T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AYRIK SONLU YAPILARDAN HATA DÜZELTEN KOD ELDE ETME

YÜKSEK LİSANS TEZİ

Necati AYAZ

Enstitü Anabilim Dalı : MATEMATİK

Tez Danışmanı : Doç. Dr. Mehmet ÖZEN

Şubat 2011

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AYRIK SONLU YAPILARDAN HATA DÜZELTEN KOD ELDE ETME

YÜKSEK LİSANS TEZİ

Necati AYAZ

Enstitü Anabilim Dalı : MATEMATİK

Bu tez 04 / 02 /2011 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof.Dr.İrfan ŞİAP	Doç.Dr.Mehmet ÖZEN	Yrd.Doç.Dr.İbrahim ÖZGÜR
Jüri Başkanı	Üye	Üye

TEŞEKKÜR

Tezin hazırlanma aşamasında bana her türlü desteği veren danışman hocam Doç. Dr. Mehmet ÖZEN'e, hayatım boyunca maddi ve manevi desteklerini esirgemeyen aileme ve bu tez çalışmasında bana yardımlarını esirgemeyen arkadaşlarıma teşekkür ediyorum.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

C	: Kod
$C^{\perp}$	: Düal kod
D	: Çakışım yapısı (tasarım)
D_p	: p noktasıyla ilgili kısıtlanmış tasarım
D^p	: p noktasıyla ilgili artık tasarım
$\det N$	: Çakışım matrisinin determinatı
$d(x, y)$	: x ve y sözleri arasındaki hamming uzaklığı
I_n	: $n \times n$ boyutlu birim matris
J	: $n \times n$ boyutlu ve tüm elemanları 1 olan matris
N	: Çakışım matrisi
N^T	: Çakışım matrisin devriği
(Q, o)	: Yarı grup
R	: Jacobsthal matris
$rankN$	:Çakışım matrisinin rangı
$\text{supp}(x)$	: x sözünün destekleyicisi
$S(x, r)$	: x merkezli r yarıçaplı küre
$V(n, F)$	: F cismi üzerindeki n boyutlu vektör uzayı
$w(x)$	: x sözünün ağırlığı
$W_C(x, y)$	: C kodunun ağırlık sayacı
$A \otimes B$	: Kronecker çarpımı
ζ	: F cisminin primitif elemanı
λ_t	: t elemanlı alt kümeyi içeren blok sayısı
χ	: Legendre sembolü

$2-(v,b,r,k,\lambda)$	: Parametreleri v,b,r,k,λ olan 2- tasarım
$\binom{n}{k}$	: n elemanlı kümeden k elemanlı alt küme seçme
$\begin{bmatrix} n \\ k \end{bmatrix}_q$	: n boyutlu vektör uzayındaki k boyutlu alt uzaylarının sayısı
$\langle x, y \rangle$	: iç çarpım işlemi
$[n,k,d]$	: n uzunluğunda , k boyutlu ve minimum uzaklığı d olan lineer kod
DTBT	: Dengeli Tamamlanmamış Blok Tasarımı
$[\![(d-1)/2]\!]$	: Tam Değer
$\left\|S_q(n,r)\right\|$	: n merkezli r yarıçaplı kürenin elaman sayısı
$py(C)$	: küre paketleme yarıçapı
$oy(C)$	: küre örtme yarıçapı
$AG(n,q)$	: q boyutlu ve n mertebeli afin düzlem
$PG(n,q)$	: q boyutlu ve n mertebeli projektif düzlem
MOLS	: Mutually Orthogonal Latin Squares

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Lineer kod, t-Tasarımlar, Hadamard matrisleri, Projektif ve Afin düzlemler, Fark kümeleri, Latin kareler, Dik dizimler.

Beş bölüm halinde düzenlenen bu çalışmanın birinci bölümünde gerekli cebirsel tanımlar, teoremler ve lineer kodlarla ilgili bilgiler verilmektedir.
İkinci bölümde tasarım teorisi hakkında temel tanım ve teoremler verildi. Ayrıca tasarımlar için metotlar incelendi ve bunlarla ilgili örnekler verildi.
Üçüncü bölümde projektif ve afin düzlem, fark kümeleri ve Latin kareler hakkında temel tanım ve teoremler verildikten sonra, bunların birbirleri ile ilişkileri incelendi.
Dördüncü bölümde sonlu vektör uzayında elde edilen tasarımlar verildi. Bunlarla ilgili örnekler oluşturuldu.
Beşinci bölümde tasarım teorisinden elde edilen bazı kodlar verildi. Özellikle simetrik tasarımdan elde edilen kodlar üzerinde duruldu. Ayrıca Latin kare ve Hadamard matrisinden elde edilen kodlarda verildi. Tasarımlardan kod elde etmeye ve kodlardan tasarım elde etmeye örnekler verildi.

OBTAINING ERROR CORRECTING CODES FROM DISCRETE FINITE STRUCTURES

SUMMARY

Keywords: Linear codes, t-designs, Hadamard Matrix, Projective and Affine planes, Difference sets, Latin squares, Orthogonal arrays.

This study consists of five chapters. In the first chapter, there is information about necessary algebraic definitions, theorems for linear codes.
In the second chapter, basic definitions and theorems about design theory are introduced. Moreover, methods for designs are examined and examples related to this are given.
In the third chapter, after basic definitions and theorems about projective and affine planes, difference sets and Latin squares are introduced, their relationships between each other and design theory are examined.
In the fourth chapter, designs which are obtained from finite vector spaces and examples of these are presented.
In the fifth chapter, some codes which are obtained from the design theory are given. Especially the codes which are obtained from the symmetric designs are determined. In addition, the codes which are obtained from Latin squares and Hadamard matrixes are also given. Finally, some examples of codes from designs and vice versa are illustrated.

BÖLÜM 1. GİRİŞ

1.1. Cebirsel Tanımlar

Tanım1.1.1: $K \neq \emptyset$ kümesinin elemanlarından oluşan her sıralı ikiliye K de bir ve yalnız bir eleman karşılık getiren bir fonksiyona K üzerinde bir ikili işlem denir. Bu işlem $*$ sembolü ile gösterildiğinde;

$$K \text{ x } K \rightarrow K$$

$$(\text{ a,b}) \rightarrow \text{a} * \text{ b}$$

ile tanımlanır.

Tanım1.1.2: G bir küme ve $*, G$ de tanımlı bir ikili işlem olsun. Eğer aşağıdaki özellikler $*$ işlemi tarafından sağlanıyorsa $(G,*)$ ikilisine bir grup denir.

1) $\forall a,b,c \in G$ için $(a*b)*c = a*(b*c)$.
2) $\forall a \in G$ için $a*e = e*a = a$ olacak biçimde bir $e \in G$ vardır .
3) $a \in G$ için $a*a' = a'*a = e$ olacak bicimde $a' \in G$ vardır.(a', a'nın tersidir.)

Ayrıca , $\forall a,b,c \in G$ için $a*b = b*a$ sağlanıyorsa G ye bir değişmeli (Abel) grup denir. Eğer sadece birinci özellik sağlanırsa G ye yarı grup denir.

Tanım1.1.3: G bir grup ve $\emptyset \neq H \subseteq G$ olsun. Eğer H , G deki işleme göre kendi başına bir grup ise H ye, G'nin bir alt grubu denir ve $H \leq G$ ile gösterilir. G sonlu bir küme ise G ye sonlu grup denir. G'nin elemanlarının sayısına G'nin mertebesi denir.

Tanım1.1.4: $R \neq \varnothing$ kümesi üzerinde tanımlı iki ikili işlem '+' ve '.' olsun. Aşağıdaki aksiyomları sağlayan $(R,+)$ cebirsel yapısına bir halka denir.

H1: $(R,+)$ bir değişmeli gruptur.

H2: '.' işleminin R de birleşme özelliği vardır.

H2: '.' İşleminin '+' işlemi üzerine sağdan ve soldan dağılma özellikleri vardır.

Tanım1.1.5: Bir halkada çarpma işlemi değişmeli ise bu halkaya değişmeli halka denir. Bir R halkasında $\forall x \in R$ için $1.x = x.1$ olacak biçimde 1 elemanı varsa R ye birimli halka denir. R birimli bir halka olsun. $u \in R$ nin, R de tersi varsa u ya R nin bir tersinir (birimsel) elamanı denir.

Tanım1.1.6: R değişmeli, birimli bir halka ve $\forall u \in R - \{0\}$ elemanı tersinir ise R ye bir cisim denir. Sonlu tane elemanı olan cisme sonlu cisim denir ve $GF\left(p^n\right)$ yada F_q ile gösterilir. Burada p asal ve n pozitif bir tamsayıdır.

Tanım1.1.7: $(V,+)$ bir abel grup F bir cisim olsun. Skaler ile çarpma işlemleri ".": $F \times V \to V$ her $a \in F$, $v \in V$ için, $(a,v) = av$ ile tanımlı ve aşağıdaki her $u, v \in V$; $a, b \in F$ için

1) $a(u+v) = au + av$

2) $(ab)u = a(bu)$

3) $(a+b)u = au + bu$

4) $1.u = u$ burada 1, F 'nin çarpımsal birimini göstermektedir.

Şartları sağlanırsa V ye F cismi üzerinde vektör uzayı denir. Eğer cismimiz q elemanlı ise vektör uzayımız kısaca $V(n,q)$ ile gösterilir.

Tanım1.1.8: V , F cismi üzerinde bir vektör uzayı ve W , V nin boş olmayan bir alt kümesi olsun. Eğer W , V yi F üzerinde vektör uzayı kılan işlemlere göre F üzerinde bir vektör uzayı ise W ya V nin bir alt uzayı denir.

1.2.Lineer Kodlar

Tanım1.2.1: $A=\{a_1,a_2,...,a_q\}$ sonlu bir küme olsun. Bu kümeye alfabe denir. A^n ise A kümesinden alınan n-lileri temsil etsin ve A^n in herhangi bir C alt kümesine q-lu blok kodu denir. C nin sözlerine kodsöz denir. Eğer $C\subset A^n$ nın M tane elemanı varsa, C ye n uzunluğunda, M elemanlı bir kod denir ve C ye kısaca (n,M)-kodu denir.

Tanım 1.2.2: C_1 ve C_2 q-lu birer (n,M) kod olsun.

$c_1c_2...c_n\in C_1 \Leftrightarrow \pi_1\left(c_{\delta(1)}\right)\pi_2\left(c_{\delta(2)}\right),...,\pi_n\left(c_{\delta(n)}\right)\in C_2$ olacak şekilde n koordinat yerleri üzerinde bir δ permütasyonu ve alfabe üzerinde $\pi_1,\pi_2,...,\pi_n$ permütasyonları varsa C_1 ile C_2 kodları denktir.

Tanım 1.2.3: x ve y aynı uzunlukta , aynı alfabe üzerinde tanımlanmış n-liler olsun. x ve y'nin farklı bileşenlerinin sayısına Hamming uzaklığı denir ve $d(x,y)$ ile gösterilir. Yani $x=(x_1,x_2,x_3,...,x_n)$ ve $y=(y_1,y_2,y_3,...,y_n)$ ise $d(x,y)=\left|\{i\,|x_i\neq y_i\}\right|$ olur.

Tanım 1.2.4: $d(C)=\min_{c,d\in C,c\neq d} d(c,d)$ sayısına C kodun minimum uzaklığı denir.

n uzunluğunda, M eleman sayısına sahip ve minimum uzaklığı d olan bir kod kısaca (n,M,d)- kodu ile gösterilir.

Teorem 1.2.1: A^n, A alfabesinden oluşan n-lilerin kümesi olsun. Hamming uzaklığı aşağıdaki özelliklere sahiptir. Her bir $x,y,z\in A^n$ için,

1.) $d(x,y)\geq 0$ (pozitif tanımlı) ve $d(x,y)=0\Leftrightarrow x=y$

2) $d(x,y)=d(y,x)$ (simetri)

3) $d(x,y)\leq d(x,z)+d(z,y)$ dir.(üçgen eşitsizliği)

(A^n, d) ikilisine metrik uzay denir[1].

Tanım 1.2.5: Eğer C kodu bir $V(n,q)$ vektör uzayının alt uzayı ise C koduna bir lineer kod denir. C'nin $V(n,q)$ üzerinde boyutu k ise C 'ye bir [n, k]- kodu denir. C'nin minimum mesafesi d ise C'ye $[n,k,d]$-kodu denir.

Tanım 1.2.6: Eğer C kodun bir kodsözünde en az bir ve en fazla t - hata meydana geldiğinde bu yeni söz kodsöz değilse bu koda t -hata tespit eden kod denir. Eğer C t -hata tespit eden fakat $t+1$ hata tespit etmeyen kod ise bu C koduna tam t -hata tespit eden kod denir.

Teorem 1.2.2: C kodu tam t -hata tespit etmesi için gerek ve yeter koşul $d(C) = t+1$ olmasıdır[1].

Örnek 1.2.1: $C = \{(0,0,0),(1,1,1)\}$ olsun. $d(C) = 3$ olduğundan C kodsözü tam 2 hata tespit eden bir koddur.

Tanım 1.2.7: Bütün eşitlik durumlarının hata olarak tespit edildiğini farz edersek, minimum uzaklık dekodlama eğer t veya daha az büyüklükteki hataları düzeltiyorsa bu C koduna t -hata düzelten fakat $t+1$ hata düzeltmeyen ise bu koda tam t -hata düzelten kod denir.

Teorem 1.2.3: C bir $[n,k,d]-$ kodu ise C kodu tam t hata düzelten olması için gerek ve yeter koşul $d = 2t+1$ veya $d = 2t+2$ olacak şekilde bir $t \in \mathbb{Z}$ olmasıdır. C koduna $t-$ hata düzelten kod denir[1].

Sonuç 1.2.1: $d(C) = d$ olması için gerek ve yeter şart C'nin tam $[\![(d-1)/2]\!]$ hata düzelten kod olmasıdır.

Tanım 1.2.8: x, A^n' nin bir sözü ve r de negatif olmayan bir tamsayı olsun. $S_q(x,r)=\{y\in A^n : d(x,y)\le r\}$ kümesine x merkezli r yarıçaplı küre denir.Kürenin hacmi $H_q(n,r)$ ise $S_q(x,r)$ kümesinin eleman sayısına eşittir. Bu hacim merkezden bağımsızdır. $H_q(n,r)=\sum_{k=0}^{t}(\binom{n}{k})(q-1)^k$ ve $H_q(n,r)=\left|S_q(n,r)\right|$ ile hesaplanır.

Tanım 1.2.9: $C\subset A^n$ kod olsun. Bütün C kod merkezli $S_q(c,r)$ kürelerin birbirleriyle ile ayrık olacak şekildeki en büyük r pozitif tamsayısına C'nin paketleme yarıçapı denir. $A^n=\underset{c\in C}{\cup} s_q(c,r)$ sağlayan en küçük r pozitif tamsayısına ise C kodunun örten yarıçapı denir. Paketleme yarıçapı $py(C)$ ve örten yarıçapı ise $oy(C)$ ile gösterilir.

Tanım 1.2.10: Eğer $py(C)=oy(C)$ ise C koduna mükemmel bir kod denir. Başka bir deyişle C merkezli ayrık $S_q(c,r)$ kürelerinin A^n'ni örtecek bir r tamsayısı varsa $C\subset A^n$ koduna bir mükemmel kod denir.

Örnek 1.2.2: $H_2(3)$ ile adlandırdığımız Hamming kodunu düşünelim. Bu kod (7, 16, 3) kodudur. $d=2t+1\Rightarrow t=1$ hata düzelten koddur. O halde kürenin hacmi $H_2(7,r)=H_2(7,1)=\sum_{k=0}^{1}(\binom{7}{k}).(2-1)^k=H_2(7,1)=(\binom{7}{0})+(\binom{7}{1})1=8$ ve $\left|A^n\right|=2^n=2^7=128$ söz vardır. $\left|C\right|=16$ olduğundan 16.8=128 olur. Bu da Hamming kodunun mükemmel olduğunu gösterir.

Teorem 1.2.4: (Küre Paketleme Şartı) C bir q-lu (n,M,d) kod olsun. C kodunun mükemmel bir kod olması için gerek ve yeter koşul $d=2t+1$ şeklinde bir tek sayı ve $M.V_q(n,t)=q^n$ yani $M=\dfrac{q^n}{\sum_{k=0}^{t}(\binom{n}{k})(q-1)^k}$ şartının sağlanmasıdır[1].

Tanım 1.2.11: Bir $c \in V(n,q)$ vektörünün $w(c)$ ile gösterilen (Hamming) ağırlığı o vektörün sıfırdan farklı olan bileşenlerinin sayısına eşittir. Bir C kodunun minimum ağırlığı $w(C)$ o kodun sıfırdan farklı vektörlerin ağırlığının en küçüğüdür.

