YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

k TEK SAYI OLMAK ÜZERE (v, k, λ) – SİMETRİK DİZAYNIN C KODU İÇİN BİR OLASILIK FONKSİYONU TAYİNİ ve DÜZENSİZLİK ÖLÇÜSÜ ÖNERİSİ

Ayten USTAMEHMETOĞLU

F.B.E. Matematik Anabilim Dalında Hazırlanan

DOKTORA TEZİ

Tez Savunma Tarihi	**: 02.Aralık 1999**	
Tez Danışmanı	**: Prof. Dr. Erol BALKANAY**	**(YTÜ)**
Jüri Üyeleri	**: Prof. Dr.Hülya ŞENKON**	**(İÜ)**
	Prof.Dr.Ayşe SOYSAL	**(BÜ)**

İSTANBUL, 1999

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

TEŞEKKÜR

Çalışmam boyunca yardımlarını esirgemeyen değerli hocam sayın Prof. Dr. Erol BALKANAY'a teşekürü bir borç bilirim.

ÖZET

Bu çalışma üç bölümden oluşmuştur. Birinci bölümde kodlar kuramı ile ilgili bilgiler, ikinci bölümde ise Simetrik dizaynlar ele alınmıştır.

Tezin özgün bölümünü oluşturan son bölümde ise k tek sayı olmak üzere (v, k, λ) – Simetrik dizaynın C kodu için C_1 alt kümesinde, X sözcüğünün izafi ağırlığı, maksimum izafi ağırlık ve izafi ağırlık oranı tanımlanarak özelikleri incelenmiştir.

Ayrıca p izafi olasılığı Shannon entropisine uygulanarak C_1 için bir düzensizlik ölçüsü önerilmiştir ve bununla ilgili örneğe yer verilmiştir.

ABSTRACT

This work consist of the three chapters. Theory of codes and symmetric design are considered in the first and the second chapters respectively.

In the third chapter which is original part of this thesis, for an odd integer k and C – code of (v, k, λ) – symmetric design, in the subset C_1, we define relative weigth of X code word and maximum relative weigth and the ratio of relative weigth and we study of their properties.

Further relative probability p applied to the Shannon entropy . A measure of uncertainity for the code words of a symmetric block design having parameters (v, k, λ) is proposed.

1. KODLAMA TEORİSİ

1.1 Kodlama Teorisine Giriş

Genel olarak q-lu bir kod denince q tane farklı sembolün oluşturduğu $F_q = \{\lambda_1, \lambda_2, ..., \lambda_q\}$ kümesinin elemanlarıyla oluşturulan dizilerden kurulan bir küme anlaşılır.

Genellikle F_q, kodun alfabesi adını alır. $a_i \in F_q$ olmak üzere $a_1, a_2, \ldots, a_n$ şeklindeki tüm sıralı n-lilerin kümesi $(F_q)^n$ ile gösterilir. $(F_q)^n$ nin elemanlarına da vektörler veya sözcükler denir. $(F_q)^n$ nin mertebesi q^n olup altkümesi n uzunluğundaki bir q koddur.

Tanım 1.1 (Binary Kod)
0 ve 1 lerden oluşan dizilerin oluşturduğu kümedir. Dizilerin herbirine kod sözcüğü denir.
0 0 0 0 0 , 1 1 1 1 1 beş uzunluklu ikili bir koddur.

Tanım 1.2 (Hamming Uzaklığı)
$x, y \in (F_q)^n$, x ve y arasındaki uzaklık, bu iki vektörün birbirinden farklı bileşenlerinin sayısıdır. Bu da $d(x,y)$ ile gösterilir.

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

2) $\forall x, y \in (F_q)^n$ için $d(x,y) = d(y,x)$

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

Bu üç şartı sağladığı için Hamming uzaklığı bir metriktir.

Tanım 1.3 (C nin minimum uzaklığı)
C nin minimum uzaklığı $d(C)$ ile gösterilir. Farklı kod sözcükleri arasındaki uzaklıklardan en küçüğüne eşittir.

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

Teorem 1.4

1) $d(C) \geq s+1$ ise C kodu s tane hatayı sezebilir.

2) $d(C) \geq 2t+1$ ise C kodu herhangi bir kod sözcüğündeki t hatayı düzeltebilir.

Örneğin $d(C)$=3 ise, C kodu 2 hata saptayan kod olarak yada tek hata düzelten kod olarak kullanılabilir (Blake ve Mullin, 1975).

Çizelge 1.1

D(C)	s C ile saptanan hata sayısı	t C ile düzeltilen hata sayısı
1	0	0
2	1	0
3	2	1
4	3	1
5	4	2
6	5	2
7	6	3
.	.	.
.	.	.

1.2 Kod Çözme Problemi

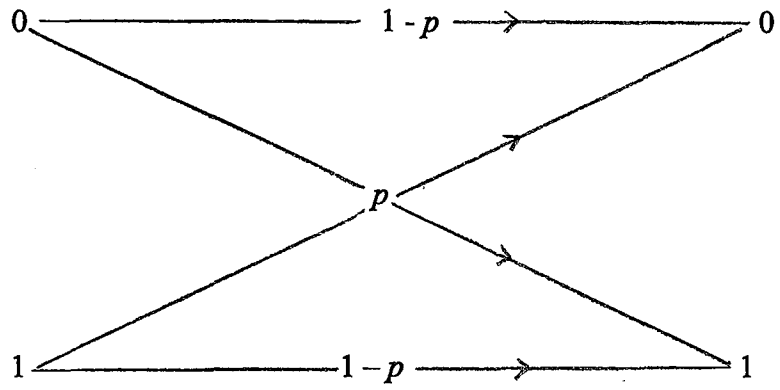
Bilinmeyen bir x kod kelimesinin bize gönderildiğini ve bizim gürültüden bozulmuş olarak bir y vektörünü aldığımızı kabul edelim. y yi x' olarak çözdüğümüzü varsayalım. Bu çözüm işlemi $d(x',y)$ nin mümkün olduğu kadar minimum yapılmasıyla gerçekleşir.

Kod çözme stratejimiz aşağıdaki gibi olsun.

1) Her sembolün hatalı gönderilme olasılığı aynıdır ($p<1/2$).

2) Eğer bir sembol hatalı alınmış ise bunun diğer $q-1$ sembolden biri olma olasılığı aynıdır.

Bu koşullara uygun bir kanal q lu simetrik kanal adını alır.



p, kanalın sembol hata olma olasılığı

Şekil 1.1

Bir binary simetrik kanaldan gönderilen n uzunluklu bir kod sözcüğünün hatasız alınma olasılığı $(1-p)^n$, bu vektörün belli bir konumda bir hata ile gönderilme olasılığı $p(1-p)^{n-1}$, belirli i tane konumda hata olma olasılığı $p^i(1-p)^{n-i}$dir (Van Lint, J.H., 1971).

1.3 Kodlama Teorisinin Temel Problemi

(n,M,d) kod denince ,

n : Kod sözcüklerinin uzunluğu

M : Kod sözcüklerinin sayısı

d : Minimum uzaklık

İyi bir (n,M,d) kod denilince küçük n, büyük M ve büyük d anlaşılır. Burada n in küçük olması mesaj gönderme hızının büyük olmasını sağlar. M in büyük olması mesaj sayısının yüksek olmasını , d nin büyük olması ise çok sayıda hatanın düzeltilmesini sağlar. O halde kodlama teorisinin temel problemlerinden biri n,M,d parametrelerinden biri verildiğinde diğer parametrelerin optimum olarak nasıl seçilmesi gerektiğini bulmaktır.Genellikle bir sözcük uzunluğu verilir.Minimum uzaklık seçilir ve bu kodun kurulması problemidir. q-lü bir (n,M,d) - kodda M in alabileceği en büyük değer $A_q(n,d)$ ile gösterilecektir (Cameron P. J. ve Van Lint, J.H., 1975).

Teorem 1.5

1) $A_q(n,1)=q^n$

ve

2) $A_q(n,n)=q$

dir.

İspat:

1) Bir kodun minimum mesafesi için en küçük değer 1 dir. Amacımız kod sözcüklerinin birbirinden farklı olduğu durumda en çok sözcük taşıyan q-lü $(n,M,1)$ kodunu elde etmektir. Bu ise $(F_q)^n$ uzayıdır. Bunun eleman sayısının $M=q^n$ olduğunu biliyoruz.

2) C nin bir q-lü (n, M, n) kod olduğunu varsayalım. $d=n$ olduğundan herhangi iki kod sözcüğünün farklı konumlarının sayısı n olmak zorundadır.O zaman bu kodun q tekrarlı kod olduğu hemen anlaşılır. Dolayısıyla $A_q(n,n)=q$ dur.

1.4 Kodların Denkliği

$S=\{x_1,x_2,...,x_n\}$ kümesinin bir permütasyonu denince S ten S e birebir ve örten bir f fonksiyonu anlaşılır. Böyle bir permütasyon $f=\begin{pmatrix} x_1.....x_n \\ f(x_1)...f(x_n) \end{pmatrix}$ şeklinde gösterilir.

Tanım 1.6

İki q-lu koddan aşağıdaki işlemlerin bir kombinasyonu ile biri diğerinden elde ediliyorsa bu iki koda denktir denir.

(A) Kodun konumlarının permütasyonu

(B) Belli bir konumdaki sembollerin permütasyonu

Eğer bir kodu sözcükleri satırlara yazmak üzere $M\times n$ matris halinde yazarsak yukarıda sözü edilen (A) işlemi matrisin sütunlarının permütasyonuna karşılık gelir. (B) isebir sütundaki elemanların yeniden etiketlenmesidir. Yukarıda sözü edilen (A) , (B) işlemleri sonucunda kod sözcükleri arasındaki uzaklık değişmez. Bunun sonucu olarak birbirine denk iki kod birer (n, M, d) koddurlar. Aynı sayıda hatayı düzeltirler.

