KESİRLİ ÇOK ETKENLİ DENEYLERDE ÇÖZÜM VE EN AZ SAPMA KAVRAMI

RESOLUTION AND MINIMUM ABERRATION CONCEPTS FOR FRACTIONAL FACTORIAL DESIGNS

NAZAN DANACIOĞLU

Hacettepe Üniversitesi

Fen Bilimleri Enstitüsü Yönetmeliğinin

İSTATİSTİK Anabilim Dalı İçin Öngördüğü

DOKTORA TEZİ

olarak hazırlanmıştır.

2005

Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Bu çalışma jürimiz tarafından **İSTATİSTİK ANABİLİM DALI'nda DOKTORA TEZİ** olarak kabul edilmiştir.

Başkan	:….. Prof. Dr. Soner GÖNEN
Üye (Danışman)	:….. Prof. Dr. Gülsüm HOCAOĞLU
Üye (Eş Danışman)	:….. Prof. Dr. F. Zehra MULUK
Üye	:….. Prof. Dr. Hülya BAYRAK
Üye	:….. Doç. Dr. Tülay SARAÇBAŞI

ONAY

Bu tez ...../...../..... tarihinde Enstitü Yönetim Kurulunca belirlenen yukarıdaki jüri üyeleri tarafından kabul edilmiştir.

...../...../.....

Prof.Dr. Ahmet R. ÖZDURAL
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ

KESİRLİ ÇOK ETKENLİ DENEYLERDE ÇÖZÜM VE EN AZ SAPMA KAVRAMI

Nazan Danacıoğlu

ÖZ

Kesirli çok etkenli en az sapma tasarımları, en iyi tasarımlar olarak değerlendirilmekte ve uygulamada yaygın olarak kullanılmaktadır.

Bu çalışmada, 2-düzeyli kesirli çok etkenli tasarımların; kelime uzunluğu yapısı, çözüm, en az sapma vb. gibi yararlı özellikleri tanıtılmıştır.

İki-düzeyli kesirli çok etkenli tasarımların cebirsel yapısı araştırılarak; kod teorisi, özellikle Hamming kodları, ile kesirli çok etkenli tasarımlar arasındaki ilişki incelenmiştir.

2-düzeyli kesirli çok etkenli tasarımlar, kodlardan (Hamming kodları, ikili doğrusal ve döngüsel kodlar) yararlanarak oluşturulmuş ve en az sapma ölçütüne göre sıralanmıştır. Tasarımlar ve kod olarak karşılıkları bir katalogda toplanmıştır.

Anahtar Kelimeler: Kesirli çok etkenli tasarımlar, kod teorisi, Hamming kodları, en az sapma

Danışman: Prof.Dr. Gülsüm HOCAOĞLU, Hacettepe Üniversitesi, İstatistik Bölümü, Yöneylem Anabilim Dalı

Eş Danışman: Prof.Dr. F. Zehra MULUK, Başkent Üniversitesi, Sigortacılık ve Risk Yönetimi Bölümü

RESOLUTION AND MINIMUM ABERRATION CONCEPTS FOR FRACTIONAL FACTORIAL DESIGNS

Nazan Danacıoğlu

ABSTRACT

Fractional factorial experiments with minimum aberration are regarded as best design and are commonly used in practice.

In this study useful characteristics of two-level fractional factorial experiments, namely word length pattern, resolution, aberration etc. are introduced.

By exploring the algebraic structure of two-level fractional factorial designs, the connection between coding theory, especially Hamming codes, and fractional factorial designs is investigated.

Two-level fractional factorial designs are constructed from codes (Hamming, binary linear and binary cyclic codes), and are ordered by the minimum aberration criterion. Designs and their corresponding codes listed in a cataloge.

Keywords: Fractional factorial designs, coding theory, Hamming codes, minimum aberration.

Advisor: Prof.Dr. Gülsüm HOCAOĞLU, Hacettepe University, Department of Statistics, Operational Research Section

Co-advisor: Prof.Dr. F. Zehra MULUK, Baskent University, Department of Insurance and Risk Management

TEŞEKKÜR

"İnsan, ancak sevdiğinden bir şey öğrenir" der Goethe…
"Bir adama bir şey öğretmek istersen, asla öğrenmez" der B. Shaw….

Ben, öğretmek isteyenlerden öğrenemedim. Öğrenme isteğimi özgür bırakıp, yol gösterenlerdi; sevip, öğrendiklerim… Bu bağlamda, değerli danışmanlarım; Prof. Dr. F. Zehra Muluk ve Prof. Dr. Gülsüm Hocaoğlu'na teşekkürü borç bilirim.

Fikir vermek, ufkunu açmak, sorularına sorular katmak; adına ne derseniz deyin, tez izleme komitesindeki katkılarından dolayı; sevgili hocalarım Doç. Dr. Tülay Saraçbaşı ve Prof. Dr. Hülya Bayrak'a teşekkürü borç bilirim.

Pek işe yaramasa da, bana sürekli zamanı hatırlattığı ve ihtiyaç duyduğumda tavsiyelerini esirgemediği için; bölüm başkanımız, sevgili hocam Prof. Dr. Süleyman Günay'a, teşekkürü borç bilirim.

Tezden önce olduğu gibi, tezden sonra da hayatımda olacak; özel bir paragrafı hak eden, herkese lazım dostum; Ar. Gör. Ayten Yiğiter'e, sadece tez süresince yaptıkları için değil; içine her şeyi katarak, teşekkürü borç bilirim.

Bir gün, bilginin efendisi olacak sevgili dostum, Ar.Gör. Yasemin Saykan'a, darısı başına diyerek teşekkürü borç bilirim.

Bu çalışma süresince, zamandan başka hiçbir şeyin sıkıntısını çekmemiş biri olarak, küçük bir paragrafa sığdıramadığım; adlarını yazamasam da kendilerini bu satırlarda görecek olan; birlikte dağıtıp, birlikte söylendiğim ve birlikte eğlendiğim bütün Ar. Gör. arkadaşlarıma; tezimin bitmesini dört gözle bekleyen çocukluktan dostlarıma, teşekkürü borç bilirim.

Ender de olsa, nefes almam için işleri askıya alan FBE'ndeki çalışma arkadaşlarıma teşekkürü borç bilirim.

Matlab'ı bir sorun olmaktan çıkaran, her eve lazım damadımız, sevgili Özge Özköse'ye, program yazımındaki katkılarından dolayı teşekkürü borç bilirim.

Hayatımda ilk sıraya otursalar da, teşekkür sayfasında hep son paragrafa yerleşen sevgili AİLEME; ne desem, ne yapsam hep borçlu kalacağım. Bilmem, bir teşekkür sayılır mı şu an yazacaklarım: "Gülleri sarı severim, toprağı ıslak; / Türküleri yanık, şiirleri hoyrat! / Havayı nemsiz, çayı demsiz…/ Bir sizi her şeye rağmen! / Bir sizi her şeyden çok! / Bir sizi, sonsuza kadar…"

İÇİNDEKİLER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

D.K.M.	Denklik Kontrol Matrisi
GF	Galois Cismi
Ü.M.	Üreteç Matrisi

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bilindiği gibi, birden fazla etkenin yanıt değişkeni üzerindeki etkisinin, etken düzeylerinin olası tüm kombinasyonlarının denenerek araştırıldığı tamamlanmış çok etkenli tasarımlar uzun zamandır kullanılmaktadır. Ancak bazı durumlarda, deneme sayısının az olduğu ve tamamlanmış bir çok etkenli tasarımın bir alt grubunun ya da kesrinin kullanıldığı kesirli çok etkenli tasarımlar ya da kesirli tekrarlar (fractional replication) tercih edilir.

Çok etkenli ve kesirli çok etkenli tasarım teorisinde pek çok sorun; geometrik, cebirsel ya da birleşimsel (combinatorial) yapıya dönüşür. Sonuç olarak; gruplar, halkalar (rings), cisimler (fields), Öklid ve izdüşümsel (projective) geometri gibi sonlu matematiksel yapılar, çok etkenli ve kesirli çok etkenli tasarımlarla ilgili pek çok sorunun çözümünde, genelleştirilmesinde ve aydınlatılmasında başarıyla kullanılmaktadır. Çok etkenli tasarımları oluşturma yöntemlerinden literatürde bulunan bazıları aşağıdaki verilmektedir (Raktoe et al.,1981).

1. Dikey dizimler (orthogonal arrays)
2. Hadamard matrisleri
3. Sonlu geometriler (finite geometries)
4. Grup teorisi (group theory)
5. Cebirsel ayrışma (algebraic decomposition)
6. Bileşim (composition): Doğrudan çarpım ve doğrudan toplam
7. Etki karışımı (confounding)
8. Blok tasarımlar (block designs)
9. Sonlu grafikler

Kesirli çok etkenli, özellikle iki düzeyli tasarımlar;

1. Önsel bilgilerden yararlanarak, belli etkileşimlerin olmadığı varsayımının yapılabildiği durumlarda,

2. Sadece değişkenlerden bir bölümünün önemli olduğunun düşünüldüğü, ön (screening) çalışmalarda,

3. Deneme gruplarının ard arda gerçekleştirildiği deneysel programlarda,

yararlıdırlar (Box and Hunter, 1961).

Deney tasarımı teorisinde en göze çarpan sorun, uygulamada yaygın olarak kullanılan 2 ve 3-düzeyli kesirli çok etkenli tasarımlardan "iyi" olanının nasıl seçileceğidir.

Bu soruna ilk yaklaşımı Box ve Hunter (1961) getirmiş, tasarımlar için bir iyilik ölçütü olarak çözüm (resolution) kavramını önermişlerdir.

Ancak çözüm kavramı, bir tasarımı diğerinden daha iyi olarak tanımlamak için yeterli bulunmamıştır.

Fries ve Hunter (1980), en yüksek çözümlü 2^{k-p} kesirli çok etkenli tasarımlar kümesinden, tasarımların en iyi alt kümesinin seçimi için bir yöntem geliştirmiş; "en iyi" ifadesini, en az sapma (minimum aberration) kavramına göre tanımlamış ve bu tür tasarımların nasıl oluşturulduğunu gösteren algoritmalar vermişlerdir. Algoritmalarda amaç, en yüksek çözüm biliniyorsa, en yüksek çözüme sahip kelime uzunluğu sayısını en az yapmak; çözüm bilinmiyorsa, hem en yüksek çözüme, hem en az kelime uzunluğuna sahip tasarımlara ulaşmaktır.