Lineer kodların önemli bir özelliği ise $d(C) = w(C)$ olmasıdır. Yani lineer bir kodun minimum uzaklığı minimum ağırlığa eşittir.

Örnek 1.2.3:

1) x=100 1101 için w(x)=4,
2) x= 1101111 için w(x)=6,
3) x= 0000010 için w(x)=1.

Tanım 1.2.12: C, n uzunluğunda bir kod olsun. C kodunda ağırlığı i olan kod sözlerin sayısı A_i olsun.

$A_i = |\{c \mid w(c) = i, c \in C\}|$ olmak üzere,

$$W_c(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)} = \sum_{i=1}^{n} A_i x^{n-i} y^i$$

polinomuna C kodunun Hamming ağırlık sayacı denir.

Tanım 1.2.13: C bir q-lu (n,M,d) kodu olsun.

$\widetilde{C} = \left\{ (c_1, c_2, ..., c_n, c_{n+1}) \middle| (c_1, c_2, ..., c_n) \in C, \sum_{k=1}^{n+1} c_k = 0 \right\}$ şeklinde tanımlanan koda C 'nin uzatılmış kodu denir.

1.2.1. Lineer kodun üreteç matrisi

Bir lineer kod bir vektör uzayı olduğundan, lineer kod vektör uzayın tabanı kullanılarak tanımlanabilir.

Tanım 1.2.1.1: C bir $[n,k]$ kodu olsun. Satırları C nin bir tabanı olan $k \times n$ tipindeki D matrisine C kodunun üreteç matrisi denir. C kodunu üreten D matrisi elementer satır veya sütün işlemleri yapılarak $G = (I_k | A)$ formunda yazılabilir. D ye denk olan bu G matrisine C kodunun standart form matrisi denir. Burada I_k, k boyutlu birim matristir.

1.2.2. Lineer kodlar ve düalleri

Tanım 1.2.2.1: $V(n,q)$ bir vektör uzayı, $u = (u_1, u_2, ..., u_n), v = (v_1, v_2, ..., v_n) \in V(n,q)$ olmak üzere u ve v nin iç çarpımı; $< u, v >= u_1 v_1 + ... + u_n v_n$ şeklinde tanımlanır.

Tanım 1.2.2.2: C bir $[n,k]$ lineer kodu olsun. $C^{\perp} = \{x \in V(n,q) :< x, c >= 0, \forall c \in C\}$ kümesine C 'nin düal kodu denir.

Teorem 1.2.2.1:

1) $G = (I_k \mid A)$ matrisi C kodu için bir üreteç matris ve $x \in V(n,q)$ olsun. $x \in C^{\perp}$ olması için gerekli ve yeterli koşul $x.G^T = 0$ olmasıdır.
2) Bir lineer kodunun düali olan $C^{\perp}$ kodu da bir $[n, n-k]$ lineer koddur.
3) Her lineer C kodu için $(C^{\perp})^{\perp} = C$ olur [1].

Eğer $C, [n,k]$ lineer kodunun üreteç matrisi $k \times n$ boyutlu G matrisinin standart formu $G = (I_k \mid A)$ ise $C^{\perp}$ in üreteç matrisi $H = (-A^T | I_{n-k})$ olur. H matrisine C kodunun kontrol (parity check) matrisi de denir.

$GH^T = \left(I_k \middle| A\right)\left(\begin{matrix}-A \\ I_{n-k}\end{matrix}\right) = -A + A = 0$. Bu ise H matrisinin satırlarının G matrisinin satırlarına dik olduğunu gösterir.

Tanım 1.2.2.3: Eğer $C \subset C^{\perp}$ ise C lineer koduna kendine dik kod denir. Eğer $C = C^{\perp}$ ise C'ye kendine düal kod denir.

Teorem 1.2.2.2: C bir $[n,k]$- binary lineer kod ve $C^{\perp}$ onun düal kodu olsun. O zaman $W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$ [1].

Teorem 1.2.2.3: Kendine dual q-lu bir $[n, n/2]$-kodun olması için gerekli ve yeterli koşul aşağıdaki koşullardan birinin sağlanmasıdır:

1) q ve n nin birer çift sayı olmaları,
2) $q \equiv 1 \bmod 4$ ve n çift bir sayı,
3) $q \equiv 3 \bmod 4$ ve n 4 ile bölünebilirdir[1].

BÖLÜM 2. TASARIMLAR

2.1. Tasarım

Tanım 2.1.1: D çakışım yapısı (incidence structure) P noktalar kümesi ve B de bloklar kümesi olmak üzere P ve B 'yi birbirine bağlayan bir bağıntıdan oluşur.

Tanım 2.1.2: P bir nokta ve B de bir blok olmak üzere (P,B) ikilisine bir flag adı verilir.

Tanım 2.1.3: Çakışım yapısının matrisi olan N 'ye çakışım matrisi denir. N matrisinin satırlarını sıralı noktalar kümesi, sütunları ise sıralı bloklar kümesi olmak üzere;

$$N=(n_{ij}) \quad i\in\{1,2,3,4,...,v\},$$

$$j\in\{1,2,3,4,...,b\} \text{ ve}$$

$$n_{ij}=\begin{cases} 1 & \mathrm{x_i}\in B_j \\ 0 & \mathrm{x_i}\notin B_j \end{cases}$$

şeklinde tanımlanır. Burada b blokların sayısını, v de noktaların sayısını gösterir.

Tanım 2.1.4: Bir çakışım yapısında her bir blok tam olarak k nokta içeriyorsa bu tasarıma düzgün tasarım denir.

Tanım 2.1.5: Bir tasarımda noktaların $t-$elemanlı her alt kümesi blokların tam olarak λ bloğunda varsa bu tasarıma $t-$tasarım veya $t-(v,k,\lambda)$ tasarımı denir. Buradaki t sayısını da λ_t ile gösterilir.

Tanım 2.1.7: Bir çakışım yapısında P nokta kümelerinin tüm k elemanlı alt kümelerinden oluşan bloklar kümesine tam tasarım denir.

Tam tasarımda nokta sayısı v , her bir bloğun eleman sayısı k ve $\lambda_t = \begin{pmatrix} v-t \\ k-t \end{pmatrix}$ olur.

2.2. Parametreler Hakkında Teoremler

n pozitif bir tamsayı olmak üzere, bu bölümde J matrisi $n\times n$ boyutlu ve tüm elemanları 1 olan matris ve I da $n\times n$ boyutlu birim matristir.

Teorem 2.2.1: D bir çakışım yapısı ve N de onun çakışım matrisi olsun. O zaman

1) D'nın bir tasarım olması için gerekli ve yeterli koşul $JN = kJ$ olmasıdır. (burada k bloğun eleman sayısıdır.)
2) D'nın bir $1-$tasarım olması için gerekli ve yeterli koşul $JN = kJ, NJ = rJ$ olacak şekilde k, r tamsayıların var olmasıdır. (r burada verilen noktayı içeren blok sayısı ve k da bloğun eleman sayısıdır.)
3) D'nın bir $2-$tasarım olması için gerekli ve yeterli koşul $JN = kJ$ ve $N.N^T = (r-\lambda)I + \lambda J$ olacak şekilde r,k,λ tam sayıların var olmasıdır. (λ verilen nokta çiftini içeren blok sayısıdır.)[3].

İspat: 1) D bir tasarım olsun. D tasarımın da her blok k noktaya sahiptir. D çakışım yapısının çakışım matrisi de N olsun. $JN = (b_{ij})$ matrisini göz önüne alalım.

$i \in \{1,2,3,4,...,v\}$ ve $j \in \{1,2,3,4,...,b\}$ olmak üzere a_{ij} elemanı j blokta k tane noktaya sahip olur. Böylece $JN = kJ$ olur. Tersine $JN = kJ$ olsun bu durum ise her bir bloktaki nokta sayısının k tane olduğunu gösterir. O halde D bir tasarım olur.

2) D'nın $1-$tasarım olduğunu kabul edelim. D tasarım olduğundan (1) öncülden) $JN = kJ$ 'dir. D, $1-$tasarım olduğundan verilen noktayı içeren blokların sayısı sabittir ve bu sayı r olsun. $NJ = (b_{ij})$ matrisini göz önüne alalım. Burada $i \in \{1,2,3,4,...,v\}$ ve $j \in \{1,2,3,4,...,b\}$ o zaman b_{ij}, i inci noktayı içeren blokların sayısı r dir. Buradan $NJ = rJ$ (k ve r sayıları için sağlanır.) Tersine $JN = kJ$ olduğundan (1) öncülden) D'nin bir tasarım olmasını gerektirir. Ayrıca verilen noktayı içeren blok sayısı sabit ve bu sayı r dir. O yüzden D $1-$tasarım olur.

3) D'nın $2-$tasarım olduğunu kabul edelim. O halde $JN = kJ$'dir. Şimdi $N.N^T = (c_{ij})$ matrisinde; $i \in \{1,2,3,4,...,v\}$ ve $j \in \{1,2,3,4,...,v\}$ için, c_{ii} elemanı i noktasını içeren blokların sayısıdır. Bu yüzden $N.N^T$ matrisinin köşegen elemanları r olur. $i \neq j$ için c_{ij}, P_i ve P_j noktalarını içeren blokların sayısı olsun. Bu iki noktayı içeren blokların sayısı λ olsun. Bu yüzden $c_{ij} = \lambda$ ve her $i \neq j$ için $N.N^T = (r-\lambda)I + \lambda J$ dır. Tersine $JN = kJ$ olduğundan D bir tasarım olur. Ayrıca $N.N^T = (r-\lambda)I + \lambda J$ olması da verilen nokta çiftini içeren blok sayısının λ olmasıdır. O halde D bir $2-$tasarım olur.

$2-$tasarım da v nokta, b blok, her nokta r blokta, her blok k noktaya sahip ve verilen iki nokta tam olarak λ blokta bulunur. Bu tasarımı $2-(v,b,r,k,\lambda)$ parametreleriyle ile gösterilir.

Teorem 2.2.2: D bir $2-(v,b,r,k,\lambda)$ tasarımı olsun. O zaman aşağıdakiler denktir.

1) $vr = bk$
2) $\lambda(v-1) = r(k-1)$ olur[3].

1 Kanıtlamak için;

$\{(P,\ell): P \in \ell \in B\}$ kümesini iki şekilde sayılır.

Birinci sayım: Birinci koordinat için v seçenek vardır. Birinci koordinat v seçenek arasından P seçildiğinde, ikinci koordinat P'yi içeren herhangi bir blok olabilir ve bunlardan r tane vardır. Demek ki kümenin elaman sayısı vr 'dir.

İkinci sayım: İkinci koordinat için b seçenek arasından ℓ seçildiğinde, birinci koordinat ℓ'deki herhangi bir nokta olabilir ve bunlardan k tane var. Demek ki kümenin eleman sayısı bk'dır. Yukarıdaki iki hesaptan $vr = bk$ çıkar.

2) İspat: P bir nokta ve r_p , P'yi içeren blokların sayısı olsun. Sabit bir P noktası için , $\{(Q,\ell): P \neq Q \in \ell \in B, P \in \ell\}$ kümesinin elemanları iki değişik şekilde sayalım. Bu eşitlikten faydalanarak sonuca gidelim.

Birinci sayım: Birinci koordinat P'den değişik herhangi bir nokta olabileceğinden, birinci koordinat için $v-1$ tane seçeneğimiz var. Birinci koordinat Q seçildikten sonra ikinci koordinat P ve Q noktalarını içeren bloktan seçilmelidir. Demek ki birinci koordinat seçildiğinde ikinci koordinat için λ seçenek var. Dolayısıyla kümenin eleman sayısı $(v-1)\lambda$ olur.

İkinci sayım: İkinci koordinat P'yi içeren herhangi bir bloktan seçileceğinden, ikinci koordinat için r_p seçeneğimiz var. Bu bloklardan biri, diyelim ℓ, ikinci koordinat olarak seçildiğinde, birinci koordinat ℓ'nin P'den değişik herhangi bir noktası olabilir. Dolayısıyla birinci koordinat seçildiğinde $k-1$ seçeneğimiz var. Demek ki kümenin elaman sayısı $r_p(k-1)$dir.

Yukarıdaki iki sayımdan $(v-1)\lambda = r_p(k-1)$ olur. P noktası ne olursa olsun, r_p değişmeyeceğinden r_p yerine r diyelim. O halde; $(v-1)\lambda = r(k-1)$ olur.

2) Şıkkı farklı bir yoldan aşağıdaki gibide ispatlanabilir.

B bloğu içinde olan birbirinden farklı iki nokta P_1 ve P_2 olsun. $\left(\{P_1, P_2\}, B\right)$ nokta ikililerini iki farklı yoldan hesaplayalım.

$$b\binom{k}{2} = \lambda\binom{v}{2} \tag{2.2}$$

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

$b.k = vr$ dir.

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

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

$$\frac{r}{\lambda} = \frac{v-1}{k-1}.$$

(2.3)

O halde 2 tasarımını $2-(v,k,\lambda)$ parametreleri belirler, bu yüzden $2-(v,b,r,k,\lambda)$ yerine $2-(v,k,\lambda)$ gösterimini kullanılır.

Sonuç 2.2.1: D bir $2-(v,b,r,k,\lambda)$ tasarımı olsun. O zaman aşağıdaki ifadeler sağlanır[4].

1) $r \geq \lambda$

2) $r = \lambda \Leftrightarrow v = k$

İspat 1) $\frac{v-1}{k-1}=\frac{r}{\lambda}\ v\geq k$ olduğundan

$v-1\geq k-1$ olur.

Ayrıca $\lambda(v-1)=r(k-1)$ idi.

$v-1\geq k-1$ olduğundan

$r\geq\lambda$ olur.

İspat 2) $r=\lambda$ ise $r(v-1)=\lambda(k-1)$

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

$\Leftrightarrow v-1=k-1\Leftrightarrow v=k$ olur.

Önerme 2.2.1: $v\times v$ boyutlu $(r-\lambda)I+\lambda J$ matrisinin determinantı

$(r-\lambda)^{v-1}(r+(v-1)\lambda)$ dır[5].

İspat: $(r-\lambda)I+\lambda J$ matrisini göz önüne alalım.

$$(r-\lambda)I+\lambda J=\begin{bmatrix} r & \lambda & \lambda & ..... & \lambda \\ \lambda & r & \lambda & ..... & \lambda \\ \lambda & \lambda & r & ..... & \lambda \\ \lambda & ..... & ..... & ..... & r \end{bmatrix}_{v\times v}.$$

Bu matrisin determinantını hesaplamak için bütün sütunları ilk sütunda toplayalım.

$$\begin{bmatrix} r+ & (v-1)\lambda & \lambda & \lambda & \lambda \\ r+ & (v-1)\lambda & \lambda & ..... & \lambda \\ .... & .... & .... & ..... & .... \\ r+ & (v-1)\lambda & \lambda & \lambda & r \end{bmatrix}_{v\times v}.$$

Birinci satırı diğer satırlardan çıkaralım,

$$\begin{bmatrix} r+(v-1)\lambda & \lambda & \lambda & \ldots\ldots\ldots & \lambda \\ 0 & r-\lambda & & \ldots\ldots\ldots & 0 \\ 0 & & & & 0 \\ 0 & 0 & \ldots\ldots & 0 & r-\lambda \end{bmatrix}_{v\times v}.$$

Oluşan üçgensel matrisin determinantı köşegen elemanlarının çarpımıdır.

$$(r-\lambda)^{v-1}\left(r+(v-1)\lambda\right)\text{olur.}$$

Sonuç 2.2.2: Eğer N matrisi, $2-(v,k,\lambda)$ tasarımının çakışım matrisi ise o zaman $v \le b$ dir[4].

Tanım 2.2.1: Nokta ve blok sayısı eşit $(v=b)$ olan tasarıma simetrik tasarım denir. Ayrıca simetrik tasarımdan $v=b$ olduğundan $k=r$ olur.

Simetrik tasarımda herhangi iki blok λ ortak noktaya sahip ve bu λ sayısı değişmezdir.

2.3. Tasarımlar İçin Metot Oluşturma

2.3.1. Eski tasarımlardan yeni tasarım elde etme

Bu bölümde, eski tasarımlardan yeni tasarım oluşturmaya bakılır.

Tanım 2.3.1.1: Blokların ve noktaların yerlerini değiştirerek oluşturulan tasarıma düal tasarım denir. Orijinal tasarımın çakışım matrisinin devriğine düal tasarımın çakışım matrisi denir.

