir ve küre tüm uzayı içerir. Yani $V_q^n(r) = q^n$'dir.

Örnek 3.49 (i) $C = \{0^{90}, 1^{90}\}$ kodunda yarıçapı 2 olan kürenin hacmi

$$1 + \binom{90}{1} + \binom{90}{2} = 1 + 90 + 4005 = 4096 = 2^{12}.$$

(ii) $C = \{0^8, 1^8, 2^8\}$ kodunda yarıçapı 2 olan kürenin hacmi

$$1 + \binom{8}{1}(3-1)^1 + \binom{8}{2}(3-1)^2 = 1 + 16 + 112 = 129.$$

Teorem 3.20 (Küre-Örtü sınırı) Her $q>1$ doğal sayısı ve $n,d\in$ olmak üzere $1\le d\le n$ için aşağıdaki sağlanır [26]:

$$A_q(n,d)\ge\frac{q^n}{V_q^n(d-1)}.$$

İspat: $|A|=q$ olmak üzere $C=\{c_1,c_2,...,c_M\}$ optimal (n,M,d) kodu olsun. Yani $M=A_q(n,d)$. C optimal olduğundan A^n'de, C'deki kodsözlere uzaklığı en az d olan bir söz yoktur. Eğer olsaydı bu söz C'ye eklenirdi ve $(n,M+1,d)$ kodu elde edilirdi. O halde her $x\in A^n$ için en az bir $c_i\in C$ var ki $x\in S_A(c_i,d-1)$ sağlar. Böylece A^n'deki her bir söz $S_A(c_i,d-1)$ kürelerinin bir tanesinde içerilmektedir. Yani,

$$A^n\subseteq\bigcup_{i=1}^{M}S_A(c_i,d-1)$$

sağlanır. $|A^n|=q^n$ ve $|S_A(c_i,d-1)|=V_q^n(d-1)$ olduğundan

$$q^n\le\sum_{i=1}^{M}|S_A(c_i,d-1)|=M\cdot V_q^n(d-1)$$

sağlanır. C optimal olduğundan $M=A_q(n,d)$ ve $q^n\le A_q(n,d)\cdot V_q^n(d-1)$ olduğundan

$$A_q(n,d)\ge\frac{q^n}{V_q^n(d-1)}$$

eşitliği sağlanır.

3.7.3 Küre-Sarma Üst Sınırı (The Sphere-Packing (Hamming) Upper Bound)

Hamming sınırı olarak da bilinen küre-sarma üst sınırı, bir kodun alacağı maksimum büyüklüğü (size) belirtir. Üst sınırdaki mantık, eğer her bir kodsözün çevresine yarıçapı $\left\lfloor\frac{d-1}{2}\right\rfloor$ olan bir küre konulursa bu küreler ayrık olmak zorundadır şeklindedir. Diğer türlü olsaydı iki kodsözden uzaklığı en fazla $\left\lfloor\frac{d-1}{2}\right\rfloor$ olan bir söz olurdu ve üçgen eşitliğinden birbirlerinden uzaklıkları en fazla $d-1$ olan iki kodsöz var olurdu. Bu yüzden sınır, uzayda sarmalanan (packed) kaç tane ayrık küre olduğunu söyler.

Teorem 3.21 (küre-örtü sınırı) $q>1$ ve n, d tam sayılar olmak üzere $1\le d\le n$ için aşağıdaki eşitlik sağlanır [26]:

$$A_q(n,d)\le \frac{q^n}{V_q^n(\left\lfloor \frac{d-1}{2} \right\rfloor)}.$$

İspat: $C=\{c_1,...,c_M\}$, $|A|=q$ ve $e=\left\lfloor \frac{d-1}{2} \right\rfloor$ olsun. $d(C)=d$ olduğundan $S_A(c_i,e)$ küreleri ayrıktır. Böylece

$$\bigcup_{i=1}^{M} S_A(c_i,e)\subseteq A^n$$

sağlanır. Burada birleşim ayrıktır. $|A^n|=q^n$ ve $|S_A(c_i,e)|=V_q^n(e)$ olduğundan

$$M\cdot V_q^n(e)\le q^n$$

olur. $M=A_q(n,d)$ eşitliği kullanılarak

$$A_q(n,d)\le \frac{q^n}{V_q^n(\left\lfloor \frac{d-1}{2} \right\rfloor)}.$$

Örnek 3.50 $C=[7,k,3]$ lineer kodunun alabileceği maksimum boyut *k* bulunsun.

$$|C|=2^k\le \frac{2^7}{\binom{7}{0}+\binom{7}{1}}=\frac{128}{1+7}=\frac{128}{8}=16.$$

Böylece $k\le 4$ olur.

Sonuç 3.22 Her $q>1$ tamsayısı ve $n,d\in$ olmak üzere $1\le d\le n$ için aşağıdaki eşitlik sağlanır [26]:

$$\frac{q^n}{V_q^n(d-1)}\le A_q(n,d)\le \frac{q^n}{V_q^n(\left\lfloor \frac{d-1}{2} \right\rfloor)}.$$

3.7.4 Gilbert – Varshamov Sınırı

Teorem 3.23 n, k ve d tamsayılar olmak üzere $2 \le d \le n$ ve $1 \le k \le n$ sağlansın. Eğer

$$V_q^{n-1}(d-1) < q^{n-k}$$

ise $\mathbb{F}_q$ üzerinde bir $[n,k]$ lineer kodu vardır ki minimum uzaklığı az d 'dir [26] .

İspat: Eğer $V_q^{n-1}(d-1) < q^{n-k}$ ise $d-1$ kolonu lineer bağımsız olan bir $H \in \mathbb{F}_q^{(n-k)\times n}$ kontrol matrisi olduğunu göstermek yeterlidir. c_j, H 'nin j. kolunu olsun. $c_1 \in \mathbb{F}_q^{n-k}$ sıfırdan farklı bir vektör olsun. c_2 de c_1 tarafından üretilmeyen bir vektör olsun. Bu şekilde devam edilerek $2 \le j \le n$ için c_j vektörü $c_1,...,c_{j-1}$ vektörlerinin $d-2$ veya daha azı tarafından üretilmemiş olsun.

İstenen kontrol matrisini elde etmek için $c_1,...,c_{n-k}$ vektörleri ile I_{n-k} birim matrisini oluşturmakla başlanır. Daha sonra $c_{n-k+1},...,c_n$ seçilir. Bu şekilde H kontrol matrisinin doğru oluşturulması için her zaman seçilebilecek bir vektörün olması gerekmektedir. Bu yüzden $c_1,...,c_j$ vektörlerinden $d-2$ veya daha azının ürettiği vektörlerin sayısı hesaplanır. i tane vektörün ürettiği vektör sayısı $(q-1)^i$ ile bulunur. Buradan $c_1,...,c_{j-1}$ $(2 \le j \le n)$ vektörlerinin $d-2$ veya daha azının ürettiği vektörlerin sayısı

$$\sum_{i=0}^{d-2}\binom{j-1}{i}(q-1)^i \le \sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i < q^{n-k}$$

olur. Böylece $c_j (2 \le j \le n)$ vektörü her zaman bulunabileceği söylenebilir. Üretilen vektör sayısı q^{n-k}'dan küçük olduğu için yeni kolonlar eklenebilir. H kontrol matrisinin tüm kolonları lineer bağımsız olduğundan ve kodun minimum uzaklığı en az d olduğundan ispat tamamlanmış olur.

Sonuç 3.24 $q > 1$ asal ve $n, d \in \square$ olmak üzere $2 \le d \le n$ sağlansın. O halde aşağıdaki eşitlik sağlanır:

$$B_q(n,d) \ge \frac{q^{n-1}}{V_q^{n-1}(d-2)}.$$

Örnek 3.51 $C=[9,k,5]$ lineer kodda boyutun üst ve alt sınırı bulunsun.

Hamming sınırına göre üst sınır bulunursa

$$|C|=2^k \le \frac{2^9}{\binom{9}{0}+\binom{9}{1}+\binom{9}{2}} = \frac{512}{1+9+36} = \frac{512}{46} \approx 11.13.$$

$k \le 3$ olur. Alt sınır için Sonuç 2.23 kullanılırsa

$$|C|=2^k \ge \frac{2^8}{\binom{9-1}{0}+\binom{9-1}{1}+\binom{9-1}{2}+\binom{9-1}{3}} = \frac{2^8}{1+8+28+56} = \frac{256}{93} \approx 2.75.$$

Böylece $2 \le k \le 3$ olur.

3.7.5 Mükemmel Kodlar (Perfect Codes)

Tanım 3.38 Eğer q'lu bir kod Hamming sınırına ulaşırsa yani

$$M = \frac{q^n}{V_q^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right)}$$

sağlarsa **mükemmel kod** olarak isimlendirilir. Mükemmel olan üç tane ikili kod vardır. Tekrarlı kod, Hamming kodları ve Golay kodları [27].

3.7.5.1 Tekrarlı Kod (Repetition Code)

Tekrarlı kod $C=(n,1,n)$ kodu trivial olduğundan n tek için $\frac{n-1}{2}$ hata düzelten mükemmel koddur [27] .

