TC İSTANBUL KÜLTÜR ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SİMETRİK DİZAYNLAR, KODLAR VE SIR PAYLAŞIM ŞEMALARI ÜZERİNE BİR ÇALIŞMA

DOKTORA TEZİ

Selda ÇALKAVUR

Anabilim Dalı : Matematik-Bilgisayar

Programı : Matematik

Tez Danışmanı : Prof. Dr. Erol BALKANAY

TEMMUZ 2010

TC İSTANBUL KÜLTÜR ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SİMETRİK DİZAYNLAR, KODLAR VE SIR PAYLAŞIM ŞEMALARI ÜZERİNE BİR ÇALIŞMA

DOKTORA TEZİ

Selda ÇALKAVUR

(0609241007)

Tezin Enstitüye Verildiği Tarih : 2 2 H a z i r a n 2 0 1 0
Tezin Savunulduğu Tarih : 1 6 T e m m u z 2 0 1 0

Tez Danışmanı: Prof. Dr. Erol BALKANAY

Diğer Jüri Üyeleri:

Prof. Dr. Haluk ORAL (Boğaziçi Üniversitesi)
Prof. Dr. A. Göksel AĞARGÜN (Yıldız Teknik Üniversitesi)
Doç. Dr. Neşe YELKENKAYA
Yrd. Doç. Dr. Ayten KOÇ

TEMMUZ 2010

ÖNSÖZ

İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü'ne bağlı Matematik-Bilgisayar Ana Bilim Dalı, Matematik Doktora programının son aşaması olan tez çalışmamda dizaynlar, simetrik dizaynlar, simetrik dizaynların kodları ve ilgili sır paylaşım şemaları arasındaki bazı ilişkiler araştırılmıştır.

Yüksek lisans eğitimimde olduğu gibi, doktora eğitimim boyunca da bilgisiyle, tecrübesiyle, iyi niyetiyle, sabrıyla tüm çalışmalarıma yön veren, manevi desteğini esirgemeyen, saygıdeğer hocam Sayın Prof. Dr. Erol BALKANAY'a teşekkürü büyük bir borç bilir, kendisine saygılarımı sunarım.

Ayrıca bu uzun yolculukta çalışmalarıma hep olumlu katkı sağlayan sevgili annem Ayşe ÇALKAVUR'a, yaşantımın her aşamasında kendisini örnek aldığım sevgili babam Yusuf ÇALKAVUR'a ve bütün aileme sonsuz teşekkürlerimi sunuyorum.

Temmuz 2010 Selda ÇALKAVUR

İÇİNDEKİLER

SİMGE LİSTESİ

$(v, b, r, k, \lambda)-$dizayn	: $(v, b, r, k, \lambda)-$ parametreli dizayn
J	: tüm elemanları 1 olan uygun boyutlu bir matris
$A=[a_{ij}]$	: $(v, k, \lambda)-$parametreli simetrik dizaynın çakışım matrisi
$n=k-\lambda$	: $(v, k, \lambda)-$parametreli simetrik dizaynın mertebesi
D^c	: $(v, k, \lambda)-$parametreli simetrik dizayn D nin tümleyeni
F_q veya $GF(q)$	: Mertebesi $q=p^r$ (p asal, r pozitif tam sayı) olan Galois cismi
$(F_q)^n$	: tüm $a=a_1a_2...a_n$, $(a_i \in F_q)$ sıralı $n-$lilerinin kümesi
$d(x, y)$	: x ve y vektörleri arasındaki Hamming uzaklığı
C	: C kodu
$d(C)$	: C kodunun minimum uzaklığı
$wt(x)$	: $(F_q)^n$ deki bir x vektörünün ağırlığı
$(n, M, d)-$kod	: n uzunluklu, M kodsözcüğü içeren ve minimum uzaklığı d olan kod
$A_q(n, d)$	: C kodundaki en büyük M değeri
$S(u, r)$	: u merkezli, r yarıçaplı küre
$[n, k, d]-$kod	: uzunluğu n, boyutu k ve minimum uzaklığı d olan kod
$C^{\perp}$	: C kodunun duali olan kod
G	: C kodunun üreteç matrisi

H	: $C^{\perp}$ dual kodunun üreteç matrisi
$S^{\perp}$	: V bir iç çarpım uzayı ve $S \subset V$ iken, S nin ortogonal tümleyeni
ψ	: $(F_p)^m$ üzerinde bir simetrik bilineer form veya skaler çarpım
C^{ψ}	: ψ ye göre C kodunun duali
$C^{gen.}$	: $(v, k, \lambda)-$parametreli simetrik dizaynın genişletilmiş F_p-kodu
B	: $(v, k, \lambda)-$parametreli simetrik dizaynın genişletilmiş F_p-kodu $C^{gen.}$ nin çakışım matrisi
s	: Sır paylaşım şemasındaki sır
$w_{\min}$	: F_q üzerinde bir $[n, k]-$kod C deki sıfırdan farklı minimum ağırlık
w_{maks}	: F_q üzerinde bir $[n, k]-$kod C deki maksimum ağırlık
χ	: F_q nun toplamsal kanonik karakteri
$Tr(ax) \quad (a \in F_q)$	: F_q dan F_p ye lineer bir fonksiyon
S_{α}	: c_{α} kodsözcüğünün sıfır olan bileşenlerinin sayısı
$T_{\alpha,\beta}$	: c_{α}, c_{β} kodsözcüklerinin ortaklaşa sıfır olan bileşenlerinin sayısı
F_q^*	: F_q cisminin sıfırdan farklı elemanlarının çarpım grubu
$[v, r]-$kod	: $(v, k, \lambda)-$parametreli D simetrik dizaynın ürettiği, uzunluğu v, boyutu r olan kod

C^c	: $(v,\ k,\ \lambda)-$parametreli simetrik dizaynın tümleyeni olan $(v,\ v-k,\ v-2k+\lambda)-$parametreli D^c nin kodu
boyC	: C kodunun boyutu

Enstitüsü : Fen Bilimleri
Dalı : Matematik - Bilgisayar
Programı : Matematik
Tez Danışmanı : Prof. Dr. Erol BALKANAY
Tez Türü ve Tarihi : Doktora – Temmuz 2010

ÖZET

SİMETRİK DİZAYNLAR, KODLAR VE SIR PAYLAŞIM ŞEMALARI ÜZERİNE BİR ÇALIŞMA

Selda ÇALKAVUR

Bu tez çalışmasının konusu, simetrik dizaynın kodu ile ilgili sır paylaşım şemaları arasındaki ilişkiyi araştırmaktır.

Tezin ilk bölümünde; $(v, b, r, k, \lambda)-$ dizayn, $(v, k, \lambda)-$ simetrik dizayn ve $t-(v, k, \lambda)-$dizayn kavramları incelenmiştir.

İkinci bölümde lineer kodlar anlatılmıştır. Bu kapsamda; Hamming uzaklığı, minimum uzaklık, Hamming ağırlığı, dual kod ve eşlik-denetim matrisi kavramları açıklanmıştır. Ayrıca bir dizaynın kodu, bir simetrik dizaynın kodu ve bir simetrik dizaynın genişletilmiş kodu verilmiştir.

Üçüncü bölüm, sır paylaşım problemine ayrılmıştır. "Sır paylaşımı" kavramı açıklanmış ve Massey'in sır paylaşım şeması anlatılmıştır. Ayrıca minimal erişim kümesi kavramı verilmiş ve dual kodlar üzerine kurulan sır paylaşım şemalarının erişim yapıları incelenmiştir. Minimal kodsözcükleri incelenmiş ve sır paylaşımının demokratiklik derecesi açıklanmıştır.

Dördüncü bölümde, simetrik dizaynın kodundan, sır paylaşım şemalarına geçiş araştırılmıştır. Simetrik dizaynın kodu üzerinde kurulan sır paylaşım şemasındaki minimal erişim küme sayısı hesaplanmıştır. Ayrıca $(v, k, \lambda)-$simetrik dizaynın ikili C kodunun dualindeki kodsözcükleri için $w_{maks} < \frac{2(k+\lambda)}{\lambda}$ ise $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcüklerinin minimal olduğu gösterilmiştir.

Anahtar Sözcükler: Dizayn, simetrik dizayn, $t-$dizayn, lineer kod, genişletilmiş kod, sır paylaşımı, sır paylaşım şeması, sır paylaşımının demokratiklik derecesi, minimal erişim kümesi, minimal kodsözcüğü.

Bilim Dalı Sayısal Kodu: 0924

University : İstanbul Kültür University
Institute : Institute of Science
Science Programme : Mathematics and Computer
Programme : Mathematics
Supervisor : Prof. Dr. Erol BALKANAY
Degree Awarded and Date : Ph. D. July 2010

ABSTRACT

SYMMETRIC DESIGNS, CODES AND A STUDY ON SECRET SHARING SCHEMES

Selda ÇALKAVUR

The subject of this thesis is to investigate the relationship between the associated secret sharing scheme and the code of a symmetric design.

In the first chapter of the thesis, $(v, b, r, k, \lambda)-$ design, $(v, k, \lambda)-$ symmetric design and $t-(v, k, \lambda)-$design concepts are examined.

In the second chapter, linear codes are explained. Within this context the concepts of Hamming distance, minimum distance, Hamming weight, dual code and parity-check matrix are given. Furthermore, the code of a design, the code of a symmetric design and the extended code of a symmetric design are explained.

Third chapter is allocated to the secret sharing problem. The secret sharing concept is explained and Massey's secret sharing scheme is described. Furthermore, minimal access set concept is given, the access structures of secret sharing schemes that are based on dual codes are explained. Minimal codewords are discussed and the degree of democratic of the secret sharing is explained.

In the fourth chapter, the transition from the code of symmetric design to secret sharing schemes are investigated. We have presented the number of minimal access sets in the secret sharing scheme that constructed over the code of symmetric designs. We also show that if $w_{maks} < \frac{2(k+\lambda)}{\lambda}$ for the dual code $C^{\perp}$ of the code C of $(v, k, \lambda)-$symmetric design then all of the codewords of $C^{\perp}$ are minimal.

Key Words: Design, symmetric design, $t-$design, linear code, extended code, secret sharing, secret sharing scheme, democratic of degree of secret sharing, minimal access set, minimal codeword.

Science Code: 0924

BÖLÜM 1

DİZAYNLAR

1.1. Dizayn ve (v, k, λ) – Parametreli Simetrik Dizayn

Tanım 1.1.1. v elemanlı bir D kümesi verilsin. D nin, her biri k elemanlı b tane alt kümesi göz önüne alınsın. Bu alt kümelere bloklar denilsin. Buna göre, D nin her bir noktası, tam r tane blokta; her nokta ikilisi de (birlikte) tam λ blokta bulunsun. Bu şekilde oluşan yapı, (v, b, r, k, λ) – parametreli dizayn adını alır. Kısaca (v, b, r, k, λ) – dizayn olarak gösterilebilir.

Şu halde, (v, b, r, k, λ) – parametreli dizaynda, noktalar kümesi ve bloklar kümesi denilen iki küme vardır. Noktalar kümesi **P**, bloklar kümesi **B** ve dizaynın kendisi **D** ile gösterilsin. Bloklar kümesi

$$\mathbf{B}=\{y_1, y_2, \cdots, y_b\}$$

olmak üzere,

$$a_{ij} = \begin{cases} 1; & x_i \in y_j \\ 0; & x_i \notin y_j \end{cases}$$

şeklinde tanımlanan $A=[a_{ij}]$ matrisine, dizaynın çakışım matrisi denir. Doğal olarak A, bir $v \times b$ matristir.

(v, b, r, k, λ) – parametreli dizayn olan **D** nin çakışım matrisi A, elemanlarının tümü 1 olan uygun boyutlu matris J olmak üzere,

$$\begin{cases} AA^T = (r-\lambda)I_v + \lambda J_{v,v} \\ AJ_{b,v} = rJ_{v,v} \\ J_{b,v}A = kJ_{b,b} \end{cases} \qquad (1.1.1.1.)$$

eşitliklerinin varlığı, dizayn tanımı kullanılarak kolaylıkla gösterilebilir.

Eğer (v, b, r, k, λ) – parametreli dizayn **D** ise parametreler arasında

- $vr = bk$
- $(v-1)\lambda = r(k-1)$. ([12])

bağıntıları vardır. Bunların ispatlanması oldukça kolaydır.

Örneğin,

$vr = bk$

olduğunu göstermek için, saymanın temel ilkeleri kullanılabilir:

Her bir nokta r tane blokta bulunduğundan (v nokta var), dizaynın oluşmasında kullanılan noktalar kolleksiyonundaki nokta sayısı vr olur. Diğer yandan, her biri k elemanlı b tane blok vardı. Bu durumda nokta sayısı (dizayn kurulurken kullanılan), bk olur.

Sonuçta,

$$vr = bk \qquad (1.1.1.2.)$$

elde edilir.

Bu kez,

$$(v-1)\lambda = r(k-1)$$

olduğu ispatlansın:

v elemandan,

$$\binom{v}{2} = \frac{v(v-1)}{2}$$

tane farklı ikili seçilebilir. Her seçilen ikili, λ blokta bulunur. Bu durumda, tüm bloklarda bulunan nokta ikilileri sayısı,

$$\frac{v(v-1)}{2}\lambda$$

olur.

Bir blok k elemanlıdır. O halde bir bloktaki noktalardan,

$$\binom{k}{2} = \frac{k(k-1)}{2}$$

tane nokta ikilisi seçilebilir. b tane blok vardı. Tüm bloklarda bulunan nokta ikilileri sayısı,

$$b\frac{k(k-1)}{2} = v\frac{r(k-1)}{2}$$

dir. Buradan,

$$\frac{v(v-1)}{2}\lambda = \frac{vr(k-1)}{2}$$

olup,

$$(v-1)\lambda = r(k-1) \qquad (1.1.1.3.)$$

bulunur. □

Hemen belirtilmelidir ki;

$vr = bk$,

$(v-1)\lambda = r(k-1)$

eşitliklerini sağlayan (v, b, r, k, λ) parametreleri için, **D** dizaynı var olmayabilir. □

Eğer (v, b, r, k, λ) – parametreli dizaynda, nokta sayısı blok sayısına eşitse, yani

$v = b$

ise,

$vr = bk$

eşitliğinden,

$k = r$

elde edilir. Bu durumda oluşan dizayn, (v, k, λ) – parametreli simetrik dizayn adını alır.