Eğer $v < b$ ise düal tasarım $2-$tasarım olmaz. Fisher eşitsizliğinden $2-$tasarım olması için $v \le b$ idi. $v < b$ olduğunda düal tasarımda blok sayısı nokta sayısından daha azdır. Genel olarak $2-$tasarımının düal tasarımında bir $2-$tasarım değildir.

Teorem 2.3.1.1: Simetrik tasarımın düal tasarımı bir $2-$tasarımdır[3].

Tanım 2.3.1.2: D bir $2-(v,k,\lambda)$ tasarımı olsun. Noktalara dokunmadan, sadece blokları değiştirerek yeni bir tasarım elde edilir. Eğer $I \in B$ eski tasarımda bir blok ise I'nın P'deki tümleyeni I^c, yani $P-I$ kümesi yeni tasarım bloğu olacaktır. D'nin tümleyeni olan bu tasarıma D'nin tümleyen tasarımı denir ve $D^{\perp}$ ile gösterilir.

Teorem2.3.1.2: $2-(v,k,\lambda)$ tasarımın tümleyen tasarımı bir $2-$tasarımıdır ve parametreleri $(v,b,b-r,v-k,b-2r+\lambda)$ dır. ($b-2r+\lambda$ sıfırdan farklıdır) [3].

Tanım 2.3.1.3: D bir simetrik (v,k,λ) tasarım ve $B_v \in D$ herhangi bir blok olsun. Noktalar kümesi B_v'deki noktalar ve blok kümesi ise $\{B \cap B_v : B \in D, B \neq B_v\}$ olan tasarıma kısıtlanmış tasarım denir.

Teorem 2.3.1.3: Simetrik (v,k,λ) tasarımından kısıtlanmış tasarımda aynı zamanda $2-$tasarımdır ve parametreleri $(k,v-1,k-1,\lambda,\lambda-1)$ dir.($\lambda=1$ aşikar durumu hariç bu parametreler verilebilir.)[3].

Tanım 2.3.1.4: D bir simetrik (v,k,λ) tasarımı ve $B_v \in D$ olan herhangi bir blok olsun. Nokta kümesi $P-B_v$'deki noktalar kümesi olmak üzere ; bloklar kümeside $\{B-B_v : B \in D, B \neq B_v\}$ olan tasarıma artık (residual) tasarım denir.

Teorem 2.3.1.4: Simetrik $2-(v,k,\lambda)$ tasarımın artık tasarımı $\lambda=k-1$ aşikar durumu hariç parametreleri $(v-k,v-1,k,k-\lambda,\lambda)$ olan $2-$tasarımdır[3].

Tanım 2.3.1.5: Eğer $2-$tasarım $(v-k, v-1, k, k-\lambda, \lambda)$ parametrelerine sahip ise bu tasarıma Quası-residual tasarım denir.

Örnek 2.3.1.1: Aşağıdaki $2-(16,6,3)$ tasarımı quası-residual tasarım fakat artık tasarım değildir. İlk iki blok 4 ortak noktaya sahiptir.

Tablo 2.1. tasarım örnekleri

1	2	3	4	5	6		2	5	8	11	13	15
1	2	3	4	7	8		2	6	7	11	12	14
1	2	9	10	12	13		2	7	8	10	14	16
1	3	10	11	12	15		3	4	11	14	15	16
1	4	9	13	14	16		3	5	6	10	13	14
1	5	7	10	14	15		3	5	8	9	12	14
1	5	7	11	13	16		3	6	7	12	13	16
1	6	8	9	11	14		3	7	8	9	13	15
1	6	8	12	15	16		4	5	6	7	10	15
2	3	9	10	11	16		4	5	7	9	11	12
2	4	12	13	14	15		4	6	8	10	11	13
2	5	6	9	15	16		4	8	9	10	12	16

Teorem 2.3.1.5: $\lambda = 1$ veya 2 için $(v-k, v-1, k, k-\lambda, \lambda)$ parametreleriyle verilen $2-$tasarımı aynı zamanda (v, k, λ) simetrik tasarımının artık tasarımı olur. [6].

2.3.2. Hadamard matrislerinden yeni tasarımlar elde etme

Tanım 2.3.2.1: $n \times n$ boyutlu ve elemanları $+1$'den ve -1'den oluşan bir H matrisi $H.H^T = nI$ koşulunu sağlıyor ise H matrisine Hadamard matrisi denir.

Örnek 2.3.2.1: $H_1 = [1]$, $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

matrisleri birer Hadamard matrisleridir.

Hadamard matrisinin herhangi bir satırını veya sütununu -1'le çarparsak yeni bir Hadamard matrisi elde ederiz. Bu dönüşümleri peşi sıra uygulayarak, herhangi bir Hadamard matrisinden, ilk satırı ve sütunundaki tüm girdileri 1 olan Hadamard matrisi elde edilir.

Tanım 2.3.2.2: Hadamard matrisinin ilk satır ve sütun elemanları 1 ise böyle bir Hadamard matrisine standart Hadamard matrisi denir.

Teorem 2.3.2.1: $n>2$ mertebeli bir standart Hadamard matrisi H ve $H=\begin{bmatrix} 1 & j^T \\ j & K \end{bmatrix}$ şeklinde yazılsın. Burada j matrisi $(n-1)\times 1$ boyutlu ve tüm elemanları 1 olan matristir. O halde ; $N=(K+J)/2$ şeklinde yazılan $(n-1)\times(n-1)$ boyutlu N matrisi, $(n-1, n/2-1, n/4-1)$ simetrik tasarımın çakışım matrisidir [7].

İspat: H standart Hadamard matrisi olsun. O halde $H.H^T=nI$ koşulunu sağlar.

$$H.H^T=\begin{bmatrix} 1 & j^T \\ j & K \end{bmatrix}\begin{bmatrix} 1 & j \\ j^T & K^T \end{bmatrix}=\begin{bmatrix} n & (j+KJ)^T \\ j+Kj & J_{n-1\times n-1} \quad +K.K^T \end{bmatrix}$$

Buradan şu sonuçları çıkarabiliriz.

$$Kj=-j \qquad (2.4)$$

$$KK^T+J=nI \qquad (2.5)$$

eşitlik(2.4) göre K matrisinin tüm satırlarının toplamı -1'dir. O halde N'nin satırları toplamı $\frac{1}{2}((n-1)-1)=\frac{n}{2}-1$ olur. Bu ise tasarımın bir bloktaki eleman sayısını (k'sını) verir. Şimdi $N.N^T=\frac{(K+J)}{2}.\frac{K^T+J^T}{2}=\frac{1}{4}(K+J)(K+J)^T$

$$=\frac{1}{4}(K+J)(K+J)^T=\frac{1}{4}(K+J)\left(K^T+J^T\right)$$

$$=\frac{1}{4}\left(K.K^T+K.J^T+J.K^T+J.J^T\right)$$

$Kj=-j$ ve $KK^T+J=nI$

$K.K^T=nI-J,\ jK^T=(Kj)^T=-j$

$(K\ j)^T=-j$ olduğundan yukarıdaki eşitlik

$$NN^T=(K.K^T+K.J^T+J.K^T+J^2.J^T)=\frac{1}{4}(nI-J-J-J+(n-1))$$

$$=\frac{1}{4}nI+\frac{1}{4}(n-4)J \qquad (2.6)$$

O halde N matrisi $(n-1,n/2-1,n/4-1)$ simetrik tasarımının çakışım matrisi olur. Oluşturduğumuz bu tasarım Hadamard $2-$tasarım olarak bilinir.

Tanım 2.3.2.3: $A=(a_{ij})$ ve $B=(b_{ij})$ iki matris olsunlar. A ve B 'nin kronecker çarpımı, $A\otimes B$ matrisi olur. Eğer A matrisi $m_1\times m_2$ boyutlu ve B matrisi $n_1\times n_2$ boyutlu ise $A\otimes B$ matrisi $m_1n_1\times m_2n_2$ boyutlu matris ve A matrisindeki a_{ij} elemanının yerine $a_{ij}B$ matrisi konularak elde edilen matristir. $A\otimes B=\left[a_{ij}B\right]$. Kronecker çarpımın şu özelliklerde mevcuttur.

$(A\otimes B)^T=A^T\otimes B^T$, $\qquad (A\otimes B)(C\otimes D)=AC\otimes BD$ olur.

Önerme 2.3.2.1: A ve B Hadamard matrisleri ise $A \otimes B$ matrisde Hadamard matrisidir. Dolayısıyla m ve n mertebeli Hadamard matrisi varsa mn mertebeli Hadamard matriside vardır [3].

Örnek 2.3.2.2**:** $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ ve $H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

$$H_2 \otimes H_4 = \begin{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \end{bmatrix}$$

Yukarıdaki kuruluş Sylvester kuruluşu olarak bilinir. Ayrıca Sylvester matrisi H_2 üzerinde Sylvester kuruluşu kullanarak oluşturulur.

Sylvester matrisi $S_0 = [1]$ ve $S_1 = H_2$ olmak üzere $S_n = H_2 \otimes S_{n-1}$ şeklinde tanımlanan $2^n x 2^n$ boyutlu matristir$(n \geq 1)$.

Örnek 2.3.2.3: H_2 matrisi kullanarak oluşturulan Sylvester kuruluşu teorem 2.3.2.1 göre $(2^r - 1, 2^{r-1} - 1, 2^{r-2} - 1)$ tasarımı bir simetrik tasarımdır. Ayrıca bu tasarım $(r \geq 2)$ Sylvester tasarım olarak bilinir.

Teorem 2.3.2.2: Simetrik $(n-1, n/2-1, n/4-1)$ tasarımı var ise o zaman $n \times n$ boyutlu Hadamard matriside vardır[7].

İspat: $(n-1, n/2-1, n/4-1)$ tasarım çakışım matrisi N ve $K = 2N - J$ olsun.

$H = \begin{bmatrix} 1 & 1 & 1 & ..... & 1 \\ 1 & ..... & ..... & ..... & ..... \\ 1 & ..... & ..... & ..... & ..... \\ 1 & ..... & ..... & ..... & K \end{bmatrix}_{nxn}$ boyutlu H matrisi oluşturalım.

$H = \begin{bmatrix} 1 & j^T \\ J & K = 2N - J \end{bmatrix} H$ matrisinde $j, (n-1)\times 1$ boyutlu ve tüm elemanları 1 olan matris olsun.

$$H.H^T = \begin{bmatrix} 1 & j^T \\ j & 2N - J \end{bmatrix} . \begin{bmatrix} 1 & j \\ j^T & 2N - J \end{bmatrix}$$

$$H.H^T = \begin{bmatrix} n & (j + (2N - J)\, j)^T \\ J + (2N - J)\, j & (2N - J)(2N - J)^T + J_{n-1 x Jn-1} \end{bmatrix}$$

N çakışım matrisinin büyüklüğü $(n/2-1)$ olduğundan

$$\begin{aligned} j + (2N - J)\, j &= j + 2Nj - Jj \\ &= j + 2(n/2-1)\, j - (n-1)\, j \\ &= (1 + 2(n/2-1) - (n-1))\, j \\ &= 0 . \end{aligned}$$

Şimdi $(2N - J)(2N - J)T + J$ matrisini göz önüne alalım.

$$(2N - J)(2N - J)^T + J = 4NN^T - 2NJ - 2JN^T + J^2 + J$$

$$= 4\left[n/4I + (n/4-1)J\right] - 4(n/2-1)J + (n-1)J + J = nI.$$

$2N - j$ tüm elemanı ± 1 olduğundan H matrisinin tüm elemanları ± 1 olur. O halde $H.H^T = nI$ olduğundan H matrisi Hadamard matrisi olur.

n'lik Hadamard matrisi ancak $n=1, n=2$ ya da n, 4'ün bir katıysa olabilir. Buna rağmen her $n>1$ sayısı için $4n\times 4n$ boyutlu tüm Hadamard matris tipleri bilinmiyor. Hadamard matrislerin satır ve sütunlarının toplamları eşit olduğundan, onları simetrik tasarım oluştururken kullanırız.

H bir Hadamard matris ve $N=(H+J)/2$ olsun. O halde N $1-$tasarımın çakışım matrisi olur. Çünkü H matrisinin sütunlarının toplamı sabittir. Ayrıca H matrisi $n\times n$ boyutlu ve her bir satırı ve sütunu tam olarak k tane 1'den oluşur. O halde;

$$4.N.N^T=(H+J)(H+J)^T$$
$$=H.H^T+(H+H^T)J+J^2$$
$$=nI+2(2k-n)J+nJ$$
$$=nI+(4k-n)J.$$

H matrisininher bir satır ve sütun k tane 1 ve $(n-k)$ tane -1 sahip olur.. Böylece N matrisi $(n,k,k-n/4)$ simetrik tasarının çakışım matrisi olur.

Diğer taraftan (v,k,λ) simetrik tasarımın çakışım matrisi N olsun. Eğer $v=4(k-\lambda)$ alırsak $2N-J$ bir Hadamard matrisi olur. Her bir satır ve sütunlarının toplamı sabittir. Bunu gösterelim

$$(2N-J)(2N-J)^T=4.N.N^T-2NJ-2N^TJ+J^2$$
$$=((k-\lambda)I+\lambda J)-2(N+N^T)J+J^2$$
$$=4(k-\lambda)I+4\lambda J-4kJ+vJ$$
$$=vI+(v-4(k-\lambda))J=vI \text{ olur.}$$

Ayrıca

$(2N-J)J=2NJ-J^2=(2k-v)J$ satırlarının toplamı sabittir.

$(2N-J)^T.J=2N^TJ-J^2=(2k-v)J$ sütunların toplamı sabittir. O halde satır ve sütunlarının toplamı da eşittir.

2.3.3. Kümelerden yeni tasarım elde etme

Bu bölümde kümeler tarafından üretilen tasarımları üzerinde durulacak.

Tanım 2.3.3.1: G bir grup ve G üzerinde bir ikili işlem tanımlı olsun. D de G grubunun bir alt kümesi olsun. O halde tasarım bloklarını $\{D+g : g \in G\}$ şeklinde kurulur. Bu tasarıma, D tarafından üretilen tasarım denir. Eğer mertebesi v olan G grubunun alt kümesi D ise D tarafından üretilen tasarım simetriktir.

2.3.4. Sonlu cisimlerden yeni tasarımlar elde etme

Bu bölümde mertebesi q olan sonlu bir F cismi üzerinde yeni tasarımlar oluşturulacaktır. Burada q asal tek sayının kuvveti şeklindedir.

Tanım 2.3.4.1: F bir cisim olsun. Legendre sembolü $\chi(a)$ fonksiyonu F cisminden $\{-1,0,1\}$' e şu şekilde tanımlansın;

$$\chi(a) = \begin{cases} 0 & a=0 \\ 1 & \{a^2 : a \in F_q \quad , a \neq 0\} \\ -1 & \{a^2 : a \notin F_q , a \neq 0\} \end{cases} (\forall a \in F)$$

.

Her $a,b, \in F$ için

$\chi(b) = \chi(a).\chi(b)$ dir. (F cismi sonlu bir cisimdir.)

Tanım 2.3.4.2: $R_{ij} = \chi(i-j)$ ve F cisminin elemanları tarafından oluşturulan sıralı sütun ve satırları olan R matrisine Jacobsthal matris denir $\left(R = R_{ij}\right)$.

Teorem 2.3.4.1: R bir Jacobshal matris olsun. O zaman aşağıdakiler sağlanır.

1) $RJ = 0$
2) $R^T = (-1)^{(q-1)/2} R$
3) $R.R^T = qI - J$ [8].

Teorem 2.3.4.2: Eğer $q = 3(\mathrm{mod}\,4)$ ise o zaman $(q,(q-1)/2,(q-3)/4)$ simetrik tasarımı vardır[9].

2.4. Genel Tasarımlar

2.4.1. t-tasarımlar

2- tasarımı, t-tasarımın özel bir haliydi, bu bölümde $(t > 2)$ daha genel tasarımlar için çalışılacak. Herhangi bir tam tasarımda blok büyüklüğü k ve k'nın her $t-$elemanlı alt kümesi bloklarda tam olarak $\lambda_t = \binom{v-t}{k-t}$ olarak bulunur. (burada $2<t \le k$) dir.

Tanım 2.4.1.1: D bir $t-(v,k,\lambda)$ tasarımı ve $p \in D$ olsun. Ω da D'nin noktalarının kümesi olsun. D'nin p noktasıyla ilgili kısıtlanmış tasarımına D_p tasarımı denir. D_p tasarımı noktaları ve blokları aşağıdaki şekilde elde edilir; $\Omega/\{p\}$ noktalar kümesi, $B = \{B \mid B \in B, B \cap p\}$ bloklar kümesidir.