$(F_2)^n$ kümesi üzerinde işlemler

F_2 kümesi $\{0,1\}$ olarak alınsın. $(F_2)^n$ üzerinde , $x+y$ ve $x \cap y$ işlemleri aşağıdaki gibi tanımlansın.

$x = x_1x_2.....x_n \in (F_2)^n$

$y = y_1y_2.....y_n \in (F_2)^n$

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

$x \cap y = (x_1y_1, x_2y_2, ...x_ny_n)$

şeklinde olup buradaki işlemler (mod 2) ye göredir.

Tanım 1.7

$(F_2)^n$ deki bir x vektöründeki 1 lerin sayısı, x vektörünün ağırlığıdır. Ağırlık $\omega(x)$ notasyonu ile gösterilir.

Teorem 1.8

Eğer $x,y \in (F_2)^n$ ise

$$d(x , y) = \omega(x + y)$$

dir.

İspat:

$x+y$ toplamında x ve y nin aynı sembol taşıyan konumlarında 0, farklı sembol taşıyan konumlarında 1 olacağından $x+y$ deki 1 lerin sayısı x ile y nin farklı konumlarının sayısına eşittir.O zaman

$$d(x , y) = \omega(x + y)$$

sonucu elde edilir.

Teorem 1.9

Eğer $x,y \in (F_2)^n$ ise

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

dir.

İspat:

$d(x,y)$= (x deki 1 lerin sayısı)+(y deki 1 lerin sayısı)-2(x ve y deki 1 lerin çakışma sayısı)

dır.

1.5 $(F_q)^n$ de Küre Kavramı

$(F_q)^n$ deki vektörler birer nokta, iki nokta arasındaki uzaklığı ise hamming uzaklığı olarak yorumlanırsa aşağıdaki tanım yapılabilir (Blake Lan F. ve Mullin Ronald C., 1975).

Tanım 1.10

$(F_q)^n$ de herhangi bir u vektörü gözönüne alınsın.Herhangi $r \geq 0$ tamsayısı için u merkezli r yarıçaplı bir küre $S(u,r)$ ile gösterilir ve

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

şeklinde tanımlanır.

Teorem 1.11

Bir q-lü $(n,M,2t+1)$ kod

$$M\left\{\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+...+\binom{n}{t}(q-1)^t\right\} \leq q^n \qquad (1.1)$$

eşitsizliğini sağlar.

Bir binary $(n,M,2t+1)$ kod için

$$M\left\{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+...+\binom{n}{t}\right\} \leq 2^n \qquad (1.2)$$

Bu teoremde verilen 1.1 ve 1.2 eşitsizliklerine küre paketi (sınırı) veya hamming sınırı denir. Verilen n, q, d değerleri için Hamming sınırı vasıtasıyla M için bir üst sınır elde edilir. Daha kesin $A_q(n,d)$ için bir üst sınır belirtilmiş olur.

Örnek

Bir binary $(7,M,3)$ kod için

$$M\left\{\binom{7}{0}+\binom{7}{1}\right\} \leq 2^7$$

$8M \le 2^7$

$8M \le 128$

$M \le 16$

dır.

Tanım 1.12

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

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

eşitliğini sağlıyorsa, yetkin kod adını alır.

1.6 Lineer Kodlar

q bir asal sayının kuvveti olmak üzere, q elemanlı $GF(q)$ cismini ele alalım. $GF(q)$ nun tüm sıralı n-lilerin kümesi $GF(q)^n$ veya $V(n,q)$ ile gösterilsin. $GF(q)$ Galois cismi kısaca F_q şeklinde alınsın. Buna göre F_q üzerinde C lineer kodu $V(n,q)$ nun bir alt uzayıdır. C nin boyutu r ise C, $[n,r]$-kod adını alır. C nin d minimum uzaklığı önemli ise $[n,k,d]$- kod notasyonu kullanılır.

$V(n,q)$ nun bir C alt kümesinin bir lineer kod olması için gerek ve yeter koşul

1) Her $u,v \in C$ için $u+v \in C$

2) $\alpha \in GF(q)$ ve $u \in C$ için $\alpha u \in C$ olmasıdır (Van Lint J.H., 1971).

Tanım 1.13

$V(n,q)$ nun bir x vektörünün ağırlığı, x in sıfırdan farklı bileşenlerinin sayısıdır. Bu önceden olduğu gibi $\omega(x)$ notasyonu ile gösterilir.

Teorem 1.14

$x, y \in V(n,q)$ ise $d(x,y) = \omega(x - y)$ dir.

İspat:

$x - y$ vektöründeki sıfırdan farklı semboller x ve y nin farklı sembol taşıdığı konumlarda bulunur. Bu da teoremin ispatlanması demektir.

Teorem 1.15

C bir lineer kod olmak üzere C nin sıfırdan farklı kod sözcükleri içinde en küçük ağırlıklısının ağırlığı $\omega(C)$ olsun. O zaman $d(C) = \omega(C)$ dir.

İspat:

$d(C) = d(x, y)$ olacak şekilde $x, y \in C$ vardır. O taktirde Teorem 1.6.2 den

$d(C) = d(x,y) = \omega(x - y) \geq \omega(C)$

dir.

Diğer yandan uygun bir $x \in C$ için $\omega(C) = \omega(x) = d(x,0) \geq d(C)$ dir. Buradan $d(C) \geq \omega(C)$ ve $d(C) \leq \omega(C)$ olup $d(C) = \omega(C)$ bulunur.

Tanım 1.16

Lineer bir $[n,k]$- kodu gözönüne alınsın.Bu kodun taban vektörlerini satırlara yazarak elde edilen bir kxn matris $[n,k]$ lineer kodun bir üreteç matrisi adını alır.

Örnek

$$C_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

kodunun üreteç matrisi $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ dir.

Tanım 1.17

$GF(q)$ üzerinde bir $[n,k]$ kod C olsun. Bir $a \in V(n,q)$ vektörü seçelim. Bu durumda

$$a + C = \{ a + x \mid x \in C \}$$

kümesi C nin bir koseti adını alır.

C nin bir koseti $a+C$ ve $b \in a+C$ ise $a+C=b+C$ olduğunu grup teoriden biliyoruz. Ayrıca Lagrange teoreminden dolayı $GF(q)$ üzerinde bir $[n,k]$ - kod C ise $V(n,q)$ nün her vektörü mutlaka bir kosette bulunur. Her koset aynı sayıda eleman içerir. C nin eleman sayısı q^k dır. C de bir koset olarak düşünüleceğinden ve C nin eleman sayısı q^k olduğundan her koset kesinlikle q^k vektör bulundurur. Herhangi iki koset ya aynı ya da ayrıktır.

Örnek

Üreteç matrisi $G=\begin{bmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\end{bmatrix}$ olan ikili [4,2]- kodu gözönüne alınsın.

C={0000, 1011, 0101, 1110 } dir.

C nin oluşturduğu kosetler

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

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

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

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

Tanım 1.18

C, bir lineer [n, k] ise onun ağırlık numaralaması

$$W_C(z)=\sum_{i=0}^{n}A_i z^i = A_0 + A_1 z + \ldots + A_n z^n$$

polinomu ile tanımlanır. Burada A_i , C deki i ağırlıklı kod sözcüklerinin sayısını gösterir (Cameron P. J. ve Van Lint, J.H., 1975).

1.7 Devresel Kodlar

Tanım 1.18

C bir lineer kod ve bir kod sözcüğünün bir devresel düzeni de yine bir kod sözcüğü ise C kodu bir devresel kod adını alır. Bu durumda a = (a_0, a_1, ... , a_{n-1}) bir kod sözcüğü ise (a_{n-1}, a_0 , a_1, ... , a_{n-2}) de bir kod sözcüğüdür.

Devresel kodlar gözönüne alındığında, bir (a_0, a_1, ... , a_{n-1}) vektörünü $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ polinomuna karşılık getirmek yararlıdır. Bu durumda (a_{n-1}, a_0, a_1, ... , a_{n-2}) sözcüğü, $a_{n-1} + a_0 x + a_1 x^2 + \ldots +, a_{n-2}x^{n-1}$ e karşılık gelir. ($a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$) x (mod ($x^n - 1$)) eşit olduğu görülmektedir.($x^n \equiv$ mod (x^n-1))

{ 000, 101, 011, 110 } kodu devresel koddur (Raymond Hill, 1986).

Tanım 1.18

(a_0, a_1, ... , a_{n-1}) bir kod sözcüğü olmak üzere

$$a(x)=\sum_{i=0}^{n-1}a_i x^i$$

polinomuna C için bir kod sözcüğü polinomu denir.

$a_0 + a_1x + ... + a_{n-1}x^{n-1}$ dir.

Tanım 1.19

$a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ olmak üzere $xa(x) = a_0x+a_1x^2+...+a_{n-1}x^n$ dir.

$x^n \equiv 1 (mod x^n-1)$ olduğundan $xa(x) = a_{n-1}+a_0x+a_1x^2+...+a_{n-2}x^{n-1}$ olur.

Buna a kod sözcüğünün devresel düzeni denir (Blakelan F. ve Mullin Ronald C.,1975).

GF(q)[x] deki polinomların eşlenik sınıflarını içeren GF(q)[x] / $(x^n - 1)$ ile ilgilenilecektir.

GF(q)[x] deki polinomların eşlenik sınıfları, derecesi n den küçük polinomlar olarak düşünülecektir.