Örnek 3.52 $d=n=2e+1$ olduğundan tekrarlı kod tam $\frac{n-1}{2}$ hata düzeltir. Bu kod için Hamming sınırı

$$2\sum_{i=0}^{\frac{n-1}{2}}\binom{n}{i} = 2\left(\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{\frac{n-1}{2}}\right) = 2^n$$

olur. Hamming sınırına eşit kodsözü olduğundan tekrarlı kod mükemmeldir.

3.7.5.2 Hamming Kodları

$r \geq 2$ ve C, $n = 2^r - 1$ olan bir lineer kod olsun. C'nin kontrol matrisi olan H'nin kolonları $\mathbb{F}_2^r$'nin tüm sıfırdan farklı vektörlerinden oluşsun. Bu C koduna $2^r - 1$ uzunluğunda **ikili (binary) Hamming kodu** denir ve $Ham(r, 2)$ ile gösterilir.

İkili Hamming kodunun parametreleri $(2^r - 1, 2^r - r - 1, 3)$ şeklindedir.

Örnek 3.53 $m = 3$ alınırsa

$(2^3 - 1, 2^3 - 3 - 1, 3) = (7, 4, 3)$

kodu elde edilir. $(7, 4, 3)$ kodunun Hamming sınırı hesaplanırsa

$$2^4 \sum_{i=0}^{1} \binom{7}{i} = 2^4 (1 + 7) = 2^7.$$

Böylece $(7, 4, 3)$ Hamming kodu mükemmeldir.

3.7.5.3 Golay Kodları

Hamming kodunun varlığı $d > 3$ sağlayan mükemmel kod var mı sorusunu ortaya çıkardı. Golay kodlar bu özelliği sağlayan kodlardır.

$G = (I_{12} \mid A)$ olmak üzere G, 12×24'lük bir matris ve A matrisi aşağıdaki gibi olsun:

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

Üreteç matrisi G olan ikili lineer koda **genişlemiş (extended) ikili Golay kodu** denir ve G_{24} ile gösterilir.

G_{24} kodunda uzunluk $n=24$, boyut $k=12$ ve minimum uzaklık $d(G_{24})=8$'dir. Yani $G_{24}=[24,12,8]$.

$\hat{G}$ 12×23'lük bir matris belirtmek üzere $\hat{G}=(I_{12}\,|\,\hat{A})$ olsun. Burada $\hat{A}$ matrisi A'nın son kolonunun silinmesiyle elde edilsin. $\hat{G}$ üreteç matrisiyle üretilen ikili lineer koda **ikili Golay kod (binary Golay code)** denir ve G_{23} ile gösterilir [26].

Örnek 3.54 $G_{23}=[23,12,7]$ kodun mükemmel kod olduğu gösterilsin.

Eğer $M=\dfrac{2^n}{V_2^n(3)}$ ise kod mükemmeldir.

$$V_2^n(3)=\binom{23}{0}+\binom{23}{1}+\binom{23}{2}=1+23+253+1771=2048=2^{11}.$$

$$M=2^{12}=\frac{2^3}{2^{11}}=\frac{2^n}{V_2^n(3)}.$$

Böylece G_{23} kodu mükemmeldir.

3.7.6 Teklik Sınırı (Singelton Bound) ve MDS Kodlar

$A_q(n,d)$ ve $B_q(n,d)$ değerleri için bir diğer üst sınır Teklik sınırıdır.

Teorem 3.25 $q>1$ tamsayısı ve $n,d\in$ değerleri için $1\le d\le n$ olsun. Aşağıdaki eşitlik sağlanır:

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

Özel olarak eğer $C=[n,k,d]$ lineer kod ise $k\le n-d+1$ sağlanır.

İspat: C bir optimal (n,M,d) kod olsun. Yani $M=A_q(n,d)$. C'deki her bir sözden son $d-1$ koordinat silinsin. $d(C)=d$ olduğundan geriye kalan $(n-d+1)$ uzunluğundaki kodsözler hala farklıdırlar. Şu durumda en fazla q^{n-d+1} tane kodsöz vardır. Böylece

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

sağlanır.

Örnek 3.55 (i) $\mathbb{F}_4$ üzerinde tanımlı $[6,3,4]$ lineer kodu ele alınırsa,

$k=3=6-4+1=n-d+1$ sağlanır ve $A_4(6,4)=4^3$ olur.

(ii) $A_q(4,3)$ büyüklüğü ele alınsın. Teklik sınırına göre

$$A_q(4,3)\le q^2$$

olur. Küre-sarma sınırı ise

$$A_q(4,3)\le \frac{q^4}{4r-3}$$

olur. $r\ge 4$ için teklik sınırı küre-örtü sınırından daha kısıtlayıcıdır.

Tanım 3.39 $[n,k,d]$ lineer kodu için $k+d=n+1$ sağlanıyorsa bu koda **MDS (Maximum Distance Separable) kod** denir [26].

Örnek 3.56 $\mathbb{F}_q$ sonlu Abelian grup olmak üzere aşağıdakiler n uzunluğunda MDS kodlardır:

(i) $\mathbb{F}^n=(n,q^n,1)$.

(ii) $(n, q^{n-1}, 2)$ parite kodu $\{c_1 c_2 ... c_n : \sum_{i=0}^{n} c_i = 0\}$.

(iii) $(n, q\ , n)$ tekrarlı kodu $\{aa...a : a \in \mathbb{F}\}$.

Teorem 3.26 (MDS kodlarının özellikleri) $C = [n, k, d]$ $\mathbb{F}_q$ üzerinde tanımlı lineer kod olmak üzere G ve H sırasıyla C'nin üreteç ve kontrol matrisi olsunlar. Aşağıdakiler denktir:

- C MDS koddur.
- H'nin her $n-k$ kolonu lineer bağımsızdır.
- G'nin her k kolonu lineer bağımsızdır.
- $C^{\perp}$ MDS koddur.

Aşağıda $d = 3,5,7$ ve $d \le n \le 12$ Küre-Örtü, Hamming ve Teklik sınırının karşılaştırmaları verilmiştir [16].

n	Sphere-covering	Hamming	Singleton
3	2	2	2
4	2	3	4
5	2	5	8
6	3	9	16
7	5	16	32
8	7	28	64
9	12	51	128
10	19	93	256
11	31	170	512
12	52	315	1024

Şekil 3. 4 $A_2(n,3)$ için sınırlar

n	Sphere-covering	Hamming	Singleton
5	2	2	2
6	2	2	4
7	2	4	8
8	2	6	16
9	2	11	32
10	3	18	64
11	4	30	128
12	6	51	256

Şekil 3. 5 $A_2(n,5)$ için sınırlar

n	Sphere-covering	Hamming	Singleton
7	2	2	2
8	2	2	4
9	2	3	8
10	2	5	16
11	2	8	32
12	2	13	64

Şekil 3. 6 $A_2(n,7)$ için sınırlar

3.7.7 Asimptotik Sınırlar (Asymptotic Bounds)

Bu kısımda uzunluğu $n \to \infty$ olan kodlar üzerinde sınırlar anlatılacaktır. Elde edilen sınırlar da asimptotik sınır olarak adlandırılır. Bir kodun oranı (rate) ve bağlı uzaklığı sırasıyla $\Re(C) = \frac{\log_q M}{n}$ ve $\delta(C) = \frac{d-1}{n}$ ile tanımlanmıştı. $\Re$ ve δ değerleri 0 ve 1 arasındadır. Bu iki değer 1'e yaklaştıkça kod iyi kod (good code) olur. O halde δ verildiğinde $\Re$ ne kadar büyük olabilir? [28].

Tanım 3.40 q asal ve $0 \le \delta \le 1$ olmak üzere $\delta \in$ olsun. $\alpha_q(\delta)$ fonksiyonu şu şekilde tanımlanır [28]:

$$\alpha_q(\delta) = \limsup_{n\to\infty} \frac{1}{n} \log_q A_q(n, \lfloor \delta n \rfloor).$$

$\alpha_q(\delta)$'nun tam değeri bilinmemektedir ve bu fonksiyonun üst ve alt sınırı hesaplanacaktır. $\alpha_q(\delta)$ ile hesaplanan üst sınır, bağlı uzaklığı δ'ye yaklaşan tüm kod ailelerinin iletim hızına sahip olduğunu ve en fazla bu üst sınır değerini aldığını gösterir. $\alpha_q(\delta)$ ile hesaplanan alt sınır ise kod uzunluğu sonsuza yaklaşan ve bağlı uzaklığı δ'ye yaklaşan bir kod ailesi olduğunu, bu ailenin iletim hızını bu alt sınıra eşit olduğunu gösterir [23].

3.7.7.1 Asimptotik Teklik Sınırı (Asymptotic Singleton Bound)

Teorem 3.27 $\delta = \lim_{n\to\infty} \delta(C)$ ve $\Re = \lim_{n\to\infty} \Re(C)$ olsun. Her bir kod C için $\delta \le 1 - \Re$ sağlanır.