O zaman (v, k, λ) – parametreli simetrik dizaynın parametreleri arasında,

$$(v-1)\lambda = k(k-1) \qquad (1.1.1.4.)$$

eşitliği vardır. ([15])

(1.1.1.4.)'ten,

$$k^2 - v\lambda = k - \lambda \qquad (1.1.1.5.)$$

$$(v-k)\lambda = (k-1)(k-\lambda) \qquad (1.1.1.6.)$$

eşitlikleri de yazılabilir. ([15])

(1.1.1.5.) ve (1.1.1.6.)'da karşılaşılan $k - \lambda$ değeri, "n" ile gösterilir ve **D** nin mertebesi adını alır. ([15]) □

I birim matris ve tüm elemanları 1 olan uygun boyutlu bir kare matris J olmak üzere (1.1.1.1.)'deki eşitlikler,

$$\begin{cases} AJ = JA = kJ \\ AA^T = A^T A = (k-\lambda)I + \lambda J = nI + \lambda J \end{cases} \qquad (1.1.1.7.)$$

haline gelir. ([15])

Önerme 1.1.1. $(v,\ k,\ \lambda)-$parametreli simetrik dizaynın çakışım matrisi A olmak üzere,

$$\det A = kn^{\frac{1}{2}(v-1)}$$

dir. ([15])

İspat. (1.1.1.7.)'den,

$$AA^T = nI + \lambda J$$

idi. Buradan,

$$\det(AA^T) = \det A \det A^T$$

yazılır.

$$\det A = \det A^T$$

olduğundan,

$$\det (AA^T) = (\det A)^2$$

elde edilir.

Sonuçta,

$$\det (nI + \lambda J) = (\det A)^2$$

dir.

$$\det (nI + \lambda J) = \begin{vmatrix} n+\lambda & \lambda & \lambda & \cdots & \lambda \\ \lambda & n+\lambda & \lambda & \cdots & \lambda \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \lambda & \lambda & \lambda & \cdots & n+\lambda \end{vmatrix}$$

$$\det (nI + \lambda J) = \begin{vmatrix} n+v\lambda & \lambda & \lambda & \cdots & \lambda \\ n+v\lambda & n+\lambda & \lambda & \cdots & \lambda \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ n+v\lambda & \lambda & \lambda & \cdots & n+\lambda \end{vmatrix}$$

$$\det (nI + \lambda J) = (n+v\lambda) \begin{vmatrix} 1 & \lambda & \lambda & \cdots & \lambda \\ 1 & n+\lambda & \lambda & \cdots & \lambda \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \lambda & \lambda & \cdots & n+\lambda \end{vmatrix}$$

$$\det (nI + \lambda J) = (n+v\lambda) \begin{vmatrix} 1 & \lambda & \lambda & \cdots & \lambda \\ 0 & n & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & n \end{vmatrix}$$

$$\det(nI+\lambda J)=(n+v\lambda)\begin{vmatrix} n & 0 & \cdots & 0 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & n \end{vmatrix}$$

$$\det(nI+\lambda J)=(n+v\lambda)n^{v-1}$$

$$\det(nI+\lambda J)=(k-\lambda+v\lambda)n^{v-1}$$

$$\det(nI+\lambda J)=(k+\underbrace{(v-1)\lambda}_{=k(k-1)})n^{v-1}$$

$$\det(nI+\lambda J)=(k+k(k-1))n^{v-1}$$

$$\det(nI+\lambda J)=k^2n^{v-1}$$

bulunur.

$$\det(nI+\lambda J)=(\det A)^2$$

idi. Buradan,

$$(\det A)^2=k^2n^{v-1}$$

$$|\det A|=kn^{\frac{1}{2}(v-1)}$$

elde edilir.

Teorem 1.1.1. (Schutzenberger) $(v,\ k,\ \lambda)-$parametreli simetrik dizaynın var olduğu kabul edilsin. v çift ise n, bir tam kare olmalıdır. ([15])

İspat. $(v,\ k,\ \lambda)-$parametreli simetrik dizayn ele alınsın. Bu simetrik dizaynın çakışım matrisi A olmak üzere, Önerme 1.1.1. gereğince,

$$\det A=kn^{\frac{1}{2}(v-1)}$$

idi. Şimdi, v nin çift olduğu kabul edilsin. Bu durumda $v-1$, bir tek sayı olacaktır. Bu ise $2 \nmid v-1$ olması demektir. $\det A$, bir tam sayı olduğundan, $kn^{\frac{1}{2}(v-1)}$ ifadesinin tam sayı olması için, n'nin bir tam kare olması gerekir.

Böylece ispat tamamlanmış olur.

Not. Bir p noktası için $p \in B$ ise p noktası, B bloğu ile çakışım durumundadır denebilir.

Örnek 1.1.1. $(v, k, \lambda)-$parametreli D simetrik dizaynında çakışım ilişkisinin tümleyeni alınarak (çakışım yerine çakışmama durumunu alarak), D^c ile belirtilen D nin tümleyeni elde edilir. D^c;

$$v' = v, \quad k' = v-k, \quad \lambda' = v-2k+\lambda$$

olmak üzere $(v', k', \lambda')-$parametreli simetrik dizayndır.

D ve D^c nin her ikisinin de mertebesi,

$$n = k-\lambda = k'-\lambda' = n'$$

dir.

$$(v-1)\lambda = k(k-1)$$

eşitliğinden,

$$\lambda\lambda' = n(n-1)$$

olduğu hemen görülür. ([15])

1.2. $t-$Dizayn

Tanım 1.2.1. v noktalı (elemanlı) bir D kümesi ve D nin, her biri k elemanlı alt kümelerinin bir topluluğu ele alınsın. Bu k elemanlı alt kümelere (önceden olduğu gibi) bloklar denilsin. D nin her bir t elemanlı alt kümesi, tam λ tane blokta bulunuyorsa bu yapı, $t-(v, k, \lambda)-$dizayn adını alır. ([16])

BÖLÜM 2

LİNEER KODLAR

2.1. Temel Kavramlar

İkili (binary) bir kod, kodsözcükleri olarak adlandırılan 0 ve 1'lerden oluşan sıralı dizilerin bir kümesidir. 0 ve 1 sembollerinin n defa tekrarlanması ile oluşan $\{00\ldots0, 11\ldots1\}$ koduna, n uzunluklu ikili tekrarlı kod denir.

Daha genel olarak $q-$lu bir kod, semboller q farklı elemanın bir $F_q = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ kümesinden seçilmek üzere, semboller dizisinin bir alt kümesidir. F_q kümesine alfabe denir. Eğer q bir asal sayının kuvveti şeklinde ($q = p^r$, p asal ve r pozitif tam sayı) ise F_q alfabesi, mertebesi q olan sonlu cisim olarak alınır. $q = 2$ için kodlara ikili (binary) kodlar, $q = 3$ için üçlü (ternary) kodlar denir.

Her biri aynı uzunlukta kodsözcüklerinden oluşan bir kod, blok kod adını alır. Kod denince, blok kod anlaşılır.

$(F_q)^n$, tüm $a = a_1a_2...a_n$, $(a_i \in F_q)$ sıralı $n-$lilerinin kümesini gösterir. $(F_q)^n$ in elemanlarına vektör denir. $(F_q)^n$ in mertebesi q^n dir. Uzunluğu n olan $q-$lu bir kod, $(F_q)^n$ in bir alt kümesidir.

Tanım 2.1.1. (Hamming Uzaklığı) $(F_q)^n$ in x ve y vektörleri arasındaki Hamming uzaklığı, x ve y nin karşılıklı olarak birbirinden farklı konumlarının sayısıdır ve "$d(x, y)$" ile gösterilir. ([12])

Hamming uzaklığı, bir metriktir ve

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

ii) Her $x,\ y \in (F_q)^n$ için $d(x, y) = d(y, x)$

iii) Her $x,\ y,\ z \in (F_q)^n$ için $d(x, y) \leq d(x, z) + d(y, z)$

koşullarını gerçekler. (

Tanım 2.1.2. (Minimum Uzaklık) Bir C kodu için önemli bir parametre minimum uzaklık olup, farklı kodsözcükleri arasındaki uzaklıkların en küçüğü olarak tanımlanır ve "$d(C)$" ile gösterilir.

$d(C) = \min\{d(x, y) \mid x,\ y \in C,\ x \neq y\}$. ([12]) □

F_2, $Z_2 = \{0, 1\}$ kümesi olarak alındığında, $(F_2)^n$ üzerinde aşağıdaki gibi ikili işlemler tanımlanır:

$x = (x_1,\ x_2, \ldots, x_n)$ ve $y = (y_1,\ y_2, \ldots, y_n)$, $(F_2)^n$ de iki vektör olmak üzere

$x + y$, $(F_2)^n$ de

$x + y = (x_1 + y_1,\ x_2 + y_2, \ldots, x_n + y_n)$

ile,

$x \cap y$ ise $(F_2)^n$ de

$x \cap y = (x_1 y_{1,}\ x_2 y_2, \ldots, x_n y_n)$

ile tanımlanan vektörlerdir. ($x \cap y$ yerine $x * y$ de yazılabilir.) $x_i + y_i$ ve $x_i y_i$ terimleri mod 2'ye göre hesaplanır. ([12])

Tanım 2.1.3. $(F_2)^n$ deki bir x vektörünün ağırlığı, x teki 1 lerin sayısıdır ve "$wt(x)$" ile gösterilir. ([12])

Yardımcı Teorem 2.1.1. $x, y \in (F_2)^n$ ise

$$d(x, y) = wt(x + y)$$

dir. ([12])

İspat. $x + y$ vektörü, x ve y nin farklı olduğu konumlarında 1 bileşenini, aynı olduğu konumlarında 0 bileşenini içerir. Böylece

$$d(x, y) = wt(x + y)$$

olur. ([12])

Yardımcı Teorem 2.1.2. $x, y \in (F_2)^n$ ise

$$d(x, y) = wt(x) + wt(y) - 2wt(x \cap y)$$

dir. ([12])

İspat. $d(x, y) = wt(x + y) = (x$ teki 1'lerin sayısı)+(y deki 1'lerin sayısı)-2(x ve y de 1 olan ortak konumların sayısı$) = wt(x) + wt(y) - 2wt(x \cap y)$. ([12]) □

Bir $(n, M, d)-$kod denince, n uzunluklu, M kodsözcüğü içeren ve minimum uzaklığı d olan bir kod anlaşılır.

İyi bir $(n, M, d)-$kod denince; n parametresi küçük (mesajların hızlı gönderilmesi için), M 'si büyük (mesajların geniş bir çeşitlilikte gönderilmesini sağlamak için) ve d 'si büyük (daha fazla hatayı düzeltmek için) bir kod anlaşılır. sahiptir. Kodlar teorisinin temel problemlerinden biri; n, M, d parametrelerinden birini, verilen diğer iki değer için optimize etmektir. Bu problemin genel hali, verilen

uzunluk ve minimum uzaklık için en büyük kodu bulmaktır. $q-$lu bir $(n,\ M,\ d)-$kod mevcut olmak üzere, "$A_q(n,d)$" ile en büyük M değeri gösterilir.

Tanım 2.1.4. $(F_q)^n$ kümesinde bir u vektörü ve bir $r \geq 0$ tam sayısı ele alınsın. u merkezli r yarıçaplı küre

$$S(u,\ r) = \{v \in (F_q)^n \mid d(u,v) \leq r\}$$

kümesi ile ifade edilir.

Yardımcı Teorem 2.1.3. r negatif olmayan tam sayısı ve $u \in (F_q)^n$ için

$$S(u,\ r) = \{v \in (F_q)^n \mid d(u,v) \leq r\}$$

kümesi r yarıçaplı küreyi ifade etmek üzere $r \leq n$ iken

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{r}(q-1)^r = \sum_{i=0}^{r}\binom{n}{i}(q-1)^i$$

sayısı, $S(u,\ r)$ nin $(F_q)^n$ deki eleman sayısını verir.

İspat. $v \in (F_q)^n$ olsun. $0 \leq m \leq r$ için $d(u,v) = m$ olan v vektörlerinin sayısını araştıralım. u vektöründen m tane farklı konuma sahip, $\binom{n}{m}$ tane v vektörü elde edilir. Ayrıca v nin her konumu $q-1$ farklı şekilde seçilebileceğinden bu sayı,

$$\binom{n}{m}(q-1)^m$$

dir. Öte yandan $0 \leq m \leq r$ olduğundan, $m = 0,\ 1, \cdots,\ r$ olabilir. Böylece $S(u,\ r)$ deki eleman sayısı,

$$\sum_{m=0}^{r}\binom{n}{m}(q-1)^m$$

olarak elde edilir. ([12])

Teorem 2.1.1. (Hamming Sınırı)

$q-$lu bir $(n,\ M,\ 2t+1)-$kod,

$$M\left\{\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{t}(q-1)^t\right\}\leq q^n \qquad (2.1.1.1.)$$

eşitsizliğini sağlar.

İspat. C, $q-$lu bir $(n,\ M,\ 2t+1)-$kod olsun. Farklı kodsözcüklerini merkez kabul eden t yarıçaplı herhangi iki küre ortak vektöre sahip değildir. Dolayısıyla M tane kodsözcüğünü merkez kabul eden t yarıçaplı M tane kürenin içerdiği vektör sayısı, (2.1.1.1.)'in sol tarafına eşittir. Bu sayı, $(F_q)^n$ uzayındaki tüm vektörlerin sayısına eşit ya da aynı sayıdan küçük olmalıdır.

Buradan,

$$M\leq\frac{q^n}{\left\{\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{t}(q-1)^t\right\}} \qquad (2.1.1.2.)$$

elde edilir.

Not. (2.1.1.1.) ifadesinde eşitlik durumu söz konusu olursa kod, mükemmel (yetkin) kod adını alır.