GF(q)[x] / $(x^n - 1)$ de polinomlar GF(q)[x] de olduğu gibi toplanır ve çıkarılır. Ancak çarpma mod$(x^n - 1)$ e göre yapılır. Burada $(x^n - 1)$ ideali $x^n - 1$ polinomu ile üretilmiştir. Kesin olarak a(x) ve b(x) gibi iki polinom varsa bunların GF(q)[x] deki çarpımı bölme algoritmasından

$$a(x)b(x) = c(x)(x^n - 1) + r(x)$$

şeklindedir.

Burada r(x) in derecesi $x^n - 1$ in derecesinden küçüktür. $v = (a_0, a_1, ..., a_{n-1})$ vektörü R_n = GF(q)[x] / $(x^n - 1)$ deki bir $a_0 + a_1x + ... + a_{n-1}x^{n-1}$ polinomuna karşılık gelsin. Aşağıdaki teorem bu eşlemeyi açıklamaktadır.

Teorem 1.20

R_n de bir C kodunun devresel olması için gerek ve yeter koşul aşağıdaki iki koşulu sağlamasıdır.

1) $a(x), b(x) \in C \Rightarrow a(x) + b(x) \in C$

2) $a(x) \in C$ ve $r(x) \in R_n \Rightarrow r(x)a(x) \in C$

İspat:

C, R_n deki bir devresel kod olsun. O taktirde C lineer kod olduğundan $a(x)+b(x) \in C$ dir.

$a(x) \in C$ ise o zaman $a(x)x \in C$ olur. Bunun gibi (a(x)x)x = $a(x)x^2$ olur. $a(x) \in C$ ve $r(x) = r_0 + r_1x + ...+ r_{n-1}x^{n-1}$, R_n de bir polinom olmak üzere r(x)a(x) göz önüne alınsın. Toplamdaki her eleman C de olduğundan

$$r(x)a(x) = r_0 a(x)+ r_1a(x)x +...r_{n-1}a(x)x^{n-1} \in C \text{ dir.}$$

Şimdi 1) ve 2) şartlarının sağlandığını kabul edelim. r(x) bir skaler olarak alındığında 1) ve 2) den C lineer olur. 2) de r(x) = x alınırsa C devresel olur.

Sonuç olarak devresel kod denince R_n de bir ideal anlaşılacaktır.

Teorem 1.21

R_n deki bir I idealinin her elemanı g(x) gibi sabit bir polinom ile üretiliyorsa esas ideal adını alır.

Eğer I esas ideal ise $\langle g(x)\rangle = I = \{r(x)g(x) : r(x) \in R_n\}$ dir.

Teorem 1.22

Herhangi $g(x) \in R_n$ için $\langle g(x)\rangle$ kümesi bir devresel koddur.g(x) ile üretilen kod adını alır.

İspat:

Her $a(x)g(x)$ ve $b(x)g(x) \in \langle g(x)\rangle$ için

$a(x)g(x)+b(x)g(x) = (a(x)+b(x))g(x) \in \langle g(x)\rangle$ dir.

Her $a(x)g(x) \in \langle g(x)\rangle$ ve her $r(x) \in R_n$ için $r(x)(a(x)g(x)) = (r(x)a(x))g(x) \in \langle g(x)\rangle$

dir.

Teorem 1.23

C , R_n de sıfırdan farklı bir devresel kod olsun.

i) C de en küçük dereceli bir tek monik polinom g(x) vardır.

ii) $C = \langle g(x)\rangle$

iii)g(x) , x^n-1 in bir çarpanıysa bir üreteç polinomu adını alır (Raymond Hill,1986).

İspat:

i) g(x) ve h(x) aynı dereceden iki monik polinom ise ve her ikiside C nin elemanı ise o zaman g(x)-h(x) polinomu derecesi g(x) veya h(x) in derecesinden küçük olan bir polinomdur. $g(x) \neq h(x)$ ise bu bir çelişkidir. Böylece g(x) , C deki en küçük dereceli tek monik polinomdur.

ii) g(x), C deki en küçük dereceli monik polinom ve $a(x) \in C$ olsun.GF(g)[x] deki bölme algoritmasından $a(x) = g(x)b(x) + r(x)$ olur. Burada $\deg r(x) < \deg g(x)$ dir.

Devresel kodun özelliklerinden $r(x) \in C$ olur.Fakat bu r(x) özdeş olarak sıfır olmadıkça g(x) in seçimiyle çelişir.Böylece $a(x) = g(x)b(x)$ den $a(x) \in \langle g(x)\rangle$

dir.

iii) g(x) ,C deki en küçük dereceli monik polinom olsun. GF(g)[x] deki bölme algoritmasından $x^n-1 = a(x)g(x) + r(x)$, $\deg r(x) < \deg g(x)$ dir.

Böylece $r(x) = -a(x)g(x) \bmod (x^n-1)$ olur. Buradan da $r(x) \in \langle g(x) \rangle$ dir. $r(x)$ özdeş olarak sıfır olmadıkça bu bir çelişkidir. Böylece $g(x) | x^n-1$ dir.

Teorem 1.24

$g(x) = g_0+g_1x+...+g_rx^r$ bir devresel kodun üreteç polinomu olsun. O taktirde g_0 sıfırdan farklıdır.

İspat:

$g_0 = 0$ kabul edilsin. O taktirde $x^{r-1}g(x) = x^{-1}g(x)$ r-1 dereceli C nin bir kod sözcüğüdür. Bu deg g(x) in minimalitesi ile çeliştiğinden g_0 sıfırdan farklı olmalıdır.

Teorem 1.25

C, r dereceli $g(x) = g_0+g_1x+...+g_rx^r$ üreteç polinomuna sahip bir devresel [n ,k]-kod olsun. C nin boyutu n-r ve C nin bir üreteç matrisi aşağıdaki gibidir.

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_r & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{bmatrix}$$

İspat:

$g(x), g(x)x, g(x)x^2, ..., g(x)x^{n-r-1}$ vektörleri lineer bağımsızdır. C deki her kod sözcüğünün $g(x), g(x)x, g(x)x^2, ..., g(x)x^{n-r-1}$ nin lineer kombinasyonu olarak yazılabildiğini göstermemiz gerekir. C nin herhangi bir a(x) elemanı q(x)g(x)
şeklinde ifade edilebilir. Burada der $q(x) \leq n-r-1$ dir.

$a(x) = q(x)g(x) = (q_0 + q_1x + ... + q_{n-r-1}x^{n-r-1})g(x)$

$= q_0g(x)+q_1g(x)x+...+q_{n-r-1}g(x)x^{n-r-1}$ elde edilir.

C nin bir üreteç matrisi , ilk satırı g(x), ikinci satırı g(x)x, üçüncü satırı $g(x)x^2$,...,k.satırı $g(x)x^{n-r-1}$ olan bir matristir. Bu yukarıda verilen matristir.

Örnek olarak ikili devresel kodlar n = 7 için kurulabilir. İlk yapılacak olan x^7-1 i çarpanlarına ayırmaktır.

$$x^7-1=(1+x)(1+x+x^3)(1+x^2+x^3)$$

dir.

$g(x) = 1 + x + x^3$ olmak üzere $C = \langle g(x) \rangle$ olduğu göz önüne alınsın. C dört-boyutludur ve aşağıdaki üreteç matrisine sahiptir.

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

Tanım 1.26

Lineer bir [n, k]-kod C olmak üzere, C nin duali $C^{\perp}$ ile gösterilir ve

$$C^{\perp} = \{ v \in V \mid vu = 0, \text{her } u \in C \text{ için} \}$$

dir. C, k boyutlu ise $C^{\perp}$, $n - k$ boyutludur.

Tanım 1.27

Bir lineer [n, k]-kod C olmak üzere $C^{\perp}$ in bir H üreteç matrisi C nin parite kontrol matrisi adını alır.

Tanım 1.28

f(x) m.dereceden bir polinom ise o zaman $x^m f(x^{-1})$ şeklinde tanımlanan polinom f(x) in karşıt (reciprocal) polinomu adını alır.

$f(x)=a_n x^n+a_{n-1}x^{n-1}+...a_1 x+a_0$ ise bunun karşıt polinomu $a_0 x^n+a_1 x^{n-1}+...+a_n$ şeklindedir.Yani katsayıların sıralanması ters olur. $C^{\perp}$, $h^*(x) = x^k h(x^{-1})$ karşıt polinomuyla üretilir.

Tanım 1.29

$g(x)h(x) = x^n-1$ ve g(x) bir C devresel [n,k] - kodunun üreteç polinomu ise o zaman h(x) e C nin kontrol polinomu denir.

Teorem 1.30

C, R_n de g(x) üreteç polinomlu ve h(x) kontrol polinomlu bir devresel kod olsun.O zaman $c(x)h(x) = 0$ olması için gerek ve yeter koşul R_n in c(x) elemanının C nin bir kod sözcüğü olmasıdır.

İspat:

R_n de $g(x)h(x) = x^n-1 = 0$ dır. $c(x) \in C$ olsun.Bir $a(x) \in R_n$ için $c(x) = a(x)g(x)$ olur.

$c(x)h(x) = a(x)g(x)h(x) = a(x).0 = 0$ bulunur.

$c(x)h(x) = 0$ alındığında bölme algoritmasından

$$c(x) = q(x)g(x) + r(x) \text{ , deg } r(x) < \text{deg } g(x) \text{ yazılabilir.}$$

$c(x)h(x) = 0$ olduğundan $r(x)h(x) = 0$ dır. Yani $r(x)h(x) \equiv 0(\bmod x^n-1)$ dir.