İspat: Teklik sınırında her bir (n,M,d) kodu için $d \le n - \log_q M + 1$ ve dolayısıyla $d-1 \le n - \log_q M$ sağlanmaktaydı. O halde

$$\delta(C) = \frac{d-1}{n} \le \frac{n}{n} - \frac{\log_q M}{n} = 1 - \Re(C) \to 1 - \Re \ .$$

3.7.7.2 Asimptotik Küre-Sarma (Hamming) Sınırı

Bundan sonra bazı kısaltım ve tanımlar şöyle olacaktır: C_n, n uzunluğundaki kodu göstermek üzere $C = \{C_n\}$ kodlar ailesi olsun. $\delta = \delta(C) = \lim_{n\to\infty} \delta(C_n)$ ve $\Re = \Re(C) = \lim_{n\to\infty} \Re(C_n)$. Bazı durumlarda aşağıdaki sınırlar her bir n için sağlanmaktadır ve bu durumda C_n için sınırlar yazılacaktır. Bazı durumlarda da $n \to \infty$ için sınırlar sağlandığından C için sınır yazılacaktır [23].

$\theta = 1 - 1/q$ kümesi ve $0 \le x \le \theta$ aralığı için $H_q(x)$ fonksiyonu şöyle tanımlansın:

$$H_q(x) = \begin{cases} 0, & x = 0 \\ x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x), & 0 < x \le \theta \end{cases}.$$

H_q fonksiyonu **Hilbert entropi (dağınım) fonksiyonu** olarak isimlendirilir [28].

Lemma 3.28: $0 \le \lambda \le \theta$ olmak üzere herhangi bir λ için aşağıdaki eşitlik sağlanır [28]:

$$\lim_{n\to\infty} \frac{1}{n} \log_q A_q(n, \lfloor \lambda n \rfloor) = H_q(\lambda).$$

Teorem 3.29 Asimptotik bağlı uzaklığı $\delta \le \frac{1}{2}$ ve iletim hızı $\Re$ olan her bir ikili C kodu için aşağıdaki eşitlik sağlanır:

$$\Re \le 1 - H(\frac{\delta}{2}).$$

İspat: $\Re = \frac{\log_q M}{n}$ olduğundan $n \cdot \Re = \log_2 M$ yazılabilir. Küre-Sarma sınırı da

$$M \le A_q(n,d) \le \frac{q^n}{V_q^n(\left\lfloor \frac{d-1}{2} \right\rfloor)}$$

olduğunu belirtir. Buradan

$$\Re n = \log M \le \log A_2(n,d) \le \log\left(\frac{2^n}{V_2^n\left\lfloor\frac{d-1}{2}\right\rfloor}\right)$$

$$= n - \log V_2^n\left(\left\lfloor\frac{d-1}{2}\right\rfloor\right) \to n - \log 2^{nH\left(\frac{d-1}{2}\right)}$$

$$= n - nH\left(\frac{\delta}{2}\right)$$

olur. Her iki taraf n ile sadeleştirilirse

$$\Re \le 1 - H\left(\frac{\delta}{2}\right).$$

3.7.7.3 Asimptotik Gilbert – Varshamov Sınırı

Teorem 3.30 $0 \le \delta \le \theta$ olmak üzere herhangi bir δ için aşağıdaki sağlanır:

$$\alpha_q(\delta) \ge 1 - H_q(\delta).$$

İspat: $\alpha_q(\delta)$ 'in tanımı kullanılırsa,

$$\alpha_q(\delta) = \limsup_{n\to\infty}\frac{1}{n}\log_q A_q(n,\lfloor\delta n\rfloor)$$

$$\ge \limsup_{n\to\infty}\frac{1}{n}\log_q A_q(n,\lfloor\delta n\rfloor+1)$$

$$\ge \lim_{n\to\infty}\frac{1}{n}\log_q\left(\frac{q^n}{V_q(n,\lfloor\delta n\rfloor)}\right)$$

$$= \lim_{n\to\infty}\left(1-\frac{1}{n}\log_q V_q(n,\delta n)\right)$$

$$= 1 - H_q(\delta).$$

BÖLÜM 4

RANK METRİK

Rank metrik ilk olarak Gabidulin tarafından tanımlanmıştır. Rank metrik üzerinde oluşturulan kodlar, kodların özel bir tipidir ve rank kodlar veya rank uzaklıklı kodlar olarak isimlendirilir. Rank metrik, alınan veride oluşan hataları düzeltmede daha verimli bir kapasiteye sahiptir. Bu metrik, faklı semboller arasında lineer bağımlılığı amaçlar ve böylece diğer metrikler üzerinde oluşturulmuş kodlardan daha fazla hata bulup düzeltmeye çalışır.

Bu bölümde rank metriğin daha iyi anlaşılması için öncelikle sonlu cisimlerin matrissel gösterimi ve rank normu tanıtılmış ve daha sonra rank metriği ve sınırlar anlatılmıştır.

4.1 Sonlu Cisimlerin Matrissel Gösterimi

$\mathbb{F}$, keyfi bir cisim ve m, n ve p pozitif tamsayılar olsunlar. $B \in \mathbb{F}^{m\times n}$ bir matris ve $L_B(C) = BC$ olacak şekilde $L_B : \mathbb{F}^{n\times 1} \to \mathbb{F}^{m\times 1}$ fonksiyonu tanımlansın. L_B (soldan B ile çarpım) matris çarpım özelliklerine göre lineer dönüşümdür (linear transformation):

$C, C_1, C_2 \in \mathbb{F}^{n\times 1}$ ve $\alpha \in \mathbb{F}$ için

$$\begin{aligned} L_B(C_1 + C_2) &= B(C_1 + C_2) \\ &= BC_1 + BC_2 \\ &= L_B(C_1) + L_B(C_2) \end{aligned}$$

ve

$$\begin{aligned} L_B(\alpha C) &= B(\alpha C) \\ &= \alpha(BC) \\ &= \alpha L_B(C). \end{aligned}$$

Eğer $\mathbb{F}_{q^m}$ cisminden bir b elemanı alınırsa, b ile soldan çarpım, $\mathbb{F}_{q^m} = V$ vektör uzayı üzerinde bir lineer dönüşüm L_b belirtir. Eğer $\mathbb{F}_{q^m} = V$ vektör uzayında herhangi bir B tabanı seçilirse bu tabana göre L_b'nin $[L_b] = [L_b]_B$ matrisi bulunabilir. Eğer farklı B tabanları seçilir ve aynı yolla $\mathbb{F}_{q^m}$'in her bir elemanının matrisi bulunursa elde edilen matris kümesi $\mathbb{F}_{q^m}$'e izomorftur. Böylece her bir taban seçimi $\mathbb{F}_{q^m}$'nin farklı matris gösterimini verir.

Matris gösterimini bulmadan önce cisimin çarpım tablosunun yazılması gerekmektedir. Ancak eş matris kullanılarak bu zorluk aşılabilir.

Tanım 4.1 Bir cisim üzerinde derecesi n olan $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1} + x^n$ monik polinomunun **eş matrisi (companion matrix)** aşağıdaki $n \times n$'lik matris ile tanımlanır:

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & 0 & \cdots & 0 & -\alpha_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -\alpha_{n-1} \end{pmatrix}.$$

Lineer cebirden A matrisi $f(A) = 0$ denklemini sağlar. Yani I, $n \times n$'lik birim matris olmak üzere

$$\alpha_0 I + \alpha_1 A + \cdots + \alpha_{n-1}A^{n-1} + A^n = 0.$$

O halde, $\mathbb{F}_q$ üzerinde tanımlı f monik polinomu için eş matris A ise $f(A) = 0$'dır ve bu da A'nın, f monik polinomunun kökünde rol oynadığını gösterir. Böylece derecesi n'den küçük, $\mathbb{F}_q$ üzerinde tanımlı A'daki polinomlar $\mathbb{F}_{q^m}$'nin elemanlarının bir gösterimini (representation) sağlar.

Örnek 4.1 $\mathbb{F}_9$ cisminin elemanlarını matrissel olarak gösterelim.

$\mathbb{F}_9$, $\mathbb{F}_3$ üzerinde derecesi 2 olan genişlemesi olduğundan $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$ monik indirgenemez polinomu alınabilir. f'nin eş matrisi $\alpha_0 = 1$ ve $\alpha_1 = 0$ olduğundan

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

olduğu görülür. Buradan

$$f(A)=\begin{pmatrix}0 & 2\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=0$$

olur. O halde aşağıdaki matris kümesi $\mathbb{F}_9$ cismine izomorfiktir:

$$\mathbb{F}_9=\{0,I,2I,A,I+A,2I+A,2A,I+2A,2I+2A\}.$$

Örnek 4.2 $\mathbb{F}_8$ cisminin elemanlarını matrissel olarak gösterelim.

$\mathbb{F}_2$ üzerinde tanımlı $f(x)=x^3+x+1$ monik indirgenemez polinomunu ele alalım. f 'nin eş matrisi $\alpha_0=1$, $\alpha_1=1$ ve $\alpha_2=0$ olduğundan

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

olur. Cismin elemanları da $\mathbb{F}_{2^3}[A]=\{0,I,A,...,A^6\}$ kümesine izomorfiktir.

4.2 Rank Normu ve Rank Kodlar

Rank kodların gösterimi iki türlüdür: vektör gösterimi ve matrissel gösterimi.