Önerme 2.4.1.1: D bir t- tasarım ise D_p' de $t-1$ tasarım olur[10].

İspat: D bir $t-$tasarım ve Ω'da noktalar kümesi olsun. D_p blokların her biri $(k-1)$ noktaya sahiptir. O halde D_p bir tasarım olur. Şimdi Ω kümesinin $(t-1)$ elemanlı alt kümelerini düşünelim. Bu alt kümeye p noktasını ekleyelim. O halde

Ω'nın p noktasını içeren $t-$elemanlı alt kümelerini bulmuş oluruz. D_p'nin $t-$elemanlı alt küme sayısı λ_t olur. o halde D_p bir $(t-1)-$tasarımdır.

Tanım 2.4.1.2: D bir $t-(v,k,\lambda)$ tasarımı ve $p\in D$ olsun. D'nin noktalar kümesi Ω olsun. D'nin artık tasarımı D^p ile gösterilir, artık tasarım şu şekilde elde edilir. $\Omega_p=\Omega-\{p\}$ noktalar kümesi olmak üzere, $B^p=B-\{B\mid B\cap p\}$ bloklar kümesi olarak tanımlanır.

Önerme 2.4.1.2: $t\geq 1$ için D bir $t-$tasarım ise D^p de $t-1$ tasarım olur. [10]

Örnek 2.4.1.1: $3-(8,4,1)$ tasarımını göz önüne alalım. Tasarım blokları şu şekildedir; $B=\{\{1,3,7,8\},\{1,2,4,8\},\{2,3,5,8\},\{3,4,6,8,\},\{4,5,7,8\},\{1,5,6,8\},$ $\{2,6,7,8\},\{1,2,3,6\},\{1,2,5,7\},\{1,3,4,5\},\{2,3,4,7\},\{2,4,5,6\},\{3,5,6,7\}\}$ şeklindedir. Bu tasarımın artık ve kısıtlanmış tasarımlarını bulalım. Artık tasarım: p=1 noktasını alırsak

Ω_p={2, 3, 4, 5, 6, 7, 8}

B^p={{2, 3, 5, 8}, {3, 4, 6, 8}, {4, 5, 7, 8}, {2, 6, 7, 8}, {2, 3, 4, 7}, {2, 4, 5, 6},

{3, 5, 6, 7}} olur. Şimdi bu tasarımın kısıtlanmış tasarımını bulalım. $p=1$ için;

$\Omega_p=\{2,3,4,5,6,7,8\}$

$B_p=\{\{3,7,8\},\{2,4,8\},\{5,6,8\}\{2,3,6\},\{2,5,7\},\{3,4,5\}\}$

Bu tasarım bir $2-(7,3,1)$ tasarımıdır.

Örnek 2.4.1.2: 3-$(8,4,1)$ tasarımına ait bloklar aşağıda verildiği gibi olsun.

$\{1,3,7,8\},\{1,2,4,8\},\{2,3,5,8\},\{3,4,6,8\},\{4,5,7,8\},\{1,5,6,8\},\{2,6,7,8\},\{1,2,3,6,\}$
$\{1,2,5,7\},\{1,3,4,5\},\{1,4,6,7\},\{2,3,4,7\},\{2,4,5,6\},\{3,5,6,7\}.$

Bu durumda çakışım matrisi aşağıda verildiği gibidir.

Tablo 2.2. Tasarımın çakışım matrisi

$$N = \begin{array}{c} \\ X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \\ X_8 \end{array} \begin{array}{c} \begin{array}{cccccccccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 & B_8 & B_9 & B_{10} & B_{11} & B_{12} & B_{13} & B_{14} \end{array} \\ \left[\begin{array}{cccccccccccccc} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \end{array}$$

Çakışım matrisine dikkat edildiğinde, bu tasarım aynı zamanda $2-(8,4,3)$ tasarımı olduğu görülür.

Önerme 2.4.1.3: Her $t-(v,k,\lambda_t)$ tasarımı aynı zamanda $(t-1)-$tasarım ve $\lambda_{t-1}=\dfrac{v-t+1}{k-t+1}.\lambda_t$ dir [8].

Tanım 2.4.1.3: D bir t-(v, k, λ) tasarımı ve $B=\{P_1,P_2.....P_k\}$ D'nin bir bloğu olsun. $B_0=\varnothing$, $B_i=\{P_1,P_2.....P_i\}$ $i\in\{1,2,.....,k\}$ ve λ_{ij}, $C\cap B_j=B_j$ şartını sağlayan D'deki C bloklarının sayısı olarak tanımlayalım. O zaman $\lambda_{i,i}=\lambda_i$ $i=0,1,2...k$ dir.

Önerme 2.4.1.4: $i\geq j$ için $\lambda_{i,j}=\lambda_{i+1,j+1}+\lambda_{i+1,j}$ dir$[2]$.

Teorem 2.4.1.5: $t-$tasarımın tümleyen tasarımda bir $t-$tasarımdır$[10]$.

2.4.2. Paskal üçgeni ile tasarımın parametreleri arasındaki ilişki

Bir D tasarımının Paskal Üçgeni ardışık $i.$elemanın bu üçgenin $i.$satırını gösteren bir sıradadır. Yani ardışık $i.$eleman $(\lambda_0^{(i-1)},\lambda_1^{(i-2)},.....,\lambda_{(i-1)}{}^0)$ biçimindedir. Eğer D bir Steiner t tasarımı ise, daha sonra bu üçgen $k+1$ satıra dönüşür. Burada k , D'nin bir bloğundaki eleman sayısıdır. Aksi takdirde; bu üçgen $t+1$ satıra sahiptir.

Paskal üçgeninde, $\lambda_0^0=b$, $\lambda_1^0=r$ ve $s\le t$ iken $\lambda_s^0=\dfrac{v-s}{k-s}\,\lambda_{s+1}^0$ olmak üzere;

$$\begin{array}{ccccccc}
 & & & \lambda_0^0 & & & \\
 & & & \lambda_1^1 & \lambda_1^0 & & \\
 & & \lambda_2^2 & \lambda_2^1 & \lambda_2^0 & & \\
 & \lambda_3^3 & \lambda_3^2 & \lambda_3^1 & \lambda_3^0 & & \\
 & \cdots & \cdots & \cdots & \cdots & \cdots & \\
\lambda_s^s & \lambda_s^{s-1} & & & & \lambda_s^1 & \lambda_s^0
\end{array}$$

biçimde yazılabilir. Bir Paskal Üçgeninin sağ kenarı $t-(v,k,\lambda)$ tasarımının parametreleri iken, sol kenarı ise aynı tasarımın tümleyen tasarımının parametreleridir.

Örnek 2.4.2.1: $2-(8,4,3)$ tasarımı dikkate alınsın; $v=8$, $k=4$, $\lambda=3$,

$$\lambda_0^0=b=\lambda\frac{\binom{v}{t}}{\binom{k}{t}}=14\ ,\quad \lambda_1^0=r=\lambda\frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}=7.$$

Burada;

$\lambda_0^0 = b$, $\lambda_1^0 = r$, $\lambda_2^0 (t = 2$ için $\lambda)$, $\lambda_3^0 (t = 3$ için $\lambda)$, ...

biçimindedir. $\lambda_0^0 = 14$, $\lambda_1^0 = 7$, $\lambda_2^0 = 3$ olarak hesaplanır.

$$\begin{array}{c} 14 \\ \text{Tümleyen tasarımın parametreleri} \leftarrow 7 \quad 7 \rightarrow \text{Tasarımın Parametreleri } 2-(8,4,3) \\ 3 \quad 4 \quad 3 \end{array}$$

tasarımı $v = 2k$ biçimindedir, bu nedenle tümleyen tasarımı kendisine eşit $2-(8,4,3,)$ tasarımıdır.

Tümleyen tasarım $k^* = v - k$ ve $\lambda^* = \lambda \dfrac{\binom{v-t}{k}}{\binom{v-t}{k-t}}$ parametrelerine sahiptir, $t-(v,k^*,\lambda^*)$ biçiminde ifade edilir.

Örnek 2.4.2.2: $3-(23,7,5)$ tasarımı dikkate alınsın; $v = 23$, $k = 7$, $\lambda = 5$

$\lambda_0^0 = b = 253$, $\lambda_1^0 = r = 77$, $\lambda_2^0 = 21$, $\lambda_3^0 = 5$

parametrelerine sahiptir. $3-(23,7,5)$ tasarımının tümleyenide, $3-(23,16,80)$ tasarımıdır ve $v = 23$, $k = 16$, $b = 253$, $r = 176$, $\lambda_2^0 = 120$, $\lambda_3^0 = 80$ parametrelerine sahiptir.

$$\begin{array}{c} 253 \\ 176 \quad 77 \\ 120 \quad 56 \quad 21 \\ 80 \quad 40 \quad 16 \quad 5 \end{array}$$

$3-(23,16,80)$ tasarımı $3-(23,7,5)$ tasarımı

BÖLÜM 3. PROJEKTİF GEOMETRİ VE TASARIMLAR

3.1. Projektif Düzlem

Tanım 3.1.1: Aşağıdaki aksiyomları sağlayan noktalar ve doğruların koleksiyonuna projektif düzlem denir.

A_1 : Farklı iki noktadan tek bir doğru geçer.

A_2 : İki doğru en az bir noktada kesişir.

A_3 : Herhangi üçü doğrudaş olmayan dört nokta vardır.

Bu düzlemde doğruları bir blok olarak görebiliriz. $(7,3,1)$ parametreleriyle verilen simetrik tasarımı düşünelim. Bu simetrik tasarımda yedi nokta vardır. Bunlar $\{1,2,3,4,5,6,7\}$ dir. Bu noktalardan oluşan bloklar kümesi $\{1,2,4\}$, $\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\}$ ve $\{7,1,3\}$ tür. Bu simetrik tasarım aşağıdaki üç özelliği sağlar.

1) Her nokta çifti bir tek bloğa aittir.
2) Her farklı iki bloğun tam olarak tek ortak noktası vardır
3) Üçü aynı blokta olmayan dört nokta vardır.

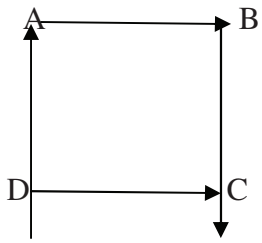
Tanım 3.1.2: Bir yay (arc) projektif düzlemde; üçü aynı doğru üzerinde olmayan noktaların kümesine denir. $k-$yay ise tam olarak k tane noktaya sahiptir.

Projektif düzlem tanımdan (A_3'ten) anlaşıldığı gibi projektif düzlem $4-$yay dır. Eğer projektif düzlemde nokta ve doğruların yerini değiştirirsek (A_1 'i A_2 yaparsak)

tersi olur. O halde A_1 ve A_2 aksiyomları birbirinin düaldir. A_3 aksiyomunun düalide doğrudur.

Önerme 3.1.1: Her projektif düzlem üçü aynı noktada kesişmeyen dört doğru içerir [5].

İspat: Her projektif düzlem en az bir $4-$yay içerir, o yüzden $4-$yay şöyle $\{A,B,C,D\}$ olsun.



Doğrularımızı AB, BC, CD, DA seçersek, üçü aynı noktada kesişmeyen dört doğru olur ve her farklı iki doğru bir tek ortak noktaya sahip olur.

Teorem 3.1.1: Projektif düzlemin düalide projektif düzlemdir [11].

Önerme 3.1.2: Projektif düzlemde herhangi iki doğru L ve M olsun. Bu doğrular üzerinde olmayan bir X noktası vardır [11].

Önerme 3.1.3: Projektif düzlemdeki her doğru aynı sayıda nokta içerir [11].

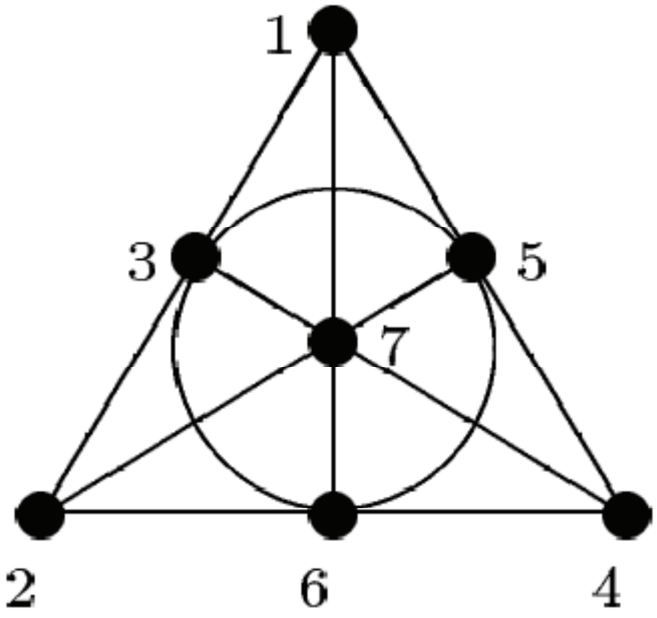
Önerme 3.1.4: Projektif düzlemde eğer bütün doğrular n nokta içeriyorsa o zaman bütün noktalar bu n tane doğru üzerinde olur [11].

Teorem 3.1.2: Sonlu bir projektif düzlem $n \geq 2$ için simetrik $2-(n^2+n+1, n+1, 1)$ tasarımıdır [12].

İspat: Projektif düzlemde her doğru aynı sayıda nokta içeriyor. Bu da $n+1$'dir. Doğruları biz blok olarak düşündüğümüzde; sonlu bir projektif düzlemin doğruların sahip olduğu nokta sayısı bloktaki eleman sayısını verir. Önerme 3.1.4'den $r=n+1$ olur. (Her noktanın üzerinde bulunduğu doğru sayısı) A_1 aksiyomundan da $\lambda=1$ olur. O halde bu düşünce bir tasarım olur. Toplam nokta sayısı $v=b=n^2+n+1$ dir. Bu ise simetrik $2-\left(n^2+n+1\right)$ tasarımı olur $(n\geq 2)$

Teorem 3.1.3: $\lambda=1$ ve en az dört noktayla verilen simetrik tasarım bir projektif düzlemdir $[12]$.

Örnek 3.3.3: $2-(7,3,1)$ simetrik tasarımına karşı gelen projektif düzlem fano düzlemdir. Fano düzlemin şekli aşağıdaki gibidir.



Şekil 3.1. Fano düzlemin şekli

Bu düzlemin noktaları $\{1,2,3,4,5,6,7\}$ bloklar kümeside ;

$\{\{1,2,3\},\{1,4,5\},\{1,6,7\},\{2,4,6\},\{2,5,7\},\{3,4,7\},\{3,5,6\}\}$.

3.2. Fark Kümeleri

Tanım 3.2.1: v negatif olmayan bir tam sayı olsun. $S=\{a_1,a_2,a_3,...,a_k\}$ k farklı tam sayılardan oluşan bir küme olsun. Her bir $i\in\{0,1,2,.....,v-1\}$ ve S kümesi için eğer $\{(x,y)\in SxS : x-y=i(\text{mod}\, v)\}$ kümesinin kardinalitesi λ ise S'ye devirli (v,k,λ) fark kümesi denir.

$D(s)$ ilişki yapısı, S kümesinden aşağıdaki gibi elde edilir. Noktalar kümesi; $P=\{0,1,2,.....,v-1\}$ bloklar kümesi; $S+u=\{a_1+u,a_2+u,...,a_k+u\}$ dir. Burada $u\in P$ ve $(\text{mod}\, v)$ göre toplama işlemi tanımlıdır.

Teorem 3.2.1: S devirli (v,k,λ) fark kümesinin çakışım yapısı olan $D(s)$ bir simetrik (v,k,λ) tasarımıdır[13].

İspat: $S+u$ kümesinin nokta sayısı k olduğundan $D(s)$ bir tasarım olur. Tasarımızdaki tüm blokları yazarsak v tane satır olur. Bu bloklar aşağıdaki gibidir.

$$S=\begin{matrix} B_1: & a_1 & a_2 & a_3 & ... & a_k \\ B_2: & a_1+1 & a_2+1 & a_3 & ... & a_k+1 \\ ... & ... & ... & ... & ... & ... \\ B_v: & a_1+v-1 & a_2+v-1 & a_3 & ... & a_k+v-1 \end{matrix}$$

$B_1(=S)$ nin ilk elemanına x dersek, birinci sütundaki kolonlar bir dizi oluşturur. Aynı şekilde $B_2(=S+1)$ de $x+1, B_3(S+2), x+2$, böyle devam edersek B_v den x+v-1=x-1 oluşur. O halde ilk sütun $\{0,1,2,3,...,v-1\}$ kümesinin her elemanını bir defa içerir. Aynı şey tüm sütunlar içinde doğrudur. Böylece her bir nokta tasarımda k defa görülür. $(r=k)$ Bu yüzden bu tasarım simetrik tasarım olur.