En az sapma ölçütü ile ilgili yapılan çalışmalarda, en az sapma ölçütünün tek başına bir iyilik ölçütü olarak kullanılmasının sakıncaları da göz önüne alınarak, her zaman ihtiyacı karşılayamayacağı belirtilmiştir. İhtiyaç duyulan tasarımın seçimini kolaylaştırmak amacıyla; Wu ve Chen (1991,1992); Sun, Chen ve Wu (1993) tarafından, deneme sayısı, kelime uzunlukları yapısı ve çözümüne göre sınıflandırılmış kataloglar geliştirilmiştir.

Çalışmanın 2. Bölümünde, özellikle, Box, Hunter ve Hunter (1978)'dan yararlanarak, çok etkenli ve 2-düzeyli kesirli çok etkenli tasarımlar hakkında kısaca bilgi verilmiş; bir tasarımın eşdeş ve tanımlayıcı bağıntı yapısı ile çözüm kavramı üzerinde durulmuştur.

En az sapma tasarımları incelenirken; grup teorisi, Galois cismi (GF) (Galois field), kod teorisi vb. konularla karşılaşılması; izomorfiklik, temel etken-ek etken ayrımı; 2'li etkileşimlerin sınıflandırılması; tanımlayıcı bağıntıların belirlenmesi gibi pek çok sorun ve kavramın bulunması; çalışmayı belirli bir hedefe yöneltmeyi zorunlu kılmış; Franklin(1984)'in optimal moment ölçütünü kullanarak oluşturduğu 2^{n-m}

optimal moment tasarımları incelenirken; üreteç ve etken sayısına (m=3,n=[4-7]) göre sınıflandırılan ve üreteç matrisi (Ü.M.) (generator matrix) olarak adlandırılan matrisin, Hamming (7,4) kodu için verilen denklik-kontrol matrisi (D.K.M) (parity-check matrix) ile aynı olması; çalışmanın kapsamını, genel olarak kod teorisi yerine, Hamming kodları çerçevesinde daraltmamıza yol açmıştır.

Bir Hamming kodu oluşturulurken, bilgi bitlerinden hesaplanan n-k tane denklik biti, bilgi vektörüne eklenerek; k uzunluğundaki bilgi vektörü, n uzunluğundaki kod kelimesine dönüştürmektir. Başka bir ifadeyle, k uzunluğunda bir kelime alınıp, n uzunluğunda bir kod kelimesi olarak kodlanmaktadır (Arazi,1988). Sadece Hamming kodlarıyla sınırlandırılan çalışma, ister istemez ikili (binary) doğrusal ve döngüsel (cyclic) kodlarla da ilgilenilmesini gerektirmiştir.

Üçüncü Bölümde, genel olarak kod teorisine ve Hamming kodlarına yer verilmiş; doğrusal ve döngüsel kodlar incelenmiştir. Hamming ağırlığı (Hamming weight), Hamming uzaklığı (Hamming distance), D.K.M. ve Ü.M. gibi tanım ve kavramlarla, kesirli çok etkenli tasarımlar arasında nasıl bir ilişki kurulacağı üzerinde düşünülmüştür.

Yapılan uygulamalarla, Hamming kodları ve genel anlamda kod teorisi ile kesirli çok etkenli tasarımlar arasındaki ilişki irdelenmiştir. Bu ilişkide, Ü.M.leri denemelerin (kod kelimelerinin) oluşturulmasında; D.K.M.leri ise, tasarımın tanımlayıcı bağıntılarını gösterdikleri için etkendir.

Dördüncü Bölümde, dikey dizimlerle hata düzeltme kodları arasındaki ilişki, ayrıntıya girilmeksizin, bugüne kadar yapılan çalışmaların ışığında incelenmiştir.

"Simetrik çok etkenli tasarımlar için, kesirli çok etkenli tasarımlar, dikey dizimlerle (orthogonal arrays) yakından ilişkilidir (Dey,1985)" ifadesinden hareketle; tasarımların oluşturulması sırasında, kesirli çok etkenli tasarımlarla dikey dizimler arasında var olduğu bilinen ilişkiden ve doğrusal kodlarla dikey dizimler arasında var olduğu çeşitli araştırmacılar tarafından gösterilen ilişkiden yararlanılmıştır.

Beşinci Bölümde, en az sapma ve çözüm ölçütlerine göre sıralanmış (Box et al.,1978; Wu and Chen,1992) kesirli çok etkenli tasarımların kod olarak karşılıkları olup olmadığına bakılmıştır. Dikey dizimlerin gücü ile, kodun en kısa uzaklığı

arasında kurulan ilişki; kesirli çok etkenli tasarımların çözüm kavramı ile en kısa uzaklık arasında kurulmuş; en az sapma ölçütüne göre en iyi tasarımların nasıl bulunacağı belirlenmiştir.

6. Bölümde, kod parametreleri girdi olarak kullanıldığında tasarımları en az sapma ölçütüne göre sıralayacak; istendiği takdirde belli bir tasarımı kodla ilişkilendirerek, tasarımın karşılık geldiği kodla ilgili ayrıntılı döküm verecek şekilde yazılan 2 farklı program tanıtılmıştır.

Son olarak 7. Bölümde, program çıktılarından yararlanarak en az sapma ölçütüne göre sıralanmış tasarımlar, karşılık geldikleri kod parametreleriyle birlikte bir çizelgede toplanmış; kesirli çok etkenli tasarımlarla kodlar arasındaki ilişki özetlenmiştir.

2. GENEL BİLGİLER

Birden fazla etkenin yanıt değişkeni üzerindeki etkisinin, etken düzeylerinin olası tüm kombinasyonlarının denenerek araştırıldığı tasarımlara çok etkenli tasarımlar denir. Her biri 2 düzeyli n etken içeren bir çok etkenli tasarım, 2^n çok etkenli tasarımı olarak adlandırılır ve tamamını bir blokta gerçekleştirmek mümkün olmadığında, etki karışımı (confounding) tasarımın birden çok blokta oluşturulmasını sağlayan bir yöntemdir.

En basit etki karışımı yapıları 2^n çok etkenli tasarımlar için olanlardır. Bir 2^n çok etkenli tasarımını, $p<n$ olmak üzere 2^p tamamlanmamış blokta tasarlamak mümkündür. Burada; n: etken sayısı ve p: bloklarla karışacak bağımsız etkileşim sayısıdır. Çok etkenli bir tasarımı bloklara ayırmadan önce, hangi etkilerin bloklarla karışacağına ve bloklarda hangi deneme kombinasyonlarının olacağına karar verilmelidir.

Bloklarla karışacak etki ya da etkileşimleri gösteren ifadeye tanımlayıcı bağıntı denir ve I ile gösterilir. Tanımlayıcı bağıntı belirlenirken; bloklarla yüksek dereceden etkileşimlerin karışması tercih edilir.

Tamamlanmış bir çok etkenli tasarımda etken sayısı arttığında, deneme kombinasyonlarının tamamının denenmesi uygulamada zorluk çıkarmaktadır. Bu nedenle; deneme sayısının az olduğu ve tamamlanmış bir çok etkenli tasarımın bir alt grubunun ya da kesrinin kullanıldığı kesirli çok etkenli tasarımlar ya da kesirli tekrarlar tercih edilir.

2^{n-p} deneme içeren bir 2^n tasarımına, 2^n tasarımının $1/2^p$ kesri ya da 2^{n-p} kesirli çok etkenli tasarımı denir. Burada; n: etken sayısı, p: üreteç ya da tanımlayıcı bağıntı sayısıdır. Bir tasarım için tanımlayıcı bağıntı yapısı, başlangıçta seçilen p tane tanımlayıcı bağıntı ve bunların 2^p - p -1 tane genelleştirilmiş etkileşiminden oluşur. Eşdeş yapısı (alias structure), her bir etkinin 2 modülünde tanımlayıcı bağıntı yapısı ile çarpılmasıyla elde edilir. Her bir etki 2^p -1 eşdeşe sahiptir. Yüksek-dereceden etkileşimlerin olmadığı varsayımı, eşdeş yapısını daha basit hale getirir (Montgomery, 1984).

2.1. Kesirli Çok Etkenli Tasarımlarda Çözüm Kavramı

İki düzeyli kesirli çok etkenli tasarımlar oluşturulurken çözüm kavramı göz önüne alınmalıdır. Bir kesirli çok etkenli tasarımın tanımlayıcı bağıntı yapısındaki en küçük etkileşim ya da en kısa kelime uzunluğu R etkenli ise, tasarımın çözümü; R'dir ve Ç-R (çözüm R) olarak gösterilir. Tasarımla birlikte çözümü de verileceği zaman, Romen rakamıyla ve alt indis olarak gösterilir. Yukarıdaki tanıma göre bir Ç-R tasarımında, hiçbir k-etkenli etkileşim, (R-k)'dan daha az etken içeren etkileşim ile karışamaz. Örneğin; 2^{3-1} tasarımının tanımlayıcı bağıntı yapısındaki, I=ABC, kelimesinin uzunluğu 3 olduğundan, çözümü 3'tür ve 2_{III}^{3-1} olarak gösterilir. Bu durumda hiçbir ana etki, (3-1=2)'den daha az etken içeren etkileşimlerle; yani diğer bir ana etkiyle karışmayacak, 2-etkenli etkileşimlerle karışacaktır. Uygulamada en çok kullanılan kesirli çok etkenli tasarımlar; III, IV, V çözümlerine sahiptir ve tanımları aşağıda verilmiştir (Box et al ., 1978; Dey, 1985).

1. *Çözüm-III tasarımları:* Bu tasarımlarda, ana etkiler diğer ana etkilerle karışmaz; ancak, ana etkiler 2-etkenli etkileşimlerle ve 2-etkenli etkileşimler 3-etkenli etkileşimlerle karışır. N, 4'ün çarpanı olmak üzere, N denemede gerçekleştirilen ve k = N-1'e kadar etken içeren tasarımlar için, Ç-III tasarımları oluşturmak mümkündür.

2. *Çözüm-IV tasarımları:* Ana etkilerin 3-etkenli etkileşimlerle ve 2-etkenli etkileşimlerin birbiriyle karıştığı tasarımların çözümü IV'tür.

Bir 2_{IV}^{k-p} tasarımı oluşturulurken;

1. İlk k-p etken için tamamlanmış 2^{k-p} çok etkenli tasarımı yazılır.