Vektörel gösterimi: $\mathbb{F}_q$ bir taban cismi ve $\mathbb{F}_{q^n}$, bu cismin derecesi n olan genişlemesi olsun. $\mathbb{F}_{q^n}^n$, $\mathbb{F}_{q^n}$ üzerinde tanımlı boyutu n olan normalize vektör uzayı olsun. $g\in\mathbb{F}_{q^n}^n$ olmak üzere $g=(g_1,g_2,...,g_n)$ vektörünün **rank normu**, $\mathbb{F}_q$ üzerinde lineer bağımsız g_j koordinatlarının maksimal sayısı olarak tanımlanır ve $r(g)$ ile gösterilir. $C\subset\mathbb{F}_{q^n}^n$ olan kümelere de **rank kodlar** veya **vektör kodlar** denir. g_1 ve g_2 vektörlerinin **rank uzaklığı** (rank distance)

$$d(g_1,g_2)=r(g_1-g_2) \tag{4.1}$$

ile tanımlıdır.

Matrissel gösterimi: $\mathbb{F}_q^{n\times n}$, $\mathbb{F}_q$ üzerinde tanımlı derecesi n olan kare matrislerin kümesi olsun. $M\in\mathbb{F}_q^{n\times n}$ matrisinin **rank normu**, bilinen matris rankı olarak tanımlanır. Yani

$\mathbb{F}_q$ üzerinde tanımlı lineer bağımsız satır veya sütunların maksimal sayısıdır ve $rank(M)$ ile gösterilir. $M \subset \mathbb{F}_q^{n\times n}$ olan matrislere de **rank kodlar** veya **matris kodlar** denir. M_1 ve M_2 matrisleri arasındaki **rank uzaklığı**

$$d(M_1, M_2) = rank(M_1 - M_2) \tag{4.2}$$

ile tanımlıdır.

$g_j \in \mathbb{F}_{q^n}$ olmak üzere $g = (g_1, g_2, ..., g_n)$, $\mathbb{F}_{q^n}$'in bir sıralı tabanı olsun. Aşağıdaki fonksiyon tanımlansın;

$$\begin{aligned} &\vartheta : \mathbb{F}_{q^n}^n \to \mathbb{F}_q^{n\times n} \\ &m = (m_1, ..., m_n) \to M \end{aligned} \tag{4.3}$$

Burada $m \in \mathbb{F}_{q^n}^n$ iken $M \in \mathbb{F}_q^{n\times n}$ matrisi, $m = gM$ eşitliğini sağlayan tek matristir. M matrisi, m vektörünün $g-$gösterimi şeklinde de bilinir. ϑ fonksiyonu rank normu ve rank uzaklığının korunduğu bijektif bir fonksiyondur [29]:

$$\begin{aligned} &r(m) = rank(M) \\ &d(g_1, g_2) = r(g_1 - g_2) = d(M_1, M_2) = rank(M_1, M_2). \end{aligned} \tag{4.4}$$

Tanım 4.2 x, elemanları $GF(q^N)$ üzerinde tanımlı n uzunluğunda bir kodsöz olsun.

$$\begin{aligned} &\ell : GF(q^N)^n \to A_N^n \\ &x = (x_1, x_2, ..., x_{n-1}) \to (N \times n) \end{aligned} \tag{4.5}$$

bijektif fonksiyonu ele alınsın.

q'ya göre x'in **rank normu**

$$r(x \mid q) = rank(A \mid q) \tag{4.6}$$

ile tanımlanır. $rank(\mathrm{A} \mid q)$ rank fonksiyonu, A'nın $GF(q)$ üzerinde tanımlı maksimum sayıdaki lineer bağımsız satır veya sütun sayısına eşittir.

Rank fonksiyonu bir metrik tanımlar [30]. Gerçekten,

$r(x \mid q) \geq 0$
$r(x \mid q) = 0 \Leftrightarrow x = 0$
$r(x + y \mid q) \leq r(x \mid q) + r(y \mid q)$
$r(ax \mid q) = \mid a \mid r(x \mid q).$

Örnek 4.3 $\alpha^3 = \alpha + 1$ olmak üzere $GF(2^3) = GF(2)(\alpha)$ kümesi ele alınsın ve $n = 5$ olsun. $x = (\alpha^6, \alpha, 0, \alpha^5, \alpha) = (\alpha^2 + 1, \alpha, 0, \alpha^2 + \alpha + 1, \alpha)$ vektörü ele alınsın. x vektörü için

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

matrisi elde edilir ve rankı $r(x) = 2$ 'dir.

4.3 Rank Metrik

Tanım 4.3 $GF(q^m)^n$, $GF(q^m)$ üzerinde tanımlı $n-$boyutlu vektör uzayı olmak üzere $a = (a_0, a_1, ..., a_{n-1}) \in GF(q^m)^n$ olsun. $\gamma_0, \gamma_1, ..., \gamma_{m-1}$ $GF(q^m)$ 'nin sıralı taban kümesi olsun. Buradan $a_{i,j} \in GF(q), i = 0,1,...,m-1$ ve $j = 0,1,...,n-1$ olmak üzere a_j koordinatı,

$$a_j = \sum_{i=0}^{m-1} a_{i,j} \gamma_i \tag{4.7}$$

şeklinde yazılabilir. Böylece a_j, $\gamma_0, \gamma_1, ..., \gamma_{m-1}$ sıralı taban kümesine göre $m-$boyutlu $(a_{0,j}, a_{1,j}, ..., a_{m-1,j})^T$ sütun vektörüne genişletilebilir. A, a vektörünün tüm koordinatlarının genişlemesi ile elde edilen $m \times n$ 'lik matris olsun. 4.7 denklemi göz önüne alınarak A matrisi aşağıdaki gibi yazılır:

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{pmatrix}.$$

a vektörünün rank normu ($GF(q)$ üzerinde) A matrisinin rank normu olarak tanımlanır. Yani

$r(a \mid q) = rank(A \mid q).$

Böylelikle $\forall a,b \in GF(q^m)^n$ olmak üzere

$$d_R(a,b) = r(a-b \mid q) \tag{4.8}$$

bir metrik belirtir ve **rank metriği** olarak isimlendirilir [30].

Tanım 4.4 $C \subseteq GF(q^m)^n$, n uzunluğunda bir kod olsun. C'nin **minimum rank uzaklığı** (minimum rank distance) aşağıdaki şekilde tanımlanır:

$d_R(C) = \min_{c_1 \neq c_2 \in C} d_R(c_1, c_2).$

Örnek 4.4 $\alpha^2 = \alpha + 1$ olmak üzere $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha^2\}$ kümesi üzerinde oluşturulan $C = \{(0,0),(1,\alpha^2),(\alpha,1),(\alpha^2,\alpha)\}$ lineer kodu ele alınsın. $d_R((0,0),(\alpha,1))$ bulunmak istensin.

$(0,0) \in \mathbb{F}_{2^2}^2$ 'dir. $\mathbb{F}_{2^2}^2$, $\mathbb{F}_{2^2}$ kümesi üzerinde bir vektör uzayı olarak düşünülebilir. O halde $(0,0)$ kodsözünün her bir koordinatı $\mathbb{F}_{2^2}$ kümesinin tabanı ile gösterilebilir. $\mathbb{F}_{2^2}$ kümesi de $\mathbb{F}_2$ üzerinde bir vektör uzayı olduğundan $\mathbb{F}_{2^2}$'nin her bir elemanı $\mathbb{F}_2$ kümesinin tabanı ile gösterilebilir. $\{1, \alpha\}$ sıralı taban kümesi ele alınırsa her bir $k \in \mathbb{F}_{2^2}$ elemanı

$k = x \cdot 1 + y \cdot \alpha \quad , \quad x, y \in \mathbb{F}_2$

şeklinde yazılabilir. O halde,

$(0,0) \in \mathbb{F}_{2^2}^2 \Rightarrow 0 \in \mathbb{F}_{2^2}, 0 \in \mathbb{F}_{2^2}$
$0 = 0 \cdot 1 + 0 \cdot \alpha$
$0 = 0 \cdot 1 + 0 \cdot \alpha$

şeklinde her bir koordinat taban kümesi ile gösterilir. Tanım gereği her bir koordinat sütun vektörüne genişletilirse $(0,0) \in \mathbb{F}_{2^2}^2$ kodsözü için

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

matrisi elde edilir. Aynı işlem $(\alpha,1)\in\mathbb{F}_{2^2}^2$ kodsözüne de uygulanırsa,

$(\alpha,1)\in\mathbb{F}_{2^2}^2 \Rightarrow \alpha\in\mathbb{F}_{2^2}, 1\in\mathbb{F}_{2^2}$

$\alpha = 0\cdot 1+1\cdot\alpha$

$1 = 1\cdot 1+0\cdot\alpha$

elde edilir. Buradan $(\alpha,1)\in\mathbb{F}_{2^2}^2$ kodsözü için

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

matrisi elde edilir. Bu iki kodsözün rank uzaklığı

$$d_R((0,0),(\alpha,1)) = r((0,0)-(\alpha,1)) = r(\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}-\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}) = r(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}) = 2$$

olur. Diğer kodsözlerin d_R'leri de bulunmak istenirse,

$$d_R((0,0),(1,\alpha^2)) = r(\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}-\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}) = r(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}) = 2.$$

$$d_R((0,0),(\alpha^2,\alpha)) = r(\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}-\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}) = r(\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}) = 2.$$

$$d_R((1,\alpha^2),(\alpha\ ,1)) = r(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}-\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}) = r(\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}) = 2.$$

$$d_R((1,\alpha^2),(\alpha^2,\alpha)) = r(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}-\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}) = r(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}) = 2.$$

$$d_R((\alpha,1),(\alpha^2,\alpha)) = r(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}-\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}) = r(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}) = 2.$$

C kodunun minimum rank uzaklığı 2 'dir.