S kümesinin farklı sıralı ikilileri $(a_1,b_1),(a_2,b_2),...,(a_\lambda,b_\lambda)$ için;

$j\in\{1,2,3,...,\lambda\}$ ve $a_j-b_j=i$ olsun.

Herhangi x ve y elemanlarını $x-y=i$ olacak şekilde göz önüne alalım. O zaman x ve y'nin oluşturduğu $S+(x-a_1),S+(x-a_2),...,S+(x-a_\lambda)$ bloklardır. Bu yüzden x ve y 'nin birlikte bulunduğu blok $S+d$ olsun. O halde $(x-d)-(y-d)=x-y=i$ ve $x-d, y-d$ S'nin elemanlarıdır. Ayrıca $x-d=a_j, y-d=b_j$ ve $S+d=S+(x-a_j)$ olur. O zaman x ve y birlikte gözüktüğü blok sayısı tam olarak λ dır.

Örnek 3.2.1: $P=\{0,1,2,...,12\}$ ve $\{(x,y)\in S\times S: x-y=i(\text{mod}13\}$ bu devirli kümenin ürettiği tasarımı bulalım. $i=\{0,1,2,....,12\}(\text{mod}13)$ ve B_i bloklar olmak üzere;

Tablo 3.1. Devirli fark kümesinden tasarım yapma

$1\equiv 6-5$	$7\equiv 8-1$	
$2\equiv 8-6$	$8\equiv 1-6$	
$3\equiv 8-5$	$9\equiv 1-5$	(mod13)
$4\equiv 5-1$	$10\equiv 5-8$	
$5\equiv 6-1$	$11\equiv 6-8$	
$6\equiv 1-8$	$12\equiv 5-6$	

B_0 : $0,1,3,9$ B_7 : $7,8,10,3$

B_1 : $1,2,4,10$ B_8 : $8,9,11,4$

B_2 : $2,3,5,11$ B_9 : $9,10,12,5$

B_3 : $3,4,6,12$ B_{10} : $10,11,0,6$

B_4 : $4,5,7,0$ B_{11} : $11,12,1,7$

B_5 : $5,6,8,1$ B_{12} : $12,0,2,8$

B_6 : $6,7,9,2$

Bu tasarım B_5 : $5,6,8,1$ bloğunun ürettiği $(13,4,1)$ devirli fark kümesidir.

Tanım 3.2.2: S bir (v,k,λ) fark kümesi ve P'de onun noktalar kümesi olsun. $S+u$ kümesine S'nin ötelemesi denir. $(u \in P)$. Eğer S devirli (v,k,λ) fark kümesi ise $-S$ ve $S+u$ kümelerinde devirli (v,k,λ) fark kümeleridir

Teorem 3.2.2: q bir asal sayı ve $q \equiv 3(mod 4)$ olsun. O zaman $(q,(q-1)/2,(q-3)/4)$ devirli fark kümesidir[3].

Örnek 3.2.2: P bir asal sayı ve n de herhangi bir pozitif tamsayı ise $k = \frac{p^n-1}{p-1}$,

$v = \frac{p^{n+1}-1}{p-1}$, $\lambda = \frac{P^{n-1}-1}{P-1}$ parametreli (v,k,λ) tasarımı bir fark kümesidir.

$\{1,2,7,9,19\}$ ve $\{1,2,5,15,17\}$ kümeleri $(21,5,1)$ kümesinin fark kümeleri ve bunların ailesi $P=4$ ve $n=2$ dir.

Örnek 3.2.3: Eğer $P = 4x^2+1$ şeklinde bir asal ve x'de tek tamsayı olsun. $(\text{mod } p)$ göre dördüncü kuvveti sıfır olmayan $(4x^2+1, x^2, (x^2-1)/4)$ formu bir fark kümesini oluşturur. Örneğin devirli $(37,9,2)$ fark kümesi $\{1,7,9,10,12,16,26,33,34\}$ kümesini oluşturur.

Örnek 3.2.4: $p = 4x^2+9$ şeklinde bir asal ve x tek bir tamsayı olsun. O zaman dördüncü dereceden kuvveti sıfır olmayan küme ile birlikte sıfır $(\text{mod } p)$ göre bir fark kümesidir.

Teorem 3.2.3: $q \equiv 1(\text{mod } 4)$ olacak şekilde bir asal sayı $(q = 4t+1, t \in Z)$ olsun. O zaman $(4t+1, 2(4t+1), 4t, 2t, 2t-1)$ tasarımından iki fark kümesi geliştirilir[3].

Örnek 3.3.5: Aşağıdaki tabloda gösterilen farklı kümeleri birer projektif düzlemdir.

Tablo 3.2.Devirli fark kümelerinden elde edilen projektif düzlemler

n	v	S
2	7	{1 2 4}
3	13	{1 2 5 7}
4	21	{1 2 5 15 17}
5	31	{1 2 4 9 13 19}
7	57	{1 2 4 14 33 44 53}
8	73	{1 2 4 8 16 32 37 55 64}
9	91	{1 2 4 10 28 50 57 62 78 82}

3.3. Afin Düzlem

Tanım 3.3.1: İki doğrunun hiçbir ortak noktası yoksa bu doğrulara paralel doğrular denir.

Tanım 3.3.2: Aşağıdaki aksiyomları sağlayan noktalar ve doğrular kümesine bir Afin düzlem denir.

$A_{1'}$: Herhangi iki farklı noktadan tek bir doğru geçer.

$A_{2'}$: Bir doğruya dışındaki bir noktadan bir tek paralel çizilir.

$A_{3'}$: Doğrudaş olmayan üç nokta vardır.

Teorem 3.3.1: Sonlu bir Afin düzlemin olması için gerekli ve yeterli koşul $n \geq 2$ için $2-(n^2,n,1)$ tasarımının olmasıdır[12].

İspat: X herhangi bir nokta olsun. $A_{1'}$ aksiyomundan bütün doğrular X noktasından geçmez. O halde $L \cap \{x\} = \varnothing$ olacak şekilde bir L doğrusu olsun. L doğrusu üzerinde n tane farklı nokta olsun. O halde x noktasından geçen $n+1$ tane doğru vardır. Eğer L'de $L' \cap \{x\} = \varnothing$ olacak şekilde başka doğru olsun. O zaman X noktasında geçen ve L ile kesişen n tane farklı doğru olur. Bundan dolayı her bir

doğru sonlu afin düzlemde n noktaya sahiptir. Bu düzlem bir tasarım olur. Tanımdaki $A_{1'}$ aksiyomundan bu tasarım $2-$tasarım olur. Bir noktadan geçen doğru sayısı $n+1$ dir$\left(r=n+1\right)$. Herhangi iki nokta bir tek doğru üzerinde olduğundan $\lambda=1$ dir. Ayrıca $\left(v-1\right)/(k-1)=r/\lambda$ den $v=n^2$ olur. $vr=bk$ eşitliğinden $b=n^2+n$ bloğa sahip olur. O zaman herhangi bir afin düzlem $2-(n^2,n,1)$ tasarımı olur. Tersine n≥2 için $2-(n^2,n,1)$ tasarımı olsun. Bu tasarıma göre iki nokta yalnız bir blokta bulunur. O zaman $A_{1'}$ aksiyomu sağlanır. Her bir nokta $n+1$ blokta bulunur. Bu yüzden $A_{2'}$ aksiyomu da sağlanır. Verilen bir doğru n tane farklı nokta içerir. Bu nedenden dolayı L ile kesişen n farklı doğru vardır. X noktasından geçen ve L ile kesişmeyen tam olarak bir tek doğru vardır. O zaman n^2 nokta vardır. Her bir doğru n tane noktaya sahiptir. O halde $2-(n^2,n,1)$ tasarımı bir afin düzlemdir. Teorem 2.3.1.5 ' e göre her sonlu düzlem $(n^2+n+1,n+1,1)$ parametreleriyle verilen simetrik tasarımın bir artık tasarımıdır. Aynı şekilde sonlu bir projektif düzlem $n\geq 2$ için $2-(n^2+n+1,n+1,1)$ simetrik tasarımıdır.

Teorem 3.3.2: P projektif düzlemi L_∞ doğrusunu içersin. P 'nin, L_∞ doğrusuna ait olmayan noktaların kümesi ile ve $L\backslash L_\infty$ doğrular kümesinden oluşturulan yapı bir afin düzlemdir. (L de P 'nin bir doğrusudur)[11].

Önerme 3.3.1: Paralellik bir denklik bağıntısıdır[3].

Teorem 3.3.3: Her afin düzlem bir doğru eklenerek projektif düzlem elde edilebilir [11].

3.4. Latin Kareler ve Dik Dizimler (Orthogonal arraylar)

Tanım 3.4.1: n elemanlı bir küme üzerinde tanımlanan $n \times n$ boyutunda bir kare matrisin her satır ve sütununda kümenin bütün elemanları birer kez kullanıyorsa bu matrise n mertebeden Latin kare denir. Kümelerimiz genellikle $\{1,2,...,n\}$ veya $\{0,1,2,....,n-1\}$ ile gösterilir.

Tanım 3.4.2: Q, n elemanlı bir küme ve "o" Q üzerinde bir ikili işlem olsun. "o" ikili işlemi Q üzerinde şu şekilde tanımlanır. Her $a,b,\in Q$ için $aox = b$ ve $yoq = b$ olacak şekilde tek çözüm varsa (Q,o) ikilisine n mertebeden yarı grup (quasıgroup) denir. Yarı grup bir Latin karedir.

Tanım 3.4.3: $L = (l_{ij})$ ve $M = (m_{ij})$ nxn boyutunda iki Latin kare olsun. Her i, $j = \{1,2....n\}$ için $\left(l_{ij}, m_{ij}\right)$ tüm sıralı ikileri farklı oluyorsa, L ve M ye birbirlerine dik iki Latin karedir.

Örnek 3.4.1:

$$L = \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix} \quad \text{ve} \quad M = \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$$

$3x3$ 'lük iki Latin kare olsun. Yukarıdaki iki Latin kareyi tek kareyle gösterelim.

$$\begin{matrix} 11 & 22 & 33 \\ 23 & 31 & 12 \\ 32 & 13 & 21 \end{matrix}$$

şeklindedir. O halde bu Latin karenin tüm ikileri farklı olduğundan L ve M Latin kareleri birbirine diktir.

n mertebeden s tane Latin karenin kümesi eğer $1 \le i \prec j \le s$ için L_i ve L_j Latin kareleri ikişerli birbirine dikse $L_1, L_2, L_3, ..., L_s$ Latin karelerine MOLS denir. (Mutually Orthogonal Latin Squares)

En önemli temel problemlerden biride n mertebeden en fazla kaç tane birbirine dik Latin kare vardır. Bu maksimum sayıyı da $N(n)$ ile gösterilir. Eğer $n=1$ ise $N(n)=\infty$ dir. Şimdi $n \ge 1$ maksimum sayıyı bulalım.

Teorem 3.4.1: n mertebenden en fazla $n-1$ tane birbirine dik Latin kare vardır $[5]$.

Teorem 3.4.2: Her p asal sayısı için, p 'inci mertebeden en fazla $p-1$ tane birbirine dik Latin kare vardır $[5]$.

Teorem 3.4.3: p asal ve a pozitif bir sayı olsun. Eğer $n = p^a$ ise n mertebeden birbirine dik tam olarak $n-1$ tane Latin kare vardır $[5]$.

Teorem 3.4.4: $n \ge 2$ aşağıdaki ifadelerden biri varsa diğer ikiside vardır.

1) $n-1$ MOLS(n) ;
2) n mertebeden afin düzlem
3) n mertebenden projektif düzlem $[12]$.

Örnek 3.4.2: Euler subay problemi 6 farklı rütbeden ve 6 farklı olaydan her rütbeden ve alaydan birer subay nasıl seçilir. 36 subay 6 farklı rütbeden ve 6 farklı olaydan seçilmiştir. Böylece her bir satır ve sütunda rütbe ve birlikleri farklı 6 subay bulunacaktır. Subayların rütbeleri bir Latin kare, geldikleri birliklerde bir Latin kare meydana getireceğinden 2 ' tane Latin kare oluşacaktır. Fakat 2 Latin karede her sıralanış sadece 1 kez tekrarlanacaktır. Eğer biz rütbeleri $1,2,3,4,5,6$ ve olayları da $1,2,3,4,5,6$ numaralandırırsak o zaman her bir subay tek bir sıralı ikiliyi temsil eder.

$(x.y) \in \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$ İlk koordinat rütbeyi, ikinci koordinat alayı belirtir. Euler subay probleminde 36 sıralı (x, y) ikilisini oluşturur.

Euler subay problemin çözümünü 1900 yılında G. Tarry böyle ikili dik latin karelerin olmadığını gösterdi $[14]$. Daha sonra ise kısa bir ispatını Doug Stinson vermiştir$[15]$.

Önerme 3.4.5: $n \times n$ boyutlu k ikili dik Latin karelerin kümesi tüm girdileri $\{1,2,...n\}$ kümesinden olan ve her bir satır, sütunu sıralı ikilileri içeren $n^2 \times (k+2)$ boyutlu bir matrise denktir$[3]$.

3.4.1 Latin karelerden afin düzlem elde etme

Afin Düzlemelerin elde edilişi için n'inci mertebeden Latin kare tam seti $(n-1$ MOLS$)$ kullanılabilir. n'inci mertebeden Latin kare tam seti L_1, L_1, L_{n-1} şeklinde olsun. Burada, noktaları

$X = \{1,2,...,n\} \times \{1,2,...,n\}$ olan Afin düzlem oluşturulacaktır. Afin Düzlemin blokları aşağıdaki gibidir.

$1 \le x \le n-1, 1 \le k \le n$

$A_{x,k} = \{(i, j) : L_x(i, j) = k\}.$

ve $1 \le k \le n$ için

$A_{n,k} = \{(i, j) : 1 \le j \le n\}$

Böylece;

$B = \{A_{x,k} \mid 1 \le x \le n+1, 1 \le k \le n\}$

şeklinde oluşur. Burada (X, B) yapısına n'nci mertebeden Afin düzlemi denir.

Örnek 3.4.3: $n=4$ mertebeden birbirine dik Latin kareler 3 tanedir.

$$\{L_1,L_2,L_3\}=\left\{\begin{bmatrix}1&2&4&3\\2&1&3&4\\4&3&1&2\\3&4&2&1\end{bmatrix},\begin{bmatrix}1&3&4&2\\4&2&1&3\\2&4&3&1\\3&1&2&4\end{bmatrix},\begin{bmatrix}1&4&2&3\\3&2&4&1\\4&1&3&2\\2&3&1&4\end{bmatrix}\right\}$$

Bu Latin kareler ikişerli olarak 16 nokta oluşturur.

$(1,1),(1,2),...,(4,4)$. Bu noktaları kolaylık olsun diye $11,12,...,44$ olarak yazılır. Doğrularımız şunlar ;

Birinci tip:

$11,12,13,14$
$21,22,23,24$
$31,32,33,34$
$41,42,43,44$

İkinci tip:

$11,21,31,41$
$12,22,32,42$
$13,23,33,43$
$14,24,34,44$

Üçüncü tip:

L_1	L_2	L_3
$11,22,33,44$	$11,32,43,24$	$11,42,23,34$
$21,12,43,34$	$41,22,13,34$	$31,22,43,14$
$41,32,23,14$	$21,42,33,14$	$41,12,33,24$
$31,42,13,24$	$31,12,23,44$	$21,32,13,44$

Tanım 3.4.4: Tüm girdileri {1, 2, 3….n} kümesinden ve k tane sütuna sahip olan bir matrisin eğer her bir t sütunlu alt kümesi; $\{1,2,3....n\}$ kümesinin her t sıralısını tam olarak λ defa içeriyorsa $t-(n,k,\lambda)$ bir dik dizim (orthogonal array) denir.

Bir $t-(n,k,\lambda)$ dik dizininde tam olarak λn^t satıra sahiptir. Çünkü n^t farklı $t-$ sıralısı var ve her $t-$sıralısı tam olarak λ defa meydana geliyor. Önerme 3.4.5'e göre k ikişerli dik Latin kareler, $2-(n,k+2,1)$ diz dizinine denktir.