2. Daha sonra, ilk k-p etken arasındaki, tek sayıda harf içeren etkileşim sütunları oluşturulur ve ek etkenlere atanır.

3. *Çözüm-V tasarımları:* Bu tasarımlarda, ana etki ve 2-etkenli etkileşimler diğer ana etki ve 2-etkenli etkileşimlerle karışmaz; ancak, ana etkiler 4-etkenli etkileşimlerle ve 2-etkenli etkileşimler 3-etkenli etkileşimlerle karışır.

Bir kesirli çok etkenli tasarımın çözümü arttıkça, etkilerin birbirlerinden daha iyi ayırt edilebildiği tasarımlar oluşacaktır.

2.2. Kesirli Çok Etkenli Tasarımlarda En Az Sapma Kavramı

Bir tasarımın çözümü, tanımlayıcı bağıntı yapısındaki en kısa kelime uzunluğu olarak ifade edilirken; bir en az sapma tasarımı, tanımlayıcı bağıntı yapısındaki en kısa uzunluktaki ya da $Ç_{max}$ uzunluktaki kelime sayısını en az yapan tasarım olarak tanımlanır. Böylece, en az sayıda ana etki $Ç_{max}$ -1 etkenli etkileşimlerle; en az sayıda 2-etkenli etkileşim $Ç_{max}$ -2 etkenli etkileşimlerle karışır.

Daha önce de belirtildiği gibi, olası en yüksek çözüme sahip bir tasarım seçilebilecek en iyi tasarımdır; ancak, aynı çözüme sahip olmasına rağmen farklı eşdeş yapısına sahip tasarımların seçimi, en az sapma ölçütüne göre yapılır. Örneğin; 2^{7-2} tasarımının sahip olabileceği en yüksek çözüm, IV 'tür. Bu tasarım için, çözümü aynı; ancak farklı tanımlayıcı bağıntı yapısına sahip 3 tasarım Çizelge 2.1'de gösterilmektedir: Tasarımlar için yalnızca birbiri ile karışmış 2-etkenli etkileşimler verilmiş, 3-etkenli ve yüksek-dereceden etkileşimlerin olmadığı varsayımı yapıldığında tahmin edilebilen 2-etkenli etkileşimler verilmemiştir (Fries and Hunter, 1980).

Çizelge 2.1. 2_{IV}^{7-2} Kesirli çok etkenli tasarımı için 3 farklı tasarım

Tasarım	**(a)**	**(b)**	**(c)**
Üreteç	F=ABC G=BCD	F=ABC G=ADE	F=ABCD G=ABCE
Tanımlayıcı Bağıntı Yapısı	I=ABCF=BCDG =ADFG	I=ABCF=ADEG =BCDEFG	I=ABCDF=ABCEG =DEFG
Eşdeş Yapısı	AB=CF AC=BF AD=FG AG=DF BD=CG BG=CD AF=BC=DG	AB=CF AC=BF AD=EG AE=DG AF=BC AG=DE	DE=FG DF=EG DG=EF

Çizelge 2.1'den görüldüğü gibi; 2_{IV}^{7-2} tasarımlarından, (a) tasarımı en fazla eşdeşe, (c) tasarımı en az eşdeşe sahiptir. (a) tasarımında tanımlayıcı bağıntı yapısında yer alan kelime uzunluğu yapısı {4,4,4}; (b) tasarımında {4,4,6} ve (c) tasarımında {4,5,5}'tir. Bu durumda, tanımlayıcı bağıntı yapısındaki en kısa kelime uzunluğunu en az yapan, (c), en az sapma tasarımıdır (Fries and Hunter, 1980).

2 tasarım için karşılaştırma yapılırken çözüm kavramı ölçüt olarak kullanılırsa; her

bir tasarımın tanımlayıcı bağıntı yapısındaki en kısa kelime uzunluğuna bakılır. Kelime uzunlukları aynı olduğu takdirde, iki tasarım eşit olarak değerlendirilir.

İki tasarım için karşılaştırma yapılırken en az sapma ölçütü kullanıldığında, önce, tanımlayıcı bağıntı yapılarındaki en kısa kelime uzunluğuna bakılır; sonra, her bir tanımlayıcı bağıntı yapısındaki bir sonraki en kısa kelime uzunluğu, bir tasarım diğerine üstünlük sağlayana kadar araştırılır. Fries ve Hunter (1980), iki tasarım karşılaştırıldığında, en az sapmaya sahip tasarımın bulunabilmesı için; aşağıdaki algoritmayı önermişlerdir.

$Ç_{max}$ çözümüne sahip (s) ve (t) gibi iki 2^{k-p} tasarımının karşılaştırılacağı varsayılsın. Bu iki tasarımın tanımlayıcı bağıntısında yer alan kelime uzunlukları aşağıdaki gibi gösterilir:

$$(\,s\,):\ \left\{\mathbf{Ç}^{\mathbf{s}_0}{}_{\max}\left(\mathbf{Ç}_{\max}+1\right)^{\mathbf{s}_1}\left(\mathbf{Ç}_{\max}+2\right)^{\mathbf{s}_2}\ldots\left(\mathbf{Ç}_{\max}+\mathbf{m}\right)^{\mathbf{s}_m}\right\}$$

$$(\,t\,):\ \left\{\mathbf{Ç}^{\mathbf{t}_0}{}_{\max}\left(\mathbf{Ç}_{\max}+1\right)^{\mathbf{t}_1}\left(\mathbf{Ç}_{\max}+2\right)^{\mathbf{t}_2}\ldots\left(\mathbf{Ç}_{\max}+\mathbf{n}\right)^{\mathbf{t}_n}\right\}$$

$s_i \neq t_i$ eşitsizliğini sağlayan ilk i alt indisine karar verilir. Eğer $s_i < t_i$ ise; (s) tasarımı daha az sapmaya sahip bir tasarımdır. Bir tasarımdan daha az sapmaya sahip bir tasarım bulunamazsa; o tasarıma, **en az sapma tasarımı** denir. Çizelge 2.1'de verilen tasarımlardan, (b) ve (c)'den hangisinin daha az sapmaya sahip olduğu, yukarıdaki algoritmadan yararlanarak bulunacaktır.

(b) ve (c) tasarımları için, $Ç_{max} = 4$'tür.

$$(\,b\,):\ \left\{\mathbf{Ç}^{\mathbf{b}_0=2}{}_{\max}\left(\mathbf{Ç}_{\max}+1\right)^{\mathbf{b}_1=0}\left(\mathbf{Ç}_{\max}+2\right)^{\mathbf{b}_2=1}\right\}$$

$$(\,c\,):\ \left\{\mathbf{Ç}^{\mathbf{c}_0=1}{}_{\max}\left(\mathbf{Ç}_{\max}+1\right)^{\mathbf{c}_1=2}\left(\mathbf{Ç}_{\max}+2\right)^{\mathbf{c}_2=0}\right\}$$

dir. $\left\{\mathbf{Ç}^{\mathbf{b}_0=2}{}_{\max}\right\}$, (b) tasarımında $Ç_{max}$ (4) uzunluğundaki kelime sayısının 2 olduğunu gösterir. $\left\{\left(\mathbf{Ç}_{\max}+1\right)^{\mathbf{b}_1=0}\right\}$, $Ç_{max}$+1 (5) uzunluğunda kelime olmadığını; $\left\{\left(\mathbf{Ç}_{\max}+2\right)^{\mathbf{b}_2=1}\right\}$, $Ç_{max}$+2 (6) uzunluğunda 1 kelime olduğunu gösterir. (c) tasarımında, $Ç_{max}$ (4) uzunluğunda 1; $Ç_{max}$+1 (5) uzunluğunda 2 kelime varken, $Ç_{max}$+2 uzunluğunda kelime olmadığı görülmektedir.

$b_i \neq c_i$ 'yi sağlayan ilk i değeri 0'dır. $b_0 = 2$ ve $c_0 = 1$ olduğundan, $b_0 \neq c_0$ ve $c_0 < b_0$; (c) tasarımının, (b)'den daha az sapmaya sahip olduğunu gösterir. Bir başka deyişle; (c) tasarımı, (b)'den daha iyi bir tasarımdır (Bkz. Çizelge 2.1).

Aynı algoritma daha basit bir şekilde ifade edilebilir: $D(2^{n-p})$, 2^{n-p} kesirli çok etkenli tasarımı olsun. $A_i(D)$, D'nin tanımlayıcı bağıntı yapısındaki i uzunluklu kelime sayısı olmak üzere, $W(D)=(A_1(D),A_2(D),... A_n(D))$, D tasarımının *kelime uzunluğu yapısı* olarak adlandırılır. D_1 ve D_2 iki 2^{n-p} kesirli çok etkenli tasarımı olsun. s, $A_s(D_1) \neq A_s(D_2)$'yi sağlayan en küçük tam sayı olmak üzere,

$$A_s(D_1) < A_s(D_2) \qquad (2.1)$$

İse, D_1, D_2'den daha az sapmaya sahiptir (Chen,1998).

2.3. Sayılar Kuramı

Bilindiği gibi, etkenlerin p düzeyli olduğu bir kesirli çok etkenli tasarım, p büyüklüğünde GF kullanılarak oluşturulabilir ve p asal bir sayı olduğunda, sonlu cisim aritmetiği, p modülünde tam sayı aritmetiğine eşittir.

Bu nedenle modüler aritmetik ile ilgili bazı tanımlar üzerinde durulacaktır:

2.3.1. Denklikler(Kongruanslar)

Tanım 2.1. $n > 0$ ve $a, b \in Z$ olsun. Eğer $n \mid a-b$ (n, a-b yi böler) ise, a sayısı n modülüne göre b'ye denktir denir ve $a \equiv b \pmod n$ şeklinde gösterilir (Kaya, 1988).

Önerme 2.1. n modülüne göre denklik bağıntısı, Z üzerinde bir denklik bağıntısıdır ve bunun tam n tane denklik sınıfı vardır.

Tanım 2.2. $x \equiv a \pmod n$ gibi bir denklik bağıntısı için n tane denklik sınıfı vardır ve her biri $\bar{0}, \bar{1}, ..., \overline{n-1}$ sınıflarından birine eşittir. Bu denklik sınıflarının açık olarak yazılımı;

$\bar{0} = \{0, \pm n, \pm 2n, ...\}$,

$\bar{1} = \{1, 1 \pm n, 1 \pm 2n, ...\}$

.
.
.