Örnek 4.5 C, $GF(2^3)$ üzerinde tanımlı $(4,2)$ kod olsun. α primitif eleman olmak üzere

$$G = \begin{pmatrix}0 & 1 & 1 & \alpha\\ 0 & \alpha^5 & \alpha^2 & 1\end{pmatrix}$$

üreteç matris olsun. $u=(0,1,1,\alpha)$ kodsözü için Hamming ağırlığı $w_H=3$ iken rank ağırlığı (normu) $r(u)=2$'dir. C'nin minimum rank uzaklığı $d_R(C)=2$'dir.

Rank metrik, $GF(q^m)^n$ üzerinde tanımlanan ve rank normu ile elde edilen bir metriktir. $x\in GF(q^m)^n$ olmak üzere rank metriğinde küre (sphere) ve yuvar (ball) şu şekilde tanımlanır [26]:

- x merkezli $t\geq 0$ yarıçaplı **küre** $S(x,t)=\{y\in GF(q^m)^n \mid r(y-x)=t\}.$
- x merkezli $t\geq 0$ yarıçaplı **yuvar** $B(x,t)=\bigcup_{i=0}^{t} S(x,i).$

Tanım 4.5 q asal, V_j'ler $GF(q)$ üzerinde m - boyutlu vektör uzayları olmak üzere

$V=V_1\times V_2\times\cdots\times V_n,$

$GF(q^m)$ üzerinde n - boyutlu vektör uzay olsun. Eğer $C\subseteq V$ için

$$\bigcup_{x\in C} S(x,t)=V$$

sağlanırsa C'ye **mükemmel t - hata – düzelten – kod** denir [31].

Vektörlerin ötelenmesinde rank metrik değişmediğinden kürelerin ve yuvarların hacimleri seçilen bir merkeze bağlı değildir. O halde küre ve yuvarın hacimleri aşağıdaki şekilde tanımlanır [26]:

- S_t, $GF(q^m)$'de t yarıçaplı kürenin hacmi olsun. S_t, $rank=t$ olan $m\times n$'lik matrislerin sayısına eşittir. Eğer $t=0$ ise $S_0=1$ ve $t=1,...,\min(n,m)$ için

$$S_t=\prod_{j=0}^{t-1}\frac{(q^n-q^j)(q^m-q^j)}{q^t-q^j}\ . \qquad (4.9)$$

İspat: $M_{m\times n}(q)$, elemanları $GF(q)$'dan olan tüm $m\times n$ matrislerin kümesi ve $M(t)=\{A\in M_{m\times n}(q) \mid rank(A)=t\}$ olsun. $S_t=|M(t)|=\prod_{i=0}^{t-1}\frac{(q^n-q^i)(q^m-q^i)}{q^t-q^i}$ olduğu gösterilecektir.

$P(t)=\{P\in M_{m\times t}(q)\mid rank(P)=t\}$ rankı t olan tüm $m\times t$ matrislerin kümesi ve $Q(t)=\{Q\in M_{t\times n}(q)\mid rank(Q)=t\}$ rankı t olan tüm $t\times n$ matrislerin kümesi olsun. $P\in P(t)$ ve $Q\in Q(t)$ olmak üzere $M(t)$'deki herhangi bir matris PQ çarpımı ile belirtilebilir. $P(t)\times Q(t)$'den $M(t)$'ye aşağıdaki şekilde bir fonksiyon tanımlansın:

$\psi:(P,Q)\to PQ.$

ψ örtendir ve bazı regüler $t\times t$ matris T'ler için

$$\psi(P_1,Q_1)=\psi(P_2,Q_2)\Leftrightarrow P_1=P_2T \quad ve \quad Q_2=TQ_1$$

vardır. Sonuç olarak, $L_t(q)$, $GF(q)$ üzerinde tüm regüler $t\times t$ matrisleri tanımlamak üzere

$$\left|P(t)\times Q(t)\right|=\left|M(t)\right|\cdot\left|L_t(q)\right|$$

sağlanır. Bu eşitlik kullanılarak

$\left|P(t)\right|=(q^m-1)(q^m-q)...(q^m-q^{t-1})$, $\left|Q(t)\right|=(q^n-1)(q^n-q)...(q^n-q^{t-1})$ ve $\left|L_t(t)\right|=(q^t-1)(q^t-q)...(q^t-q^{t-1})$ olur ki ispat tamamlanmış olur.

- B_t, $GF(q^m)$'de t yarıçaplı yuvarın hacmi olsun. B_t, $rank\le t$ olan $m\times n$'lik matrislerin sayısına eşittir. O halde,

$$\forall t=0,...,\min(n,m),\qquad B_t=\sum_{i=0}^{t}S_i\,. \tag{4.10}$$

İspat: Kürenin tanımı ve S_t'den elde edilir.

4.4 Rank Metrikte Küre ve Yuvar Sınırları

Önerme 4.1 $t=0,...,\min(n,m)$ olmak üzere aşağıdaki eşitlikler sağlanır [26]:

$$\begin{cases} q^{(m+n-2)t-t^2}\le S_t\le q^{(m+n+1)t-t^2} \\ q^{(m+n-2)t-t^2}\le B_t\le q^{(m+n+1)t-t^2+1} \end{cases} \tag{4.11}$$

İspat: *Küre hacmi ele alınırsa*, (4.11) formülü şöyle yazılabilir:

$$S_t = q^{(m+n)t-t^2} \prod_{j=0}^{t-1} \frac{(1-q^{j-n})(1-q^{j-m})}{1-q^{j-t}}.$$

Tüm $j = 0,...,t-1$ için $t \le \min(n,m)$ olduğundan

$$\begin{cases} (1-q^{t-n-1})(1-q^{t-m-1}) \le (1-q^{j-n})(1-q^{j-m}) \le 1 \\ 1 \quad \ge \quad 1-q^{j-t} \quad \ge \quad 1-\frac{1}{q} = \frac{q-1}{q} \end{cases}$$

yazılabilir. Aynı sebepten $(1-q^{-1}) \le (1-q^{t-\min(n,m)-1})$ yazılabilir. Böylece,

$$(1-2q^{-1}+q^{-2}) \le (1-q^{t-n-1})(1-q^{t-m-1}).$$

q asal olduğundan $q \ge 2$'dir. Bu durum $(1-2q^{-1}) \ge 0$ ve $q^{-2} \le (1-q^{t-n-1})(1-q^{t-m-1})$ sağlar. Aynı şart ile $\frac{q}{q-1} \le q$'de sağlanır. Böylece çarpımın her biri aşağıdakini sağlar:

$$\forall j = 0,...,t-1, \qquad q^{-2} \le \frac{(1-q^{j-n})(1-q^{j-n})}{1-q^{j-t}} \le q.$$

Yuvar hacmi ele alınırsa: Aynı yarıçap değerinde yuvarın hacmi kürenin hacminden büyük olduğu için alt sınır direkt olarak kürenin alt sınırından gelir. $L = m+n+1$ olsun. O halde küre hacminin üst sınırı aşağıdaki eşitliği sağlar:

$$B_t \le \sum_{i=0}^{t} q^{Li-i^2} = q^{Lt-t^2} \left(1 + \sum_{i=0}^{t-1} q^{(L-i-t)(i-t)} \right).$$

$i = 0,...,t-1$ için $L-i-t \ge L-t$ ve $(i-t) < 0$ sağlar. Böylece $q^{(L-i-t)(i-t)} \le q^{(L-t)(i-t)}$ olur. Buradan değişkenler yerlerine yazılırsa,

$$B_t \le q^{Lt-t^2} \left(1 + \sum_{j=1}^{t} q^{-(L-t)j} \right)$$

elde edilir. Toplam işlemi hesaplanırsa,

$$1 + \sum_{j=1}^{t} q^{-(L-t)j} = \frac{1-q^{-(L-t)(t+1)}}{1-q^{-(L-t)}} \le \frac{1}{1-q^{-(L-t)}}.$$

$t \le \min(n,m)$ ve $q \ge 2$ olduğundan $\dfrac{1}{(1-q^{-(L-t)})} \le 2 \le q$ sağlanır.

4.5 Teklik Sınırı ve MRD kodlar

Bir kodun minimum rank uzaklığı özel olarak sınırlandırılabilir. İlk olarak $GF(q^m)$ üzerinde tanımlı kodun minimum uzaklığı d_R, m ile sınırlandırılır. $d_R = m$ özelliğini sağlayan kodlar ful rank uzaklıklı kodlar (full rank distance codes) olarak isimlendirilir ve [32]'da çalışılmıştır.