1) Satırların sırasını değiştirelim.
2) Sütunların sırasını değiştirelim.
3) Verilen bir sütunda girdilerin permutasyonu yaparsak (örneğin tüm 1'lerin ve 2 'lerin yerini değiştirelim.) Satırların sırasını değiştirsek değişmez. Çünkü her bir $t-$ sıralısının sayısı değişmez. Sütunların sırasını değiştirsek sonuç değişmez. Çünkü girdilerimiz değişmiyor. 1 yerine 2 ve 2 yerine 1 yazdığımızdan $t-$sıralı değişmez. O halde dikdizimler bu işlemler altında dik dizimdir.

Tanım3.4.5: Eğer A_2 dizininden $(i),(ii),(iii)$ işlemleri yaparak A_1 dizimi elde edilebiliyorsa A_1 ve A_2 dizilerine denk dizimler denir.

3.5. Cisimden Dik Dizim Oluşturma

3.5.1. Cebirsel yolla latin kare elde etme

$(F,+,.)$ q elemanlı bir cisim ve $q=p^n$ olacak şekilde p asal sayı ve n doğal sayı olsun. $2-(q,q+1,1)$ dik dizimi aşağıdaki gibi oluşturalım.

F cisminde ζ primitif eleman olsun. Dizinimizin satırları $(q+1)-$sıralısıdır.

$(x, y \in F)$

$(x, y, x+y, x+\zeta y, ..., x+\zeta^{q-2} y)$

Şimdi $q^2 x(q+1)$ matrisini aşağıdaki gibi elde ederiz.

$1 \le i, j \le q$ ve i, j şimdi $q^2 \times (q+1)$ matrisini düşünelim.

$(q+1)-$sıralı $(x_i, x_j, x_i+\zeta^0 x_j, ..., x_i+\zeta^{q-2} x_j)$ oluşturulan matrisin satırlarıdır.

$$\begin{bmatrix}
x_1 & x_1 & x_1 + x_1 & x_1 + \zeta x_1 & \ldots\ldots\ldots & x_1 + \zeta^{q-2} x_1 \\
x_1 & x_2 & x_1 + x_2 & x_1 + \zeta x_2 & \ldots\ldots\ldots & x_1 + \zeta^{q-2} x_2 \\
\ldots\ldots\ldots & & & & \ldots\ldots\ldots & \\
x_1 & x_q & x_1 + x_q & x_1 + \zeta x_q & \ldots\ldots\ldots & x_1 + \zeta^{q-2} x_q \\
\ldots\ldots & & & & \ldots\ldots\ldots & \\
x_q & x1 & x_q + x_1 & x_q + \zeta x_1 & \ldots\ldots\ldots & x_q + \zeta^{q-2} x_1 \\
x_q & x_2 & x_q + x_2 & x_q + \zeta x_2 & \ldots\ldots\ldots & x_q + \zeta^{q-2} x_2 \\
\ldots\ldots\ldots & & & & \ldots\ldots\ldots & \\
x_q & x_q & x_q + x_q & x_q + \zeta x_q & \ldots\ldots\ldots & x_q + \zeta^{q-2} x_q
\end{bmatrix}$$

Eğer biz birinci x'e $(i+3)-$inci sütunu alalım. $q-2 \geq i \geq 0$ olduğundan ζ^{-1} vardır.

$$(x_k, x_k + (n^4 - n^2)/2^i + x_{t_1}) = (x_k, x_k + \zeta^i x_{t_2})$$

$$\Leftrightarrow x_{t_1} = x_{t_2}.$$

Eğer biz ikinci ve $(i+3)^{th}$ sütunu alırsak $q-2 \geq i \geq 0$ o zaman ζ^{-1} vardır.

$$(x_k, x_{i_1} + \zeta^{\mathrm{i}} x_k) = (x_k, x_{i_2} + \zeta^{\mathrm{i}} x_k)$$

$$\Leftrightarrow X_{i_1} = X_{i_2}.$$

Son olarak biz $(m_1+3)^{th}$ ve $(m_2+3)^{th}$ sütunları $o \leq m_1, m_2 \leq q-2$ alırsak

$$\left(X_{i_1} + \zeta^{m_1} X_{i_2}, X_{i_1} + \zeta^{m_2} X_{i_2} \right) = \left(X_{j_1} + \zeta^{m_1} X_{j_2}, X_{j_1} + \zeta^{m_2} X_{j_2} \right)$$

$$\Leftrightarrow \zeta^{m_1}(x_{j_2} - x_{i_2}) = \zeta^{m_2}(x_{j_2} - x_{i_2})$$

$$\Leftrightarrow \quad \zeta^{m_1} = \zeta^{m_2}$$

$$\Leftrightarrow \quad m_1 = m_2$$

Böylece her bir sütun çifti her bir $2-$sıralı bir defa içerir $[16]$.

Teorem 3.5.1: Mertebesi n olan afin düzlem $2-(n,n+1,1)$ dik dizinine eşittir$[3]$.

3.5.2. Cebirsel yolla yarı grup elde etme

$(F,+,.)$ q elemanlı bir sonlu cisim olsun. Kabul edelim ki $F=\{1,2,.....q\}$ ve q burada sıfır elemanı gösteriyor. Her $q\neq k\in F$ için F üzerinde $o(k)$ ikili işlemi şu şekilde tanımlansın.

$xo(k)y=xk+y$ o zaman $(F,o(k))$ bir yarı gruptur. Kabul edelim ki
$xo(k)y=xo(k)z\Rightarrow xk+y=xk+z$ buradan $y=z$ olur. Öte yandan eğer
$yo(k)x=zo(k)x\Rightarrow yk+x=zk+x\Rightarrow yk=zk\Rightarrow y=z$ olur. $k\neq q$ olduğundan
$(F,o(k))$ bir yarı grup olur$[16]$. (Aynı zamanda Latin karedir)

Örnek 3.5.1: 4 mertebeden yarı grup aşağıdaki şekilde oluşturulur. 4. mertebeden cisim üzerindeki indirgenmez polinomumuz $1+x+x^2$ olsun.

Tablo3.3. Cisimden elde edilen Latin kareler

+	0	1	x	1+x
0	0	1	x	1+x
1	1	0	1+x	x
x	x	1+x	0	1
1+x	1+x	x	1	0

.	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
$1+x^2$	0	$1+x^2$	1	x

Cismimizin $0,1,x$ ve $1+x$ elemanları sırasıyla $4,1,2,3$ ile adlandırırsak tablomuz aşağıdaki gibi olur.

Tablo 3.4. 4. mertebeden cisim üzerinde toplama ve çarpma

+	4	1	2	3
4	4	1	2	3
1	1	4	3	2
2	2	3	4	1
3	3	2	1	4

.	4	1	2	3
4	4	4	4	4
1	4	1	2	3
2	4	2	3	1
3	4	3	1	2

F cismimizin sıfır dışındaki elemanları $1, 2$, ve 3 'tür.

O halde 3 tane yarı grup oluşturulur.

Tablo3.5. Cismin elemanlarından oluşan yarı gruplar

Q(1)	4	1	2	3
4	4	1	2	3
1	1	4	3	2
2	2	3	4	1
3	3	2	1	4

Q(2)	4	1	2	3
4	4	1	2	3
1	2	3	4	1
2	3	2	1	4
3	1	4	3	2

Q(3)	4	1	2	3
4	4	1	2	3
1	3	2	1	4
2	1	4	3	2
3	2	3	4	1

Bu tablolar 4. Mertebeden F cismi üzerinden toplama ve çıkarma işlemi yapılarak yazılmıştır.

Teorem 3.5.2: $(F,+,.)$ q mertebeli sonlu bir cisim olsun. $(F=\{1,2,3....q\}, q=0)$ o zaman $(F,o(1)),(F,o(2)),....,(F,o(q-1))$ mertebesi q olan dik yarı grup olur$[16]$.

İspat: $(F,o(k))$ yarı grubunu $L(k)$ Latin karesi göstersin. O zaman bu Latin karelerin dikliğini gösterelim. Bunun içinde $1 \le k < l < q$ ve $L(k)$ ve $L(\ell)$ iki Latin kare olsun. Şimdi iki parmak kuralı ile bu iki Latin karenin dikliği ispatlayalım. Kabul edelim ki (i_1, j_1) ve (i_2, j_2) hücrelerini aynı sembolü $L(k)$ ve $L(\ell)$ Latin kareleri içersin. O zaman $i_1 = i_2$ ve $j_1 = j_2$ eşit olduğunu kanıtlamalıyız. Kolaylık olsun diye $x.y$ yerine xy diyeceğiz. Ayrıca

$(F,o(k))$ ve $(F,o(k))$ yarı grup olduklarından (tanımdan)

$$i_1k + j_1 = i_2k + j_2$$
$$i_1\ell + j_1 = i_2\ell + j_2$$
$$i_1k + j_1 - i_2k = j_2 = i_2\ell + j_1 - i_2\ell \text{ veya}$$
$$(i_1 - i_2)k = (i_1 - i_2)\ell$$

$k \neq \ell$ ve k, $\ell \neq 0$ olduğundan bu eşitlik ancak $i_1 - i_2 = 0$ olduğunda sağlanır. O zaman $j_1 = j_2$ olur. Önerme 3.4.5.'e göre $q-1$ ikişerli dik Latin karenin kümesi, $2-(q,q+1,1)$ dik dizemine denktir. Bu yüzden bizim dik dizinimizde $2-(q,q+1,1)$ olur.

BÖLÜM 4. VEKTÖR UZAYLARI VE TASARIMLAR

4.1. Vektör Uzayı

Bu bölümde $2-$tasarımları için sonlu boyutlu vektör uzayını düşüneceğiz. F cismi üzerindeki $n-$boyutlu vektör uzayını $V(n,F)$ ile gösterilir.

Tanım 4.1.1: $q-$Gauss katsayı olmak üzere

$\begin{bmatrix} n \\ k \end{bmatrix}_q$ veya $\begin{bmatrix} n \\ k \end{bmatrix}$ sayısı q elemanlı F cismi üzerindeki $n-$boyutlu vektör uzayının $k-$boyutlu alt uzaylarının sayısıdır.

$\begin{bmatrix} n \\ 0 \end{bmatrix}=1$ olduğunu kabul ediyoruz.

Gaus katsayılarında $\begin{bmatrix} n \\ k \end{bmatrix}=\begin{bmatrix} n \\ n-k \end{bmatrix}$ olduğundan; $\begin{bmatrix} n \\ n \end{bmatrix}=1$dir.

Şimdi $\begin{bmatrix} n \\ 1 \end{bmatrix}$'lisi $n-$boyutlu vektör uzayının $1-$boyutlu alt uzaylarının sayısıdır. Bu sayıyı hesaplayalım. $V=V(n,q)$ vektör uzayının $1-$boyutlu alt uzayları $U_1,U_2,U_3,....U_r$ olsun. $i\in\{1,2,.....,r\}$ için $U_i\backslash\{0\}$ kümeleri vektör uzayını $V\backslash\{0\}$ kümelerine ayırır. O halde ; $|U_i|=q$ her i için

$r(q-1)=q^n-1 \quad \Rightarrow \quad r=\dfrac{q^n-1}{q-1}$ olur.

O zaman $\begin{bmatrix} n \\ 1 \end{bmatrix} = \frac{q^n - 1}{q - 1}$.

$\begin{bmatrix} n \\ k \end{bmatrix}$ ile (B, U) ikilerinin sayısını hesaplanır; burada B, U 'nun sıralı bir bazı , U da V nin bir alt uzayı ve $\dim U = k$ dır. Her bir B sıralı bazı U alt uzayını belirtir. Bu yüzden $\begin{bmatrix} n \\ k \end{bmatrix}$'lisi q elemanlı F cismi üzerindeki $n-$boyutlu vektör uzayının k elemanlı lineer bağımsız kümelerin sayısıdır. Bu sayı $(q^n - 1)(q^n - q)(q^n - q^2)....(q^n - q^{k-1})$. Diğer taraftan eğer U, V vektör uzayının $k-$boyutlu alt uzayı ise U 'nun bir bazı $(q^k - 1)(q^k - q)....(q^k - q^{k-1})$ olur.

$$(q^n - 1)(q^n - q)....(q^n - q^{k-1}) = \begin{bmatrix} n \\ k \end{bmatrix}.(q^k - 1)(q^k - q)....(q^k - q^{k-1}).$$

Böylece

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{(q^n - 1)(q^n - q).....(q^n - q^{k-1})}{(q^k - 1).(q^k - q).....(q^k - q^{k-1})} \qquad (4.1)$$

$$= \frac{(q^n - 1)(q^{n-1} - 1).....(q^{n-k+1} - 1)}{(q^k - 1).(q^{k-1} - 1).....(q - 1)}.$$

O zaman $[n] = \begin{bmatrix} n \\ 1 \end{bmatrix}$ ve $[n]! = [n].[n-1]....[1]$ (4.2) belirtir. O halde (4.1) eşitliğine göre

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]!}{[k]![n-k]!}. \qquad (4.2)$$

Eğer $q = 1$ alırsak $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{pmatrix} n \\ k \end{pmatrix}$ olur. Ayrıca Eşitlik (4.2) den $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}$ eşit olur.

Teorem 4.1.1: $V = V(n,q)$ olsun. V 'nin $1-$boyutlu alt uzayı noktalar kümesi, V 'nin $k-$boyutlu alt $(1<k<n)$ uzaylarını bloklar kümesini göstersin ve çakışım yapısı D olsun. O zaman D

$V=[n],\ b=\begin{bmatrix} n \\ k \end{bmatrix},\ r=\begin{bmatrix} n-1 \\ k-1 \end{bmatrix},\ "k"=[k],\ \lambda=\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ parametreleriyle verilen bir $2-$ tasarımdır $[17]$.

İspat: n-boyutlu V vektör uzayının $1-$boyutlu alt uzay sayısı [n] dir. O halde D'nin $[n]$ noktası olur. q Gauss katsayıların tanımı gereğince V 'nin $k-$boyutlu alt uzayı sayısı $\begin{bmatrix} n \\ k \end{bmatrix}$ dır. O zaman D'nin $\begin{bmatrix} n \\ k \end{bmatrix}$ bloğu olur.

Şimdi her bir bloğun içerdiği nokta sayısını hesaplayalım. V 'nin $1-$boyutlu alt uzayı noktalar kümesinin, $k-$boyutlu her alt uzayı $\begin{bmatrix} k \\ 1 \end{bmatrix}$ noktaya sahiptir. Bu yüzden D çakışım yapısı bir tasarımdır. Her bir $1-$boyutlu alt uzay çifti $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ $k-$boyutlu alt uzaya aittir. O zaman D bir $2-$tasarım ve $\lambda=\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ dir. Son olarak $1-$boyutlu alt uzay sayısı $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ $k-$boyutlu alt uzaya ait olur.

Eğer $k=n-1$ alırsak Teorem 4.1.2 gereğince simetrik tasarım elde ederiz.

Eğer $k=2$ alırsak $\lambda=\begin{bmatrix} n-2 \\ 0 \end{bmatrix}=1$ olur.

Eğer $n=3$ ve $k=2$ alırsak $\lambda=1$ ile verilen simetrik tasarım olur. Bu simetrik tasarım q mertebeden bir projektif düzlemdir.

Tanım 4.1.2: $V(n,F)$ bir vektör uzayı olsun. V 'nin bir $(n-1)-$boyutlu alt uzayına hiper düzlem denir.

Teorem 4.1.2: $V=V(n,q)$ ve V 'nin hiper düzlemi H olsun. D çakışım yapısı V 'nin $1-$boyutlu alt uzayı fakat H 'nin noktaları değil ve V 'nin $k-$boyutlu alt uzayı $(1<k<n)$ D nin blokları fakat H ' nin blokları değil ise o zaman D çakışım yapısı bir 2 tasarım olur. O halde D

$V=q^{n-1}, b=q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}, r=\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}, "k"=q^{k-1}, \lambda=\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ parametreleriyle verilen bir $2-$tasarımdır$[17]$.

İspat: V 'nin $k-$boyutlu alt uzay sayısı $\begin{bmatrix} n \\ k \end{bmatrix}$ ve H 'nin $k-$boyutlu alt uzay sayısı $\begin{bmatrix} n-1 \\ k \end{bmatrix}$ dır. O halde D 'nin blok sayısı

$$\begin{bmatrix} n \\ k \end{bmatrix}-\begin{bmatrix} n-1 \\ k \end{bmatrix}=\frac{(q^n-1)(q^n-q)....(q^n-q^{k-1})-(q^{n-1}-1)(q^{n-1}-q)...(q^{n-1}-q^{k-1})}{(q^{k-1}-1)...(q^{k-1}-q).....(q^{k-1}-q^{k-2})}$$

$$=q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$

V 'nin $k-$boyutlu bir alt uzayı $\begin{bmatrix} k \\ 1 \end{bmatrix}$ $1-$boyutlu alt uzaya ve H hiper düzlemi $\begin{bmatrix} k-1 \\ 1 \end{bmatrix}=q^{k-1}$ noktaya sahiptir. Teorem 4.1.2 gereğince her bir nokta $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ bloğa aittir. Her bir nokta çifti $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ blokta bulunur.