Bundan dolayı $r(x) = 0$ ve $c(x) = q(x)g(x) \in C$ bulunur.

Teorem 1.31

C, $h(x) = h_0 + h_1x + ... + h_kx^k$ kontrol polinomlu bir devresel [n,k]- kod olsun.

i) C nin parite kontrol matrisi

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & h_k & h_{k-1} & \dots & \dots & \dots & h_0 \end{bmatrix}$$

ii) $C^{\perp}$, $h^* = h_k + h_{k-1}x + ... + h_0x^k$ polinomu ile üretilen devresel koddur (Van Lint J. H.,1971).

GF(2) üzerinde x^7-1 örneği ele alınsın.

$$x^7-1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$$

dir. Üreteç polinomu $1 + x + x^3$ olan C devresel kodu için bir üreteç matrisi kurulmuştur. Şimdi C için bir parite kontrol matrisi bulunabilir. $h(x)$ kontrol polinomu $h(x) = (1+x)(1+x^2+x^3)$ dir. Bunun karşıt polinomu $x^4(1 + x^{-1} + x^{-2} + x^{-4}) = 1 + x^2 + x^3 + x^4$ olarak bulunur. Buradan C için bir parite kontrol matrisi aşağıdaki gibidir.

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

2. SİMETRİK DİZAYNLAR

2.1 Simetrik Dizaynlara Giriş

Bir Çakışım yapısı, P ile göstereceğimiz noktalar kümesi, B ile göstereceğimiz bloklar kümesi ve noktalar ile bloklar arasında R ile göstereceğimiz bir çakışım bağlantısından oluşur. Bir çakışım yapısı (P, B, R) ile gösterilir. pRy ifadesi " p, y üzerindedir " y, p yi içerir " veya " p, y ile çakışım durumundadır " şeklinde okunur.

p nin çakışım durumunda olduğu bloklar kümesi $< p >$ ile, y nin çakışım durumunda olduğu noktalar kümesi $< y >$ ile, p noktasının kaç tane blokla çakışım durumunda olduğu $| p |$ ile ve y bloğunun kaç tane nokta ile çakışım durumunda olduğu da $| y |$ sembolleriyle gösterilir.

Bundan böyle yapı denince çakışım yapısı anlaşılacaktır. Bir S yapısında noktaların sayısı v ile bloklarının sayısı da b ile gösterilir. p noktası x bloğu üzerinde ise p noktası x denklik sınıfındadır denir. S nin blokları üzerinde $< x > = < y >$ ise xRy dir, şeklinde bir R denklik bağıntısı tanımlanabilir. Bu durumda bir x bloğunun katlılığı x bloğunun temsil ettiği denklik sınıfının eleman sayısı olur (Hughes et all, 1985).

Tanım 2.1 (Tekrarlı Blok)

S yapısında herhangi bir x bloğunun katlılığı 1 den büyük ise bu x bloğuna tekrarlı bir blok adı verilir (Hughes et all, 1985).

Tanım 2.2 (İndirgenmiş Yapı)

S/R yapısı, S yapısı ve yukarıdaki gibi tanımlanan R denklik bağıntısı vasıtasıyla tanımlanır. S/R nin noktalar kümesi, S nin noktalar kümesidir. Bloklar kümesi ise R ye göre oluşan denklik sınıflarıdır. Tekrarlı bloğu olmayan bir S yapısı, S nin indirgenmiş yapısıdır (Hughes et all, 1985).

Tanım 2.3 (Dolu Eleman)

S nin bir elemanı, diğer olası tüm elemanlarla çakışım durumunda ise böyle bir noktaya dolu eleman denir.

Tanım 2.4 (Yalıtık Eleman)

S teki bir eleman 0 veya 1 tane elemanla çakışım durumundaysa bu elemana yalıtık eleman denir.

Tanım 2.5 (S nin Standartlaştırılmışı)

Bir S yapısı verildiğinde önce dolu elemanları sonra yalıtık elemanları, sonra tekrar dolu elemanları v.b. atılarak yeni bir yapı elde edilebilir. Buna standartlaştırılmış yapı denir. Standartlaştırılmış yapı $\overline{S}$ ile gösterilir.

Tanım 2.6 (Çakışım Matrisi)

Bir S yapısında v noktalar, b bloklar ($v > 0, b > 0$) olmak üzere, S nin noktaları $p_1, p_2, p_3,...,$ p_v ve blokları $x_1, x_2,..., x_b$ şeklinde etiketlenmiş (indekslenmiş) olsun.

S yapısının $A = [\, a_{ij} \,]_{v \times b}$ çakışım matrisi $v \times b$ boyutlu bir matris olup,

$$a_{ij} = \begin{cases} a_{ij} = 1; & p_i \, noktası \, x_j \, blogu \; üzerinde ise \\ a_{ij} = 0; & aksi \; halde \end{cases}$$

şeklinde tanımlanır.Görüldüğü gibi A bir (0,1) – matristir. S yapısı hakkındaki tüm bilgiler A çakışım matrisinden elde edilebilir. S nin blokları ve noktaları farklı bir şekilde etiketlendiğinden , A çakışım matrisi doğal olarak değişir. S yapısının farklı çakışım matrisleri arasında çok yakın bir ilişki vardır.

S nin noktaları $p_1, p_2,...p_v$ blokları ise $x_1, x_2,...x_b$ şeklinde etiketlendiğinde çakışım matrisi A, noktalar $q_1, q_2,...q_v$ şeklinde bloklar ise $x_1, x_2,...x_b$ şeklinde etiketlendiğinde de çakışım matrisi B olsun. Noktalar farklı , bloklar aynı şekilde etiketlenmiştir.Her q_i ve p_j noktası olduğuna göre $\{1,2,3,....,v\}$ nin bir θ permütasyonu elde edilir.Bu permütasyon $\theta(i) = j \Leftrightarrow q_i = p_j$ şeklinde tanımlanmıştır. Bunun anlamı B nin i.satırının A nın $\theta(i)$ inci satırı olmasıdır. Diğer bir deyişle B matrisi A nın satırlarının permütasyonu alınarak elde edilir.

Sonuç olarak, bloklarda farklı şekilde etiketlenebileceğinden bir S yapısının iki çakışım matrisi A ve B ise $PA\theta = B$ şeklinde P ve θ permütasyon matrisleri vardır. Şu halde iki çakışım matrisi birbirine denktir.

Tanım 2.7(Permütasyon Matrisi)

Her bir satır ve sütununda birer tane birim(veya 1) bulunan ve diğer elemanları 0 olan bir kare matristir.

Tanım 2.8 (Bir biçimli Yapı)

S yapısı verildiğinde, S yapısının bloklar kümesi boş kümeden farklı ve her blok tam $k>0$ tane nokta içeriyorsa S yapısına bir biçimli denir.

Tanım 2.9(Düzgün Yapı)

Bir S yapısında tüm p noktaları için $|p|=r>0$ ise bu yapıya düzgün bir yapı denir.

Tanım 2.10 (t-yapı)

v noktalı bir S yapısı verilsin. $0\le t\le v$ olmak üzere S nin t noktalı her alt kümesi tam λ tane blok ile çakışım durumundaysa bu yapıya bir t- yapı denir. Blok genişliği k olan düzgün bir t- yapı , t-(v, k, λ) yapı adını alır. Bir biçimli t- yapılar, $0\le s\le t$ koşulunu sağlayan her s için, birbiçimli s-yapıdır.

Teorem 2.11

Bir t-(v ,k, λ) yapı S olsun. Bu durumda $0\le s<t$ koşulunu sağlayan her s tamsayısı için S nin noktalarından oluşan bir s-küme ile çakışım halinde olan

$$\lambda_s=\lambda\frac{(v-s)(v-s-1).....(v-t+1)}{(k-s)(k-s-1).....(k-t+1)}$$

tane blok vardır (Hughes et all, 1985).

İspat:

S nin s tane noktasından oluşan belli bir altküme B olsun. S nin B yi içeren bloklarının sayısını m ile gösterelim.Bu durumda amaç m yi teoremdeki gibi belirtmektir. (Yani $m=\lambda_s$ olduğunu göstermektir.)

Burada m' nin B kümesinin seçimine bağlı olmayıp sadece s sayısına bağlı olduğu gösterilmelidir.Bunun için olası (J , y) ikilileri tanımlansın. Burada J ile B kümesini içeren t noktalı bir küme gösterilir. y ise J' yi içeren bir bloktur. Bu şekilde oluşan (J , y) ikililerini aşağıdaki biçimde iki yolla sayalım.

B yi kapsayan m bloktan herbiri , B yi kapsayan $\binom{k-s}{t-s}$ tane t- küme içerir. O zaman olası ikililerin sayısı $m\binom{k-s}{t-s}$ olur. Diğer yandan B yi kapsayan t-noktalı bir J kümesinin seçimi $\binom{v-s}{t-s}$ yolla yapılabilir. Bu kümelerin herbiri tam λ tane blok üzerindedir. Yani bu kümelerin herbiri ortaklaşa tam λ tane blokta birlikte bulunurlar.

Dolayısıyla olası (J, y) ikililerinin sayısı $\lambda\binom{v-s}{t-s}$ olur. Yukarıdaki gibi elde edilen olası çiftlerin sayısı eşitlenirse

$$m\binom{k-s}{t-s}=\lambda\binom{v-s}{t-s}$$

$$m=\lambda\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}=\lambda\frac{(v-s)(v-s-1).....(v-t+1)}{(k-s)(k-s-1).....(k-t+1)}=\lambda_s$$

bulunur.