2.2. Lineer Kodlar

Lineer kodlar incelenirken F_q alfabesi, $GF(q)$ Galois cismi olarak alınır. (Burada $q,$ bir asal sayının kuvveti şeklindedir.) ([12]). $(F_q)^n$, F_q cismi üzerinde bir vektör uzayıdır.

$GF(q)$ üzerinde bir lineer kod, $(F_q)^n$ vektör uzayının bir alt uzayıdır.

Bu durumda $(F_q)^n$ vektör uzayının bir C alt kümesi ancak ve ancak

i) Her $u, v \in C$ için $u + v \in C$

ii) Her $u \in C,\ r \in GF(q)$ için $ru \in C$

koşullarını gerçekliyorsa, lineer bir koddur. ([12])

Sonuç olarak, ikili (binary) bir kod ancak ve ancak herhangi iki kodsözcüğünün toplamı yine bir kodsözcüğü ise lineerdir.

Tanım 2.2.1. $C,\ (F_q)^n$ vektör uzayının $k-$boyutlu bir alt uzayı ise bu lineer C koduna, bir $[n, k]-$kod denir. Eğer C nin, d minimum uzaklığını da belirtmek gerekirse bu kod, bir $[n, k, d]-$kod olarak adlandırılır. ([12])

Not.

i) $q-$lu bir $[n, k, d]-$kod, aynı zamanda bir $(n, q^k, d)-$koddur. Fakat her $(n, q^k, d)-$kod, bir $[n, k, d]-$kod değildir.

ii) Her lineer kod, 0 vektörünü içerir. ([12])

Tanım 2.2.2. (Hamming Ağırlığı) $(F_q)^n$ deki bir x vektörünün sıfırdan farklı sembollerinin sayısına, x in Hamming ağırlığı denir ve "$wt(x)$" ile gösterilir. x in ağırlığı denince, Hamming ağırlığı anlaşılacaktır.

Yardımcı Teorem 2.2.1. $x, y \in (F_q)^n$ olmak üzere,

$$d(x, y) = wt(x - y)$$

dir. ([12])

İspat. x ve y nin farklı olduğu konumlarında $x-y$ vektörü sıfırdan farklı semboller içerir. Bu durumda,

$$d(x,\ y) = wt(x-y)$$

olur. ([12])

Teorem 2.2.1. C lineer bir kod olsun. C nin sıfırdan farklı kodsözcüklerinden ağırlığı en küçük olanın ağırlığı $wt(C)$ olmak üzere,

$$d(C) = wt(C)$$

dir. ([12])

İspat. $d(C) = d(x,\ y)$ olacak şekilde C nin x ve y gibi kodsözcükleri vardır. $x-y,\ C$ lineer kodunun bir kodsözcüğü olduğundan, Yardımcı Teorem 2.2.1'e göre,

$$d(C) = wt(x-y) \geq wt(C) \qquad (2.2.1.1.)$$

dir.

Diğer taraftan $0 \in C$ olduğundan, C nin uygun bir x kodsözcüğü için,

$$wt(C) = wt(x) = d(x,\ 0) \geq d(C) \qquad (2.2.1.2.)$$

dir.

(2.2.1.1.) ve (2.2.1.2.)'den,

$$d(C) = wt(C)$$

elde edilir. ([12])

Tanım 2.2.3. Satırları, lineer bir $[n,\ k]-$kodun bir tabanını oluşturan $k \times n$ matrise, kodun bir üreteç matrisi denir. ([12])

2.2.1. Lineer Bir Kod İle Kodlama

C, üreteç matrisi G olmak üzere, $GF(q)$ üzerinde bir $[n, k]-$kod olsun. C, q^k kodsözcüğü içerir ve q^k farklı mesajdan herhangi birini iletmek için kullanılabilir. Bu mesajlar, $(F_q)^k$ vektör uzayının q^k tane sıralı $k-$lıları ile tanımlanır ve bir $u = u_1 u_2 ... u_k$ mesaj vektörü, G nin satırları $r_1, r_2, \ldots, r_k$ olmak üzere,

$$uG = \sum_{i=1}^{k} u_i r_i$$

şeklinde kodlanır. Bu durumda uG, C nin bir kodsözcüğü olur. Kodlama fonksiyonu,

$$\varphi : u \to uG$$

dir. φ fonksiyonu, $(F_q)^k$ vektör uzayını, $(F_q)^n$ in $k-$boyutlu bir alt uzayı (yani C kodu) üzerine resmeder.

G üreteç matrisi standart formda ise kodlama daha kolay yapılır:

$G = [I_k \mid A]$ ($A = [a_{ij}]$, bir $k \times (n-k)$ matristir.) olmak üzere, u mesaj vektörü

$$x = uG = x_1 x_2 ... x_k x_{k+1} ... x_n$$

şeklinde kodlanır. Burada

$x_i = u_i$, $\quad 1 \le i \le k$ (mesaj sembolleri)

ve

$$x_{k+i} = \sum_{j=1}^{k} a_{ji} u_j , \quad 1 \le i \le n-k \quad \text{(kontrol sembolleri)}$$

dir. ([12])

Örnek 2.2.1.1. İkili bir $[7, 4, 3]-$kod olan C kodunun üreteç matrisi standart forma dönüştürülsün.

$$G=\begin{bmatrix}1&1&1&1&1&1&1\\1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix}\xrightarrow[r_3\to r_3-r_1]{r_2\to r_2-r_1}\begin{bmatrix}1&1&1&1&1&1&1\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&1&1&0&0&0&1\end{bmatrix}\xrightarrow[r_4\to r_4-r_2]{r_1\to r_1-r_2}$$

$$\begin{bmatrix}1&0&0&0&1&0&1\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&0&0&1&0&1&1\end{bmatrix}\xrightarrow[r_3\to r_3-r_4]{r_2\to r_2-r_3}\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}=[I_4\mid A]$$

dır.

Buna göre bir (u_1, u_2, u_3, u_4) mesaj vektörü,

$$(u_1\ u_2\ u_3\ u_4)\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}=(u_1,\ u_2,\ u_3,\ u_4,\ u_1+u_2+u_3,\ u_2+u_3+u_4,$$

$$u_1+u_2+u_4)$$

şeklinde kodlanır. Örneğin,

$0\ 0\ 0\ 0 \xrightarrow{\varphi} 0\ 0\ 0\ 0\ 0\ 0\ 0$

$1\ 0\ 0\ 0 \xrightarrow{\varphi} 1\ 0\ 0\ 0\ 1\ 0\ 1$

$1\ 1\ 1\ 0 \xrightarrow{\varphi} 1\ 1\ 1\ 0\ 1\ 0\ 0$

şeklindedir.

2.2.2. Dual Kod ve Eşlik-Denetim (Parity-Check) Matrisi

$(F_q)^n$ de, $u=(u_1, u_2, \ldots, u_n)$ ve $v=(v_1, v_2, \ldots, v_n)$ vektörlerinin iç çarpımı,

$$< u, v >= u_1v_1 + u_2v_2 + ... + u_nv_n$$

şeklinde tanımlanan skalerdir. Yani, $GF(q)$ nun bir elemanıdır.

Tanım 2.2.2.1. C, lineer bir $[n, k]-$kod olmak üzere, C nin her bir kodsözcüğüne ortogonal olan $(F_q)^n$ in vektörlerinin kümesine, C nin dual kodu denir ve "$C^{\perp}$" ile gösterilir.

$$C^{\perp} = \{v \in (F_q)^n \mid vu = 0, \ \forall u \in C\}$$ ([12])

Yardımcı Teorem 2.2.2.1. C, üreteç matrisi G olan bir $[n, k]-$kod olsun. Bu durumda, $(F_q)^n$ in bir v vektörünün $C^{\perp}$ ne ait olması için gerek ve yeter koşul; v nin, G üreteç matrisinin her satırına ortogonal olmasıdır. Yani,

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

dır. (Burada G^T ile G nin transpozesi belirtilmektedir.) ([12])

Teorem 2.2.2.1. C, $GF(q)$ üzerinde lineer bir $[n, k]-$kod olsun. Bu durumda, C nin $C^{\perp}$ dual kodu, lineer bir $[n, n-k]-$koddur. ([12])

Teorem 2.2.2.2. Herhangi bir $[n, k]-$kod C için

$$(C^{\perp})^{\perp} = C$$

dir. ([12])

İspat. C deki her bir vektör, $C^{\perp}$ deki her vektöre ortogonal olduğundan,

$$C \subseteq (C^{\perp})^{\perp}$$

dir. Fakat,

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

dir. Böylece,

$$(C^{\perp})^{\perp} = C$$

olur. ([12])

Tanım 2.2.2.2. C bir $[n, k]-$kod olmak üzere, $C = C^{\perp}$ ise C ye, self-dual denir. C self-dual ise $boyC = boyC^{\perp}$ dir, yani

$$k = n-k \Rightarrow 2k = n \Rightarrow k = n/2$$

dir.

Tanım 2.2.2.3. C bir $[n, k]-$kod olmak üzere, her $u, v \in C$ için $uv = 0$ ise C self-ortogonaldir, yani $C \subseteq C^{\perp}$ dir.

Gerçekten, her $u, v \in C$ için $uv = 0$ ise $u, v \in C^{\perp}$ dir. $(C \subseteq C^{\perp})$

C self-ortogonal ise $boy\ C \leq n/2$ dir. Eğer C self-ortogonal ikili bir kod ise, C nin her sözcüğü çift ağırlıklıdır, o halde $C^{\perp}$ dual kodu 1 vektörünü içerir.

Tanım 2.2.2.4. Tüm sözcüklerinin ağırlıkları 4 ile bölünebilen ikili bir koda, katlı-çift (doubly-even) denir.

Tanım 2.2.2.5. $C,$ bir $[n, k]-$kod olmak üzere, $C^{\perp}$ nin bir H üreteç matrisine, C nin bir eşlik-denetim (parity-check) matrisi denir. Bu durumda $H,$ bir $(n-k)\times n$ matristir ve $GH^{T} = 0$ eşitliğini gerçekler. ([12])

H, C nin bir eşlik-denetim matrisi ise,

$$C = \{x \in (F_q)^n \mid xH^T = 0\}$$

dır.

Bu yolla lineer bir kod, bir eşlik-denetim matrisi ile tamamen belirlenebilir. ([12])

Teorem 2.2.2.3. C, bir $[n, k]-$kod olmak üzere, C nin standart formdaki üreteç matrisi $G = [I_k \mid A]$ ise, C için bir eşlik-denetim matrisi,

$$H = [-A^T \mid I_{n-k}]$$

dır. ([12])

İspat.

$$G = \begin{bmatrix} 1 & \cdots & 0 & a_{11} & \cdots & a_{1,n-k} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & a_{k1} & \cdots & a_{k,n-k} \end{bmatrix}$$

olduğu kabul edilsin.

$$H = \begin{bmatrix} -a_{11} & \cdots & -a_{k1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{1,n-k} & \cdots & -a_{k,n-k} & 0 & \cdots & 1 \end{bmatrix}$$

olsun.

Bu durumda H, bir eşlik-denetim matrisi için istenen boyuttadır ve H nin satırları lineer bağımsızdır. Böylece H nin her bir satırının, G nin her bir satırına ortogonal olduğu gösterilmelidir.

G nin i ninci satırı ile H nin j ninci satırının iç çarpımı,

$$0 + \ldots + 0 + (-a_{ij}) + 0 \ldots + 0 + a_{ij} + 0 + \ldots + 0 = 0$$

dır.

Böylece ispat tamamlanmış olur. ([12])

Tanım 2.2.2.6. Bir H eşlik-denetim matrisi için,

$$H = [B \mid I_{n-k}]$$

ise H ye, standart formda denir.

Eğer bir kod, standart formdaki bir $H = [B \mid I_{n-k}]$ eşlik-denetim matrisi ile belirlenirse, bu kodun bir üreteç matrisi,

$$G = [I_k \mid -B^T]$$

dir. ([12])

2.2.3. Bir Dizaynın Kodu

Tanım 1.1.1.'de $(v, b, r, k, \lambda)-$parametreli dizayn tanımlanmıştı. Bu kısımda ise, dizaynın kodundan söz edilecektir.

I. bölümde de açıklandığı gibi söz konusu dizaynın parametreleri (v, b, r, k, λ) olduğunda; v ile dizayndaki nokta sayısı, b ile dizayndaki toplam blok sayısı, r ile her bir noktanın ait olduğu blok sayısı, k ile her bir bloktaki nokta sayısı ve λ ile herhangi iki elemanlı alt kümenin bulunduğu blok sayısı gösterilmektedir.

Tanım 2.2.3.1. $(v, b, r, k, \lambda)-$parametreli dizayn olan **D** nin çakışım matrisi A olsun. $F_q = GF(q)$ cismi üzerinde, **D** nin C kodu denince,

$$(F_q)^b = \{(x_1, x_2, \cdots, x_b) \mid x_i \in F_q\}$$

uzayının, A nın satırları ile üretilmiş alt uzayı anlaşılır.

□

C bir $[v, r]-$kod olduğuna göre dual kod $C^{\perp}$,

$$C^{\perp} = \{y \in (F_q)^v \mid \forall_{x \in C} \ [< x, y >= 0]\}$$

şeklinde tanımlanır.

$C^{\perp}$ lineerdir ve $[v, v-r]-$koddur. □

V bir iç çarpım uzayı olsun. Bir $S \subset V$ alalım.

$$S^{\perp} = \{y \in V \mid < x, y >= 0, \ \forall x \in S \ \}$$

kümesi, S nin ortogonal tümleyeni adını alır.

V nin herhangi S alt kümesi için $S^{\perp}$, V nin bir alt uzayıdır.

2.2.4. Bir Simetrik Dizaynın Kodu

Tanım 2.2.4.1. $(v, k, \lambda)-$parametreli simetrik dizaynın F_p-kodu, Tanım 2.2.3.1'e göre, $(F_p)^v$ nin A çakışım matrisinin satırları ile üretilen alt uzayıdır.