Teorem 4.2 $|C| = M$ olmak üzere $C \subseteq GF(q^m)^n$ rank kod ve $d_R(C) = d$ olsun. Aşağıdaki eşitlik sağlanır [33]:

$$M \le q^{\min\{m(n-d+1),n(m-d+1)\}}. \tag{4.12}$$

İspat: c_1 ve c_2 iki kodsöz olsun ve bu kodsözlerin ilk $n-d+1$ koordinatı aynı olsun. Bu durumda $c_1 - c_2$'in $n-d+1$ koordinatı 0 olur ve sonuçta $d_R(c_1,c_2) < d$ olur ki C'nin minimum rank uzaklığı d ile çelişir. Bu durum C'de ilk $n-d+1$ koordinatı eşit olan iki kodsöz olmadığını gösterir. Böylece C'nin büyüklüğü $n-d+1$ sayısı ile üstten sınırlandırılmış olur:

$$M \le \left|GF(q^m)^{n-d+1}\right| = q^{m(n-d+1)}. \tag{4.13}$$

$GF(q)$ üzerinde tanımlı $GF(q^m)$ vektör uzayından herhangi bir b tabanı seçilsin ve rank metrik tanımındaki gibi, C'deki her bir kodsözün tüm koordinatları b'ye göre gösterimleri (representation) ile değiştirilsin. Bu şekilde her bir kodsöz, elemanları $GF(q)$'de olan $m \times n$'lik matrislere eşleşir (map) ve bu matrisler $B(c)$ ile gösterilsin. Herhangi iki kodsöz c_1 ve c_2 için $r(c_1,c_2)$ rankı, $B(c_1) - B(c_2)$ matrisinin rankına eşittir. Bir matrisin rankı, o matrisin satır rankına eşit olduğundan, $B(C) = \{B(c) : c \in C\}$ kümesinde ilk $m-d+1$ satırı aynı olan iki matris yoktur. Böylece, $B(C)$'deki eleman sayısı, $GF(q)$ üzerindeki tüm $(m-d+1)\times n$ matrislerinin kümesinin büyüklüğü $q^{n(m-d+1)}$'i geçemez. Ancak C'den $B(C)$'ye olan fonksiyon birebir olduğundan $M \le q^{n(m-d+1)}$ yazılır. Bu eşitlik (4.13) ile birleştirilerek ispat tamamlanmış olur.

Büyüklüğü teklik sınırına eşit olan rank metrik kodlara **maksimum rank uzaklıklı (Maximum Rank Distance - MRD) kodlar** denir [15]. Yani, $GF(q^m)$ üzerinde tanımlı (n, M, d) kodu aşağıdaki eşitliği sağlarsa MRD kod olarak isimlendirilir [26]:

- $M = q^{m(n-d+1)}, \quad n \le m$
- $M = q^{m(n-d+1)}, \quad n > m$

Örnek 4.6 $GF(q^m)$ üzerinde tanımlı $[n,1,n]$ kodu MRD koddur.

MRD kodların inşasında gerekli lemma ve teoremler için [33] ve [34] makalelerine bakılabilir. Aşağıda MRD kodların inşasından kısaca bahsedilecektir.

M, $GF(q)$ üzerinde tanımlı $n \times n$'lik matris olsun. Bu matrisin kolon elemanları, $GF(q)$ üzerindeki herhangi bir tabanın genişlemesi olan $GF(q^n)$ cisminin bir elemanının gösterimi (representation) olarak düşünülebilir. Bu ise, $M \leftrightarrow m$ birebir fonksiyon tanımlar. Burada m, elemanları $GF(q^n)$'de olan n uzunluğunda bir vektördür. m'nin rankı, lineer bağımsız koordinatlarının sayısı olarak tanımlanmıştı. Bu rank M matrisinin rankına eşittir. Böylece MRD kodu inşa edilebilir ve daha sonra matrisler üzerine eşleştirilir (map).

Genel olarak bir vektörden matris inşası şu şekildedir: $g_1, g_2, ..., g_n$, $GF(q^n)$ cisminin lineer bağımsız elemanları olsunlar. Sonlu cisim lineer kod C'nin üreteç matrisi aşağıdaki gibi olsun:

$$G = \begin{pmatrix} g_1 & g_2 & g_3 & \cdots & g_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & g_3^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}.$$

Bu C kodu, rank uzaklığı $d_R = n - k + 1$ olan MRD koddur.

Özel olarak ful-rank MRD kodun inşası şu şekildedir: α, $GF(q^n)$ cisminin ilkel elemanı olmak üzere $c = \left(1, \alpha, \alpha^2, ..., \alpha^{n-1}\right)$ kodsözü tanımlansın. Bu vektörün tüm elemanları $GF(q)$ üzerinde lineer bağımsızdır ve kod q^n vektörlü küme olarak verilir,

$C = \left\{0, \alpha^i \cdot c, i = 0, ..., q^n - 2\right\}$. Karşılık gelen matris kod, c'nin elemanlarının, bu elemanların $GF(q)$ üzerinde kolon gösterimi ile değiştirilmesi ile elde edilir. Rank MRD kodların özel formu eş matris ile tanımlanır:

$$\mathbb{C} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ -b_0 & -b_1 & \cdots & -b_{n-1} \end{pmatrix}$$

$$c = \left[\alpha, \alpha^2, ..., \alpha^n\right]^T$$

İlkel indirgenemez polinom $f(x)$, $b_i \in GF(q)$ katsayılarını tanımlar ve C kodunu verir:

$$f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

$$C = \left\{0, \mathbb{C}, \mathbb{C}^2, ..., \mathbb{C}^{q^n-2}, \mathbb{C}^{q^n-1}\right\}.$$

C'nin $n \times n$'lik matrisleri, rank uzaklığı n olan q^n elemanlı lineer MRD kodu tanımlar. Eş matris, cismin matrissel gösterimi ile ilgilidir. Bu sebeple $f(x)$'in seçimi MRD kodun, kod özelliklerini etkilemez [35].

Örnek 4.7 $GF(2^2)^2$ vektör uzayı ele alınsın ve ilkel polinom $f(x) = x^2 + x + \alpha$ seçilsin. Bu polinomun katsayıları $GF(2^2)$ cismindedir ve $GF(2)$ üzerinde tanımlı $\alpha^2 + \alpha + 1 = 0$ ilkel polinomu ile hesaplansın. MRD kodu tanımlayalım.

MRD kodun matris gösterimi eş matris kullanılarak $GF(2^2)^2$ vektör uzayından aşağıdaki şekilde elde edilebilir:

$$C^0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad C^1 = \begin{pmatrix} 0 & \alpha \\ 1 & 1 \end{pmatrix}, \quad C^2 = \begin{pmatrix} \alpha & \alpha \\ 1 & \alpha^2 \end{pmatrix}$$

$$C^3 = \begin{pmatrix} \alpha & 1 \\ \alpha^2 & 1 \end{pmatrix}, \quad C^4 = \begin{pmatrix} 1 & \alpha \\ 1 & 0 \end{pmatrix}, \quad C^5 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$

$$C^6 = \begin{pmatrix} 0 & \alpha^2 \\ \alpha & \alpha \end{pmatrix}, \quad C^7 = \begin{pmatrix} \alpha^2 & \alpha^2 \\ \alpha & 1 \end{pmatrix}, \quad C^8 = \begin{pmatrix} \alpha^2 & \alpha \\ 1 & \alpha \end{pmatrix}$$

$$C^9=\begin{pmatrix}\alpha & \alpha^2\\ \alpha & 0\end{pmatrix},\quad C^{10}=\begin{pmatrix}\alpha^2 & 0\\ 0 & \alpha^2\end{pmatrix},\quad C^{11}=\begin{pmatrix}0 & 1\\ \alpha^2 & \alpha^2\end{pmatrix}$$

$$C^{12}=\begin{pmatrix}1 & 1\\ \alpha^2 & \alpha\end{pmatrix},\quad C^{13}=\begin{pmatrix}1 & \alpha^2\\ \alpha & \alpha^2\end{pmatrix},\quad C^{14}=\begin{pmatrix}\alpha^2 & 1\\ \alpha^2 & 0\end{pmatrix}$$

$$C^5=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Böylece rank kod $\left\{C^0,C^1,C^2,...,C^{15}\right\}$ bir MRD koddur.

Örnek 4.8 $GF(5^2)$ üzerinde tanımlı $[2,1,2]$ MRD kodu tanımlayalım.

$GF(5)$ üzerinde tanımlı $f(x)=x^2+4x+2$ ilkel polinomu ele alınsın. Eş matris aşağıdaki gibi olur:

$$\mathbb{C}=\begin{pmatrix}0 & -2\\ 1 & -4\end{pmatrix}=\begin{pmatrix}0 & 3\\ 1 & 1\end{pmatrix}.$$

$GF(5)$ üzerinde, $C=\left\{0,\mathbb{C},\mathbb{C}^2,...,\mathbb{C}^{24}\right\}$ ile tanımlanan matrissel kod minimum rank uzaklığı 2 olan MRD koddur.

Tanım 4.6 $n\le m$ için $g=(g_1,g_2,...,g_n)\in GF(q^m)$ lineer bağımsız elemanlar olsunlar. $[i]=q^i$ olmak üzere G üreteç matrisi şöyle tanımlansın:

$$G=\begin{Vmatrix} g_1 & g_2 & \cdots & g_n\\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]}\\ g_1^{[2]} & g_2^{[2]} & \cdots & g_n^{[2]}\\ \cdots & \cdots & \cdots & \cdots\\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]}\end{Vmatrix}$$

G ile üretilen koda **Gabidulin kodu** denir. Boyutu k ve minimum rank uzaklığı $d_R=n-k+1$'dir.