Bu teoremin sonucu olarak $t>0$ için bir t-(v,k,λ) yapı S olsun. Eğer s, $0<s<t$ koşulunu sağlayan bir tamsayı ise bu durumda S nin bir s-(v,k,λ_s) yapı olduğu söylenebilir. S nin bir t-(v, k, λ) yapı ise bu yapıdaki blokların sayısı b ile gösterilir. $t\geq 1$ ise Teorem 2.11 den dolayı bir noktadan geçen blokların sayısı sabittir. Yani bir noktanın çakışım durumunda olduğu blok sayısı sabittir.Bu sabit sayı r ile gösterilecektir.

Sonuç 2.12

S bir t-(v,k,λ) yapı olsun.

1) $b=\lambda\frac{v(v-1).....(v-t+1)}{k(k-1).....(k-t+1)}$

dir.

2) $t>0$ ise $bk=vr$

dir.

3) $t>1$ ise $r(k-1)=\lambda_2(v-1)$

dir.

Tanım 2.13 (Kare Yapı)

Bir S yapısının blok sayısı nokta sayısına eşit ise ($b=v$ ise) bunun çakışım matrisi kare matris olur. Bu nedenle bir yapıda $b=v$ ise bu yapıya kare yapı denir.

Tanım 2.14 (Trivial Yapı)

Blok genişliği k olan bir biçimli bir yapıda noktaların her k-kümesi en azından bir blokla çakışım halinde ise bu yapıya trivial yapı denir.

Tanım 2.15 (Dizayn)

Bir biçimli indirgenmiş bir yapıya dizayn denir.

Tanım 2.16 (Bir Yapının Duali)

S nin duali S^T ile gösterilir. S^T yapısında S nin blokları noktalar , noktalarıda bloklarıdır. S nin her p noktası için S^T nin bir p' bloğu vardır. S nin her bir x bloğu için S^T nin bir x' noktası vardır.

S^T deki çakışım bağıntısı ise " Ancak ve ancak S deki p noktası x bloğu üzerinde ise x' noktası p' bloğu üzerindedir, " şeklinde tanımlanır. Ayrıca $(S^T)^T=S$ dir (Hughes et all, 1985).

Teorem 2.17

Bir S yapısının çakışım matrisi A ise A nın transpozesi olan A^t matriside S^T nin çakışım matrisidir.

İspat:

S nin noktaları $p_1,p_2,....,p_v$ blokları $x_1,x_2,....,x_b$ şeklinde gösterilsin. A çakışım matrisinde ancak ve ancak $a_{ij}=1$ ise p_i noktası x_j bloğu üzerindedir. S^T nin noktaları $x_1',x_2',....,x_b'$ blokları ise $p_1',p_2',....,p_v'$ ile gösterilmiş olsun. Burada ancak ve ancak x_i' noktası p_j' bloğu üzerinde ise $b_{ij}=1$ dir. S^T nin tanımından p_j noktası x_i bloğu üzerinde ise yani ancak ve ancak $a_{ij}=1$ ise $b_{ij}=1$ dir. Dolayısıyla $b_{ij}= a_{ij} \Leftrightarrow B = A^t$ olmasıdır.

Örnek

S nin noktaları $\{1,2,3,4,5,6,7\}$

Blokları $f_1=\{1,2,4\}$ $f_2=\{2,3,5\}$ $f_3=\{3,4,6\}$ $f_4=\{4,5,7\}$ $f_5=\{5,6,1\}$

$f_6=\{6,7,2\}$ $f_7=\{7,1,3\}$ olsun.

S^T nin noktaları $f_1',f_2',f_3',f_4',f_5',f_6',f_7'$ blokları ise $1',2',3',4',5',6',7'$ şeklinde gösterilsin.

$1'=\{f_1',f_5',f_7'\}$ $2'=\{f_1',f_2',f_6'\}$ $3'=\{f_2',f_3',f_7'\}$ $4'=\{f_1',f_3',f_4'\}$ $5'=\{f_2',f_4',f_5'\}$ $6'=\{f_3',f_5',f_6'\}$

$7'=\{f_4',f_6',f_7'\}$

şeklinde verildiğinde

$$A=\begin{bmatrix}1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\\1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix} \qquad A^t=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\\1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\1&0&1&0&0&0&1\end{bmatrix}$$

$A^t=B$ olduğu görülür.

Tanım 2.18 (S Yapısının tümleyeni)

S nin tümleyeni $C(S)$ ile gösterilsin. $C(S)$ nin noktaları tamamıyle S nin noktalarından oluşur. S nin bir x bloğu için $C(S)$ nin bir x^* bloğu elde edilir. Bir p noktası ancak ve ancak bir x bloğu üzerinde değilse , bir x^* bloğu üzerindedir.

Örnek

S yapısının noktaları $\{1,2,3,4,5,6,7\}$

Blokları $f_1=\{1,2,4\}$ $f_2=\{2,3,5\}$ $f_3=\{3,4,6\}$ $f_4=\{4,5,7\}$ $f_5=\{5,6,1\}$ $f_6=\{6,7,2\}$

$f_7=\{7,1,3\}$ olsun.

$C(S)$ de bloklar $f_1^*=\{3,5,6,7\}$ $f_2^*=\{1,4,6,7\}$ $f_3^*=\{1,2,5,7\}$ $f_4^*=\{1,2,3,6\}$

$f_5^*=\{2,3,4,7\}$ $f_6^*=\{1,3,4,5\}$ $f_7^*=\{2,4,5,6\}$

olur.

Yardımcı Teorem 2.19

1) S nin bir biçimli olması için gerek ve yeter koşul $C(S)$ nin bir biçimli olmasıdır.
2) S nin düzgün olması için gerek ve yeter koşul $C(S)$ nin düzgün olmasıdır.
3) S nin dizayn olması için gerek ve yeter koşul $C(S)$ nin dizayn olmasıdır

Teorem 2.20

$2\le k\le v-2$ olmak üzere (v, k, λ) için bir 2- yapı S olsun. Bu durumda $C(S)$ $(v, v-k, b-2\lambda_1+\lambda)$ parametreli 2-yapıdır.

İspat :

A ve B , $C(S)$ yapısının iki farklı noktası olsun. S nin noktalarının sayısı v olduğundan $C(S)$ nin noktalarının sayısıda v olacaktır. S nin her bloğunda k tane nokta varsa

tümleyen tanımından $C(S)$ nin $v-k$ tane noktası vardır. A ve B aynı zamanda S ninde noktalarıdır. A noktası S de λ_1 tane blok ile çakışım durumunda B de S de λ_1 tane blok ile çakışım durumundadır. A yı B yi içerenlerin sayısı $2\lambda_1$ tanedir. Tanım gereği hem A yı hem B yi içerenlerin sayısı ise λ dır. A dan ve B den sadece birini içerenlerin sayısı $2\lambda_1-\lambda$ dır. S nin A yı ve B yi içermeyen bloklarının sayısı $b-(2\lambda_1-\lambda)=b-2\lambda_1+\lambda$ dır ve bu da A ve B yi birlikte içeren $C(S)$ nin bloklarının sayısına eşittir. Bu taktirde $C(S)$ nin bloklarının her iki alt kümesi $b-2\lambda_1+\lambda$ tane blok ile çakışım durumundadır.Bu ise $C(S)$ nin $(v, v-k, b-2\lambda_1+\lambda)$ parametreli 2- yapı olması demektir.

Tanım 2.21

$n=r-\lambda_2$ sayısı S nin mertebesi adını alır. (r, bir noktadan geçen blokların sayısı , λ_2 ise herhangi 2-li kümenin ortaklaşa bulunduğu blok sayısıdır.)

$b=\lambda_0$, $r=\lambda_1$,$\lambda=\lambda_t$ alınır.

Teorem 2.22

$2\le k\le v-2$ olmak üzere S , (v, k, λ) için bir 2-yapı ise $C(S)$ nin mertebesi S nin mertebesine eşittir.

İspat:

Bir önceki teoremden $C(S)$, $(v, v-k, b-2\lambda_1+\lambda)$ için bir 2-yapıdır. A noktasından geçen A ile çakışım durumunda olan S nin r tane bloğu vardır. Yani $C(S)$ nin $b-r$ tane bloğu A ile çakışım durumundadır.

Mertebe tanımından $b-r-(b-2r+\lambda)=r-\lambda$ dır.

Tanım 2.23 (İç Yapı)

p yi içeren herbir blok bir bloktur. p nin dışındaki noktaları düşünelim. Bu noktalardan yukarıdaki bloklardan en az birine ait noktalar kümesi ile oluşturulan yapı S_p ile gösterilir. Buna iç yapı denir.

Teorem 2.24

S bir yapı olsun. S nin bir noktasıda p olsun.

1) $t\ge 2$ olacak şekilde S bir t-yapı ise S_p de $(t-1)$ - yapıdır.

2) $t\ge 2$ ve (v,k,λ) için S bir biçimli t-yapı ise S_p de $(v-1,k-1,\lambda)$ için bir $(t-1)$ – yapıdır.

3) $t \geq 2$ olacak şekilde S bir t-(v, k , λ) dizaynı ise S_p de (t-1)-(v-1 , k-1 , λ) dizayndır.

İspat:

S_p deki noktaların her (t-1) kümesine p eklenerek S içindeki noktaların bir t kümesi elde edilir. S içindeki noktaların her t kümesi λ tane blok ile ortaklaşa çakışım halindedir. S_p nin her (t-1) kümesi S_p içinde λ ortak bloğu ile çakışım halindedir.S_p nin nokta sayısı v-1 dir. S nin her bloğu k tane nokta içerir. S_p nin her bloğu k-1 nokta içerir.