Tanım 2.2.4.2. ψ, $(F_p)^m$ üzerinde bir simetrik bilineer form (veya skaler çarpım) ise ψ ye göre C kodunun duali,

$$C^{\psi} = \{x \in (F_p)^m \mid \psi(x, y) = 0, \ \forall \ y \in C \text{ için}\}$$

kodudur.

Eğer $C \subseteq C^{\psi}$ ise C koduna, ψ ye göre self-ortogonaldir denir.

Eğer $C = C^{\psi}$ ise C koduna, ψ ye göre self-dualdir denir. ([15])

2.2.5. Bir Simetrik Dizaynın Genişletilmiş Kodu

Tanım 2.2.5.1. $(v, k, \lambda)-$parametreli simetrik dizayn D nin F_p-kodu $C^{gen.}$, genişletilmiş çakışım matrisinin satırları ile üretilen koddur. Genişletilmiş çakışım matrisi,

$$B=\left[\begin{array}{ccc|c} & & & 1 \\ & & & \vdots \\ & A & & 1 \\ \hline - & - & - & - \\ \lambda & \cdots\lambda & & k \end{array}\right]_{(v+1)\times(v+1)}$$

dir. ([15]) □

İki farklı bloğun skaler çarpımı, (mod p) ye göre, A çakışım matrisinin bu bloklara karşılık gelen satırlarının skaler çarpımı olup, söz konusu blokların kesişiminin eleman sayısına (λ) eşittir.

Teorem 2.2.5.1. $(v, k, \lambda)-$parametreli simetrik dizayn D nin F_p-kodu C olsun. Bu durumda,

i) Eğer $p \mid k-\lambda$ ise $2 \le boyC \le \frac{1}{2}(v+1)$ dir.

ii) Eğer $p \nmid k-\lambda$ ve $p \mid k$ ise $boyC = v-1$ dir.

iii) Eğer $p \nmid k-\lambda$ ve $p \nmid k$ ise $boyC = v$ dir. (Lander 50)

İspat.

i) $p \mid k-\lambda$ olsun.

1) Eğer $p \mid k$ (buradan aynı zamanda $p \mid \lambda$) ise iki bloğun (mod p) ye göre skaler çarpımı, daima sıfırdır. Çünkü D nin F_p-kodu C, bu bloklar tarafından üretilir ve C, bilinen skaler çarpıma göre self-ortogonaldir $(C \subseteq C^{\perp})$. Böylece,

$$boyC \le \frac{1}{2}v$$

dir.

2) $p \nmid k$ olsun.

Şimdi, bilinen skaler çarpım yerine, aşağıda ψ ile verilen bilineer form tanımlansın. (Lander 50)

$$\psi(\bar{x}, \bar{y}) = x_1y_1 + \cdots + x_vy_v - \lambda x_{v+1}y_{v+1}$$

Burada $\bar{x} = (x_1, \cdots, x_{v+1})$ ve $\bar{y} = (y_1, \cdots, y_{v+1})$ dir. ($\bar{x} = (x_1, x_2, \cdots, x_v, 1)$ veya son satır vektörü, $(\lambda, \lambda, \cdots, \lambda, k)$ dır.)

$\bar{x}$ ve $\bar{y}$, B matrisinin satırları olduğuna göre,

$\psi(\bar{x}, \bar{y}) = k - \lambda$ veya $\psi(\bar{x}, \bar{y}) = 0$

dır.

Gerçekten, $\bar{x} = (x_1, x_2, \cdots, x_v, 1)$ ve $\bar{y} = (y_1, y_2, \cdots, y_v, 1)$ iken,

$$\psi(\bar{x}, \bar{y}) = \underbrace{x_1y_1 + x_2y_2 + \cdots + x_vy_v}_{\lambda} - \lambda.1.1 = 0$$

veya $\bar{x} = (x_1, x_2, \cdots, x_v, 1)$ ve $\bar{y} = (\lambda, \lambda, \cdots, \lambda, k)$ iken,

$$\psi(\bar{x}, \bar{y}) = k\lambda - \lambda k$$

$$= 0$$

dır.

$\bar{x} = (x_1, x_2, \cdots, x_v, 1)$ ve $\bar{y} = (\lambda, \lambda, \cdots, \lambda, k)$ iken

$$\psi(\bar{x}, \bar{x}) = k - \lambda$$

ve

$$\psi(\bar{y}, \bar{y}) = \underbrace{\lambda^2 + \lambda^2 + \cdots + \lambda^2}_{v \tan e} - \lambda k k$$

$$= v\lambda^2 - \lambda k^2$$

$$= \lambda(v\lambda - k^2) \qquad (2.2.5.1.1.)$$

dır. (1.1.1.4.) gereğince,

$$(v-1)\lambda = k(k-1)$$

idi. Buradan,

$$(v-1)\lambda = k^2 - k$$

$$v\lambda - k^2 = \lambda - k \qquad (2.2.5.1.2.)$$

elde edilir. (2.2.5.1.2.) ifadesi, (2.2.5.1.1.)'de yerine yazılacak olursa,

$$\psi(\bar{y}, \bar{y}) = \lambda(\lambda - k)$$

olur. Yani,

$$\psi(\bar{y}, \bar{y}) = \lambda^2 - k\lambda \qquad (2.2.5.1.3.)$$

dır. (1.1.1.6.) gereğince,

$$(v-k)\lambda = (k-1)(k-\lambda)$$

idi. Buradan,

$$v\lambda - k\lambda = (k-1)(k-\lambda)$$

$$v\lambda - (k-1)(k-\lambda) = k\lambda$$

$$v\lambda - k^2 + k\lambda + k - \lambda = k\lambda \qquad (2.2.5.1.4.)$$

elde edilir. (2.2.5.1.4.) ifadesi, (2.2.5.1.3.)'te yerine yazılacak olursa,

$$\psi(\bar{y}, \bar{y}) = \lambda^2 - v\lambda + k^2 - k\lambda - k + \lambda$$

$$= \lambda^2 - (v\lambda - k^2) - k\lambda - k + \lambda \qquad (2.2.5.1.5.)$$

elde edilir. (2.2.5.1.2.)'deki $(v\lambda - k^2)$ nin karşılık geldiği ifade (2.2.5.1.5.)'te yerine yazılacak olursa,

$$\psi(\bar{y}, \bar{y}) = \lambda^2 - (\lambda - k) - k\lambda - k + \lambda$$

$$= \lambda^2 - \lambda + k - k\lambda - k + \lambda$$

$$= \lambda^2 - k\lambda$$

$$= \lambda(\lambda - k)$$

$$= -\lambda(k - \lambda) \qquad (2.2.5.1.6.)$$

elde edilir. Bundan dolayı,

$$\psi(\bar{x}, \bar{y}) \equiv 0 \pmod{p}$$

dir.

Yani, $p \nmid k$ iken de iki bloğun (mod p) ye göre skaler çarpımı sıfırdır. Çünkü, D nin genişletilmiş F_p – kodu $C^{gen.}$, genişletilmiş çakışım matrisinin satırlarıyla üretilir ve $C^{gen.}$, bilinen skaler çarpıma göre self-ortogonaldir ($C^{gen.} \subseteq C^{gen.\perp}$). Böylece,

$$boyC^{gen.} \le \frac{1}{2}(v+1)$$

dir.

Şimdi de, sadece $p \nmid k$ iken $boyC^{gen.} = boyC$ eşitliğinin sağlandığı gösterilmelidir.

B nin ilk v tane sütununun toplamı,

$$\begin{bmatrix} k \\ \vdots \\ k \\ v\lambda \end{bmatrix}$$

dır. Bu sütunun (mod p) ye göre k^{-1} katı alınacak olursa,

$$k^{-1}\begin{bmatrix} k \\ \vdots \\ k \\ v\lambda \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ v\lambda k^{-1} \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ k \end{bmatrix} \qquad (\text{mod } p)$$

elde edilir. Çünkü, (1.1.1.4.) gereğince,

$$(v-1)\lambda = k(k-1)$$

idi. Buradan,

$$v\lambda - \lambda = k^2 - k$$

$$v\lambda = k^2 - k + \lambda$$

elde edilir. Böylece,

$$v\lambda k^{-1} \equiv (k^2 - k + \lambda)k^{-1} \qquad (\text{mod } p)$$

$$\equiv (k^2 - \underbrace{(k-\lambda)}_{\equiv 0})k^{-1} \qquad (\text{mod } p)$$

$$\equiv k \qquad (\text{mod } p)$$

bulunur. Yani B matrisinin son sütunu, B nin ilk v tane sütununun toplamının (mod p) ye göre $-k$ katıdır.

Şimdi, B matrisinin ilk v tane satırı toplansın. Bu durumda,

$$[k, k, \cdots, k, v]$$

bulunur. Bunun, (mod p) ye göre λk^{-1} katı alınsın. Bu durumda,

$$\lambda k^{-1}[k, k, \cdots, k, v] \equiv [\lambda, \lambda, \cdots, \lambda, v\lambda k^{-1}] \qquad (\text{mod } p)$$

$$\equiv [\lambda, \lambda, \cdots, \lambda, (k^2 - \underbrace{(k-\lambda)}_{\equiv 0})k^{-1}] \qquad (\text{mod } p)$$

$$\equiv [\lambda, \lambda, \cdots, \lambda, k] \qquad (\text{mod } p)$$

elde edilir. Yani B matrisinin son satırı, B nin ilk v tane satırının toplamının (mod p) ye göre λk^{-1} katıdır.

B matrisi, A matrisine bir satır ve bir sütun eklenerek elde edilmişti. Yukarıdaki ifadelerden; B matrisinin son sütununun, A matrisinin sütunlarının bir lineer kombinasyonu; B matrisinin son satırının ise A matrisinin satırlarının bir lineer kombinasyonu olduğu görülmektedir. Bunun sonucunda,

$$rankA = rankB$$

bulunur. A, C nin çakışım matrisi; B, genişletilmiş $C^{gen.}$ nin çakışım matrisi olduğundan bu durumda,

$$boyC = boyC^{gen.}$$

dir. (C ve $C^{gen.}$ in her biri, birer F_p – kod olarak alınmaktadır.) Sonuçta alt sınır,

$$2 \le boyC$$

dir.

ii) $p \nmid k-\lambda$ ve $p \mid k$ olsun. A nın her satırı, (bilinen skaler çarpıma göre)

(1, 1, 1,…,1) vektörüne ortogonaldir. Gerçekten,

$$(x_1, x_2, \cdots, x_v)(1, 1, \cdots,1) = x_1 + x_2 + \cdots + x_v = k \equiv 0 \pmod{p}$$

dir. Bundan dolayı,

$$boyC \leq v-1$$

dir. i ninci sütunda sıfırı içeren tüm satırların toplamı,

$$(k-\lambda,\cdots,k-\lambda, 0, k-\lambda,\cdots,k-\lambda)$$

vektörüdür. Burada 0, i ninci sütundadır. Bu vektörler, $(F_p)^m$ nin $(v-1)-$boyutlu bir alt uzayını üretirler.

iii) $p \nmid k-\lambda$ ve $p \nmid k$ olsun. Önerme 1.1.1. gereğince

$$\det A = k(k-\lambda)^{\frac{1}{2}(v-1)}$$

olduğundan, A matrisi, F_p üzerinde tersi alınabilen bir matristir.

Bundan dolayı,

$$boyC = v$$

dir.

Örnek 2.2.5.1. $(7, 3,1)-$simetrik dizaynda;

$$v = 7,\ k = 3,\ \lambda = 1$$

olduğundan,

$$k-\lambda = 3-1 = 2$$

dir. Bu durumda $(7, 3,1)-$simetrik dizaynın F_2-kodu için,

$p \mid k-\lambda$ yani 2|2

dir. O halde

$2 \le boyC \le 4$

tür.

Teorem 2.2.5.2. Bir p asalı için, $p \mid k-\lambda$, $(p,\ k)=1$, $p^2 \nmid k-\lambda$ olmak üzere $(v,\ k,\ \lambda)-$parametreli simetrik dizaynın F_p-kodunun boyutu, $\frac{v+1}{2}$ dir.

İspat. A çakışım matrisinin satırları ile üretilen F_p-kod C nin boyutu,

$boyC = r$

olsun. Bu durumda,

$boyC^{\perp} = v-r$

dir.

$boyC^{\perp} = s$

olarak alınsın. Yani,

$v-r=s$

olsun. $(v,\ k,\ \lambda)-$parametreli simetrik dizaynın A çakışım matrisinin satırları ile üretilen F_p-kod C nin H eşlik-denetim matrisi,

$H=[I_s : P]$

olsun. H, bir $s\times v$ matristir.

$C^{\perp}$ dual kodunun çakışım matrisi,

$$K = \begin{bmatrix} I_s & \vdots & P_{s\times r} \\ \cdots & \vdots & \cdots \\ 0 & \vdots & I_r \end{bmatrix}$$

olsun. K, bir $v\times v$ matristir.

$$\det(AK^T) = \det A \det K^T$$

dir.

$$\det K = \det K^T = 1$$

olduğundan,

$$\det(AK^T) = \det A$$

dır. Önerme 1.1.1. gereğince,

$$\det A = kn^{\frac{1}{2}(v-1)}$$

idi. Böylece,

$$\det(AK^T) = kn^{\frac{1}{2}(v-1)}$$

elde edilir.

$$AK^T = A\begin{bmatrix} I_s & \vdots & 0 \\ \cdots & \vdots & \cdots \\ P_{s\times r} & \vdots & I_r \end{bmatrix}$$

olup; AK^T, A çakışım matrisinin satırları ile $C^{\perp}$ dual kodunun çakışım matrisinin satırlarının iç çarpımıdır. Sonuçta, AK^T nin ilk s sütununda, p nin katları elde edilir ($\equiv 0 \pmod{p}$ olmalı). O zaman, $\det(AK^T)$ nin ilk s sütunundan, p çarpanları determinant dışına çıkarılırsa ($\det(AK^T) = \det A$ idi), $\det A$'nın p^s ile bölündüğü ortaya çıkar. Yani,

$p^s \mid \det A$

dır. Buradan,

$p^s \mid kn^{\frac{1}{2}(v-1)}$

yazılır.