Eğer $k=n-1$ alırsak bu tasarım Teorem 4.1.2 gereğince simetrik tasarımın bir artık tasarımı olur.

Eğer $n=3, k=2$ ise bu tasarımdan afin düzlem elde edilir.

Örnek 4.1.1: 3 boyutlu 2 mertebeli $2-(15,7,3)$' ye ait 3-boyutlu hiper düzlemler ve üzerindeki noktalar aşağıdaki gibidir. (q boyutlu n mertebeli projektif düzlem $PG(n,q)$ ile gösterilir.)

Tablo 4.1. Projektif düzlemden elde edilen tasarım

	B_1	B_2	B_3	B_4	B_5	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}
X_1	0	1	0	1	0	0	0	0	0	0	1	0	1	0
X_2	1	0	0	1	1	0	0	1	1	0	1	1	0	0
X_3	0	0	1	1	0	1	1	0	0	1	1	0	0	1
X_4	1	1	1	0	0	0	0	1	1	1	0	0	0	0
X_5	0	1	0	0	1	1	1	0	1	0	0	1	0	1
X_6	1	0	0	0	0	1	1	1	1	0	0	0	1	1
X_7	0	0	1	0	1	0	0	0	0	1	0	1	1	0
X_8	1	1	1	1	1	1	1	0	0	0	0	0	0	0
X_9	0	1	0	1	0	0	0	1	1	1	0	1	0	1
X_{10}	1	0	0	1	1	0	0	0	0	1	0	0	1	1
X_{11}	0	0	1	1	0	1	1	1	1	0	0	1	1	0
X_{12}	1	1	1	0	0	0	0	0	0	0	1	1	1	1
X_{13}	0	1	0	0	1	1	1	1	1	1	1	0	1	0
X_{14}	1	0	0	0	0	1	1	0	0	1	1	1	0	0
X_{15}	0	0	1	0	1	0	0	1	1	0	1	0	0	1

Burada hiper düzlemler, bloklar gibi düşünüldüğünde bunun bir simetrik tasarım çakışım matrisi olduğu görülür. Bu tasarım 2-(15,7,3) simetrik tasarımıdır.

Aynı örneği afin düzlem için yapalım. Birinci hiper düzlem ve bu düzleme ait noktalar çıkarılsın. Bu durumda bir $AG(n,q)$ ya ait doğrular ve üzerindeki noktalar; (q boyutlu n mertebeli afin düzlem $AG(n,q)$ ile gösterilir.)

Tablo 4.2. Afin düzlemden elde edilen tasarım

	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}
X_1	1	0	1	0	1	0	1	0	1	0	1	0	1	0
X_3	9	1	1	0	0	1	1	0	0	1	1	0	0	1
X_5	1	0	0	1	0	1	1	0	1	0	0	1	0	1
X_7	9	1	0	1	1	0	1	0	0	1	0	1	1	0
X_9	1	0	1	0	1	0	0	1	0	1	0	1	0	1
X_{11}	9	1	1	0	0	1	0	1	1	0	0	1	1	0
X_{13}	1	0	0	1	0	1	0	1	0	1	1	0	1	0
X_{15}	9	1	0	1	1	0	0	1	1	0	1	0	0	1

şeklinde olacaktır.

Görüldüğü gibi $2^3 = 8$ noktalı ve $\left(2^4 - 2\right)/\left(2-1\right) = 14$ hiper düzlemli bir afin geometri elde edilir. Bu tasarım aynı zamanda $2-\left(8,4,3\right)$ tasarımıdır.

BÖLÜM 5.TASARIM TEORİSİNDEN KOD OLUŞTURMA

5.1. Tasarım ve Kod

Önerme 5.1.1: $2-(v,k,\lambda)$ tasarımın çakışım matrisi vxb boyutlu N matrisi olsun. Eğer $n=b, M=v, d=2(r-\lambda), t=r-\lambda-1$ ise $w(c)=r$ her $c\in C$ için N çakışım matrisinin satırlarının oluşturduğu C kodu $t-$hata düzelten bir (n,M,d) kodudur$[5]$.

Örnek 5.1.1: $P=\{P_1,P_2,P_3\}$ noktaların kümesi olsun. $B_1=\{P_1,P_2\}, B_2=\{P_2,P_3\}$ ve $B_3=\{P_1,P_3\}$ bloklar kümesi olsun. O halde $B=\{B_1,B_2,B_3\}$ bloklar kümesidir. Bu tasarımın parametreleri $(v,k,\lambda)=(3,2,1)$ ve $b=3, r=\lambda(v-1)/(k-1)$

$r=(3-1)/(2-1)=2$ ve $d=2(r-\lambda)=2.(2-1)=2$ olur. Bu tasarımın çakışım matrisi $N_1=\begin{pmatrix}1&0&1\\1&1&0\\0&1&1\end{pmatrix}$ dir.

Bu matris $(3,3,2)$ ikili kodunu oluşturur. Bu kod hiç hata düzeltmez. Ancak bir hata tespit eder.

Eğer $B_4=B_1, B_5=B_2$ ve $B_3=B_6$ alıp bloklar kümesini $B=\{B_1,B_2,B_3,B_4,B_5,B_6\}$ olarak düzenlersek tasarımımız bir DTBT tasarımı ve parametreleri $(v,k,\lambda)=(3,2,2)$ dir. O halde $b=6, r=4, d=4$ ve $t=1$ olur. Bu tasarımın çakışım

matrisi $N=\begin{pmatrix}1&0&1&1&0&1\\1&1&0&1&1&0\\0&1&1&0&1&1\end{pmatrix}$ olur. Bu tasarım $(6,3,4)$ kodunu oluşturur. Bu kod tek hata düzeltir.

Örnek 5.1.2: Bloklar kümesi $B=\{B_1,B_2,B_3,B_4,B_5,B_6,B_7,B_8,B_9,B_{10},B_{11},B_{12}\}$ ve noktalar kümesi $P=\{1,2,.....,9\}$ olsun. $B_1=\{1,2,3\}$, $B_2=\{1,4,7\}$, $B_3=\{1,5,9\}$, $B_4=\{1,6,8\}$, $B_5=\{2,4,9\}$, $B_6=\{2,5,8\}$, $B_7=\{2,6,7\}$, $B_8=\{3,4,8\}$, $B_9=\{3,5,7\}$, $B_{10}=\{3,6,9\}$, $B_{11}=\{4,5,6\}$ *ve* $B_{12}=\{7,8,9\}$ bloklarımız olmak üzere o zaman bu tasarım bir $DTBT$ tasarımıdır. Tasarımın parametreleri $(v,k,\lambda)=(9,3,1)$ şeklindedir. Bu tasarımda $b=12$ ve $r=\lambda(v-1)/(k-1)=4$ olur. Bu tasarımın çakışım matrisi

$$\begin{array}{c} \\ 1\\2\\3\\4\\5\\6\\7\\8\\9\end{array}\begin{array}{c}\begin{array}{cccccccccccc}B_1&B_2&B_3&B_4&B_5&B_6&B_7&B_8&B_9&B_{10}&B_{11}&B_{12}\end{array}\\\begin{pmatrix}1&1&1&1&0&0&0&0&0&0&0&0\\1&0&0&0&1&1&1&0&0&0&0&0\\1&0&0&0&0&0&0&1&1&1&0&0\\0&1&0&0&1&0&0&1&0&0&1&0\\0&0&1&0&0&1&0&0&1&0&1&0\\0&0&0&1&0&0&1&0&0&1&1&0\\0&1&0&0&0&0&1&0&1&0&0&1\\0&0&0&1&0&1&0&1&0&0&0&1\\0&0&1&0&1&0&0&0&0&1&0&1\end{pmatrix}\end{array}$$

Matrisin satırlarının oluşturduğu kod ise $(12,9,6)$ kodudur. Bu kod iki hata düzeltir. Şimdi bu matrisin sütunların oluşturduğu koda bakalım. Her bir nokta çifti yalnız bir bloğa aittir ve herhangi iki bloğun arakesiti yalnız bir noktadır. O halde $\lambda=1$ dir. Her bir blokta 3 nokta vardır. O halde $d=2(r-\lambda)=2(3-1)=4$ olur. Matrisin sütunların oluşturduğu kod $(9,12,4)$ kodudur. Bu kod tek hata düzeltir.

5.2. Simetrik Tasarımdan Kod Oluşturma

(v,k,λ) parametreleri simetrik tasarımın parametreleri olsun. O halde (v,k,λ) tasarımı simetrik olduğundan $(v-1)\lambda = k(k-1)$ eşitliğinden $v = 1+\frac{k(k-1)}{\lambda}$ olur. O halde bu tasarımın var olabilmesi için λ'nın $k(k-1)$ bölmesi gerekir.

Teorem 5.2.1: D bir (v,k,λ) simetrik tasarımı olsun. Eğer v çift sayı ise $k-\lambda$ tam karedir[3].(Shutzenberger)

Teorem 5.2.2: (Bruck- Ryser-chowla) (v,k,λ) simetrik tasarımı olduğunukabul edelim. Eğer v tek sayı ise $x^2 = (-1)^{(v-1)/2}\lambda z^2 + (k-\lambda)y^2$ eşitliğini sağlayan ve hepsi sıfır olmayan x, y, z tamsayıları bir çözümü vardır[3].

Teorem 5.2.3: (v,k,λ) tasarımı bir simetrik tasarım olsun. v tek sayı ve $\neq$ $n = k-\lambda$ olsun. O zaman her bir p tek asal sayısı için;

1) Eğer $p \nmid n^*$ ve $p \mid \lambda^*$ ise n sayısı $(\text{mod } p)$ göre karedir.
2) Eğer $p \mid n^*$ ve $p \nmid \lambda^*$ ise $(-1)^{(v-1)/2}\lambda^*$ sayısı $(\text{mod } p)$ göre karedir.
3) Eğer $p1n^*$ ve $p1\lambda^*$ ise $(-1)^{(v-1)/2}.\left(\frac{\lambda^*}{p}\right).\left(\frac{n^*}{p}\right)$ sayısı $(\text{mod } p)$ göre karedir [18].

(m^*, m^*m çarpımını tam kare yapacak şekildeki en küçük pozitif tamsayıdır.) Teorem 5.2.3'nin 2 ve 3. koşulları simetrik tasarımla ilişkili kendine düal kodun var olduğunu iddia etmektedir. Teorem 5.2.2'e göre n'nın hangi değerleri için n mertebeden projektif düzlemin olmadığını belirtir. $\lambda = 1$ ve $v = n^2+n+1$ tek ise eğer $n \equiv 1$ veya $2 \,(\text{mod } 4)$ ise eşitlik $nX^2 = Y^2 + Z^2$ şekline dönüşür. Bu eşitliğin tam sayılarda aşikâr çözümünden başka çözümün olması için gerekli ve yeterli koşul n'nin iki tam sayının karesi şeklinde yazılmasıdır. Bu durumda $n = 6, 14, 21, 22, 30$

ve 32 mertebeleri için projektif düzlem yoktur. Örneğin $6 = a^2 + b^2$ olacak şekilde a, b tam sayıları yoktur.

Simetrik (v, k, λ) tasarımın olması için gerekli ve yeterli şart λ'nın $k(k-1)$ bölmesi ve Shutzenberger Teoremin ve Bruck-Ryser Chowla Teoreminin sağlamasıdır.

Örnek 5.2.1: N aşağıda verilen simetrik tasarımın çakışım matrisi olsun. Simetrik tasarımın parametreleri $(16, 6, 2)$ ve $N.N^T = 4I_{16} + 2J_{16}$ dır.

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

O halde bu simetrik tasarımın üreteceği kodun parametreleri $n = b = v = 16$, $M = v = 16$ ve $d = 2(r - \lambda) = 2(6 - 2) = 8$ olur. $(16, 6, 2)$ simetrik tasarımı $(16, 16, 8)$ kodunu üretir. $2t + 2 = 8 \Rightarrow 2t = 6 \Rightarrow t = 3$ hata düzelten kod dur. v çift olduğundan $k - \lambda = 6 - 2 = 4$ tam karedir.

Şimdi standard Hadamard matrisine göz atalım. Eğer $t \geq 2$ için $(4t-1, 2t-1, t-1)$ Hadamard tasarımı varsa simetrik tasarımda vardır.

Örnek 5.2.2: $t=2$ için parametreler $(7,3,1)$ tasarımını verir ki bu tasarım ikinci mertebeden projektif düzlemdir. Diğer adıyla Fano düzlemdir. Bu tasarımın parametreleri $(7,3,1)$ dir. Bu tasarımı noktaları kümesi de $P=\{1,2,....,7\}$, bloklar kümesi ise 7 bloktan oluşur bunlar ;

$B_1=\{1,2,3\}$, $B_2=\{1,4,7\}$, $B_3=\{1,5,7\}$, $B_4=\{2,4,6\}$, $B_5=\{2,5,7\}$, $B_6=\{3,4,5\}$
$B_7=\{3,6,7\}$ dir.

Çakışım matrisi $N=\begin{pmatrix}1&1&1&0&0&0&0\\1&0&0&1&1&0&0\\1&0&0&0&0&1&1\\0&1&0&1&0&1&0\\0&0&1&0&1&1&0\\0&0&1&1&0&0&1\\0&1&0&0&1&0&1\end{pmatrix}$ olur.

Şimdi bu tasarımdan elde edilen Hadamard matrisi de bulalım. Çakışım matrisinde sıfır olan her yere -1 yazalım. Bileşenlerin tümü 1 olan 1. satır ve 1. sütün ekleyerek matrisi genişletelim. O halde çakışım matrisinden elde edilen Hadamard matrisi (standart Hadamard matrisi)

$H=\begin{pmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&-1&-1&-1&-1\\1&1&-1&-1&1&1&-1&-1\\1&1&-1&-1&-1&-1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&-1&-1&1&-1&1&1&-1\\1&-1&-1&1&1&-1&-1&1\\1&-1&1&-1&-1&1&-1&1\end{pmatrix}$ olur.

Bu tasarımın ürettiği kod ise $M=v=n=b, d=2.(r-\lambda)$ eşitliklerinden

$\left.\begin{array}{l} v=7 \\ r=3 \\ \lambda=1 \end{array}\right\} \Rightarrow$ O halde Hadamard matrisinden elde edilen Dengeli Tamamlanmamış Blok Tasarımdan elde edilen kod $(7,7,4)$ kodu olur. Şimdi yaptığımız işlemi genelleştirelim. Mertebesi $4t-1$ olan bir Hadamard tasarımının çakışım matrisinin ürettiği kod $(t \leq 2)$ $(4t-1,4t-1,2t)$ şeklindedir. Simetrik tasarımlardan farklı şekilde kodlar elde edilebilirler. Biz birkaç yol üzerinde durulacak. Şimdi simetrik tasarımdan elde edilen düal kodları inceleyelim. D bir simetrik (v,k,λ) tasarımı ve N de çakışım matrisi olsun.

$G=[I:N]$ olsun.

$$G.G^T=[I:N]\begin{bmatrix} I \\ N^T \end{bmatrix}=I+N.N^T$$

$$=(k+1-\lambda)I+\lambda J$$

Eğer $k+1$ ve λ'nın her ikiside p'ye bölünüyorsa $G.G^T \equiv 0(\text{mod}\, p)$ olur. O zaman G satır uzayı $GF(p)$ üzerinde kendine dik kod olur. Bu yüzden $\lambda \equiv 0, k \equiv -1 \,(\text{mod}\, p)$ ise $\det N = k(k-\lambda)^{(v-1)/2}$ olur. fakat $\det N$, p'ye bölünmez. Bu yüzden G'nin rankı $GF(p)$ üzerinde rankı v olur. O halde kendine düal kod olur.

Örnek 5.2.3: P ikinci mertebeden bir projektif düzlem olsun. $\{1,2,3\}$, $\{1,3,6\}$, $\{1,4,7\}$, $\{2,3,7\}$, $\{2,4,6\}$, $\{3,4,5\}$ ve $\{5,6,7\}$ bloklarını düşünelim. P'nin çakışım matrisi

$$N=\begin{bmatrix}1&1&1&0&0&0&0\\1&0&0&0&1&1&0\\0&1&0&1&0&1&0\\0&0&1&0&1&1&0\\1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&1&0&0&1\end{bmatrix}$$ dir.