$\overline{n-1} = \{n-1, (n-1) \pm n, (n-1) \pm 2n, ...\}$

şeklindedir ve n modülüne göre kalan sınıfları olarak adlandırılır.

$$Z_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$$

kümesine, n modülüne göre kalan sınıflarının kümesi;

{0, 1, 2, …, n-1 }

kümesine, n modülüne göre en küçük pozitif kalanlarının kümesi ve eğer,

$$\{\overline{a}_0, \overline{a}_1, ..., \overline{a}_{n-1}\}$$

kümesi, kalan sınıflarının tam kümesi ise;

$$\{a_0, a_1, ..., a_{n-1}\}$$

kümesine de n modülüne göre kalanların tam kümesi ya da temsilciler sistemi denir (Dey, 1985; Çallıalp, 1999).

2.3.2. Euler Φ-fonksiyonu

p asal bir sayı olmak üzere, Z_p'nin p-1 tane sıfırdan farklı her öğesi tersinirdir (p asal olduğunda, Z_p'nin sıfırdan farklı her öğesinin Z_p içinde bir tersi vardır). Tanım 2.3, rastgele bir n>1 tam sayısı için Z_n'nin tersinir öğelerinin sayısını bulmaya yöneliktir (Kaya, 1988).

Tanım 2.3. n>1 için, Z_n içindeki tersinir öğelerin sayısı Φ(n) ile gösterilir ve n→ Φ(n) bağıntısına ya da kısaca Φ(n)'ye Euler fonksiyonu denir.

Z_n'deki tersinir öğelerin kümesini Z_n^* ile gösterirsek, Φ fonksiyonu;

$$\Phi : Z^+ - \{1\} \rightarrow Z^+$$

$$n \rightarrow \#(Z_n^*)$$

şeklinde tanımlanan bir dönüşüm olur (#(Z_n^*) gösterimi, Z_n^*'ın öğe sayısını gösterir). $\overline{a} \in Z_n$ alınsın.

$\overline{a}$ tersinir $\Leftrightarrow$ $\overline{a}$ x $\equiv$ $\overline{1}$'in Z_n içinde bir çözümü vardır.

$\Leftrightarrow$ a x $\equiv$ 1 (mod n)'nin Z'de bir çözümü vardır.

$\Leftrightarrow$ (n,a) |1'dir.

$\Leftrightarrow$ (n,a) = 1, yani; n ile a aralarında asaldır.

Buna göre, $\overline{a}$ kalan sınıfının tersinir olması için, bu sınıfın temsilci öğesi olan a ile n'nin aralarında asal olması gerekli ve yeterlidir (Kaya, 1988; Çallıalp, 1999).

Φ(n) ile gösterilen sayı; Z_n'nin öğelerinden, n'den küçük ya da eşit olup, n ile aralarında asal olan tam sayıların sayısıdır. Örneğin, Φ(8)=4'tür; çünkü, $\overline{1},\overline{3},\overline{5},\overline{7}$, 8 ile aralarında asaldır.

Özellik 2.1. (Euler) n, a $\in$ Z ve n>0 olsun.

(n,a)=1 ise, $a^{\Phi(n)} \equiv 1(\text{mod } n)$'dir (Kaya,1988).

Sonuç 2.1. (Fermat) p, a $\in$ Z olsun. p asal ve p$\times$ a (p, a'yı bölmez) ise,

$a^{p-1} \equiv 1 \text{ (mod p)}$'dir.

Sonuç 2.2. (Fermat) p asal ise, her a $\in$ Z için,

$a^{p} \equiv a \text{ (mod p)}$'dir (Gallian, 1986).

2.4. Sonlu Cisimler

Bir F cismi, "+" ve "." olmak üzere, iki ikilik işlem için kapalı olan ve bütün a,b,c $\in$ F için aşağıdaki aksiyomları sağlayan elemanlar kümesidir.

i) a + (b+c) = (a+b) +c

ii) a + b = b+ a

iii) a + 0 = a yapacak, 0 $\in$ F elemanı vardır.

iv) a + (-a) = 0 yapacak, bir –a $\in$ F elemanı vardır.

v) a.(b.c) = (a.b).c

vi) a.b = b.a

vii) a.1=a yapacak şekilde bir $1 \in$ F elemanı vardır.

viii) Her bir $a \neq 0$ için, $a.a^{-1} = 1$ yapacak , bir $a^{-1} \in$ F elemanı vardır.

ix) a.(b+c) = a.b + a.c

Gerçel sayılar, rasyonel sayılar ve kompleks sayılar cisimlere örnek olarak verilebilir ve her biri sonsuz sayıda elemana sahiptir. Sadece, sonlu sayıda eleman içeren bir cisim, sonlu cisim (finite field) olarak adlandırılır. Örneğin, n tamsayı modülü Z_n ile gösterildiğinde, mod n'de yapılan standart toplama ve çarpma işlemlerine göre, Z_n sonlu bir cisimdir (Wiggert, 1978; Vanstone and Oorschot,1989).

Teorem 2.1. Z_n yalnız ve yalnız n asal sayı ise sonlu bir cisimdir.

Tanım 2.4. F bir cisim olsun. F cisminin karakteristiği;

$$\sum_{i=1}^{m} 1 = 1 + 1 + ... + 1 = 0$$

eşitliğini sağlayan en küçük pozitif m tamsayısıdır. Eğer m yoksa, karakteristik 0 olarak tanımlanır.

Örneğin, Z_2 için karakteristik 2; Z_5 için 5'tir. Sonuç olarak Z_p, p karakteristiğine sahiptir (Vanstone and Oorschot,1989).

Teorem 2.2. F, p karakteristiğine sahip sonlu bir cisimse, bu durumda F, n pozitif tamsayısı için, p^n elemanlıdır.

F, q elemanlı sonlu bir cisimse, genellikle GF(q) ile gösterilir ve q elemanlı GF olarak adlandırılır. Buradaki q, p^n biçimindedir ve bir asal sayı ya da asal sayının kuvvetidir. GF(p^n), p karakteristikli bir cisimdir ve Z_p cismi, GF(p) olarak gösterilir (Dey,1985; Vanstone and Oorschot,1989).

2.4.1. Galois cismi

p bir asalsa, $F_p = <F_p , +_p , .p >$ sistemi, $F_p = \{0, 1, 2, ..., p-1\}$ olmak üzere, bir GF'dir ve GF(p) ile gösterilir. Gerçekte, F_p , en basit GF'dir (Dey,1985).

Teorem 2.3. p asal olduğunda, 0,1,...,p-1 tam sayıları; p modülünde toplama ve çarpma işlemleri altında GF(p)'yi oluşturur (http://www.ee.ucla.edu/~matache/rsc/node2.html).

x, GF(p)'nin herhangi bir elemanıysa, Fermat Teoremi'nden (Bkz. Sonuç 2.1, Sonuç 2.2);

$$x^{p-1} = 1$$

dir ve 1, ($\overline{1}$) kalan sınıfı olup, GF(p)'nin birim elemanıdır.

Tanım 2.5. β, GF(p)'nin bir elemanı olsun. β'nın derecesi, β^m=1'i sağlayan en küçük pozitif tam sayıdır (http://www.ee.ucla.edu/~matache/rsc/ node2.html).

r, x^r =1 yapan en küçük pozitif tamsayı olsun. Bu durumda r, x'in derecesidir ve r en büyük değeri, p-1'i aldığında; x'e GF(p)'nin **ilkel elemanı** (primitive element) denir.

Tanım 2.6. GF(p)'de (p-1) dereceli bir eleman, GF(p)'nin ilkel elemanı olarak adlandırılır.

Her GF(p)'de ilkel bir eleman vardır. x ilkel elemansa, GF(p)'nin sıfır olmayan bütün elemanları, aşağıdaki diziye dahildir.

$$x^0 = 1, x, x^2, ..., x^{p-2} \qquad (2.2)$$

Tanım 2.7. GF(p)[x], $\{a_i\}$ katsayıları GF(p) cisminde olan, rastgele dereceli $a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1}$ polinomlarının birleşimidir (http://www.ee.ucla. edu/~matache /rsc /node3.html).

Tanım 2.8. GF(p)[x]'de düşük dereceden polinomların çarpımı şeklinde yazılamayan f(x) fonksiyonuna, GF(p)'de indirgenemez denir.

f(x), GF(p)'de indirgenemezse, GF(p^n)'nin elemanlarını oluşturmak için en küçük

fonksiyondur. En küçük fonksiyon f(x) uygun olarak seçilirse; x ile gösterilen sınıf, GF(p^n)'nin **ilkel elemanı** olacaktır ve bu durumda, GF(p^n)'nin sıfır olmayan bütün elemanları aşağıdaki gibi ifade edilebilir.

$$x^0 = 1, x, x^2, ..., x^{p^n-2} \quad (2.3)$$

Eş. 2.3'teki ifade, x'in güç döngüsü olarak adlandırılır. Bazı güç döngüleri Çizelge 2.2'de verilmektedir (Dey,1985).

Çizelge 2.2. Bazı GF(2^n) cisimleri için en küçük fonksiyonlar ve güç döngüleri

p^n	En Küçük Fonksiyon	Güç Döngüsü
2^2	x^2+x+1	1,x,x+1
2^3	x^3+x^2+1	1,x,x^2, x^2+1, x^2+x+1,x+1,x^2+x
2^4	x^4+x^3+1	1,x, x^2, x^3, x^3+1, x^3+x+1, x^3+x^2+x+1, x^2+x+1, x^3+x^2+x, x^2+1, x^3+x, x^3+x^2+1,x+1, x^2+x, x^3+x^2

Örnek 2.1. GF(2^2) için güç döngüsü oluşturulsun. GF(2^2)'nin cisim elemanları bulunurken, derecesi n=1 olan bir polinomdan yararlanılır.

$p(x)= a_0 + a_1x$ ya da $p(x) =a_1x + a_0$, $a_i \in Z$, i=0,1, $a_1 \neq 0$ olmak üzere;

$p(x)= a_1x + a_0$

0 0 $\rightarrow$ **0**

0 1 $\rightarrow$ **1**

1 0 $\rightarrow$ **x**

1 1 $\rightarrow$ **x+1**

dir. **GF(2^2) için** Çizelge 2.2'de verilen en küçük polinom, $1+x+x^2$'dir ve aynı zamanda Çizelge 2.3'te indirgenemez polinom olarak gösterilmiştir. Eş. 2.3'teki güç döngüsü kullanıldığında;

$$x^0 = 1, x, x^2, ..., x^{p^n-2} \rightarrow 1, x, \mathbf{x}^{2^2-2} = x^2 \rightarrow 1, x, x^2$$

elde edilir.