$(p,\ k) = 1$

olduğundan,

$p \nmid k$

dır. Dolayısıyle,

$p^s \nmid k$

dır. Buradan,

$p^s \mid kn^{\frac{1}{2}(v-1)}$ ve $p^s \nmid k$

olduğundan,

$p^s \mid n^{\frac{1}{2}(v-1)}$

dır.

$p^2 \nmid n$ ve $p \mid n$ idi. Böylece,

$$s \leq \frac{1}{2}(v-1)$$

olur. Yani,

$$v - r \leq \frac{1}{2}(v-1)$$

dir. Buradan,

$$2v - 2r \leq v - 1$$

$$2v - v + 1 \leq 2r$$

$$v + 1 \leq 2r$$

$$r \geq \frac{v+1}{2}$$

bulunur. Yani,

$$boyC \geq \frac{v+1}{2} \qquad (2.2.5.2.1.)$$

dir. Teorem 2.2.5.1. i)'e göre,

$$p \mid n \text{ iken } boyC \leq \frac{v+1}{2} \qquad (2.2.5.2.2.)$$

idi. (2.2.5.2.1.) ve (2.2.5.2.2.)'den,

$$boyC = \frac{v+1}{2}$$

elde edilir.

BÖLÜM 3

SIR PAYLAŞIM ŞEMALARI

GİRİŞ

Her türlü özel anahtar, şifre, gizli bir aracın planı veya ürünün formülü gibi gizli tutulması zorunlu bilgilere "sır" denilmektedir. Söz konusu sır, bir formülle de ifade edilebilir. Sırrın saklanması zorunluluğu vardır.

Sır paylaşım problemi denince; söz konusu sırrın formüle edilip parçalara ayrılarak, bütünün saklanması yerine, parçaların farklı yerlerde veya konumlarda saklanması problemi anlaşılmaktadır.

Sır paylaşımı, 20 yıldan fazla bir süreden beri çalışılan bir konudur.[1] Sır paylaşım şemalarının oluşturulması için, kodlar teorisinden büyük ölçüde yararlanılmakta olup; lineer kodlar, sır paylaşım şemalarının kuruluşunda önemli bir rol oynamaktadır.

Sır paylaşım şemalarından, 1979'da Blakley ([5]) ve Shamir ([27]) söz etmişlerdir. Daha sonra bu konuda pek çok yeni yöntem önerilmiştir. Shamir'in sır paylaşım şeması ve Reed-Solomon Kodları arasındaki ilişki, 1981'de Mc Eliece ve Sarwate ([19]) tarafından belirtilmiştir. Daha sonra hata düzeltme kodları kullanılarak, sır paylaşım şemalarının kurulması üzerine çalışılmıştır. ([31], [9], [14], [17], [18], [20], [22])

Massey ([17], [18]), sır paylaşımı için lineer kodlardan faydalanarak, ilgili kodun dualinin minimal kodsözcükleri ve erişim yapısı arasındaki ilişkiyi belirtmiştir.

---

(1) Bu bölümün giriş bölümü büyük ölçüde, Jin Yuan ve Cunsheng Ding'in "Secret Sharing Schemes From Three Classes Of Linear Codes" ([31[) isimli makalesine dayanmaktadır.

Belli kodlar için minimal kodsözcükleri araştırılarak, bu kodların dual kodları üzerine kurulan sır paylaşım şemalarının erişim yapıları karakterize edilmiştir. ([24], [1], [2], [30])

3.1. Massey'in Sır Paylaşım Şeması

Massey'in sır paylaşım şemasının kurulması, tamamen lineer kodlarla yapılmaktadır ([21]). Bu kısımda önce lineer kodlar üzerinde oluşturulan sır paylaşım şeması anlatılacak, daha sonra $C^{\perp}$ dual kodu üzerinde kurulan sır paylaşım şemasının bazı özelikleri sunulacaktır.

F_q üzerinde lineer bir $[n, k, d]-$kod C, $(F_q)^n$ in bir alt uzayıdır.

$G=(g_0, g_1,\cdots, g_{n-1})$, $[n, k, d]-$kod C nin üreteç matrisi olsun. Burada $g_0, g_1,\cdots, g_{n-1}$, G nin sütun vektörleridir. G açık şekilde yazılacak olursa,

$$G=\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}_{k\times n}$$

gibidir.

Sır paylaşım şemalarını oluşturmak için, içinde katılımcıların ve bir Yönetici'nin bulunduğu bir sır uzayı ele alınır. Bu sır uzayı F_q olarak düşünülsün ve $n-1$ tane katılımcı da $P_1, P_2,\cdots, P_{n-1}$ olsun.

Yönetici, bir "sır" oluşturur. (Sır "s" olsun.) Sır oluşturma işlemi aşağıdaki gibidir:

Herhangi bir $u=(u_0, u_1,\cdots, u_{k-1})\in (F_q)^k$ vektörü seçilir. Sır,

$$s=ug_0$$

şeklinde oluşturulur.

s sırrını oluşturmak için seçilebilecek $u \in (F_q)^k$ vektörlerinin sayısı q^{k-1} olur:

Gerçekten; $u \in (F_q)^k$ olduğuna göre, $(F_q)^k$ nın sıfırdan farklı vektörlerinin sayısı q^{k-1} olup, u için seçenek q^{k-1} dir. □

"Yönetici, oluşturduğu sırrı nasıl paylaştırır?" sorusunun yanıtı, konunun temellerinden ilkidir.

$u = (u_0, u_1, \cdots, u_{k-1}) \in (F_q)^k$ dan, u 'ya karşılık gelen

$$uG = (t_0, t_1, \cdots, t_{n-1}) = t$$

kodsözcüğü hesaplanır ve her $i = 1, 2, \ldots, n-1$ için P_i katılımcısına t vektörünün t_i bileşeni pay olarak verilir.

$$t_0 = ug_0 = s$$

olduğuna göre, $P_1, P_2, \ldots, P_{n-1}$ katılımcılarına dağıtılan $n-1$ parça içerisinden m tanesi alınacak olursa, paylaşımların bir alt kümesi

$$\{t_{i_1}, t_{i_2}, \cdots, t_{i_m}\}$$

olur. □

"Patron veya sır sahibi herhangi bir nedenle sırrı yitirirse (emeklilik, ölüm, kayıp, v.b.), bu sırra nasıl ulaşılabilir?" sorusunun yanıtlanması da, konunun diğer önemli bir parçasıdır.

Önerme 3.1.1. Sırrın belirlenmesi için gerek ve yeter koşul;
$g_0 = (g_{11}, g_{21}, \cdots, g_{k1})^T$ ın, $g_1, g_2, \cdots, g_{n-1}$ sütun vektörlerinin lineer kombinasyonu olarak yazılabilmesidir. ([31])

İspat.

$\Leftarrow$: $g_0;\ g_1, g_2,\cdots, g_{n-1}$ in lineer kombinasyonu olarak yazılabilsin. Bu durumda,

$$g_0 = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_{n-1} g_{n-1} \qquad (\alpha_i \in F_q,\quad 1 \le i \le n-1)$$

$$(g_{11}, g_{21},\cdots, g_{k1})^T = \alpha_1 (g_{12}, g_{22},\cdots, g_{k2})^T + \cdots + \alpha_{n-1} (g_{1n}, g_{2n},\cdots, g_{kn})^T$$

$$(g_{11}, g_{21},\cdots, g_{k1})^T = (\alpha_1 g_{12} + \cdots + \alpha_{n-1} g_{1n},$$

$$\alpha_1 g_{22} + \cdots + \alpha_{n-1} g_{2n},\cdots, \alpha_1 g_{k2} + \cdots + \alpha_{n-1} g_{kn})^T$$

olur. Buradan,

$$\begin{cases} g_{11} = \alpha_1 g_{12} + \cdots + \alpha_{n-1} g_{1n} \\ g_{21} = \alpha_1 g_{22} + \cdots + \alpha_{n-1} g_{2n} \\ \vdots \\ g_{k1} = \alpha_1 g_{k2} + \cdots + \alpha_{n-1} g_{kn} \end{cases}$$

elde edilir.

$s = g_{11}u_0 + g_{21}u_1 + \cdots + g_{k1}u_{k-1}$ ifadesinde $g_{11}, g_{21},\cdots, g_{k1}$ in değerleri yerine yazılırsa, s sırrı belirlenir.

$\Rightarrow$: s belirlenmiş olsun. Bu durumda,

$s = ug_0$

olduğundan,

$s = g_{11}u_0 + g_{21}u_1 + \cdots + g_{k1}u_{k-1}$

ifadesi biliniyor demektir. Bu ise $g_0 = (g_{11}, g_{21},\cdots, g_{k1})^T$ ın bilinmesi demektir.

G üreteç matrisinin tanımından dolayı, $(n > k)$ kolaylıkla

$$\begin{cases} g_{11} = \alpha_1 g_{12} + \cdots + \alpha_{n-1} g_{1n} \\ g_{21} = \alpha_1 g_{22} + \cdots + \alpha_{n-1} g_{2n} \\ \vdots \\ g_{k1} = \alpha_1 g_{k2} + \cdots + \alpha_{n-1} g_{kn} \end{cases}$$

yazılabilir. Buradan,

$$(g_{11},\, g_{21}, \cdots,\, g_{k1})^T = \alpha_1 (g_{12},\, g_{22}, \cdots,\, g_{k2})^T + \cdots + \alpha_{n-1} (g_{1n},\, g_{2n}, \cdots,\, g_{kn})^T$$

elde edilir ki bu da,

$$g_0 = (g_{11},\, g_{21}, \cdots,\, g_{k1})^T \text{ ın, } g_1 = (g_{12},\, g_{22}, \cdots,\, g_{k2})^T, \cdots, g_{n-1} = (g_{1n},\, g_{2n}, \cdots,\, g_{kn})^T$$

in lineer kombinasyonu olması demektir.

Önerme 3.1.2. G, F_q üzerinde bir $[n, k]-$kod C nin üreteç matrisi olsun. C üzerinde kurulan sır paylaşım şemasında $\{t_{i_1},\, t_{i_2}, \cdots,\, t_{i_m}\}$, $(1 \le i_1 < \cdots < i_m \le n-1$ ve $1 \le m \le n-1)$ paylaşımlar kümesinin sırrı belirleyebilmesi için gerek ve yeter koşul; $C^{\perp}$ dual kodunda,

$$v = (1,\, 0, \cdots, 0,\; c_{i_1}, 0, \cdots, 0, c_{i_2}, 0, \cdots,\; 0,\; c_{i_m}, 0, \cdots, 0) \qquad (3.1.2.1.)$$

kodsözcüğünün var olmasıdır. Burada $c_{i_j} \neq 0$ dır. ([31])

$C^{\perp}$ de (3.1.2.1.) kodsözcüğü varsa, bu durumda g_0 vektörü, $g_{i_1}, \cdots,\, g_{i_m}$ nin bir lineer kombinasyonudur.

İspat.

$\Leftarrow$: $C^{\perp}$ de (3.1.2.1.) kodsözcüğü varsa, g_0 vektörünün $g_{i_1},\, g_{i_2}, \cdots,\, g_{i_m}$ lerin, bir lineer kombinasyonu olarak yazılabileceği gösterilmelidir. $C^{\perp}$ dual kodunun tanımından,

$$vG^T = 0$$

olmalıdır. O halde,

$$(1,\ 0,\cdots,0,\ \ c_{i_1},0,\cdots,0,c_{i_2},0,\cdots,\ 0,\ \ c_{i_m},0,\cdots,0)\begin{bmatrix} g_{11} & g_{21} & \cdots & g_{k1} \\ g_{12} & g_{22} & \cdots & g_{k2} \\ \vdots & \vdots & \cdots & \vdots \\ g_{1n} & g_{2n} & \cdots & g_{kn} \end{bmatrix} = 0$$

$$g_{11} + g_{1i_1}c_{i_1} + g_{1i_2}c_{i_2} + \cdots + g_{1i_m}c_{i_m} = 0 \Rightarrow g_{11} = -(g_{1i_1}c_{i_1} + g_{1i_2}c_{i_2} + \cdots + g_{1_{i_m}}c_{i_m})$$

$$g_{21} + g_{2i_1}c_{i_1} + g_{2i_2}c_{i_2} + \cdots + g_{2i_m}c_{i_m} = 0 \Rightarrow g_{21} = -(g_{2i_1}c_{i_1} + g_{2i_2}c_{i_2} + \cdots + g_{2i_m}c_{i_m})$$

.....

$$g_{k1} + g_{ki_1}c_{i_1} + g_{ki_2}c_{i_2} + \cdots + g_{ki_m}c_{i_m} = 0 \Rightarrow g_{k1} = -(g_{ki_1}c_{i_1} + g_{ki_2}c_{i_2} + \cdots + g_{ki_m}c_{i_m})$$

dir. Buradan,

$g_0 = (g_{11},\ g_{21},\cdots,\ g_{k1})^T$ vektörünün $g_{i_1},\ g_{i_2},\ \cdots,\ g_{i_m}$ nin lineer kombinasyonu olduğu görülür. Yani,

$$g_0 = \sum_{j=1}^{m} x_j g_{i_j}$$

dir.

Bu durumda sır, belirlenmiş olur.

$\Rightarrow$: C üzerinde kurulan sır paylaşım şemasında $\{t_{i_1},\ t_{i_2},\cdots,\ t_{i_m}\}$,
$(1 \le i_1 < \cdots < i_m \le n-1$ ve $1 \le m \le n-1)$ paylaşımlar kümesi, sırrı belirlemiş olsun.
$C^{\perp}$ dual kodunda

$$v = (1,\ 0,\cdots,0,\ \ c_{i_1},0,\cdots,\ 0,\ \ c_{i_2},\ 0,\cdots,\ c_{i_m},\ 0,\cdots,\ 0) \qquad (3.1.2.1.)$$

kodsözcüğünün bulunduğunu gösterelim.