N matrisinin her satırının sonuna ekstradan 1 ekleyelim, ve elde edilen yeni matrise G diyelim. C ikili kodu G'nin satırları üretsin. G'nin $F=\{0,1\}$ cismi üzerindeki rankı en az dörttür. Birinci, beşinci, altıncı ve yedinci satırlar lineer bağımsızdırlar. N matrisinin herhangi iki satırın iç çarpımı da $1 \pmod 2$ eşittir. Bundan dolayı herhangi iki nokta tek bir bloğa ait olur. G'nin herhangi iki satırın iç çarpımı da $0 \pmod 2$. Hatta $G.G^T = 0 \pmod 2$. Bu sebepten dolayı G'nin sıfır uzayı, G^T sütun uzayını aynı zamanda G'ninde satır uzayını içerir. O halde G'nin sıfır uzayının boyutu en az dörttür. Bu yüzden G'nin rankı 4 olur. O halde C bir $[8,4]-$ kodu olur.

$$G^1=\begin{bmatrix}1&1&1&0&0&0&0&1\\1&0&0&0&0&0&1&1\\0&1&0&0&1&0&1&1\\0&0&1&1&0&0&1&1\end{bmatrix}$$

matrisini G'nin birinci, beşinci, altıncı ve yedinci satırları oluşturur. G^1 matrisi C'nin üreteç matrisi olur.

Şimdi C'nin herhangi bir kodsözün ağırlığının dörde bölündüğünü gösterelim. $x, y \in C$ olsun. O halde $\langle x, y\rangle = 0$. Çünkü G^1 herhangi iki satırın iç çarpımı sıfır ve herhangi iki vektörün, aynı zamanda G^1 matrisinin satırlarının lineer kombinasyonu da sıfırdır. Bu yüzden eğer x ve y, C'nin iki sözü ise onların koordinat pozisyonunun

sayısı olarak çift olur. x ve y sözlerinin pozisyonların sayısı $2t$ olsun. bundan dolayı eğer $w(x)$ ve $w(y)$ dörde bölünür. O halde

$$w(x+y) = (w(x) - 2t) + (w(y) - 2t)$$
$$w(x+y) = w(x) + w(y) - 4t \text{ olur.}$$

O halde $w(x+y)$ de dörde bölünür. Fakat G'nin her bir satırın ağırlığında dörde de bölünüyor ve G'nin her bir satırın lineer kombinasyonları ağırlığı da dörde bölünündüğünden , C kodunun boyutu 4 olur. (F_2 üzerinde) C'nin 16 tane kodsözü olur. C'nin bir tane kodözü sıfır bir tanesinde bir diğerleri ise tam olarak dört tane bir içeren kodsözlerdir.

Tanım 5.2.2: Mertebesi $n \equiv 2 \pmod 4$ olan projektif düzleminin çakışım matrisi N olsun. Eğer C ikili lineer kodu N matrisin satırlarından üretiliyorsa o zaman C'nin uzatılmış kodu kendi dual ve ağırlığı dörde bölünür.

5.3. Support Tasarım

Tanım 5.3.1: $x = (x_1, ..., x_n)$ sıfırdan farklı bir vektör ve x'in sıfırdan farklı bileşenlerin kümesine x'in support denir ve supp(x) ile gösterilir.

Supp$(x) = \{i | x_i \neq 0\}$ ve $x_i \in F_q = \{0,1,2,3,...,q-1\}$. Support tasarımı şu şekilde yapılır. C sıfır vektörünü içeren n uzunluğunda koddan ağırlığı sıfırdan farklı w kodsözleri noktalar kümesi olarak seçebilir, bloklar kümesinde n koordinat pozisyonuna sahip kodun tüm w ağırlığındaki kodsözlerin supportu olarak alınır.

Tanım 5.3.2: $t-(v,k,\lambda)$ tasarımında eğer $\lambda = 1$ ise bu tasarıma Steiner sistem denir.

Teorem 5.3.1: (Assmus and Mattson)Bir lineer $[n,k,d=2t+1]$ kodun F_q üzerinde mükemmel olması için gerek ve yeter koşul minimum ağırlığındaki kodsözlerin support tasarımının $(t+1)-(n,2t+1,(q-1)^t)$ tasarım olmasıdır[12].

Teorem 5.3.2: n uzunluğundaki binary kodun minimum uzaklığı $d = 2t+1$ ve sıfır vektörünü içeriyorsa mükemmel kod olması için gerek ve yeter koşul minimum ağırlığındaki kodsözlerin support tasarımının bir Steiner $S(t+1, 2t+1, n)$ tasarımı olmasıdır. Ayrıca bu kodun uzatılmış kodununda minimum ağırlığındaki kodsözlerin support tasarımının bir Steiner $S(t+2, 2t+2, n+1)$ tasarımı olmasıdır[12].

Örnek 5.3.1: Hamming$[7,4,3]$ mükemmel kodunun genişletilmesi olan $[8,4,4]$ kodu Teorem 5.3.2 göre bir $S(3,4,8)$ steiner tasarımını oluşturur.

Örnek 5.3.2: Hamming $[7,4,3]$ mükemmel kodun oluşturduğu tasarımları bulalım.

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{4x7} .$$

Hamming kodunun ürettiği kodsözler ve ağırlıkları aşağıdaki gibidir.

Tablo 5.1. Kodun ağırlık sayacının bulunuşu

Kodsözler							Ağırlıklar
0	0	0	0	0	0	0	0
1	1	0	1	0	0	0	3
0	1	1	0	1	0	0	3
0	0	1	1	0	1	0	3
0	0	0	1	1	0	1	3
1	0	1	1	1	0	0	4
1	1	1	0	0	1	0	4
1	1	0	0	1	0	1	4
0	1	0	1	1	1	0	4
0	1	1	1	0	0	1	4
0	0	1	0	1	1	1	4
1	0	0	0	1	1	0	3
1	0	1	0	0	0	1	3
1	1	1	1	1	1	1	7
0	1	0	0	0	1	1	3
1	0	0	1	0	1	1	4

Ağırlığı 3 olan kodsözler $2-(7,3,1)$ tasarımını oluştururlar. Ağırlığı 4 olanlar ise $2-(7,4,2)$ tasarımını oluşturlar. YukarıdakiTeorem 5.3.1 insağlandığını da görülür.

Teorem 5.3.3: F_q üzerinde C bir lineer $[n,k,d]$ kodu ise $C^{\perp}$ dual kodu da $\left[n,n-k,d^{\perp}\right]$ dur. $n_o \le n$ olacak şekilde en büyük tamsayı n_0 ve $n_o - \dfrac{n_o+q-2}{q-1} < d$ Benzer şekilde $n_o{}^{\perp}$ sayısıda $C^{\perp}$ için sağlansın. Bazı t tamsayıları için $0<t<d$ ve $C^{\perp}$ in $w \le n-t$ olacak şekildeki ağırlığı sıfırdan farklı w sözlerin sayısı en fazla $d-t$ dir. O zaman :

1) C'nin $d \le u \le n_0$ olacak şekildeki herhangi u ağırlığındaki kodsözlerin support tasarımı bir $t-$tasarımıdır.
2) $C^{\perp}$' in $d^{\perp} \le w \le \min\left\{n-t, n_0^{\perp}\right\}$ olacak şekildeki herhangi w ağırlığındaki sözlerin support tasarımı bir $t-$tasarımıdır[12].

Örnek 5.3.4: Uzatılmış binary Golay $[24,12,8]$ kodu ağırlık sayaçlarına göre $A_0 = A_{24} = 1$ $A_8 = A_{16} = 759$, $A_{12} = 2576$ ayrılır. O halde bu koddan teoreme göre elde edilen tasarımlar aşağıdaki gibi olur.

$$A_8 = \{\text{supp}(c) | c \in C_8\} \to 5-(24,8,1)$$
$$A_{12} = \{\text{supp}(c) | c \in C_{12}\} \to 5-(24,12,48)$$
$$A_{16} = \{\text{supp}(c) | c \in C_{16}\} \to 5-(24,16,78).$$

Örnek 5.3.5: Mükemmel kodlara karşılı gelen tasarımlar şunlardır.

Tablo 5.2. Mükemmel kodlara karşılık gelen tasarımlar

t	q	n	Kod	Tasarım
1	Asal bir sayı	$\frac{q^m-1}{q-1}$	Hamming kodu	$2-\left(\frac{q^m-1}{q-1}, 3, q-1\right)$
2	3	11	TernaryGolay kodu G_{11}	$4-(11,5,1)$
3	2	23	BinaryGolay kodu G_{23}	$4-(23,7,1)$

5.4. Hadamard Matrisinden Kod Oluşturma

$p | n$ ve p tek asal sayı olsun. $GF(p)$ üzerinde $n \times n$ Hadamard matrisinin satırlarının elde edilen kodu düşünelim.

Tanım 5.4.1: A ve B iki tam sayı matrisi olsun. Eğer A ve B matrislerinin denk olması için; P ve Q gibi tamsayı matrisleri var öyle ki $\det P = \det Q = 1$ ve $PAQ = B$ dir.

Teorem 5.4.1: $n \times n$ boyutlu A matrisi olsun. O zaman bir tek köşegen matrisi var

$D = diag\{d_1, d_2, ...d_n\}$ öyleki;

1) D matrisi A matrisine elementer olarak denktir.

2) $i = 1,2,3....n-1$ için $d_i \mid d_{i+1}$

$d_1, d_2.....d_n$ sayıları elementer bölenlerdir. Herhangi bir cisim üzerinde $\det A = \det B$ ise bu matrisler aynı ranka sahiptir[19].

Örnek 5.4.1: 12 mertebeden Hadamard matrisi H olsun. O halde $H.H^T = 12I$ ve $\det H = 12^6$ dır. Teorem 5.3.1'den H matrisinin bir köşegen matrisi vardır. Öyleki $3^6 \mid \det H$, $3^6 \mid \det D$ olur. D köşegen matrisin en fazla 6 tane terimi 3 bölünebilir. O halde $H.H^T$ ve D rankı en az 6 olur. Fakat $GF(3)$ üzerinde $H.H^T = 0$. O halde $\operatorname{rank} H$ en fazla 6 olur. $rank(H) = 6$ ve H 'nin satır uzayları $(12,6)$ kendine dual liner kod üretirler.

5.5. Latin Karelerden Kod Üretme

Teorem 5.5.1: $q-(4,q^2,3)$ kodunun olması için gerek ve yeter koşul, q dereceden birbirine dik iki Latin karenin olmasıdır [20].

Teorem 5.5.2: $q-(n,q^2,n-1)$ parametreleri kodun olması için gerek ve yeter koşul, q dereceli $n-2$ tane birbirine dik Latin kare çiftinin olmasıdır[20].

Örnek 5.4.1: 5 mertebeden birbirine dik 4 Latin kare aşağıdaki gibi olsun. Bu Latin karelerin oluşturduğu kodu bulalım. (mod 5 göre işlemler)

$$\begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 1 & 0 & 4 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 \\ 3 & 2 & 1 & 0 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 2 & 1 & 0 & 4 & 3 \\ 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 4 & 3 & 2 \\ 3 & 2 & 1 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 3 & 2 & 1 & 0 & 4 \\ 1 & 0 & 4 & 3 & 2 \\ 4 & 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 4 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 0 \\ 3 & 2 & 1 & 0 & 4 \\ 2 & 1 & 0 & 4 & 3 \\ 1 & 0 & 4 & 3 & 2 \end{bmatrix}$$

$C = \{(i, j, a_{ij}, b_{ij}, c_{ij}, d_{ij}) \mid i, j = \{0,2....4\}\}$.

$C = \{(0,0,0,0,0,0),(0,1,4,4,4,4),(0,2,3,3,3,3),(0,3,2,2,2,2),(0,4,1,1,1,1),(1,0,1,2,3,4),$

$(1,1,0,1,2,3),(1,2,4,0,1,2),(1,3,3,4,0,1),(1,4,2,3,4,0),(2,0,2,4,1,3),(2,1,1,3,0,2),$
$(2,2,0,2,4,1),(2,3,4,1,3,0),(2,4,3,0,2,4),(3,0,3,1,4,2),(3,1,2,0,3,1),(3,2,1,4,2,0),$
$(3,3,0,3,1,4),(3,4,4,2,0,3),(4,0,4,3,2,1),(4,1,3,2,1,0),(4,2,2,1,0,4),(4,3,1,0,4,3),$
$(4,4,0,4,3,2)\}$ kodu lineer kod tur.

BÖLÜM 6. SONUÇLAR

Tasarım teorisiyle ile lineer kodlar arasındaki ilişki incelendi. Tasarımlardan elde edilen kodların özellikleri verildi. Tasarımdan kod üretmeye ve koddan tasarım üretmeye örnekler oluşturuldu.

BÖLÜM 7. TARTIŞMA VE ÖNERİLER

Tasarım teorisinde $t > 5$ için $t-(v,k,1)$ parametreli bir Steiner sistemin varlığı araştırılabilir. Eğer varsa böyle tasarımlar, bunların sonlu sayıda olup olmadığı araştırılabilir. Bu tasarımların Steiner sistemine karşılık gelen kodsözleri bulunabilir.

KAYNAKLAR

[1] ROMAN, S., Coding and İnformation Theory, Graduate Texts in Mathematics, Springer Verlag, 1992.

[2] MACWILLIAMS, F.J., SLOANE, N.J., The Theory of Error Correcting Codes, North Holland Pub. Co.,39-72, 1977.

[3] STINSON, D.R., Combinatorial Designs : Constructions and Analysis, Springer-Verlag, New York , pp. 1–19, 23-39, 73-98,41-69,101-119, 124-152, 2004

[4] CAMERON, P. J., Combinatorics: Topics,Techniques,Algorithms, Queen mary ,Westfield College, London, Cambridge University Press, 261-262 ,1994

[5] MERRİS, R., Combinatorics, Wiley, New Jersey, 421-471, 453-455,2003.

[6] STREET, A.P., WALLIS, W.D., Combinatorial Theory: An Introduction , The Charles Babbage Research Centre , Canada, 1977

[7] GODSIL, C., Lecture Notes (unpublished)

[8] PLESS, V., Introduction to the Theory of Error-correcting Codes, John - Willey, New York , 1982

[9] LANDER, E.S., Symmetric Designs: An Algebraic Approach, Cambridge University Pres ,Cambridge, 5-11, 1983

[10] CAMERON, P.J., VAN LINT J.H., Designs, Graphs, Codes and Their Links, Cambridge Univ. Press, 1-28, 1991.

[11] KAYA, R., Projektif Geometri , Anadolu Üniversitesi Fen –Edebiyat Fakültesi Yayınları ; no:27, 1992

[12] COLBOURN, C. J., DINITZ, J. H., "The CRC Handbook of Combinatorial Designs", CRC Pres, Boca Raton, New York, London, Tokyo, 694-708,517-530, 1996

[13] MARSHALL HALL, JR., Combinatorial Theory, A Wiley interscience P. John Wiley-Sons , New York, Chichester, Brisbane , Toronto, Ssingapore. 147-200, 1986

[14] TARRY , G., Le Probléme des 36 Officers, C.R.Assoc.Fr.Av.Sci., Vol.29, pp 170-203, 1900

[15] STINSON, D.R., Short Proof of the nonexistence of a Pair of Orthogonal Latin Squares of Order Six , J. Combinatorial Th(A) ,vol.36, pp 373-376, 1984

[16] LINDER , C.C., RODGER, C.A., Design Theory , C.R.C Press, Boca Raton New York,93-128, 1997

[17] SANE, S.S., SHRIKHANDE, M.S., Quasi-Symmetric designs , Cambridge University Press, Cambridge, 1991

[18] CARY, W.H., PLESS , V., Fundamentals of Error-Correcting Codes, Cambridge University Press , 291-337, 2003

[19] HARTLEY, B., HAWKES, T.O., Rings Modules and linear Algebra, Cambridge University Press, Cambridge, 1983.

[20] RAYMOND, H., A First Course in Coding Theory, Published in the United States by Oxford University Press inc., New York, 113-124, 1986

ÖZGEÇMİŞ

Necati AYAZ, 01.01.1983 te Erzurum da doğdu. İlkokul eğitimine Erzurum da başlayıp İstanbul da bitirdi. Orta ve lise eğitimini İstanbul da tamamladı. 2000 yılında başladığı Şair Abay Kunanbay lisesini 2003 yılında birincilikle bitirdi. Aynı yıl Sakarya Üniversitesi Matematik bölümünü kazandı. 2007 yılında Sakarya Üniversitesi Matematik bölümünü (3,5 yıl) birincilikle bitirdi. 2008 yılında Sakarya Üniversitesinde yüksek lisansa başladı.