Tanım 2.25 (Dış Yapı)

S bir yapı ve p, S nin bir noktası olsun. Bloklar, p ile çakışım durumunda olmayan S nin tüm blokları noktaları , bu noktaların en az biri üzerinde bulunan S nin tüm noktaları olan yapıya S nin p noktasındaki dış yapısı denir ve S^p ile gösterilir. S bir yapı ve x, S nin bir bloğu olsun. Noktaları, x bloğu üzerinde bulunmayan S nin tüm noktaları, blokları ise x üzerinde bulunmayan en az bir noktayı içeren tüm bloklar kümesi olan yapıya S nin x bloğundaki dış yapısı denir ve S^x ile gösterilir.

Teorem 2.26

S bir yapı ve p , S nin bir noktası olsun.

1) $t \geq 2$ olmak üzere S, (v, k , λ) parametreli bir biçimli bir t- yapı ise o zaman S^p de (v-1 , k , $\lambda_{t-1}-\lambda$) parametreli bir biçimli (t-1)- yapıdır.

2) $t \geq 2$ olacak şekilde S bir t- (v ,k, λ) dizayn ise S^p de bir (t-1)- (v-1 , k , $\lambda_{t-1}-\lambda$) dizayndır.

İspat:

1) şıkkını ıspatlamak yeterlidir. İndirgenmiş bir biçimli yapıya dizayn diyorduk. S tekrarlı blok içermiyorsa S^p de tekrarlı blok içermiyecektir yani indirgenmiştir.S nin her bloğu k nokta içeriyorsa S^p de noktaların herhangi bir (t-1) kümesi S nin λ_{t-1} bloğu üzerindedir. S^p nin blokları S nin p yi içermeyen bloklarıdır. S^p nin noktaları bu blokların en az biri ile çakışım durumunda olan noktalarda bulunur. Dolayısıyla bu şekilde tanımlı noktaların her (t-1) kümesi λ_{t-1} blok ile çakışım durumunda olacaktır.Fakat p' yi içeren her t-küme λ tane blok ile çakışım durumunda olduğundan bu λ_{t-1} blok içinde p yi içeren λ tane blok vardır.

Buradan p yi içermeyen S^p nin noktalarının her $(t\text{-}1)$ kümesi $\lambda_{t-1}-\lambda$ tane blok ile çakışım durumundadır.

Tanım 2.27 ((v,k,λ) - Parametreli Simetrik Dizayn)

($v,k,\ \lambda$) - parametreli simetrik blok dizayn aşağıdaki aksiyomları sağlayan bir çakışım yapısıdır.

i) v sayıda nokta vardır.

ii) v sayıda blok vardır.

iii) Her bir nokta k tane blok ile çakışım durumundadır.

iv) Her bir blok k tane nokta ile çakışım durumundadır.

v) Herhangi iki bloğun ortaklaşa çakışım durumunda oldukları nokta sayısı λ dır.

vi) Herhangi iki noktanın ortaklaşa çakışım durumunda oldukları blok sayısı λ dır

(Lander, 1985).

Tanım 2.28

$n=k-\lambda$ tamsayısına ($v,k,\ \lambda$) - parametreli simertik dizaynın mertebesi denir.

Tanım 2.29 (Simetrik Dizaynın Çakışım Matrisi)

Bir ($v,k,\ \lambda$) - parametreli simetrik dizaynda

$P=\{p_1,p_2,\ldots,p_v\}$ ve $B=\{B_1,B_2,\ldots,B_v\}$ olmak üzere, elemanları

$$a_{ij}=\begin{cases}1 & p_j \text{ noktası } B_i \text{ bloğu ile çakışım durumunda ise}\\ 0 & p_j \text{ noktası } B_i \text{ bloğu ile çakışım durumunda değil ise}\end{cases}$$

olan

$A=\left[a_{ij}\right]_{v\times v}$ matrisine Simetrik Dizaynın Çakışım Matrisi denir.

Özelik 2.30

($v,k,\ \lambda$) - parametreli simetrik blok dizaynın parametreleri arasında

1) $(v\text{-}1)\,\lambda=k(k\text{-}1)$

2) $k^2\text{-}\,v\lambda=k-\lambda$

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

bağıntıları vardır.

İspat:

1) Bir q noktası seçilsin. $p \neq q$ olmak üzere p ve q ile çakışım durumunda olan B blokları ile p noktalarından oluşturulan (p, B) ikilileri iki farklı yolla sayılsın. Sonra bunlar eşitlensin. p, q ikilisi $(p \neq q)$ ortaklaşa λ tane blok ile çakışım durumundadır. q yu sabit tutarak p yi v-1 şekilde seçebileceğimizden istenen koşula uyan (p, B) ikililerinin sayısı $(v\text{-}1)\lambda$ olur.

Diğer taraftan B bloklarının tam k tanesinde q vardır. Bu k bloktan q lar atılırsa, her birinde k-1 eleman kalır. Yani q yu içeren B bloğu ile k-1 tane (p, B) ikilisi oluşturulur. q yu içeren k tane blok olduğundan, istenen (p, B) ikililerinin sayısı $k(k\text{-}1)$ dir.

Sonuç olarak $(v\text{-}1)\lambda = k(k\text{-}1)$ bulunur.

2) ve 3) şıklarının ıspatı da 1) den kolaylıkla görülür.

Özelik 2.31

Elemanların hepsi +1 olan $v \times v$ boyutlu kare matris J, I ise uygun boyutlu birim matris olmak üzere

i) $AJ = JA = kJ$

ii) $AA^t = A^tA = (k - \lambda)I + \lambda J = nI + \lambda J$

iii) $|\det A| = kn^{v-1/2}$

bağıntıları vardır.

İspat:

i ve ii nin ispatı aşikardır.

iii) $AA^t = nI + \lambda J$ eşitliğinden,

$$\det AA^t = \det(nI + \lambda J)$$

$$= \begin{vmatrix} n+\lambda & \lambda & \cdots & \lambda \\ \lambda & n+\lambda & \cdots & \lambda \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \lambda & \lambda & \cdots & n+\lambda \end{vmatrix}$$

2, 3,. . . , v sütunlar 1.sütuna eklenerek

$$= \begin{vmatrix} n+v\lambda & \lambda & . & . & . & \lambda \\ n+v\lambda & n+\lambda & . & . & . & \lambda \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ n+v\lambda & \lambda & . & . & . & \lambda \end{vmatrix}$$

$$= (n+\lambda v) \begin{vmatrix} 1 & \lambda & . & . & . & \lambda \\ 1 & n+\lambda & . & . & . & \lambda \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 1 & \lambda & . & . & . & n+\lambda \end{vmatrix}$$

$$= (n+\lambda v) \begin{vmatrix} 1 & \lambda & . & . & . & \lambda \\ 0 & n & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & n \end{vmatrix}$$

$$= (n+\lambda v)\, n^{v-1}$$

bulunur. Yani,

$\det(AA^t) = (n+\lambda v)\, n^{v-1}$ dir. $n+\lambda v = k^2$ olduğundan

$\det(AA^t) = k^2 n^{v-1}$ olur.

Buradan

$|\det A| = kn^{v-1/2}$

bulunur.

Tanım 2.32 (Simetrik dizaynın kodu)

(v, k, λ) parametreli simetrik dizaynın kodu, dizaynın A çakışım matrisinin satırları ile üretilen alt uzayıdır. Bu C ile gösterilir.

Örnek

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

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

Bloklar kümesi $\{ B_1, B_2, ..., B_7 \}$ olur.

(7, 3, 1) - simetrik dizayndır.

	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	0	0	0	1	0	1
2	1	1	0	0	0	1	0
3	0	1	1	0	0	0	1
4	1	0	1	1	0	0	0
5	0	1	0	1	1	0	0
6	0	0	1	0	1	1	0
7	0	0	0	1	0	1	1

0 ve 1 lerden oluşan matris, dizaynın çakışım matrisidir.

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

Bu çakışım matrisi kullanılarak aşağıdaki yolla bir C kodu elde edilir. Buna kısaca D dizayn kodu denir.

0	0	0	0	0	0	0
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
1	0	1	1	0	0	0
0	1	0	1	1	0	0
0	0	1	0	1	1	0
0	0	0	1	0	1	1
0	1	1	1	0	1	0
0	0	1	1	1	0	1
1	0	0	1	1	1	0
0	1	0	0	1	1	1
1	0	1	0	0	1	1
1	1	0	1	0	0	1
1	1	1	0	1	0	0

Diğer kod sözcükleri 0 yerine 1, 1 yerine 0 yazılarak oluşturulur. Burada daima $x, y \in C$ için $x + y \in C$ dir.

16 tane kod sözcüğü elde edilmiştir. Buna C kodu diyelim. $d = 3$ olduğunu gösterelim. C nin minimum uzaklığının 3 olduğunu yani $x , y \in C$ için $d(x, y) \geq 3$ olduğu gösterilmelidir.

$n = 7 , q = 2 , M = 16$ olup $d = 3$ olduğunu gösterelim :

1) $d (a_i , a_j) = \omega (a_i) + \omega (a_j) - 2\, \omega (a_i \cap a_j)$; $(i \neq j)$

$= 3 + 3 - 2.1$

$= 6 - 2$

$= 4$

2) $d (b_i , b_j) = \omega (b_i) + \omega (b_j) - 2\, \omega (b_i \cap b_j)$

$= 4$

3) $d (0, a_i) = 3$ $d (0, b_i) = 4$ $d (0, 1) = 7$

4) $d (1, a_i) = 4$ $d (1, b_i) = 3$ $d (1, 0) = 7$

5) $d (a_i, b_i) = 7$

6) $i \neq j$ için $d(a_i, b_j) = ?$

a_i ile b_j nin farklı olduğu konumlar a_i ile a_j nin aynı olduğu konumlara eşittir. Dolayısıyla

$$d(a_i, b_j) = 7 - d(a_i, a_j) = 7 - 4 = 3$$
$$d(C) = 3$$

tür.