Tersini kabul edelim. Yani $C^{\perp}$ dual kodunda (3.1.2.1.) kodsözcüğü bulunmasın. Bu durumda ispat oldukça kolaydır. □

Sır paylaşım şemalarında temel amaçlardan biri; gerekli durumlarda belli sayıda (k diyelim) katılımcının bir araya gelerek sırrı çözümleyebilmesi, daha az sayıda katılımcının sırra erişememesinin sağlanmasıdır. Örneğin, Yönetici herhangi bir şekilde devreden çıkarıldığında, Yönetici'nin oluşturmuş olduğu sırra ulaşılabilmelidir.

Bu durum, aşağıdaki gibi de açıklanabilir:

Önerme 3.1.2. gereğince; $C^{\perp}$ dual kodunda
$v = (1, 0, \cdots, 0, \ c_{i_1}, 0, \cdots, 0, c_{i_2}, 0, \cdots, \ 0, \ c_{i_m}, 0, \cdots, 0)$ kodsözcüğü varsa; bu durumda g_0 vektörü, $g_{i_1}, g_{i_2}, \cdots, g_{i_m}$ nin $(1 \le i_1 < \cdots < i_m \le n-1$ ve $1 \le m \le n-1)$ bir lineer kombinasyonudur.

Yani

$$g_0 = \sum_{j=1}^{m} x_j g_{i_j}$$

dir. O halde s sırrı,

$$s = ug_0 = u\sum_{j=1}^{m} x_j g_{i_j} = u(x_1 g_{i_1} + x_2 g_{i_2} + \cdots + x_m g_{i_m})$$

$$s = (u_0, u_1, \cdots, u_{k-1})(x_1 g_{i_1} + x_2 g_{i_2} + \cdots + x_m g_{i_m})$$

$$s = (x_1 g_{i_1} + x_2 g_{i_2} + \cdots + x_m g_{i_m})u_0 + (x_1 g_{i_1} + x_2 g_{i_2} + \cdots + x_m g_{i_m})u_1$$

$$+ \cdots + (x_1 g_{i_1} + x_2 g_{i_2} + \cdots + x_m g_{i_m})u_{k-1}$$

$$s = x_1(g_{i_1}u_0 + g_{i_1}u_1 + \cdots + g_{i_1}u_{k-1}) + x_2(g_{i_2}u_0 + g_{i_2}u_1 + \cdots + g_{i_2}u_{k-1})$$

$$+ \cdots + x_m(g_{i_m}u_0 + g_{i_m}u_1 + \cdots + g_{i_m}u_{k-1)}$$

$$s = x_1 t_{i_1} + x_2 t_{i_2} + \cdots + x_m t_{i_m}$$

$$s = \sum_{j=1}^{m} x_j t_{i_j}$$

nin hesaplanması ile belirlenir.

Tanım 3.1.1. (Minimal Erişim Kümesi) k elemanlı katılımcılar kümesi ele alınsın. Bu küme, elemanları bir araya gelerek sırrı çözmüş olsun. Fakat, bu k elemanlı katılımcılar kümesinin, k dan daha az elemanlı her bir alt kümesi, sır hakkında hiçbir ipucu elde edemesin. Bu durumda k elemanlı kümeye, minimal erişim kümesi denir. ([31])

Yani minimal erişim kümesi, bir araya gelerek sırra ulaşabilen katılımcıların oluşturduğu öyle bir kümedir ki; kümeden herhangi bir eksilme, sırra erişilmesini olanaksız kılar.

Tanım 3.1.2. Bir $c = (c_0, c_1, \cdots, c_{n-1}) \in (F_q)^n$ vektörünün desteği,

$$\{0 \le i \le n-1 \mid c_i \neq 0\}$$

olarak tanımlanır.([31])

Tanım 3.1.3. $c_1, c_2 \in (F_q)^n$ olmak üzere, c_2 kodsözcüğünün c_1 kodsözcüğünü örtmesi denince; c_2 kodsözcüğünün desteğinin, c_1 kodsözcüğünün desteğini kapsadığı anlaşılır.

Örneğin;

$$c_1 = (0011010) \in (F_2)^7, \quad c_2 = (1111011) \in (F_2)^7$$

olsun. Bu durumda, c_1 in desteği $\{2, 3, 5\}$, c_2 nin desteği $\{0, 1, 2, 3, 5, 6\}$ dır. Buradan, c_2 kodsözcüğünün, c_1 kodsözcüğünü örttüğü görülür.

Tanım 3.1.4. (Minimal Kodsözcüğü) Sıfırdan farklı bir c kodsözcüğü, yalnızca kendisinin skaler katlarını örtüyorsa, c ye minimal kodsözcüğü denir. ([31]) □

Minimal erişim kümelerinin kümesi ile $C^{\perp}$ dual kodundaki ilk koordinatı 1 olan minimal kodsözcükleri kümesi arasında bire-bir bir eşleme vardır. ([31])

Sır paylaşım şemasının erişim yapısını belirlemek için, $C^{\perp}$ dual kodundaki, yalnızca ilk koordinatı 1 olan minimal kodsözcükleri kümesini belirlemek gerekir. ([31])

Tanım 3.1.5. (Sır Paylaşımının Demokratiklik Derecesi) Bir sır paylaşım şemasında, eğer her $t-$li katılımcı grubu aynı sayıda minimal erişim kümesinde bulunuyorsa, bu sır paylaşımı, t. dereceden demokratik adını alır. $(t \geq 1)$ ([31])

3.2. $C^{\perp}$ Dual Kodu Üzerinde Kurulan Sır Paylaşım Şemalarının Bazı Özelikleri

Önerme 3.2.1. F_q üzerinde bir $[n, k]-$kod C ve $G = (g_0, g_1, \cdots, g_{n-1})$, C nin üreteç matrisi olsun. (Burada tüm g_i $(1 \leq i \leq n-1)$ ler sıfırdan farklıdır.) C nin sıfırdan farklı her bir kodsözcüğü minimal ise bu durumda $C^{\perp}$ dual kodu üzerinde kurulan sır paylaşım şemasında, tam olarak q^{boyC-1} tane minimal erişim kümesi vardır. (Burada "$boyC$" ile C kodunun boyutu olan "k" gösterilmektedir.)[1] ([10])

İspat. G üreteç matrisinin tüm sütun vektörleri sıfırdan farklı olduğundan, $g_0 \neq 0$ dır. $u \in (F_q)^k$ olmak üzere, her u için q^{k-1} farklı kodsözcüğü yazılabilir. Dolayısıyle ug_0 çarpımı da, tam q^{k-1} kez yapılır. ug_0 çarpımı, u ile G üreteç matrisinin ilk sütununu çarpmak demektir. Yani, bu çarpma işleminin sonucunda, kodsözcüğünün ilk koordinatı belirlenmektedir. $u = 0$ ise, ilk koordinatı sıfır olan q^{k-1} kodsözcüğü vardır.

$(F_q)^k$ daki her u vektöürü için yazılabilecek q^{k-1} seçenek vardı. İlk koordinat F_q nun elemanı olduğundan, q çeşit değer alır. Dolayısıyle, ilk koordinatı F_q nun herhangi bir elemanı olan,

$$qq^{k-1} = q^k$$

kodsözcüğü vardır. Bu durumda C deki ilk koordinatı sıfır olmayan kodsözcüklerinin sayısı ise

$$q^k - q^{k-1}$$

dir. Bunlar içinde biri diğerinin skaler katı olmayanların sayısı,

$$\frac{q^k - q^{k-1}}{q-1} = q^{k-1}$$

dir. Bu sayı, ilk koordinatı sıfırdan farklı olan, minimal kodsözcüklerinin sayısıdır. Bu da aynı zamanda minimal erişim kümelerinin sayısını verir. ([10])

Önerme 3.2.2. F_q üzerinde bir $[n, k]-$kod C ve $G = (g_0, g_1, \cdots, g_{n-1})$, C nin üreteç matrisi olsun. (Burada tüm g_i $(1 \le i \le n-1)$ ler sıfırdan farklıdır.)

i) $1 \le i \le n-1$ olmak üzere g_i, g_0 ın bir skaler katı ise bu durumda P_i numaralı katılımcı, her minimal erişim kümesinde olmalıdır. Böyle bir katılımcıya, diktatör katılımcı denir.

ii) $1 \le i \le n-1$ olmak üzere g_i, g_0 ın bir skaler katı değilse, P_i numaralı katılımcı, q^{boyC-1} minimal erişim kümesinden, $(q-1)q^{boyC-2}$ tanesinde bulunmalıdır. ([10])

---

(1) İleriki bölümlerde simetrik dizaynın k parametresi ile C kodunun boyutu olan k birbiriyle karışabileceğinden, yukarıda k yerine "$boyC$" yazılmıştır. İleride bu karmaşıklığı önlemek için, $boyC = r$ olarak alınacaktır.

İspat. i) $1 \le i \le n-1$ olmak üzere $g_i = ag_0 \ \ (a \in F_q^*)$ ise

$ug_i = a \neq 0$ olması $ug_0 = 1$

olduğu manasına gelmektedir. Bundan dolayı P_i numaralı katılımcı, her minimal erişim kümesinde bulunmalıdır. ([10])

ii) $1 \le i \le n-1$ olmak üzere g_0 ve g_i lineer bağımsız ise, $u \in (F_q)^k$ olduğunda, ug_0 ve ug_i çarpımları, $(F_q)^k$ nın her bir elemanı üzerinde q^{k-2} kez yapılır. Bundan dolayı,

$$|\{(u : ug_0 \neq 0 \text{ ve } ug_i \neq 0)\}| = (q-1)^2 q^{k-2}$$

ve

$$|\{(u : ug_0 = 1 \text{ ve } ug_i \neq 0)\}| = (q-1)q^{k-2},$$

P_i numaralı katılımcının bulunduğu minimal erişim kümelerinin sayısıdır. ([10])

3.3. Minimal Kodsözcüklerinin Karakterizasyonları

3.3.1.Ağırlıkları Kullanarak

Yardımcı Teorem 3.3.1.1. Bir $2-(v, k, \lambda)$ dizaynın çakışım matrisi $A_{b\times v}$ olsun. Üreteç matrisi A olan ikili (binary) kodun dualinin minimum ağırlığı $w_{\min}$ için,

$$w_{\min} \ge \frac{(r+\lambda)}{\lambda}$$

dır. Burada $r,$ bir noktanın bulunduğu blok sayısıdır. ([7])

Yardımcı Teorem 3.3.1.2. Bir $2-(v, k, \lambda)$ dizaynın çakışım matrisi $A_{b\times v}$ olsun. O zaman,

$$\begin{bmatrix} 1 & \vdots & \\ \vdots & \vdots & A \\ 1 & \vdots & \end{bmatrix}$$

matrisinin satırları ile üretilen ikili kodun duali için minimum ağırlık,

$$w_{\min} \geq \min\{\frac{b+r}{r}, \frac{r+\lambda}{\lambda}\}$$

dır. ([7])

Teorem 3.3.1.1. (Ashikmin-Barg) F_q üzerinde bir $[n, k]-$kod C de $w_{\min}$ ve w_{maks}, sırası ile sıfırdan farklı minimum ve maksimum ağırlıklar olsun. Eğer

$$\frac{w_{\min}}{w_{maks}} > \frac{q-1}{q}$$

ise bu durumda; C nin sıfırdan farklı tüm kodsözcükleri minimaldir. ([31])

3.3.2. Üstel Toplamları Kullanarak

$q = p^k$ olsun. Burada p asal sayı ve k, pozitif bir tam sayıdır. χ, F_q nun toplamsal kanonik karakterini belirtmektedir.

$$\chi(x) = e^{i\frac{2\Pi Tr(x)}{p}} = \cos\left(\frac{2\Pi}{p}Tr(x)\right) + i\sin\left(\frac{2\Pi}{p}Tr(x)\right).$$

F_q dan F_p ye her bir lineer fonksiyon, $Tr(ax)$ $(a \in F_q)$ şeklinde yazılabilir. Bununla birlikte, üreteç matrisi G olan, F_p üzerindeki herhangi bir lineer $[n, k]-$kod C için; her bir kodsözcüğü,

$$c_\alpha = (Tr(g_1\alpha), \cdots, Tr(g_n\alpha)) \ , \quad (\alpha \in F_q)$$

şeklinde ifade edilebilir. Burada $g_1, g_2, \cdots, g_n \in F_q$ dur. ([31)] □

Şimdi C nin sıfırdan farklı iki kodsözcüğü olan c_α ve c_β ele alınsın. Burada $\beta/\alpha \notin F_p$ dir.

$\beta/\alpha \in F_p$ ise bu durumda iki kodsözcüğü, birbirlerinin skaler katları olmalıdır. ([31])

Gerçekten de,

$$\frac{\beta}{\alpha} = t \in F_p \Rightarrow \beta = \alpha t$$

$$c_\beta = (Tr(g_1\beta), \cdots, Tr(g_n\beta)) = (Tr(g_1\alpha t), \cdots, Tr(g_n\alpha t))$$

$$c_\beta = t(Tr(g_1\alpha), \cdots, Tr(g_n\alpha))$$

$$c_\beta = tc_\alpha$$

dır. □

S_α, c_α nın sıfır olan bileşenlerinin sayısı; $T_{\alpha,\beta}$, c_α ve c_β nın ortaklaşa sıfır olan bileşenlerinin sayısı olsun. Tanım gereğince,

$$S_\alpha \geq T_{\alpha,\beta}$$

dır. ([31])

Örneğin;

$$c_\alpha = (11001), \quad c_\beta = (01101)$$

olsun. Bu durumda,

$$S_\alpha = 2, \quad T_{\alpha,\beta} = 1$$

dir. Yani,

$$S_\alpha \geq T_{\alpha,\beta}$$

dır. □

c_α nın c_β yı örtmesi için gerek ve yeter koşul $S_\alpha = T_{\alpha,\beta}$ olmasıdır. ([31])

Gösterelim:

$\Leftarrow$: $S_\alpha = T_{\alpha,\beta}$ olsun. Bu durumda c_α nın sıfırdan farklı bileşenlerinin konum numaralarının kümesi, c_β nın sıfırdan farklı bileşenlerinin konum numaralarının kümesini içerir. (Yani c_α nın desteği, c_β nın desteğini içerir.) O halde c_α, c_β yı örter.