Ancak $x^2 \equiv x+1 \pmod{x^2+x+1}$ olduğundan, güç döngüsü;

1, x, x+1

olacaktır (Bkz. Çizelge 2.2). Görüldüğü gibi, cismin 0 dışındaki elemanları, güç döngüsünü oluşturmaktadır.

Örnek 2.2. GF(2^3) için güç döngüsü oluşturulsun. GF(2^3)'ün elemanları bulunurken, derecesi n=2 olan bir polinomdan yararlanılır.

$p(x)= a_2x^2 + a_1x + a_0$, $a_i \in Z$, i=0,1, $a_1 \neq 0$ olmak üzere;

$p(x)= a_2x^2 + a_1x + a_0$

0	0	0	$\rightarrow$ **0**
0	0	1	$\rightarrow$ **1**
0	1	0	$\rightarrow$ **x**
0	1	1	$\rightarrow$ **x+1**
1	0	0	$\rightarrow$ **x^2**
1	0	1	$\rightarrow$ **x^2 +1**
1	1	0	$\rightarrow$ **x^2+x**
1	1	1	$\rightarrow$ **x^2+x+1**

elde edilir ki, GF(2^3) için, Çizelge 2.2'de verilen en küçük fonksiyon $x^3 + x^2 + 1$ kullanılarak, Eş. 2.3'ten bulunan güç döngüsü;

$x^0 = 1, x, x^2, ..., x^{p^n-2} \rightarrow 1, x, x^2, x^3, x^4, x^5, x^6$ 'dır.

1, x, x^2, $x^3 \equiv$ **x^2 +1**, $x^4 \equiv (x^2+1).x \equiv x^3+x \equiv$ **x^2+x+1,**

$x^5 \equiv x^4 .x \equiv (x^2+x+1).x \equiv x^3+x^2+x \equiv (x^2+1) + x^2+x \equiv$ **x+1,**

$x^6 \equiv x^5. x \equiv (1+x).x \equiv$ **x^2+x,**

dir (Bkz. Çizelge 2.2).

Örnek 2.3. GF(2^4) için güç döngüsü oluşturulsun. GF(2^4)'ün elemanları bulunurken, derecesi n=3 olan bir polinomdan yararlanılır.

$p(x)= a_3x^3 + a_2x^2 + a_1x + a_0$, $a_i \in Z$, i=0,1, $a_3 \neq 0$ olmak üzere,

$p(x)= a_3x^3 + a_2x^2 + a_1x + a_0$

0	0	0	0	$\rightarrow$ **0**
0	0	0	1	$\rightarrow$ **1**
0	0	1	0	$\rightarrow$ **x**
0	0	1	1	$\rightarrow$ **x+1**
0	1	0	0	$\rightarrow$ **x^2**
0	1	0	1	$\rightarrow$ **x^2+1**
0	1	1	0	$\rightarrow$ **x^2+x**
0	1	1	1	$\rightarrow$ **x^2+x+1**
1	0	0	0	$\rightarrow$ **x^3**
1	0	0	1	$\rightarrow$ **x^3+1**
1	0	1	0	$\rightarrow$ **x^3+x**
1	0	1	1	$\rightarrow$ **x^3+x+1**
1	1	0	0	$\rightarrow$ **x^3+x^2**
1	1	0	1	$\rightarrow$ **x^3+x^2+1**
1	1	1	0	$\rightarrow$ **x^3+x^2+x**
1	1	1	1	$\rightarrow$ **x^3+x^2+x+1**

elde edilir. Eş. 2.3'ten bulunan güç döngüsü;

$x^0 = 1, x, x^2, ..., x^{p^n-2} \rightarrow 1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}, x^{12}, x^{13}, x^{14}$'tür.

1, x, x^2, x^3 , $x^4 \equiv$ **(x^3 +1),** $x^5 \equiv x^4 .x \equiv (x^3+1).x \equiv x^4+x \equiv$ **x^3+x+1**,

$x^6 \equiv x^5. x \equiv (x^3+x+1).x \equiv x^4+x^2+x \equiv x^3 +1+ x^2 +x \equiv$ **x^3 +x^2 +x+ 1,**

$x^7 \equiv x^6. x \equiv (x^3 +x^2 +x+ 1).x \equiv x^4+x^3+x^2+x \equiv (x^3+1)+ x^3+x^2+x \equiv$ **x^2 +x+ 1,**

$x^8 \equiv x^7. x \equiv (x^2 +x+ 1).x \equiv$ **x^3+x^2+x,**

$x^9 \equiv x^8 .x \equiv (x^3+x^2+x).x \equiv (x^3+1)+ x^3+x^2 \equiv \mathbf{x^2+1,}$

$x^{10} \equiv x^9.x \equiv (x^2+1).x \equiv \mathbf{x^3+x,}$

$x^{11} \equiv x^{10}.x \equiv (x^3+1).x \equiv \mathbf{x^3 +x^2 + 1,}$

$x^{12} \equiv x^{11}.x \equiv (x^3+x^2+1).x \equiv (x^3+1)+ x^3+x \equiv \mathbf{x+1,}$

$x^{13} \equiv x^{12}.x \equiv (x+1).x \equiv \mathbf{x^2 + x,}$

$x^{14} \equiv x^{13}.x \equiv (x^2 + x).x \equiv \mathbf{x^3+x^2,}$

1, x, x^2, x^3, x^3+1, x^3+x+1, x^3 +x^2 +x+ 1, x^2 +x+ 1, x^3+x^2+x, x^2+1, x^3+x, x^3 +x^2 + 1, x+1, x^2 + x, x^3 +x^2

dir ve Çizelge 2.2'den de görülebilir.

2.4.2. İndirgenemez polinomlar

Bilindiği üzere, p^n elemanlı bir cisim oluşturmak için, GF(p)[x]'de n. dereceden bir indirgenemez polinoma ihtiyaç vardır. Asıl sorun, GF(p)[x]'de her pozitif n sayısı için, n. dereceden bir polinomun olup olmadığıdır. Gerçekte bakılması gereken, monik bir indirgenemez polinomdur. Monik polinom, x'in en yüksek kuvvetinin sıfır olmayan katsayısı 1 demektir (http://www.mathworld.wolfram.com/Irreducible Polynomial).

GF(p)[x]'de derecesi 1 olan p tane, derecesi 2 olan p^2 tane monik polinom vardır. Bunlardan biri indirgenebilirse, 1. dereceden iki monik polinomun çarpımıdır. Bunları kullanarak $\binom{p}{2}+p$ tane indirgenebilir karesel monik polinom oluşturulabilir (iki farklı monik polinom ya da herhangi iki monik polinomun karesi seçilebilir). Bu nedenle, indirgenemez karesel monik polinomların sayısı;

$$I_2 = p^2 - \binom{p}{2} - p = \binom{p}{2} > 0, \quad p \geq 2$$

dir (Vanstone and Oorschot,1989; http://www.mathworld.wolfram.com/Irreducible Polynomial).

Tanım 2.9. (2 ya da 3. dereceler için İndirgenebilirlik Testi) F bir cisim olsun. $f(x) \in F[x]$ ve $degf(x)=2$ ya da 3 ise; f(x), yalnız ve yalnız F'de sıfır değerini alıyorsa, F'de indirgenebilirdir (Gallian, 1986).

Teorem 2.4. $f(x) \in F[x]$ olsun. f(x), Q (rasyonel sayılar)'da indirgenebilir ise, aynı zamanda Z üzerinde de indirgenebilirdir (Stewart,1973).

Teorem 2.5. (Mod p İndirgenemezlik Testi) p asal, f(x)'in derecesi ≥ 1 ve $f(x) \in Z[x]$ olsun. $\bar{f}(x)$, Z(p)[x]'de, f(x)'in bütün katsayılarının mod p'de indirgenmesiyle f(x)'den elde edilen bir polinom olsun. $\bar{f}(x)$, Z(p)'de indirgenemezse ve $\bar{f}(x)$ ile f(x)'in dereceleri eşitse, f(x) Q'da indirgenemezdir (Gallian, 1986).

Teorem 2.6. (Eisenstein Ölçütü) $f(x) = a_0 + a_1x + ...+ a_{n-1}x^{n-1}+ a_nx^n \in Z[x]$ olsun.

1) $p \nmid a_n$,

2) $p \mid a_{n-1}$, ..., $p \mid a_0$,

3) $p^2 \nmid a_0$,

koşullarını sağlayan asal bir p varsa, bu durumda, f(x), Q'da ve dolayısıyla Z'de indirgenemezdir (Stewart,1973).

Sonuç 2.3. Herhangi bir $p \geq 2$ asal için,

$$\phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+...+x+1 \,, \in Z[x]$$

Q üzerinde ve dolayısıyla Z'de indirgenemezdir.

Örnek 2.4. Aşağıdaki polinomlar indirgenemezdir (Gallian,1986).

$$\Phi_2(x)=1+x$$

$$\Phi_3(x)=1+x+x^2$$

$$\Phi_5(x)=1+x+x^2+x^3+x^4$$

$$\Phi_7(x)=1+x+x^2+x^3+x^4+x^5+x^6$$

Çizelge 2.3'te, mod 2 için, dereceleri n=1'den 5'e kadar olan indirgenemez polinomlar listelenmektedir (http://www.mathworld.wolfram.com/Irreducible Polynomial).

Çizelge 2.3. Mod 2'de n. dereceden indirgenemez polinomlar

n	İndirgenemez Polinomlar
1	$1+x$, x
2	$1+x+x^2$
3	$1+x+x^3$, $1+x^2+x^3$
4	$1+x+x^4$, $1+x+x^2+x^3+x^4$, $1+x^3+x^4$
5	$1+x^2+x^5$, $1+x+x^2+x^3+x^5$, $1+x^3+x^5$, $1+x+x^3+x^4+x^5$, $1+x^2+x^3+x^4+x^5$, $1+x+x^2+x^4+x^5$

Örneğin, $1+x+x^3$, Z_2'de indirgenemezdir; çünkü, Z_2'de $0^3 + 0 + 1 \neq 0$ ve $1^3 + 1 + 1 \neq 0$'dır.

2.4.3. En küçük polinom

Tanım 2.10. F, p karakteristikli bir cisim olsun ve F^* 0 olmayan cisim elemanlarını göstersin. $\alpha \in F^*$ 0 olmayan eleman olsun. GF(q)'ya göre α'nın en küçük polinomu; GF(q)[x]'de en küçük dereceli monik bir polinom, m(x)'dir ve $m(\alpha) = 0$'dır.

Tanım 2.11. Bir α elemanının en küçük polinomu tektir.