Örnek 4.9 $GF(2^4)$ üzerinde tanımlı Gabidulin kodu için $n=4$ ve $k=3$ olsun. α primitif eleman olsun. O halde $\alpha^{15}=1$ ve $\alpha^4=\alpha+1$ olur. Buradan

$$GF(16)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha+1,\alpha^2+\alpha,\alpha^3+\alpha^2,\alpha^2+1,\alpha^3+\alpha,\alpha^3+\alpha+1,\alpha^3+\alpha^2+\alpha,$$
$$\alpha^3+\alpha^2+\alpha+1,\alpha^3+\alpha^2+1,\alpha^3+1\}$$

olur. $(1,\alpha,\alpha^2,\alpha^3)$, $GF(16)$ için taban olsun. $g=(g_1,g_2,g_3,g_4)\in\mathbb{F}_{2^4}^4$ elemanları şu şekilde seçilsin:

$g_1=\alpha\rightarrow 0100$
$g_2=\alpha^2\rightarrow 0010$
$g_3=\alpha^3\rightarrow 0001$
$g_4=\alpha^4=\alpha+1\rightarrow 1100$

$g=(g_1,g_2,g_3,g_4)$ lineer bağımsızdır.

$$G=\begin{pmatrix} g_1 & g_2 & g_3 & g_4 \\ g_1^{[1]} & g_2^{[1]} & g_3^{[1]} & g_4^{[1]} \\ g_1^{[2]} & g_2^{[2]} & g_3^{[2]} & g_4^{[2]} \end{pmatrix}$$

$$G=\begin{pmatrix} \alpha & \alpha^2 & \alpha^3 & \alpha+1 \\ \alpha^2 & \alpha+1 & \alpha^3+\alpha^2 & \alpha^2+1 \\ \alpha+1 & \alpha^2+1 & \alpha^3+\alpha^2+\alpha+1 & \alpha \end{pmatrix}$$

G, Gabidulin kodun üreteç matrisidir. d bu kodun minimum rank uzaklığı olmak üzere $d-1=n-k$ eşitliğine bakalım.

$$d((\alpha,\alpha^2,\alpha^3,\alpha+1)-(\alpha^2,\alpha+1,\alpha^3+\alpha^2,\alpha^2+1))=\begin{pmatrix} 0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{pmatrix}-\begin{pmatrix} 0&1&0&1\\0&1&0&0\\1&0&1&1\\0&0&1&0\end{pmatrix}$$
$$=\begin{pmatrix} 0&1&0&0\\1&1&0&1\\1&1&1&1\\0&0&0&0\end{pmatrix}=3$$

$$d((\alpha^2,\alpha+1,\alpha^3+\alpha^2,\alpha^2+1)-(\alpha+1,\alpha^2+1,\alpha^3+\alpha^2+\alpha+1,\alpha))=\begin{pmatrix}0&1&0&1\\0&1&0&0\\1&0&1&1\\0&0&1&0\end{pmatrix}-\begin{pmatrix}1&1&1&0\\1&0&1&1\\0&1&1&0\\0&0&1&0\end{pmatrix}$$

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

$$d((\alpha,\alpha^2,\alpha^3,\alpha+1)-(\alpha+1,\alpha^2+1,\alpha^3+\alpha^2+\alpha+1,\alpha))=\begin{pmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{pmatrix}-\begin{pmatrix}1&1&1&0\\1&0&1&1\\0&1&1&0\\0&0&1&0\end{pmatrix}$$

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

$d_R(C)=2$ olduğu görülmüştür. O halde $d-1=n-k$ eşitliği için

$2-1=4-3$

sağlanmaktadır.

4.6 Küre – Sarma Sınırı ve Mükemmel Kodlar

Küre – Sarma sınır problemi, $GF(q^m)$, n uzunluğu ve r yarıçapı verildiğinde $GF(q^m)^n$'de yarıçapı r olan ve kesişmeyen maksimum yuvar sayısı ile ilgilidir. Yine bu problem, r yarıçaplı kodsözlerinin oluşturduğu küreleri birbiriyle kesişmeyen, minimum uzaklığı $d \geq 2r+1$ olan n uzunluğundaki kodun maksimum kardinalitesini bulmaya eşdeğerdir. Ayrıca bu kesişmeyen küreler tüm uzayı sarıyorsa kod mükemmel kod olarak adlandırılır [36].

Teorem 4.3 (Küre – Sarma Sınırı) $t=\lfloor (d-1)/2 \rfloor$ ve $C \subseteq V$ t - hata – düzelten – kod olsun. Aşağıdaki eşitlik sağlanır [31]:

$$|C| \cdot B_t \leq q^{mn}.$$

İspat: C, t- hata – düzelten – kod olsun. x kodsözünün çevresindeki t yarıçaplı küreler ayrık olduğundan $|C|$ tane kürenin her biri B_t tane vektör içerir ve V uzayındaki toplam vektör sayısı q^{mn} tanedir.

Lemma 4.4 Eğer C mükemmel kod ise $|C| = q^{mk} (k \in N)$ [31].

İspat: C, t- hata – düzelten – kod olsun.

$$|C|\left(1+\frac{q^n-1}{q-1}\left(q^m-1\right)+\frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)}\left(q^m-1\right)\left(q^m-q\right)+\cdots\right.$$
$$\left.+\frac{(q^n-1)...(q^n-q^{t-1})}{(q^t-1)...(q^t-q^{t-1})}\left(q^m-1\right)...\left(q^m-q^{t-1}\right)\right) \qquad (4.14)$$
$$= q^{mn}.$$

$q = p^e$ ve p asal olsun. (4.14) eşitliği, $1 \le s \le emn$ olan bazı pozitif tamsayı s'ler için $|C| = p^s$ sağlar. Bu nedenle,

$$1+\frac{q^n-1}{q-1}\left(q^m-1\right)+\frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)}\left(q^m-1\right)\left(q^m-q\right)$$
$$+\frac{(q^n-1)...(q^n-q^{t-1})}{(q^t-1)...(q^t-q^{t-1})}\left(q^m-1\right)...\left(q^m-q^{t-1}\right)$$
$$= p^{emn-s}$$

veya

$$\left(p^{em}-1\right)\left(\frac{q^n-1}{q-1}+\frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)}\left(q^m-q\right)\right.$$
$$\left.+\frac{(q^n-1)...(q^n-q^{t-1})}{(q^t-1)...(q^t-q^{t-1})}\left(q^m-q\right)...\left(q^m-q^{t-1}\right)\right)$$
$$= p^{emn-s}-1$$

olur. Böylece $p^{emn-s}-1$, $p^{em}-1$ tarafından bölünebilir. Buradan em, $emn-s$'nin bölenidir. Yani $s = emk$.

Teorem 4.5 1- hata – düzelten mükemmel kod yoktur [31].

İspat: C, 1- hata – düzelten mükemmel kod olsun. O halde

$$|C|\cdot\left(1+\frac{q^n-1}{q-1}\left(q^m-1\right)\right)=q^{mn}.$$

Lemma (4.4)'ten

$$1+\frac{q^n-1}{q-1}\cdot\left(q^m-1\right)=q^{mr}$$

veya

$$(q^m-1)(q^{n-1}+...+q+1)=q^{mr}-1. \tag{4.15}$$

Burada $r=n-\log_{q^m}|C|$ tamsayıdır. Eğer $r=1$ ise (4.15)'e göre ya $q^m-1=0$ yada $q^{n-1}+...+q+1=1$ olmalıdır. Yani $m=0$ veya $n=1$. Bu $3=2t+1\le d\le m,n$ sağlayan 1- hata – düzelten kod için imkânsızdır.

Eğer $r\ge 2$ ise (4.15)'ten

$$q^{n-1}+q^{n-2}+...+q+1=(q^m)^{r-1}+...+q^m+1,$$

Böylece $m=0$, $n=r$ olur. Bu ise C 'nin 1- hata – düzelten kod olmasıyla çelişir.

Lemma 4.6 $t\ge 1$ için aşağıdaki eşitlik sağlanır [31]:

$$1+\sum_{i=0}^{t}\begin{bmatrix} n \\ i \end{bmatrix}(q^m-1)...(q^m-q^{i-1})<q^{t(m+n)}.$$

İspat: $t=1$ için açıktır. $t\ge 2$ olsun. Herhangi bir $t\ge i\ge 2$ için

$$\frac{(q^n-1)...(q^n-q^{i-1})}{(q^i-1)...(q^i-q^{i-1})}(q^m-1)...(q^m-q^{i-1})<q^{i(m+n)}\frac{1}{(q^i-q^{i-1})^i}\le q^{i(m+n)-i^2+i}.$$

Bu nedenle,

$$1+\sum_{i=1}^{t}\frac{(q^n-1)...(q^n-q^{i-1})}{(q^i-1)...(q^i-q^{i-1})}(q^m-1)...(q^m-q^{i-1})<q^{m+n}+\sum_{i=2}^{t}q^{i(m+n)-i^2+i}<q^{t(m+n)}.$$

Teorem 4.7 V_j'ler $GF(q)$ üzerinde m- boyutlu vektör uzayları olmak üzere $V=V_1\times V_2\times...\times V_n$'de $n\le m$ uzunluğunda trivial olmayan hata – düzelten mükemmel kod yoktur [31].

İspat: $2t \le d-1 \le n - \log_{q^m} |C|$, minimum uzaklığı d olan herhangi bir C kodu için sağlanır. Böylece Lemma 4.6'dan

$$|C|\left(1+\sum_{i=0}^{t}\begin{bmatrix} n \\ i \end{bmatrix}(q^m-1)...(q^m-q^{i-1})\right) < |C|q^{2tm} \le |C|q^{(n-\log_{q^m}|C|)m} \le q^{mn}.$$

Bu eşitlik, $t \ge 1$ olan mükemmel kod olmadığını gösterir.