$\Rightarrow$: c_α, c_β yı örtmüş olsun. Bu durumda c_α nın sıfırdan farklı bileşenlerinin konum numaralarının kümesi, c_β nın sıfırdan farklı bileşenlerinin konum numaralarının kümesini içerir. Dolayısıyle c_α nın sıfır olan bileşenlerinin sayısı, c_α ve c_β nın sıfır olan bileşenlerinin sayısına eşittir. Yani $S_\alpha = T_{\alpha,\beta}$ dır. Örneğin;

$c_\alpha = (010011)$, $c_\beta = (010001)$ olursa bu durumda,

$S_\alpha = 3$ ve $T_{\alpha,\beta} = 3$ olur. Yani,

$S_\alpha = T_{\alpha,\beta}$

dır. Böylece c_α, c_β yı örter.

Önerme 3.3.2.1. Her $\alpha \in F_q^*$ için; c_α nın minimal olması için gerek ve yeter koşul, $\beta / \alpha \notin F_p$ olan her $\beta \in F_q^*$ için $S_\alpha > T_{\alpha,\beta}$ olmasıdır. (F_q^*, F_q cisminin sıfırdan farklı elemanlarının çarpım grubunu belirtmektedir.) ([31])

İspat.

$\Leftarrow$: $\beta / \alpha \notin F_p$ olan her $\beta \in F_q^*$ için $S_\alpha > T_{\alpha,\beta}$ olsun. Her $\alpha \in F_q^*$ için c_α nın minimal olduğunu gösterelim.

$\beta / \alpha \notin F_p$ ise c_α ve c_β, birbirlerinin skaler katları değildir.

$S_\alpha > T_{\alpha,\beta}$ ise c_α nın sıfır olan bileşenlerinin sayısı, c_α ve c_β nın sıfır olan bileşenlerinin sayısından fazla olacağından c_α, c_β yı örtmez. (c_β, c_α yı örter.) Bu durumda c_α, yalnızca kendisinin skaler katlarını örter.

O halde c_α, minimal kodsözcüğüdür.

$\Rightarrow$: Her $\alpha \in F_q^*$ için c_α minimal olsun. $\beta / \alpha \notin F_p$ olan her $\beta \in F_q^*$ için $S_\alpha > T_{\alpha,\beta}$ olduğunu gösterelim.

c_α minimal ise; c_α, yalnızca kendisinin skaler katlarını örter, sıfırdan farklı diğer kodsözcüklerini örtmez. Bu durumda c_α ve c_β, birbirlerinin skaler katları olamaz. Yani $\beta / \alpha \notin F_p$ dir.

c_α, c_β yı örtmediğine göre, (c_α ve c_β farklı konumlarda sıfır değerini almıştır.) c_α nın sıfır olan bileşenlerinin sayısı, c_α ve c_β nın sıfır olan bileşenlerinin sayısından fazladır. Yani, $S_\alpha > T_{\alpha,\beta}$ dır. □

BÖLÜM 4

SİMETRİK DİZAYNIN KODU, SIR PAYLAŞIM ŞEMASI VE MİNİMAL KODSÖZCÜKLERİ

$(v, k, \lambda)-$parametreli D simetrik dizaynı ele alınsın. D nin çakışım matrisi,

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1v} \\ a_{21} & a_{22} & \cdots & a_{2v} \\ \vdots & \vdots & \cdots & \vdots \\ a_{v1} & a_{v2} & \cdots & a_{vv} \end{bmatrix}_{v\times v}$$

olsun.

Simetrik dizaynın F_q-kodu olan C ($q=p^t$, p asal ve t pozitif tam sayı), $(F_q)^v$ nin A çakışım matrisinin satırları ile üretilen alt uzayıdır. A dan, C kodunun üreteç matrisi G, kolaylıkla elde edilir. C kodunun üreteç matrisi $(g_0, g_1, \cdots, g_{v-1})$ olsun. Burada $g_0, g_1, \ldots, g_{v-1}$ ile G nin sütun vektörleri gösterilmektedir. C nin boyutu $boyC=r$ olmak üzere, G açık şekilde yazılacak olursa,

$$G=\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1v} \\ g_{21} & g_{22} & \cdots & g_{2v} \\ \vdots & \vdots & \cdots & \vdots \\ g_{r1} & g_{r2} & \cdots & g_{rv} \end{bmatrix}_{r\times v}$$

dir.

Önerme 4.1. C, $(v, k, \lambda)-$parametreli D simetrik dizaynının ürettiği, F_q üzerinde lineer $[v, r]-$kod olsun.[1] $C^{\perp}$ dual kodundaki sıfırdan farklı her kodsözcüğü minimal kabul edilsin. Bu durumda C kodu üzerinde kurulan sır paylaşım şemasında minimal erişim kümelerinin sayısı, tam $q^{boyC^{\perp}-1}$ dir. (Önerme 3.2.1.'den)

Önerme 4.2. $(v, k, \lambda)-$parametreli simetrik dizaynın F_q üzerinde ürettiği $[v, r]-$kod C olsun. Eğer C ve $C^{\perp}$ dual kodu üzerinde kurulan sır paylaşım şemaları aynı sayıda minimal erişim kümesi içeriyorsa v, çift sayıdır.

İspat. Önerme 3.2.1. gereğince; F_q üzerinde bir $[n, r]-$kod C nin sıfırdan farklı her bir kodsözcüğü minimal olduğunda $C^{\perp}$ dual kodu üzerinde kurulan sır paylaşım şemasında, tam olarak q^{r-1} tane minimal erişim kümesi vardı. Önerme 4.1.'de, $(v, k, \lambda)-$parametreli D simetrik dizaynının ürettiği, F_q üzerindeki lineer $[v, r]-$kod C nin $C^{\perp}$ dual kodunun sıfırdan farklı her kodsözcüğü minimal olmak üzere C kodu üzerinde kurulan sır paylaşım şemasında tam olarak q^{v-r-1} tane minimal erişim kümesinin var olduğu ifade edildi.

---

(1) Simetrik dizaynın parametreleri v, k, λ ile gösterilir. Lineer bir C kodunu da $[n, k]-$kod diye göstermek adettir. $[n, k]-$daki n, kodun uzunluğu olup, bizde v olarak alınmıştır. k ise C nin boyutunu gösterir. Ancak, C nin boyutu olan k nın, simetrik dizaynın k parametresi ile karışmaması için, $boyC = r$ alınacaktır. Dolayısıyle, lineer $[v, r]-$kodundan söz edilecektir.

Buradan,

$$q^{r-1} = q^{v-r-1}$$

yazılabilir. Böylece,

$$r-1 = v-r-1$$

$$2r = v$$

$$r = \frac{v}{2}$$

elde edilir ki bu da v nin çift olması gerektiğini ifade eder.

Sonuç 4.1. F_q üzerinde $(v, k, \lambda)-$parametreli simetrik dizaynın ürettiği lineer $[v, r]-$kod C olsun. Eğer C nin $C^{\perp}$ dual kodunun sıfırdan farklı her kodsözcüğü minimal ise $k-\lambda$ bir tam karedir.

İspat. Önerme 4.2.'den, v çifttir. Schutzenberger Teoremi'ne (Teorem 1.1.1.) göre v çift ise $n = k-\lambda$, bir tam karedir.

Önerme 4.3. F_p üzerinde $(v, k, \lambda)-$parametreli simetrik dizayn D için $[v, r]-$kod C nin, $C^{\perp}$ dual kodunun sıfırdan farklı her kodsözcüğü minimal ise, C kodu üzerinde kurulan sır paylaşım şemasındaki minimal erişim küme sayısı $p^{\frac{v-2}{2}}$ dir.

İspat. Önerme 4.2.'den, F_p üzerinde $(v, k, \lambda)-$parametreli simetrik dizayn D için $[v, r]-$kod C nin $C^{\perp}$ dual kodunun, sıfırdan farklı her kodsözcüğü minimal ise,

$$r = \frac{v}{2}$$

dir.

$boyC^{\perp} = v - r$ olduğundan

$$boyC^{\perp} = v - \frac{v}{2}$$

$$= \frac{v}{2}$$

olur. Önerme 4.1.'den, C kodu üzerinde kurulan sır paylaşım şemasında tam olarak $p^{boyC^{\perp}-1}$ tane minimal erişim kümesi vardı. Buradan,

$$p^{boyC^{\perp}-1} = p^{\frac{v}{2}-1} = p^{\frac{v-2}{2}}$$

bulunur.

Önerme 4.4. Eğer $(v, k, \lambda)-$parametreli simetrik dizaynda $p \mid k - \lambda$ ve bu simetrik dizaynın F_p-kodu C nin, $C^{\perp}$ dual kodundaki sıfırdan farklı her kodsözcüğü minimal ise C kodu üzerinde kurulan sır paylaşım şemasındaki minimal erişim küme sayısı m olmak üzere,

$$p^{\frac{v-3}{2}} \leq m \leq p^{v-3}$$

tür.

İspat. $(v, k, \lambda)-$parametreli simetrik dizaynın F_p-kodu C için Teorem 2.2.5.1.i) gereğince,

$$p \mid k - \lambda \text{ ise } 2 \leq boyC \leq \frac{v+1}{2}$$

idi. $boyC = v - boyC^{\perp}$ olduğundan,

$$2 \leq v - boyC^{\perp} \leq \frac{v+1}{2}$$

eşitsizliğinden,

$$\frac{v-1}{2} \le boyC^{\perp} \le v-2$$

elde edilir. Buradan,

$$\frac{v-1}{2} - 1 \le boyC^{\perp} - 1 \le v-3$$

$$\frac{v-3}{2} \le boyC^{\perp} - 1 \le v-3 \quad (p \text{ asal})$$

$$p^{\frac{v-3}{2}} \le p^{boyC^{\perp}-1} \le p^{v-3}$$

bulunur. Yani

$$p^{\frac{v-3}{2}} \le m \le p^{v-3}$$

dır.

Önerme 4.5. Eğer $(v, k, \lambda)-$parametreli simetrik dizaynda $p \nmid k-\lambda$ ve $p \mid k$ ve bu simetrik dizaynın F_p-kodu C nin, $C^{\perp}$ dual kodundaki sıfırdan farklı her kodsözcüğü minimal ise bu simetrik dizaynın F_p-kodu C üzerinde kurulan sır paylaşım şemasında sadece bir minimal erişim kümesi vardır.

İspat. $(v, k, \lambda)-$parametreli simetrik dizaynın F_p-kodu C için Teorem 2.2.5.1.ii) gereğince,

$p \nmid k-\lambda$ ve $p \mid k$ ise $boyC = v-1$ dir.

Bu durumda, $boyC = v - boyC^{\perp}$ olduğundan,

$$boyC^{\perp} = v-(v-1) = 1$$

olur.

$(x_1, x_2, \cdots, x_v) \in C$ olmak üzere,

$$(x_1, x_2, \cdots, x_v)(1, 1, \cdots, 1) = x_1 + x_2 + \cdots + x_v = k$$

dır. $p \mid k$ olduğundan,

$$(x_1, x_2, \cdots, x_v)(1, 1, \cdots, 1) \equiv 0 \pmod{p}$$

elde edilir. Dolayısıyle $(\underbrace{11\cdots1}_{v \tan e}) \in C^{\perp}$ dir.

$(\underbrace{11\cdots1}_{v \tan e}) \in C^{\perp}$ ve $boyC^{\perp} = 1$ olduğundan $C^{\perp}$ dual kodu, $(\underbrace{11\cdots1}_{v \tan e})$ kodsözcüğü tarafından üretilir. $C^{\perp}$ dual kodundaki ilk koordinatı 1 olan minimal kodsözcükleri, minimal erişim kümelerini oluşturduğundan, buradaki minimal erişim kümesi yalnızca,

$$\{\underbrace{11...1}_{v \tan e}\}$$

dir. Gerçekten de Önerme 4.1. gereğince, C kodu üzerinde kurulan sır paylaşım şemasındaki minimal erişim küme sayısı,

$$p^{boyC^{\perp}-1} = p^{1-1} = p^0 = 1$$

dir. □

Yukarıdaki önermeden elde edilen sonuç, aşağıdaki gibi yorumlanabilir ki bu, oldukça önemlidir:

Önerme 4.5.'teki koşullar sağlandığında oluşturulacak olan minimal erişim kümesi yalnızca bir tane olduğundan, bu küme, sır paylaşımı için kullanışlı olmayabilir. Çünkü, bu minimal erişim kümesindeki katılımcılardan herhangi birinin kaybı, sırra erişimi olanaksız hale getirir.

Önerme 4.6. Eğer $(v, k, \lambda)-$parametreli simetrik dizaynda $p \nmid k-\lambda$ ve $p \mid k$ ve bu simetrik dizaynın F_p-kodu C nin, $C^{\perp}$ dual kodundaki sıfırdan farklı her

kodsözcüğü minimal ise, bu simetrik dizaynın F_p – kodu C üzerinde kurulan sır paylaşım şemasında minimal erişim kümesi yoktur.

İspat. (v, k, λ) – parametreli simetrik dizaynın F_p – kodu C için Teorem 2.2.5.1.iii) gereğince,

$$p \nmid k-\lambda \text{ ve } p \nmid k \text{ ise } boyC = v \text{ dir.}$$

Bu durumda; $boyC = v - boyC^{\perp}$ olduğundan,

$$boyC^{\perp} = v - v = 0$$

olur. Bu ise $C^{\perp} = \{\underbrace{00\cdots0}_{v \tan e}\}$ olması demektir. $C^{\perp}$ dual kodunda ilk koordinatı 1 olan minimal kodsözcüğü bulunmadığından, burada minimal erişim kümesinden söz edilemez. Gerçekten de Önerme 4.1. gereğince, C kodu üzerinde kurulan sır paylaşım şemasındaki minimal erişim küme sayısı hesaplanacak olursa,

$$p^{boyC^{\perp}-1} = p^{0-1} = p^{-1}$$

bulunur ki böyle bir minimal erişim küme sayısı olamaz. Böylece buradan da minimal erişim kümesinin varlığından söz edilemeyeceği görülür. □

Önerme 4.6.'dan, aşağıdaki sonuç elde edilir:

Eğer (v, k, λ) – parametreli simetrik dizaynda $p \nmid k-\lambda$ ve $p \nmid k$ ise, bu simetrik dizaynın F_p – kodu C nin, $C^{\perp}$ dual kodunun sıfırdan farklı tüm kodsözcükleri minimal olduğunda C üzerinde kurulan sır paylaşım şemasında minimal erişim kümesi olmadığından, sırra erişilemez.