Teorem 2.7. $\alpha \in F^*$ için, α'nın en küçük polinomu $m_\alpha(x)$, indirgenemez bir polinomdur.

Tanım 2.12. $\alpha \in F$ için, t, $\alpha^{p^t} = \alpha$ yapan en küçük pozitif tamsayı olsun. GF(q)'ya göre α'nın çekimler (conjugates) kümesi;

$$C(\alpha) = \left\{ \alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^{t-1}} \right\} \tag{2.4}$$

ve p karakteristikli F cisminde, bütün i'ler için, $C(\alpha) = C(\alpha^{p^i})$'dir.

Teorem 2.8. F, p karakteristikli bir cisim ve $\alpha \in F^*$ olsun. $C(\alpha)$, GF(q)'ya göre α'nın çekimler kümesi olduğunda,

$$m(x) = \prod_{\beta \in C(\alpha)} (x - \beta) \tag{2.5}$$

katsayıları GF(q)'da olan bir polinomdur (Vanstone and Oorschot,1989).

Örnek 2.5. F=GF(2^3) cismi oluşturulsun. Öncelikle, Z_2'de indirgenemez kübik bir

polinoma ihtiyaç vardır ve Çizelge 2.3'ten, **$f(x)= x^3 + x +1$** alınmıştır.

F'nin elemanları: {[0], [1], [x], [1+x], [$x+x^2$], [x^2], [$1+x^2$], [$1+x+x^2$] }'dir. Elemanların çarpımları f(x) polinom modundadır. $x^3 + x +1 \equiv 0$ (mod f(x)) olduğundan, $x^3 \equiv -x-1 = x+1$(mod f(x))'dir (Z_2'de 1≡-1'dir).

Cismin elemanları için $a_2x^2 + a_1x + a_0$ gösterimi kullanılırsa;

0=(000)	x^2 = (100)
1=(001)	x^2+1= (101)
x=(010)	x^2+x= (110)
x+1=(011)	x^2+x+1= (111)

olarak yazılabilir. α=x, F'nin ilkel elemanı ya da üretecidir. Gerçekte, bu cisim için 1 dışındaki 0 olmayan her eleman (x, x+1, x^2, x^2+1, x^2+x, x^2+x+1), cismin üretecidir.

Tanım 2.12'den, $\alpha^{p^t} = \alpha$ yapan en küçük pozitif tamsayı bulunur ve $C(\alpha)=\left\{\alpha,\alpha^{p},\alpha^{p^2},...,\alpha^{p^{t-1}}\right\}$ çekimler kümesi oluşturulur. α=x olarak belirlenmişti. Z_2'nin karakteristiği 2 olduğundan p=2'dir.

α=x olduğuna göre, çekimler kümesi, $C(x)=\left\{x,x^2,x^{2^2},...,x^{2^{t-1}}\right\}$ olarak yazılabilir. Bu durumda;

x = x

$x^2 = x^2$

$x^4 = x^3 .x =(x+1).x = x^2+x$'dir ($x^3 \equiv -x-1 = x+1$ olduğundan).

$x^8 = x^3.x^3.x^2 = (x+1)(x+1).x^2 = (x^2+2x+1). x^2 = x^4 + x^2 = x^2 +x+x^2 =2x^2+x=x$'dir.

$\alpha^{p^t} = \alpha = x^{2^t} = x$ yapan en küçük pozitif t sayısı 3'e eşittir. Bu durumda çekimler kümesi;

$C(x)=\left\{x,x^2,x^{2^{3-1}}\right\}=\left\{x,\ x^2,x^4\right\}=\left\{\alpha,\ \alpha^2,\alpha^4\right\}= C(\alpha)$'dır.

β=(101) alınsın ve $m_\beta(x)$ hesaplansın. En küçük polinom için, karışıklık olmaması amacıyla, x yerine y kullanılmıştır. Teorem 2.8'den;

$$m_\beta(y)=\prod_{\delta\in C(\beta)}(y-\delta)=(y-\beta)(y-\beta^2)(y-\beta^4)$$

dir. $\beta^8=\beta$ olduğundan;

$$(y-\beta)(y-\beta^2)(y-\beta^4)=y^3+(\beta+\beta^2+\beta^4)y^2+(\beta\beta^2+\beta\beta^4+\beta^2\beta^4)y+\beta\beta^2\beta^4$$

şeklinde hesaplanır. Çarpmayı kolaylaştırmak için, 0 olmayan her bir elemanın gösterimi için, α'nın kuvvetleri kullanılır. α=x için,

$\boldsymbol{\alpha^0}$ = x^0 = 1 = **(001)**

$\boldsymbol{\alpha^1}$ = x^1 = x = **(010)**

$\boldsymbol{\alpha^2}$ = x^2 = x^2 = **(100)**

$\boldsymbol{\alpha^3}$ = x^3 = x+1= **(011)** ($x^3 + x + 1 \equiv 0$ ve $x^3 \equiv -x-1 = x+1$ olduğundan)

$\boldsymbol{\alpha^4}$ = x^4 = x^3 .x = (x+1) .x = x^2+x = **(110)**

$\boldsymbol{\alpha^5}$ = x^3 . x^2 = (x+1) . x^2 = x^3 + x^2 = x+1+x^2 = **(111)**

$\boldsymbol{\alpha^6}$ = x^6 = x^3 . x^3 = (x+1)(x+1) = x^2 +2x+1 = x^2+1= **(101)**

$\boldsymbol{\alpha^7}$ = x^7 = x^3 . x^3 . x = (x+1)(x+1)x = x^3 +2x^2 +x = 2x+1= **1=$\boldsymbol{\alpha^0}$**

dir. Örneğin, α^8 de x'e; yani, α^1'e eşittir.

$\boldsymbol{\alpha^8}$ = x^8 = x^3 . x^3 . x^2 = (x^2 +2x+1) x^2 = x^4 +2x^3 + x^2 = x^2+x+x^2= **x** = $\boldsymbol{\alpha^1}$

β= (101) = $\boldsymbol{\alpha^6}$ olduğundan, $\beta^2 = (\alpha^6)^2 = \alpha^{12} = \alpha^5$ ve $\beta^4 = (\alpha^6)^4 = \alpha^{24} = \alpha^3$'tür. Görüldüğü gibi, üstel aritmetikte mod, 8-1=7'dir ve α tarafından oluşturulan döngüsel grubun derecesidir (Bkz. Tanım 2.5).

$\beta + \beta^2 + \beta^4 = \alpha^6 + \alpha^5 + \alpha^3$

= (101)+(111)+(011)=(001)=1 ya da başka bir ifadeyle;

= (x^2+1)+(x^2+x+1)+(x+1)=1'dir.

$\beta^3 + \beta^5 + \beta^6 = \beta\beta^2 + \beta\beta^4 + \beta^2\beta^4$ 'ü α'lı ifade edersek;

$= \alpha^6 . \alpha^5 + \alpha^6 . \alpha^3 + \alpha^5 . \alpha^3$

$= \alpha^{11} + \alpha^9 + \alpha^8$

$= \alpha^4 + \alpha^2 + \alpha$ bulunuyor. Değerler yerine konulduğunda,

$= x^2 + x + x^2 + x = 0$ elde edilir.

$\beta\beta^2\beta^4 = \beta^7$

$\beta^7 = \beta\beta^2\beta^4 = \alpha^6 . \alpha^5 . \alpha^3$

$= (1+x^2). (1+x^2+x). (1+x)= 1$ bulunur.

Bulunan değerler $m_\beta(y)$ eşitliğinde yerine konulursa;

$$m_\beta(y) = y^3 + (\beta + \beta^2 + \beta^4)y^2 + (\beta\beta^2 + \beta\beta^4 + \beta^2\beta^4)y + \beta\beta^2\beta^4$$

$= y^3 + y^2 + y.0 +1$'dir ve

$m_\beta(y) = \mathbf{y^3 + y^2 + 1}$

elde edilir ve aynı zamanda **β^4 ve β^2'nin** en küçük polinomudur. **α**'nın en küçük polinomu ise, aynı zamanda **α^2 ve α^4'ün** en küçük polinomu olup;

$$m_\alpha(y) = \mathbf{y^3 + y + 1}$$

dir. Bir başka deyişle, **α,α^2** ve **α^4 , $\mathbf{m}_\alpha(\mathbf{y})$ 'nin kökleridir.**

β^4 için kontrol edilsin.

$\beta^4 = \alpha^3 = x^3 = x+1= (011)$'dır. Yani, β, bu kez (011)'e eşittir.

$m_\beta(y) = \prod_{\delta \in C(\beta)} (y - \delta) = (y - \beta)(y - \beta^2)(y - \beta^4)$ ve

$$(y - \beta)(y - \beta^2)(y - \beta^4) = y^3 + (\beta + \beta^2 + \beta^4)y^2 + (\beta\beta^2 + \beta\beta^4 + \beta^2\beta^4)y + \beta\beta^2\beta^4$$

eşitliği değişmeyecektir.

$\beta = (011)=x+1$ alınmıştı. Bu durumda;

$\beta^2 = (1+x)^2 = x^2+2x+1= x^2+1$ ve

$\beta^4 = \beta^2 . \beta^2 = (x^2+1) . (x^2+1) = x^4 + 2x^2 +1 = x^2 + x + 1$'dir.

$\beta + \beta^2 +\beta^4 = \alpha^3 + \alpha^6 + \alpha^5$

= (011)+(101)+(111)

= (1+x) + (x^2+1)+(x^2 + x + 1) = 1'dir.

$\beta^3 + \beta^5 + \beta^6 = \beta\beta^2 + \beta\beta^4 + \beta^2\beta^4$ 'ü α'lı ifade edersek;

= α^3 . α^6 + α^3 . α^5 + α^6 . α^5

= α^9 + α^8 + α^{11}

= α^2 + α + α^4

= x^2 + x + x^2 + x = 0

elde edilir.

$\beta\beta^2\beta^4 = \beta^7$ hesaplanırsa;

$\beta^7 = \beta\beta^2\beta^4 = \alpha^3$. α^6 . α^5

= (1+x) (1+x^2). (1+x^2+x). = 1 bulunur.

Dolayısıyla,

$m_\beta(y) = y^3 + (\beta + \beta^2 + \beta^4)y^2 + (\beta\beta^2 + \beta\beta^4 + \beta^2\beta^4)y + \beta\beta^2\beta^4$

= y^3 + y^2 + y.0 +1 ve

$m_\beta(y) =$ **y^3 + y^2 +1**'dir.