Dolayısıyla elde edilen kod, (7, 16, 3) - koddur.

3. k TEK SAYI OLMAK ÜZERE (v, k, λ) - SİMETRİK DİZAYN İLE ÜRETİLEN KODLARLA İLGİLİ BİR OLASILIK FONKSİYONU TAYİNİ

3.1 İzafi Ağırlık

Tanım 3.1

k tek sayı olmak üzere (v, k, λ) - Simetrik dizaynın C kodunun C_1 alt kümesi,

1) Simetrik dizaynın çakışım matrisinin satırları
2) Çakışım matrisinde 0 lar yerine 1, 1 ler yerine 0 alarak elde edilen satır vektörleri
3) $0 = (0\ 0\ \ldots\ 0)$ ve $1 = (1\ 1\ \ldots\ 1)$ sözcüklerinden oluşan küme

olsun. C_1 in bir X vektörü ele alınsın. Bu sözcükteki 1 lerin bulunduğu konumlar $s_1, s_2, \ldots, s_k$ ise

$$s_1 + s_2 + \ldots + s_k$$

toplamına X kod sözcüğünün İzafi Ağırlığı adını verelim ve bunu

$$S(X) = s_1 + s_2 + \ldots + s_k$$

ile gösterelim. Örneğin

$X = 1000101$ ise $S(X) = 1 + 5 + 7 = 13$

olur.

Bu durumda $(1\ 1\ 1\ 1\ 1 \ldots 1) \in C_1$ olduğundan bunun ağırlığı

$$1 + 2 + 3 + \ldots + v = \frac{v(v+1)}{2}$$

olur. Buna simetrik dizaynın bu yolla tanımlanan C kodunun Maksimum İzafi Ağırlığı denebilir. Bir $X \in C_1$ kod sözcüğü için

$$e(X) = \frac{S(X)}{\textit{Maksimum izafi ağırlık}}$$

gösterimini kullanalım. Buna da sözcüğün izafi ağırlık oranı diyebiliriz.

Eğer $X_i, X_j \in C_1$ ise

$$e(X_i + X_j) = e(X_i) + e(X_j) - 2\,e(X_i\, X_j)$$

olduğu kolaylıkla görülebilir. Gerçekten $X_i + X_j$ toplamında 1+1 = 0 olacağından, ikinci tarafta X_i ve X_j de 1 olan konumlar, $X_i\, X_j$ çarpımında 1.1 = 1 olup, X_i den ve X_j den ayrı ayrı gelen fazlalıklar $2e(X_i\, X_j)$ küçüklüğünün çıkartılmasıyla giderilir.

Bu kavramları (7, 3, 1) - simetrik dizaynın kodu üzerinde açıklayabiliriz.

Örnek

(7, 3, 1) – parametreli simetrik dizaynın F_2- kodu bir (7, 16, 3) – koddur. Bu kod C ile gösterilsin.

Kod Sözcükleri	e(X_i)
0 0 0 0 0 0 0	0/28
1 1 1 1 1 1 1	28/28
1 0 0 0 1 0 1	13/28
1 1 0 0 0 1 0	9/28
0 1 1 0 0 0 1	12/28
1 0 1 1 0 0 0	8/28
0 1 0 1 1 0 0	11/28
0 0 1 0 1 1 0	14/28
0 0 0 1 0 1 1	17/28
0 1 1 1 0 1 0	15/28
0 0 1 1 1 0 1	19/28
1 0 0 1 1 1 0	16/28
0 1 0 0 1 1 1	21/28
1 0 1 0 0 1 1	17/28
1 1 0 1 0 0 1	14/28
1 1 1 0 1 0 0	11/28

$X_1 = 1\,0\,0\,0\,1\,0\,1$ $\qquad X_1X_2 = 1\,0\,0\,0\,0\,0\,0$

$X_2 = 1\,1\,0\,0\,0\,1\,0$ $\qquad X_1 + X_2 = 0\,1\,0\,0\,1\,1\,1$

$$e(X_1 + X_2) = e(X_1) + e(X_2) - 2\,e(X_i\,X_j)$$

$$= 13/28 + 9/28 + 2.\ 1/28$$

$$= 20/28$$

Teorem 3.2

(v, k, λ) – simetrik dizaynının yukarıdaki gibi tanımlanan kodu C ve çakışım matrisinin satırlarından oluşan kod sözcükleri $X_1, X_2, ..., X_v$ ise

$$\sum_{i=1}^{v} e(X_i) = k$$

dır.

İspat:

$$\sum_{i=1}^{v} e(X_i) = e(X_1) + e(X_2) + ... + e(X_v)$$

$$= \frac{S(X_1)}{\max.izafi\ ağ.} + \frac{S(X_2)}{\max.izafi\ ağ.} + ... + \frac{S(X_v)}{\max.izafi\ ağ.}$$

$$= \frac{S(X_1) + S(X_2) + ... + S(X_v)}{\max.izafi\ ağ.}$$

$$= \frac{S(X_1) + S(X_2) + ... + S(X_v)}{v(v+1)/2}$$

dir.

(v, k, λ) –Simetrik dizaynın tanımından çakışım matrisinin satırlarından oluşan v tane kod sözcüğünde her konumda eşit sayıda ve tam k tane 1 vardır.

1 inci konumda k

2 inci konumda k

.

.

v inci konumda k tane " 1 " olduğundan, v kod sözcüğü için

$$S(X_1) + S(X_2) + ... + S(X_v) = k(1 + 2 + ... + v) = k\,\frac{v(v+1)}{2}$$

bulunur. Sonuçta

$$\sum_{i=1}^{v} e(X_i) = k$$

olur..

Teorem 3.3

k tek sayı olmak üzere (v,k,λ)–Simetrik dizaynın tümleyeninin çakışım matrisinin satır vektörleri de dizaynın binary C kodunun kod sözcükleridir.

İspat:

(v,k,λ)–Simetrik dizaynın A çakışım matrisinin her bir sütununda k sayıda 1 olacağından, A nın v tane satırının toplanmasıyla

$$(k,k,...,k) \equiv (1,1,...,1)\ (\mathrm{mod}\ 2)$$

elde edilir ($k = 2t + 1 \equiv 1\ (\mathrm{mod}\ 2)$). O zaman A nın bir satır vektörü X olmak üzere

$$X + (1,1,...,1)$$

vektörü C nin bir kod sözcüğü olup, D dizaynının tümleyeninin satır vektörleri kümesine aittir.

Teorem 3.4

k tek sayı olmak üzere (v, k, λ)- Simetrik dizaynın tümleyeni D' ve D' nün çakışım matrisinin satırlarından oluşan kod sözcükleri $X'_1, X'_2, ..., X'_v$ ise

$$\sum_{i=1}^{v} e(X'_i) = v - k$$

dır.

İspat:

$$\sum_{i=1}^{v} e(X'_i) = e(X'_1) + e(X'_2) + ... + e(X'_v)$$

$$= \frac{S(X'_1)}{\max.izafi\ ağ.} + ... + \frac{S(X'_v)}{\max.izafi\ ağ.}$$

$$= (v-k)\frac{v(v+1)/2}{v(v+1)/2}$$

$$= v - k$$

dır.

Sonuç 3.5

k tek sayı olmak üzere (v, k, λ) – Simetrik dizaynın çakışım matrisinin satır vektörleri, dizaynın tümleyeninin çakışım matrisinin satır vektörleri ve (0,0,...,0) , (1,1,...,1) vektörlerinden oluşan kod sözcüklerinin kümesi C_1 olduğundan

$$\sum_{X_i \in C_1} e(X_i) = v + 1$$

dir.

İspat:

$X_1 = (1\ 1\ 1\ ...1)$ için $\frac{1+2+...+v}{1+2+...+v} = 1$ olduğundan $e(X_1) = 1$ dir.

$$\sum_{X_i \in A} e(X_i) = k$$

$\sum_{X_i' \in A'} e(X_i') = v - k$ (D nin tümleyeninin çakışım matrisi A' dür.)

$$\sum_{X_i \in C_1} e(X_i) = k + v - k + 1 = v + 1$$

bulunur.

Örnek

D bir (7, 3, 1) - simetrik dizayn ise

$$\sum_{i=1}^{7} e(X_i) = e(X_1) + e(X_2) + e(X_3) + e(X_4) + e(X_5) + e(X_6) + e(X_7)$$

$$= \frac{13+9+12+8+11+14+17}{28}$$

$$= \frac{84}{28}$$

$$= 3$$

$$\sum_{i=1}^{7} e(X_i') = e(X_1') + e(X_2') + e(X_3') + e(X_4') + e(X_5') + e(X_6') + e(X_7')$$

$$= \frac{15+19+16+20+17+14+11}{28}$$

$$= \frac{112}{28}$$

$$= 4$$

Tanım 3.6

D dizaynının A çakışım matrisinin satırları ve D nin tümleyeninin A' çakışım matrisinin satırları kümesine 0 ve 1 in katılmasıyla elde edilen küme C_1 olmak üzere C_1 için aşağıdaki gibi tanımlayacağımız bir izafi olasılıklar kümesini C_o ile gösterelim. X_i kod sözcüğünün izafi olasılığı

$$p(X_i) = \frac{S(X_i)}{(v+1)(Maks.\ izafi\ ağ.)}$$

şeklinde tanımlansın. Maksimum izafi ağırlık $\frac{v(v+1)}{2}$ olduğundan

$$p(X_i) = \frac{S(X_i)}{(v+1).\frac{v(v+1)}{2}}$$

$$p(X_i) = \frac{2.S(X_i)}{v(v+1)^2}$$

dir.