4.1. (v, k, λ) – Parametreli Simetrik Dizayn ve Çakışım Matrisi

(v, k, λ) – parametreli simetrik dizayn D; A, bu dizaynın çakışım matrisi ve A nın satırları ile üretilen kod C olsun. Bu durumda;

$$AA^T = (k-\lambda)I + \lambda J$$

$$JA = AJ = kJ$$

eşitlikleri geçerlidir.

D nin tümleyeni olan D^c, $(v', k', \lambda') = (v, v-k, v-2k+\lambda)$ – parametreli simetrik dizayn, bu dizaynın çakışım matrisi B ve C^c ise B nin satırları ile üretilen kod olsun. Biliyoruz ki B, bir $v \times v$ matris olup; A matrisinde sıfırlar yerine 1, birler yerine 0 yazılarak elde edilir. Bu durumda,

$$BB^T = (k-\lambda)I + (v-2k+\lambda)J$$

$$BJ = JB = (v-k)J$$

eşitlikleri vardır.

Önerme 4.1.1. (v, k, λ) – parametreli simetrik dizayn D; A, bu dizaynın çakışım matrisi ve A nın satırları ile üretilen kod C olsun. D nin tümleyeni olan D^c, $(v', k', \lambda') = (v, v-k, v-2k+\lambda)$ – parametreli simetrik dizayn, bu dizaynın çakışım matrisi B ve C^c ise B nin satırları ile üretilen kod olsun. p bir asal sayı olmak üzere,

$p \mid k-\lambda$ ise $C^c \subseteq C^{\perp}$

dir.

İspat. B nin tanımından,

$$B = J - A$$

dır. İspat için,

$$AB^T = 0$$

olduğu gösterilmelidir.

$$AB^T = A(J - A)^T$$

$$= A(J - A^T)$$

$$= AJ - AA^T$$

$$= kJ - (k - \lambda)I - \lambda J$$

$$= (k - \lambda)J - (k - \lambda)I$$

$$= (k - \lambda)(J - I)$$

bulunur. $p \mid k - \lambda$ olduğundan

$$AB^T \equiv 0 \pmod{p}$$

dir.

Şu halde C^c nin kodsözcükleri, C nin sözcüklerine ortogonaldir. $C^\perp$ ise $(GF(p))^n$ uzayındaki C nin sözcüklerine dik vektörlerin tümünün kümesiydi. Böylece,

$$C^c \subseteq C^\perp$$

elde edilir. □

$(v', k', \lambda') = (v, v-k, v-2k+\lambda)$ – parametreli simetrik dizayn D^c nin B çakışım matrisinin satırları ile üretilen F_p – kod C^c için $p \mid k' - \lambda'$ olup, Teorem 2.2.5.1.i)'e göre,

$$2 \le boy C^c \le \frac{1}{2}(v+1)$$

dir.

Sonuç 4.1.1. $(v, k, \lambda)-$parametreli simetrik dizaynda p , bir asal sayı olmak üzere, $p \mid k-\lambda$, $(p, k)=1$ ve $p^2 \nmid k-\lambda$ ise $(p, k')=(p, v-k)=p$ dir.

İspat. $p \mid k-\lambda$ ise $k-\lambda=px$ (4.1.1.1.)

gibi $x \in Z^+$ vardır.

$(p, k)=1$ ise $pt+ks=1$ (4.1.1.2.)

gibi $t, s \in Z$ vardır.

(1.1.1.4.) gereğince,

$(v-1)\lambda=k(k-1)$

idi. Buradan,

$(v-1)\lambda=k^2-k$

$k-\lambda=k^2-v\lambda$

elde edilir.

$k-\lambda=px$ (4.1.1.1.) ifadesinden,

$k^2-v\lambda=px$

$k^2=px+v\lambda$ (4.1.1.3.)

bulunur.

Şimdi $pt+ks=1$ ifadesinin her iki yanı $v-k$ ile çarpılsın. Bu durumda,

$(v-k)pt+(v-k)ks=v-k$ (4.1.1.4.)

$vpt-kpt+vks-k^2s=v-k$

elde edilir. Burada k^2 yerine (4.1.1.3.)'ten, $k^2=px+v\lambda$ yazılsın. Yani,

$$vpt - kpt + vks - s(px + v\lambda) = v - k$$

$$p(vt - kt - sx) + vs(\underbrace{k - \lambda}_{px}) = v - k$$

$$p(vt - kt - sx) + pxvs = v - k$$

$$p(vt - kt - sx + xvs) = v - k$$

dır. Buradan,

$$p \mid v - k$$

elde edilir. Bu ise

$$(p,\ k') = (p,\ v - k)$$

$$= p$$

olması demektir.

4.2. Kodsözcüklerinin Minimal Olması

$(v,\ k,\ \lambda)$ – parametreli simetrik dizaynın kodu C nin, $C^{\perp}$ dual kodunun sıfırdan farklı kodsözcüklerinin minimal olup olmadığının bilinmesi, sır paylaşım şeması için oldukça önemlidir. Aşağıdaki özelik ile bu soruya yanıt vermekteyiz.

Teoerem 4.2.1. $(v,\ k,\ \lambda)$ – parametreli simetrik dizaynın ikili (binary) C kodunun $C^{\perp}$ dual kodundaki maksimum ağırlıklı bir kodun ağırlığı " w_{maks} " ile gösterilmek üzere, ikili (binary) $C^{\perp}$ dual kodunda

$$w_{maks} < \frac{2(k + \lambda)}{\lambda}$$

ise $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcükleri minimaldir.

İspat. Bir C kodu için $C^{\perp}$ dual kodu, yine lineer bir koddur. Ashikmin-Barg Teoremi'ne (Teorem 3.3.1.1.) göre, $C^{\perp}$ dual kodundaki sıfırdan farklı kodsözcüklerinin minimum ve maksimum ağırlıkları için eğer

$$\frac{w_{\min}}{w_{maks}} > \frac{q-1}{q}$$

ise $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcükleri minimaldir. $q = 2$ alınırsa ikili (binary) kod için,

$$\frac{w_{\min}}{w_{maks}} > \frac{1}{2}$$

ise ikili (binary) $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcükleri minimaldir.

Şu halde eğer

$$w_{maks} < \frac{2(k+\lambda)}{\lambda} \text{ ise } \frac{w_{\min}}{w_{maks}} > \frac{1}{2}$$

olduğu gösterilmelidir.

Yardımcı Teorem 3.3.1.1.'e göre, bir $2-(v,\, k,\, \lambda)$ dizaynın çakışım matrisi $A_{b\times v}$ olsun. Üreteç matrisi A olan ikili (binary) kodun dualinin minimum ağırlığı $w_{\min}$ için,

$$w_{\min} \geq \frac{(r+\lambda)}{\lambda}$$

dır. Burada r, bir noktanın bulunduğu blok sayısıdır.

Özel olarak $(v,\, k,\, \lambda)-$parametreli simetrik dizaynda $k = r$ olup, A matrisinin satırları ile üretilen C kodunun, $C^{\perp}$ dual kodunun minimum ağırlığı

$$w_{\min} \geq \frac{k+\lambda}{\lambda}$$

olur.

$$w_{maks} < \frac{2(k+\lambda)}{\lambda} \qquad (4.2.1.1.)$$

olsun. Bu durumda

$$\frac{1}{w_{maks}} > \frac{\lambda}{2(k+\lambda)} \qquad (4.2.1.2.)$$

dır. (4.2.1.2.) eşitsizliğinin her iki yanı $\frac{k+\lambda}{\lambda}$ ile çarpılırsa,

$$\frac{\frac{k+\lambda}{\lambda}}{w_{maks}} > \frac{1}{2} \qquad (4.2.1.3.)$$

elde edilir.

$$w_{\min} \geq \frac{k+\lambda}{\lambda}$$

idi. (4.2.1.3.) ifadesinde $\frac{k+\lambda}{\lambda}$ yerine $w_{\min}$ yazılırsa,

$$\frac{w_{\min}}{w_{maks}} > \frac{1}{2}$$

elde edilir. Bu da $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcüklerinin minimal olması demektir.

Teorem 4.2.2. (v, k, λ) – parametreli simetrik dizaynın çakışım matrisi A olmak üzere,

$$\begin{bmatrix} 1 & \vdots & \\ \vdots & \vdots & A \\ 1 & \vdots & \end{bmatrix}$$

matrisinin satırları ile üretilen ikili (binary) C kodunun $C^{\perp}$ dual kodunda eğer

$$w_{maks} < \frac{2(v+k)}{k}$$

ise $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcükleri minimaldir.

İspat. Yardımcı Teorem 3.3.1.2.'ye göre, bir $2-(v,\ k,\ \lambda)$ dizaynın çakışım matrisi $A_{b\times v}$ olsun. O zaman,

$$\begin{bmatrix} 1 & \vdots & \\ \vdots & \vdots & A \\ 1 & \vdots & \end{bmatrix}$$

matrisinin satırları ile üretilen ikili kodun duali için minimum ağırlık,

$$w_{\min} \geq \min\{\frac{b+r}{r},\ \frac{r+\lambda}{\lambda}\} \qquad (4.2.2.1.)$$

dır. $(v,\ k,\ \lambda)-$parametreli simetrik dizayn için $k=r$, $b=v$ alınırsa, (4.2.2.1.) eşitsizliği,

$$w_{\min} \geq \min\{\frac{v+k}{k},\ \frac{k+\lambda}{\lambda}\} \qquad (4.2.2.2.)$$

haline gelir. Burada da $k>\lambda$ olduğundan,

$$\frac{v+k}{k} < \frac{k+\lambda}{\lambda}$$

dır. Gerçekten,

$$\frac{k+\lambda}{\lambda} - \frac{v+k}{k} = \frac{k(k+\lambda)-\lambda(v+k)}{k\lambda}$$

$$= \frac{k^2-\lambda v}{k\lambda}$$

$$= \frac{k-\lambda}{k\lambda}$$

$$> 0$$

dır.

Yani

$$\min\{\frac{v+k}{k},\ \frac{k+\lambda}{\lambda}\} = \frac{v+k}{k}$$

dır. Şu halde

$$w_{\min} \geq \frac{v+k}{k}$$

elde edilir. Buradan,

$$\frac{w_{\min}}{w_{maks}} \geq \frac{\frac{v+k}{k}}{w_{maks}} \qquad (4.2.2.3.)$$

bulunur.

$$w_{maks} < \frac{2(v+k)}{k}$$

kabul edelim. Bu durumda,

$$\frac{1}{w_{maks}} > \frac{k}{2(v+k)} \qquad (4.2.2.4.)$$

olur. (4.2.2.4.) eşitsizliğinin her iki yanı $\frac{v+k}{k}$ ile çarpılırsa

$$\frac{\frac{v+k}{k}}{w_{maks}} > \frac{1}{2} \qquad (4.2.2.5.)$$

elde edilir. (4.2.2.3.) ve (4.2.2.5.)'ten,

$$\frac{w_{\min}}{w_{maks}} > \frac{1}{2}$$

bulunur. İspatlanması gereken de budur. □

Bu çalışmada, IV. bölümde sunulan aşağıdaki sonuçlar elde edilmiştir:

$(v, k, \lambda)-$parametreli simetrik dizaynın F_p $-$kodu C nin, $C^{\perp}$ dual kodunun sıfırdan farklı tüm kodsözcükleri minimal olmak üzere C kodu üzerinde kurulan sır paylaşım şemasındaki,

i) $p \mid k-\lambda$ iken

ii) $p \nmid k-\lambda$ ve $p \mid k$ iken

minimal erişim küme sayıları araştırılmıştır.

$(v, k, \lambda)-$parametreli D simetrik dizaynının tümleyeninin kodu (C^{c}) ile söz konusu dizaynın kodunun dual kodu $(C^{\perp})$ arasındaki ilişki bulunmuştur.

$(v, k, \lambda)-$parametreli simetrik dizaynın ikili (binary) C kodunun $C^{\perp}$ dual kodundaki sıfırdan farklı kodsözcüklerinin w_{maks}'a bağlı minimal olma durumları araştırılmış ve $(v, k, \lambda)-$parametreli simetrik dizaynın çakışım matrisi A olmak üzere,

$$\begin{bmatrix} 1 & \vdots & \\ \vdots & \vdots & A \\ 1 & \vdots & \end{bmatrix}$$

matrisinin satırları ile üretilen ikili (binary) C kodunun $C^{\perp}$ dual kodunda $w_{maks} < \dfrac{2(v+k)}{k}$ ise $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcüklerinin minimal olduğu belirlenmiştir.

ÖZGEÇMİŞ

Adı-Soyadı	**:** Selda Çalkavur
Doğum Tarihi	**:** 07. 11. 1978
Doğum Yeri	**:** Erzincan
İlkokul	**:** 1984-1987, Hürriyet İlkokulu (Kütahya) 1987-1989, Azot İlkokulu (Kütahya)
Ortaokul	**:** 1989-1992, Kütahya Lisesi (Kütahya)
Lise	**:** 1992-1993, Kütahya Lisesi (Kütahya) 1993-1995, Atatürk Lisesi (Van)
Lisans	**:** 1996-2000, Dumlupınar Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü
Yüksek Lisans	**:** 2004-2006, İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü Matematik-Bilgisayar Ana Bilim Dalı Matematik-Bilgisayar Programı
Doktora	**:** 2006-2010, İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü Matematik-Bilgisayar Ana Bilim Dalı Matematik Programı
Çalıştığı Kurum	**:** 2000-(Devam ediyor.) İHKİB Yenibosna Kız Teknik ve Meslek Lisesi
Görevi	**:** Matematik Öğretmeni
Mesleki Kuruluşlara Üyelikler	**:** Türk Matematik Derneği