<u>β^2 için kontrol edilsin.</u>

$\beta^2 = \alpha^5 = x^5 = x^2 + x + 1 = (111)$'dir.

$\beta^2 = (\alpha^5)^2 = \alpha^3$ **=** x+1 ve

$\beta^4 = \beta^2 . \beta^2$ = (x+1) .(x+1) = x^2 +1'dir.

β + β^2 +β^4 = α^5 + α^3 + α^6

= (111)+(011)+(101)

= (x^2 +x +1)+(1+x) + (x^2+1) = 1'dir.

$\beta^3 + \beta^5 + \beta^6 = \beta\beta^2 + \beta\beta^4 + \beta^2\beta^4$ 'ü α'lı ifade edersek;

= α^1 + α^4 + α^2

= x + x^2 + x+ x^2 = 0

elde edilir.

$\beta\beta^2\beta^4 = \beta^7$ hesaplanırsa;

$\beta^7 = \beta\beta^2\beta^4 = \alpha^0 = 1$ bulunur.

$$(y-\beta)(y-\beta^2)(y-\beta^4) = y^3 + (\beta+\beta^2+\beta^4)y^2 + (\beta\beta^2+\beta\beta^4+\beta^2\beta^4)y + \beta\beta^2\beta^4$$

eşitliğinde değerler yerine konulduğunda, en küçük polinom;

$$m_\beta(y) = \mathbf{y^3 + y^2 + 1}$$

olarak bulunur. Sonuç olarak; β^4, β^2 ve β'nın en küçük polinomları aynıdır.

$\beta = \propto^4 = x^2 + x = (110)$ alındığında, en küçük polinom nedir?

$$m_\beta(y) = \prod_{\delta \in C(\beta)} (y-\delta) = (y-\beta)(y-\beta^2)(y-\beta^4)$$

$$(y-\beta)(y-\beta^2)(y-\beta^4) = y^3 + (\beta+\beta^2+\beta^4)y^2 + (\beta\beta^2+\beta\beta^4+\beta^2\beta^4)y + \beta\beta^2\beta^4$$

eşitliklerinden;

$$(\beta+\beta^2+\beta^4) = (\alpha^4+\alpha^1+\alpha^2) = (x^2+x+x+x^2) = 0$$

$$(\beta\beta^2+\beta\beta^4+\beta^2\beta^4) = (\alpha^5+\alpha^6+\alpha^3) = (x^2+x+1+x^2+1+x+1) = 1$$

$\beta\beta^2\beta^4 = \alpha^0 = 1$ ve en küçük polinom; $m_\beta(y) = y^3 + y + 1$'dir.

$\beta = \propto^2 = x^2 = (100)$ için;

$$(\beta+\beta^2+\beta^4) = (\alpha^2+\alpha^4+\alpha^1) = (x^2+x^2+x+x) = 0$$

$$(\beta\beta^2+\beta\beta^4+\beta^2\beta^4) = (\alpha^6+\alpha^3+\alpha^5) = (x^2+1+x+1+x^2+x+1) = 1$$

$\beta\beta^2\beta^4 = \alpha^0 = 1$ ve en küçük polinom; $m_\beta(y) = y^3 + y + 1$'dir.

$\beta = \propto^1 = x = (010)$ için;

$$(\beta+\beta^2+\beta^4) = (\alpha^1+\alpha^2+\alpha^4) = (x+x^2+x^2+x) = 0$$

$$(\beta\beta^2+\beta\beta^4+\beta^2\beta^4) = (\alpha^3+\alpha^5+\alpha^6) = (x+1+x^2+x+1+x^2+1) = 1$$

$\beta\beta^2\beta^4 = \alpha^0 = 1$ ve en küçük polinom; $m_\beta(y) = y^3 + y + 1$'dir.

Böylelikle cismin üreteci **$\alpha = x$** alındığında, cisim elemanlarının en küçük fonksiyonları bulunmuştur. Daha sonra, **$\alpha = 1+x$** alınıp, aynı işlemler yapılmış ve sonuçlar Çizelge 2.4'te özetlenmiştir.

Çizelge 2.4. En küçük polinomu $f(x)=x^3 + x +1$ alınan $GF(2^3)$ cismi

$GF(2^3)$ Cismi için $f(x)=x^3 + x +1$ ve $\alpha=x$ alındığında	
$\beta=(011) = x+1 = \alpha^3$ $\beta=(111) = x^2+x+1 = \alpha^5$ $\beta=(101) = x^2+1= \alpha^6$	$m_\beta(y)= y^3 + y^2 +1$
$\beta=(010) = x = \alpha^1$ $\beta=(100) = x^2 = \alpha^2$ $\beta=(110) = x^2+x= \alpha^4$	$m_\beta(y)= y^3 + y +1$
$GF(2^3)$ Cismi için $f(x)=x^3 + x +1$ ve $\alpha=1+x$ alındığında	
$\beta=(011) = x+1 = \alpha^1$ $\beta=(101) = x^2+1= \alpha^2$ $\beta=(111) = x^2+x+1 = \alpha^4$	$m_\beta(y)= y^3 + y^2 +1$
$\beta=(100) = x^2 = \alpha^3$ $\beta=(010) = x = \alpha^5$ $\beta=(110) = x^2+x= \alpha^6$	$m_\beta(y)= y^3 + y +1$

$F=GF(2^3)$ cismini oluşturmak için Çizelge 2.3'ten, bu kez, Z_2'de indirgenemez kübik polinom olarak **$f(x)= x^3+x^2+1$** alınmış; **$\alpha=x$** ve **$\alpha=1+x$** üreteçleri için, cisim elemanlarının en küçük fonksiyonları Çizelge 2.5'te özetlenmiştir.

Çizelge 2.5. En küçük polinomu $f(x)=x^3 + x^2 +1$ alınan $GF(2^3)$ cismi

$GF(2^3)$ Cismi için $f(x)=x^3 + x^2 +1$ ve $\alpha=x$ alındığında	
$\beta=(010) = x = \alpha^1$ $\beta=(100) = x^2 = \alpha^2$ $\beta=(111) = x^2+x+1 = \alpha^4$	$m_\beta(y)= y^3 + y^2 +1$
$\beta=(101) = 1+x^2 = \alpha^3$ $\beta=(011) = x +1= \alpha^5$ $\beta=(110) = x^2+x= \alpha^6$	$m_\beta(y)= y^3 + y +1$
$GF(2^3)$ Cismi için $f(x)=x^3 + x^2 +1$ ve $\alpha=1+x$ alındığında	
$\beta=(010) = x = \alpha^3$ $\beta=(111) = x^2+x+1= \alpha^5$ $\beta=(100) = x^2 = \alpha^6$	$m_\beta(y)= y^3 + y^2 +1$
$\beta=(011) = x+1 = \alpha^1$ $\beta=(101) = x^2 +1= \alpha^2$ $\beta=(110) = x^2+x = \alpha^4$	$m_\beta(y)= y^3 + y +1$

$f(x)= x^3 + x^2 +1$ ve $f(x)=x^3 + x +1$ indirgenemez polinomlarında olduğu gibi, elde edilen en küçük polinomlar aynıysa, elemanların isimleri farklı olsa da bu iki cisim izomorfik olarak adlandırılır (Vanstone and Oorschot,1989).

Çizelge 2.4 ve Çizelge 2.5'ten yararlanarak, GF(2^3)'ün elemanları ve bunların en küçük polinomları, aşağıdaki gibi listelenebilir.

GF(2^3)'ün elemanları	**En küçük polinomlar**
$\propto, \propto^2, \propto^4$	$m_\beta(y) = y^3 + y^2 + 1$
$\propto^3, \propto^5, \propto^6$	$m_\beta(y) = y^3 + y + 1$
$\propto^7 = 1$	x+1
0	x

Bu en küçük polinomların her biri, x^8-x'i bölmelidir ve derecelerinin toplamı 8 olmalıdır. GF(2^3) için, x^8-x = x(x+1)(x^3+x+1)(x^3+x^2+1)'dir (Pless,1998).

Örnek 2.6. Çizelge 2.3'te , ikinci dereceden indirgenemez polinom, f(x)=x^2 + x +1 olarak verilmiştir ve tektir. Bu kez F=GF(2^2) cismi oluşturulsun.

F = GF(2^2). f(x)=x^2 + x +1 $\in$ Z_2[x] ve α=x cismin üretecidir.

α^0 = x^0 = 1 = **(01)**

α^1 = x^1 = x = **(10)**

α^2 = x^2 = x+1=**(11)**

α=x olduğuna göre, Eş. 2.4'teki çekimler kümesi, $C(x)=\{x, x^2, x^{2^2}, ..., x^{2^{t-1}}\}$ olarak yazılabilir. Bu durumda;

x = x

x^2 = x^2

x^4 =(x+1).(x+1) = x^2+2x+1=x+1+1=x'dir

$\alpha^{p^t} = \alpha = x^{2^t} = x$ yapan en küçük pozitif t sayısı 2'ye eşittir ve çekimler kümesi;

$C(x)=\{x, x^2\}=\{\alpha, \alpha^2\}=C(\alpha)$ 'dır.

β =(10)= α^1 alınsın.

$$m_\beta(y)=\prod_{\delta\in C(\beta)}(y-\delta)=(y-\beta)(y-\beta^2)=y^2+y(\beta^2+\beta)+\beta^3$$

$$(\beta^2+\beta)=(\alpha^2+\alpha)=(x+1+x)=1$$

ve en küçük polinom, $m_\beta(y)=y^2+y+1$'dir.

β =(11)= α^2 alınsın.

$$(\beta^2+\beta)=(\alpha^1+\alpha^2)=(x+x+1)=1$$

ve en küçük polinom, $m_\beta(y)=y^2+y+1$'dir.

2.5. Vektör Uzayları

F sonlu bir cisim ve V bir küme olsun (F'nin elemanları skalerler ve V'nin elemanları vektörler olarak adlandırılır). +, V üzerinde bir ikili işlem olsun ve bir λv elemanı; $\lambda \in$ F, v$\in$V'nin her çiftiyle ilişkili bir skaler çarpım olarak adlandırılsın. V, F üzerinde bir vektör uzayı ise, aşağıdaki özellikleri sağlar (http://en.wikipedia.org/wiki/Vector_space):

V1 + işlemine göre kapalı, birleşme özelliğine sahip ve değişmelidir. Birim elemanı 0'dır. Her bir u$\in$V, toplamaya göre –u tersine sahiptir. Hepsi için $\lambda, \mu \in$ F; u, v $\in$ V'dir.