4.7 Gilbert – Varshamov Sınırı

Önerme 4.8 m, n, M ve d pozitif tamsayılar olsunlar. Eğer

$$M \times B_{d-1} < q^{mn}.$$

(4.16)

ise $GF(q^m)$ üzerinde tanımlı bir $(n, M+1, d)$ kod vardır [26].

İspat: n, d, M tamsayıları için (4.16) eşitliği sağlansın. İlk olarak verilen parametrelerle bir kod inşa edilsin: $c \in GF(q^m)^n$ keyfi kodu seçilsin. $M \ge 1$ olduğu için (4.16) eşitliğinden

$$GF(q^m)^n \setminus B(c, d-1) \ne \varnothing$$

olur. Böylece en azından bir tane $d \in GF(q^m)^n \setminus B(c, d-1)$ vardır. c ve d 'den oluşan kod ele alınsın. Bu kodda minimum rank uzaklığı en az d 'dir.

$M' \le M$ olmak üzere inşa edilen C kodu (n, M', d) kod olsun. Kodsözlerin çevresindeki $d-1$ yarıçaplı yuvarların birleşiminden oluşan küme ele alınsın. Yani,

$$V = \bigcup_{c \in C} B(c, d-1).$$

Bu küme $|V| \le M \times B_{d-1}$ sağlar. (4.16) eşitliğinden $a \in GF(q^m)^n \setminus V$ vardır. Böylece $C' = C \cup \{a\}$ bir $(n, M'+1, d)$ koddur.

Tanım 4.7 Eğer bir (n, M, d) kodu aşağıdaki sınırı sağlıyorsa **GV üzerindedir** denir [26]:

$$(M-1) \times B_{d-1} < q^{mn} \le M \times B_{d-1}. \qquad (4.17)$$

BÖLÜM 5

SONUÇ VE ÖNERİLER

Kodlama teorisi anlatılarak kodlar üzerindeki sınırlar incelenmiş ve bu sınırlar rank metriğine uygulanmıştır. Rank metriği üzerinde tanımlı kodların yapısı incelenmiş ve MRD kodların inşası anlatılmıştır. Hamming metrikte mükemmel kod olmasına karşılık rank metrikte mükemmel kod olmadığı ispatlanmıştır.

Rank metrik için özellikler ve ilgili problemler, Hamming metrik özellikleri kadar derinlemesine keşfedilmemiştir. Örneğin, bir lineer kodun minimum rank uzaklığı ile dualinin minimum rank uzaklığı arasındaki bağlantıyı kuracak MacWilliams dönüşüm eşitliği çözülmeyi bekleyen bir problemdir.

KAYNAKLAR

[1] Ling, S. ve Xing, C., (2004). Coding Theory, A First Course, Cambridge University Press, New York.

[2] Wan, Z.X., (2003). Lectures on Finite Fields and Galois Rings, World Scientific Publishing Co. Pte. Ltd., Singapore.

[3] Justesen, J. ve Høholdt, T., (2004). A Course In Error – Correcting Codes, European Mathematical Society, İsviçre.

[4] Roth, R.M., (2006). Introduction to Coding Theory, Cambridge University Press, New York.

[5] Neubauer, A., Freudenberger, J. ve Kühn, V., (2007). Coding Theory, Algorithms, Architectures, and Applications, John Wiley & Sons, Ltd, İngiltere.

[6] Blahut, R. E., (2003). Algebraic Codes for Data Transmission, Cambridge University Press, New York.

[7] Roman, S., (1997). Introduction to Coding Theory and Information Theory, Springer – Verlag, New York.

[8] Huffman, W. C. ve Pless, V., (2003). Fundamentals of Error – Correcting Codes, Cambridge University Press, New York.

[9] Kschischang, F., (2007). Error – Control Codes : Syndrome Decoding, http://www.comm.utoronto.ca/frank/ece1501/protected/index.html, 01 Mart 2012.

[10] Peterson, W. W. ve Weldon, E. J., (1996). Error – Correcting Codes, Second Edition, The Mit Press, İngiltere.

[11] Loidreau, P., (2006). Proporties of Codes in Rank Metric, http://arxiv.org/pdf/cs.DM/0610057/ , 10 Haziran 2010.

[12] Sanders, G., (2004). Perfect Codes, http://courses.csusm.edu/math540ak/codes.pdf, 19 Nisan 2012.

[13] Walker, J. L., (1991). Codes and Curves, Mathematics Subject Classification, ABD.

[14] Ourivski, A. V., Gabidulin, E. M., Honary B., ve Ammar B, (2003). "Reducible rank codes and their applications to cryptography." IEEE Transactions on Information Theory, 49(12):3289-3293.

[15] Gadouleau E. ve Yan Z., (2006). "Properties of codes with the rank metric", Proc. IEEE Globecom 2006, San Francisco.

[16] Delsarte, P., (1978). "Bilinear forms over a finite field, with applications to coding theory", Journal of Combinatorial Theory A, 25: 226–241.

[17] Roth, R. M., (1991). "Maximum-rank array codes and their application to crisscross error correction", IEEE Trans. Info. Theory, 37(2):328–336.

[18] Gabidulin, E. M., (1985). "Optimal codes correcting lattice-pattern errors", Problems on Information Transmission, 21(2):3–11.

[19] Kshevetskiy, A. ve Gabidulin, E. M., (2005). "The new construction of rank codes", Proceedings of IEEE International Symposium on Information Theory 2005: 2105–2108.

[20] Gabidulin, E. M. ve Loidreau, P. (2005). "On subcodes of codes in rank metric", Proceedings of IEEE International Symposium on Information Theory, 121-123, Adelaide, Australia.

[21] Gabidulin, E. M. ve Loidreau, P., (2008). Properties of subspace subcodes of optimum codes in rank metric, http://arxiv.org/pdf/cs.IT/0607108, 10 Haziran 2010.

[22] Loidreau, P., (2005). "A Welch-Berlekamp like algorithm for decoding Gabidulin codes", WWC, 36-45.

[23] Richter, G. ve Plass, S., (2004). "Fast decoding of rank-codes with rank errors and column erasures", Proceedings of IEEE ISIT 2004.

[24] Roth, R. M., (1997). "Probabilistic crisscross error correction", IEEE Trans. Info Theory, 43(5):1425–1438.

[25] Gadouleau E. ve Yan Z., (2006). "Decoder error probability of MRD codes", Proceedings of IEEE International Theory Workshop, 264–268.

[26] Gadouleau E. ve Yan Z., (2006). "Error performance analysis of maximum rank distance codes", Submitted to IEEE Transactions on Information Theory, http://arxiv.org/pdf/cs.IT/0612051.

[27] Sripati, U. ve Sundar R. B., (2003) "On the rank distance of cyclic codes," Proc. IEEE Int. Symp. on Information Theory, 72.

[28] Vasantha, W. B. ve Suresh B. N., (1999). "On the covering radius of rankdistance codes", Ganita Sandesh, 13:43–48.

[29] Gabidulin, E. M. ve Pilipchuk N. I., (2005). "Symmetric matrices and codes correcting rank errors beyond the $\lfloor (d-1)/2 \rfloor$ bound", Discrete Applied Mathematics 154:305-312.

[30] Plass, S., Richter, G., ve Vinck, A.J.H., (2008). "Coding Schemes for Crisscross Error Patterns", Wireless Personal Communications, 47(1).

[31] Chen, K., (1996). "On the Non-Existence of Perfect Codes with Rank Distance", Mathematische Nachrichten, 182(1):89-98.

[32] Manoj, K. N. ve Rajan, B. S., (2002) "Full Rank Distance codes", IISc, Bangalore.

[33] Gabidulin, E. M., (1985). “Theory of codes with maximum rank distance” Problems on Information Transmission, 21(1):1–12.

[34] Kshevetskiy, A. ve Gabidulin, E. M., (2005), “The New Construction of Rank Codes”, Proceedings of IEEE International Symposium on Information Theory (ISIT) 2005, 2105–2108.

[35] Lusina, P., (2003). “Maximum Rank Distance Codes as Space – Time Codes”, IEEE Trans. Inf. Theory, 49(10):2757–2760.

[36] Gadouleau, M. ve Yan, Z., (2010). “Packing and Covering Properties of Rank Metric Codes”, IEEE Transactions on Information Theory 56(5): 2097-2108.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : İlhami KALKAN

Doğum Tarihi ve Yeri : 10.08.1985 BURSA

Yabancı Dili : İngilizce

E-posta : ilhami1985@hotmail.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Y. Lisans	Matematik	Yıldız Teknik Üniversitesi	2012
Lisans	Matematik	Yıldız Teknik Üniversitesi	2009
Lise	Fen Bilimleri	Yıldız Tekstil Lisesi	2003

İŞ TECRÜBESİ

Yıl	**Firma/Kurum**	**Görevi**
2012-devam	Inforcept	Java Developer
2011-2012	Kafein	Danışman
2011	Profect Business Academy	Java Developer

Proje

1. Kurumsal Java (Java EE) ile İK Uygulama Geliştirme, 01.08.2011 -01.11 2011, Profect Business Academy.