Özelik 3.7

$\sum_{X_i \in C_1} p(X_i) = 1$ dir.

İspat:

Simetrik dizaynın bloklarına karşılık gelen kod sözcükleri için p ler toplamı

$$\frac{2k\frac{v(v+1)}{2}}{v(v+1)^2} = \frac{k}{v+1} \quad (A \text{ nın satır vektörleri için}) \qquad (3.1)$$

olur. Simetrik dizayndaki her blokta 0 lar yerine 1 ler, 1 ler yerine 0 lar yazılarak elde edilen kod sözcükleri için p ler toplamı

$$\frac{2(v-k)\frac{v(v+1)}{2}}{v(v+1)^2} = \frac{v-k}{v+1} \quad (A' \text{nın satır vektörleri için}) \qquad (3.2)$$

olur.

(1 1 1 ... 1) kod sözcüğü için

$$\frac{2\frac{v(v+1)}{2}}{v(v+1)^2} = \frac{1}{v+1} \qquad (3.3)$$

dir.

(3.1), (3.2) ve (3.3) ün toplanmasıyla

$$\sum_{X_i \in C_1} p(X_i) = \frac{k}{v+1} + \frac{v-k}{v+1} + \frac{1}{v+1} = 1$$

bulunur.

Tanım 3.8

S_n , $\{ P \equiv (p_1,...,p_n) \mid p_i \geq 0, i = 1,2,...,n, \sum p_i = 1 \}$

olmak üzere tüm sonlu kesikli olasılık dağılımlarının kümesi olsun. $p \in S_n$ ve $n = 1,2,...$ için

$$H_n(p_1,...,p_n) = -\sum p_i \log p_i \qquad (3.4)$$

dir. Burada, 0log0 = 0 kabul edilecektir. $n = 2$ için (3.4) ün özel durumu, Shannon Entropi fonksiyonu adını alır (Mathai ve Rathie, 1975).

Shannon Entropisi

$H_2(p, 1-p) = -p\log p - (1-p)\log(1-p)$

olmak üzere

$$f(p) = H_2(p, 1-p) \qquad (3.5)$$

diyelim.

P dağılımının Shannon entropisi $P = \{p_1,...,p_i\}$ olmak üzere

$$H_n(P) = \sum_{i=2}^{n} r_i f(p_i/r_i)$$

şeklinde ifade edilir ($\forall i = 1,2,...,n$ *iç in* , $r_i = p_1+...+p_i$)

Yukarıdaki p yi, daha önce tanımladığımız k tek sayı olmak üzere (v, k, λ) - simetrik dizaynın söz konusu C_1 alt kümesine ait kod sözcükleri için tanımlanan izafi olasılık olarak alalım. O zaman bu da kod sözcüğünün bir belirsizlik ölçüsü olarak alınabilir.

(S_n, C_0 olarak alınmıştır.)

3.2 Entropi' nin Özellikleri

i) $H_n(P) \geq 0$

ii) $p_1, p_2 \in [0,1]$, $p_1 + p_2 \in [0,1]$, $f(0) = f(1)$ ve $f(1/2) = 1$ olmak üzere f,

$$f(p_1) + (1-p_1) f\left(\frac{p_2}{1-p_1}\right) = f(p_2) + (1-p_2) f\left(\frac{p_1}{1-p_2}\right) \qquad (3.6)$$

fonksiyonel denklemini sağlar.

$f(p_1) = -p_1\log p_1 - (1-p_1)\log(1-p_1)$

$f(p_2) = -p_2\log p_2 - (1-p_2)\log(1-p_2)$

yerine konulursa

$$f(p_1) + (1-p_1) f\left(\frac{p_2}{1-p_1}\right) = -p_1\log p_1 - p_2\log p_2 - \log(1-p_1-p_2) + p_1\log(1-p_1-p_2)$$

$$+ p_2\log(1-p_1-p_2)$$

$$f(p_2)+(1-p_2)f(\frac{p_1}{1-p_2}) = - p_1\log p_1 - p_2\log p_2 - \log(1 - p_1 - p_2) + p_1\log(1 - p_1 - p_2)$$

$$+ p_2\log(1 - p_1 - p_2)$$

olur. Buradan

$$f(p_1)+(1-p_1)f(\frac{p_2}{1-p_1}) = f(p_2)+(1-p_2)f(\frac{p_1}{1-p_2})$$

dir.

Bunu bir örnekle açıklayalım :

C , (7, 16, 3) -kod olsun. $p(X_1)$ ve $p(X_2)$ izafi olasılıkları sırasıyla X_1 ve X_2 kod sözcüklerinin belirsizlik ölçüleridir.

$X_1 = 1\ 0\ 0\ 0\ 1\ \ 0\ 1$

$X_2 = 1\ 1\ 0\ 0\ 0\ 1\ 0$ ise

$$p(X_1) = \frac{2.S(X_1)}{v(v+1)^2} = \frac{2.13}{7.8^2} = \frac{26}{448} = \frac{13}{224}$$

$$p(X_2) = \frac{2.S(X_2)}{v(v+1)^2} = \frac{2.9}{7.8^2} = \frac{18}{448} = \frac{9}{224}$$

dir.

$p(X_1)$ ve $p(X_2)$ (3.6) da yerine yazılırsa eşitlik sağlanır.

4. SONUÇ

İstatistikte deneylerin düzenlenmesinde kullanılan dizaynlar matematikçilerin, özellikle cebirin elemanlarını kullanmaları sonunda gelişmiştir. Dizaynlar matematikçilerin çalışma alanı durumuna gelmiştir. Bu çalışma ile de bu alana bir katkıda bulunulmuştur.

(v, k, λ) - parametreli bir dizayn sınıfının oluşturulması , istatistikte kullanım alanı olarak oldukça önem taşır. (v, k, λ) - parametreli Simetrik dizaynın kodu, dizaynın A çakışım matrisinim satırları ile üretilen alt uzayıdır.

k tek sayı olmak üzere (v, k, λ) - Simetrik dizaynın C kodu için C_1 alt kümesinde, X sözcüğünün izafi ağırlığı, maksimum izafi ağırlık ve izafi ağırlık oranı tanımlanarak özellikleri incelenmiştir. p izafi olasılığı Shannon entropisine uygulanarak C nin kod sözcükleri için bir düzensizlik ölçüsü önerilmiştir.

KAYNAKLAR

Aczel, J. (1966), Lectures on Functional Equations and Their Applications, Academic Press, New York.

Aczel, J. (1968), " On Different Characterizations of Entopies ", Lecture Notes in Mathematics, Vol.89, Springer - Verlag : 1 - 11

Balkanay,E. Simetrik Dızaynlar, Ders Notları

Blake , I.F. ve Mullin ,R.C., (1975), The Mathematical Theory of Codıng , Academic Press, New York

Blake , I.F. ve Mullin ,R.C., (1976), An Introduction to Algebraic and Combinatorial Coding Theory, Academic Press, New York.

Berlekamp, E.R., (1968), Algebraic Coding Theory, McGraw - Hill, New York.

Blahut, R.E., (1983), Theory and Practise of Error Control Codes, Addison - Wesley, Reading, Mass.

Cameron, P.J. ve Lint, J.H.V, (1975), Graph Theory - Coding Theory and Block Designs, Cambridge University Press.

Campbell, L.L., (1965), " A Coding Theorem and Rényi's Entropy ", Infomation and Control, 8 : p.p. 423 - 429.

Daroczy, Z., (1971), " On The Measurable Soluation of A Functional Equation ", Acta Math.Acad.Sci. Hungar.,22 : p.p. 11-18

Forte, B. ve Daroczy, Z., (1968), " A Characterization of Shannon's Entropy ", Boll. U.M.I., 4 : p.p. 631 -635

Hall, M., (1980), Combinatorial Theory, Wiley, New York.

Hamming, R.W., (1980), Coding and Information Theory, Prentice - Hall, New Jersey.

Hill, R.A., (1986), A First Course in Coding Theory, Clarenden Press, Oxford .

Hughes, D.R. ve Piper, F.C., (1985), Design Theory, Cambridge University.

Lloyd, S.P., (1957), " Binary Block Coding ", Bell Syst. Tech. J, 36 : p.p. 517 - 535.

Lander, E.S., (1983), Symmetric Designs : An Algebraic Appraoch, Cambridge University Press.

Mathai, A.M. ve Rathie, P. N., (1975), Basic Concepts in Information Theory and Statistic

McElliece, R.J., (1977), The Theory of Information and Coding. Addison Wesley, Reading, Mass.

Robinson, D.J.S., (1982), A Course in the Theory of Groups, Springer - Verlag

Singleton, R.C., (1964), " Maximum Distance q-nary Codes ", IEEE Trans. Info.Theory, 10 : p.p.116-118

Van Lint, J.H., (1971), Coding Theory. Lecture Notes in Mathematics Vol 201. California Institute of Technology : 42 – 59

ÖZGEÇMİŞ

Doğum Tarihi	5 Ağustos 1966	
Doğum Yeri	Trabzon	
Lise	1977 - 1984	Boğaziçi Behçet Kemal Çağlar Lisesi
Lisans	1984 – 1988	Marmara Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü
Yüksek Lisans	1988 – 1990	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Bölümü Matematik Anabilim Dalı
Doktora	1990 – 1999	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Bölümü Matematik Anabilim Dalı

Çalıştığı Kurum(lar)

1989 – Devam ediyor	YTÜ Fen Edebiyat Fak. Öğretim Görevlisi