V2 $\lambda v \in$ V'dir.

V3 $\lambda(u+v)=\lambda u+\lambda v$'dir.

V4 $(\lambda+\mu)u=\lambda u+\mu u$'dir.

V5 $(\lambda\mu)u=\lambda(\mu u)$'dir.

V6 1u = u olacak şekilde 1, F'nin çarpmaya göre birim elemanıdır.

Önerme 2.2. F bir cisim, V de F'nin elemanlarının bütün n-haneli/boyutlu (tuple) kümesi olsun. Toplama;

$$(u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) = (u_1+v_1, \ldots, u_n+v_n)$$

ve skaler çarpım;

$$\lambda(u_1, u_2, \ldots, u_n) = (\lambda u_1, \lambda u_2, \ldots, \lambda u_n)$$

olarak tanımlandığında, V, F üzerinde bir **vektör uzayıdır**.

X'in doğrusal bir birleşimi; $\lambda_1, \ldots \lambda_n \in$ F olmak üzere;

$\lambda_1 x_1 + \ldots + \lambda_n x_n$

vektörü biçimindedir.

X'i ayıran (span) küme, X'deki bütün vektörlerin doğrusal birleşiminin kümesidir.

V'nin bir alt uzayı, kendisi de bir vektör uzayı olan, V'nin bir alt kümesidir.

- Tek bir x vektörünün doğrusal bir birleşimi, c'nin bir skalerle çarpımından oluşan bir vektördür.
- Bir vektör uzayı pek çok alt kümeye sahiptir ve çoğu alt uzay değildir.
- V, kendisinin bir alt uzayıdır ve sadece 0 vektörünü içeren küme V'nin bir alt uzayıdır.

Önerme 2.3. Herhangi bir $X \subseteq V$ için, <X> V'nin bir alt uzayıdır.

k-boyutlu bir alt uzay, $V_n(F)$'deki k tane doğrusal bağımsız vektörle tanımlanır. (Vanstone and Oorschot , 1989).

Önerme 2.4. X'deki hiçbir vektör, diğerlerinin doğrusal birleşimi olarak yazılamıyorsa, X doğrusal bağımsızdır.

{o} vektörünü içeren bir küme doğrusal bağımsızdır.

V'nin bir temeli (basis), V'yi ayıran doğrusal bağımsız bir kümedir. Başka bir deyişle, X doğrusal bağımsız ve <X>=V ise, X bir temeldir (http://www.mcs.vuw.ac.nz/courses/MATH314/2003T2/Notes/314_notes_2003_02.pdf).

V, elemanları sonlu sayıda olan bir temele sahipse, sonlu boyutludur (finite dimensional).

Örnek 2.7. V(3,3) göz önüne alınsın ve X={(0,1,1), (1,1,0)} olsun.

Burada <X>'i elde edebilmek için, X'in bütün doğrusal birleşimleri bulunmalıdır.

0.(0,1,1) + 0(1,1,0) = (0,0,0)

0.(0,1,1) + 1(1,1,0) = (1,1,0)

0.(0,1,1) + 2(1,1,0) = (2,2,0)

1.(0,1,1) + 0(1,1,0) = (0,1,1)

1.(0,1,1) + 1(1,1,0) = (1,2,1)

1.(0,1,1) + 2(1,1,0) = (2,0,1)

2.(0,1,1) + 0(1,1,0) = (0,2,2)

2.(0,1,1) + 1(1,1,0) = (1,0,2)

2.(0,1,1) + 2(1,1,0) = (2,1,2)

dir.

<X>={(0,0,0), (1,1,0), (2,2,0), (0,1,1), (1,2,1), (2,0,1), (0,2,2), (1,0,2), (2,1,2)}

kümesi, V(3,3)'ün bir alt uzayıdır. Başka bir deyişle, bu küme kendi başına bir vektör uzayıdır. Örneğin, (2,2,0) + (1,2,1) = (0,1,1) $\in$ <X> ve aynı zamanda, 2(1,2,1)=(2,1,2) $\in$ <X>'dir. <X>, skaler çarpıma her zaman kapalıdır.

Önerme 2.5. V sonlu boyutlu bir vektör uzayı, X ve Y de temeller ise, X ve Y aynı sayıda vektör içerir.

V(n,q) ve q bir asal kuvvet ise,

{(1,0,...,0), (0,1,...,0),...(0,0,...1)}, V(n,q) için bir temeldir. Bu nedenle, V(n,q), n boyutludur.

Bir vektör uzayı, pek çok temele sahiptir. Yukarıda tanımlanan bunların en uygunudur ve çoğunlukla V(n,q)'nun **standart temeli** olarak adlandırılır (Vanstone and Oorschot , 1989).

Önerme 2.6. V, k-boyutlu bir vektör uzayı olsun. V'deki vektörlerin bir X kümesi, yalnız ve yalnız, X doğrusal bağımsız ve k vektöre sahipse, bir temeldir.

2.5.1. Doğrudan çarpım ayrıştırması

U bir vektör uzayı ve V,Y $\subset$ U alt uzaylar olsun. V ve Y, U'yu ayırır ve u$\in$U, v$\in$V ve y$\in$Y için u=v+y'nin toplamları olarak ifade edilebilirse, U=V+Y yazılabilir.

V $\cap$ Y ={0} ise, V ve Y, U'nun doğrudan toplam ayrıştırmasını belirler denir ve U=V $\oplus$ Y olarak gösterilir (http://www.PlanethMath.org/DirectSum.html).

Önerme 2.7. U sonlu boyutlu olsun. V ve Y ancak ve ancak, V'nin $v_1,v_2,...v_m$ her

temeli için ve Y'nin $y_1,y_2,...y_n$ her temeli için,

$$v_1,v_2,...v_m,\ y_1,y_2,...y_n$$

birleşmiş listesi U'nun temeliyse; tümleyendir (complement).

Her $V \subset U$ alt uzayı için, V'nin dik tümleyeni, $V^{\perp}$ tanımlanabilir.

$$V^{\perp} = \{ u \in U: \langle v,u \rangle = 0, \text{ her } u \in V \text{ için } \}$$

Önerme 2.8. U sonlu boyutlu ve $V \subset U$ bir alt uzay olsun. Bu durumda, V ve dik tümleyeni $V^{\perp}$, U'nun doğrudan çarpım ayrıştırmasını belirler.

Teorem 2.9. V ve Y, sonlu boyutlu U vektör uzayının alt uzayları olsun. Yalnız ve yalnız, dimU=dimV+dimY ve $V \cap Y=\{0\}$ ise, $U = V \oplus Y$'dir.

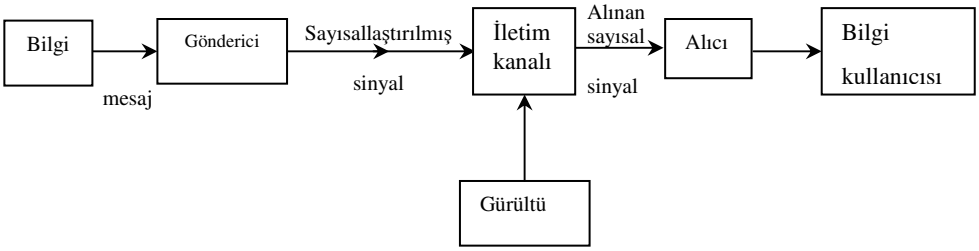
3. İKİLİ KODLAR

Kod teorisi, bilgisayarların kullanılmaya başlamasıyla gelişmiştir. İlk bilgisayarlar bugünkülerle karşılaştırıldığında; güvenilirlikleri düşük, büyük makineler olduğundan, tek bir mekanik kanalda meydana gelebilecek bir hata, hesaplamanın hatalı olmasına neden olabilirdi. Sonrasında, hatalı kanalları bulup değiştirebilmenin yöntemleri keşfedildi. R.W. Hamming (1950), Bell Laboratuarları için çalışırken, hatayı bulan makinenin, hatayı düzeltmesinin de mümkün olması gerektiğinden yola çıkarak, bilgiyi şifrelemenin bir yolunu bulmuş; böylece, bulunabilen hatanın düzeltilebilmesi de mümkün olmuştur. Hamming'in çalışmasına bağlı olarak, Claude Shannon, kod teorisi için teorik çatıyı geliştirmiştir.

Hata düzeltme kodları günümüzde manyetik ve optik diskler; ses bantlı modemler; telsiz; fiber optik iletim sistemleri; uydu iletişimi gibi birçok sistemde geniş ölçüde kullanılmaktadır.

Bir haberleşme sistemi, Şekil 3.1'deki gibi ifade edilebilir. Göndericiden alıcıya bilgi, "bit"ler olarak bilinen ikili kümelerle iletilir. Kaynaktan alıcıya bitlerin geçtiği yol, kanal olarak adlandırılır. Kanaldayken bitler gürültüye maruz kalırsa hata meydana gelir; yani, alınan bitlerin bazılarının değeri, karşılık gelen iletilmiş bitlerin tam tersidir. Hata düzeltme kodlamasının ortaya çıkmasının sebebi, iletim kanalında gürültüden kaynaklanan bozulmalardır (http://www theory.dcs.st-

and.ac.uk/~sal/school/CS2010/Lectures/forhtml/node3.html).



Şekil 3.1. Haberleşme sistemi

Gönderici, sayısal kodlayıcıdır. Alıcı ise, kod çözücüdür; gönderici tarafında hazırlanan kodları, göndericinin tersi bir işlem yaparak çözer ve mesajı tekrar oluşturur.

Alıcıya iletilecek olan bilgi ikili düzende olmadığı için, öncelikle göndericide bu bilgilerin sayısallaştırılıp "kodlanması" gerekir. Alınan sinyal, alıcıda ikili düzende hata düzeltmesine tabi tutulur, sonra da tekrar ikili düzenden "kod çözme" işlemi gerçekleştirilir. Bu şekilde bilgi, alıcı tarafına iletilmiş olur.

Aksi belirtilmedikçe, bloklarda iletilen bitlerin sabit uzunluklu olduğu varsayılmıştır. Bloğa hiçbir bit alınıp, hiçbir bit silinemez ve her zaman blok eşlemesinin (synchronization) olduğu varsayılır (Alıcı her zaman, bloğun nerede başlayıp nerede bittiğini bilir). Örneğin, ikili blok kodlar, mesajların ikili düzende ifade edileceği ve kodların n adet 0 ve 1'lerden oluşan "kelimelerle" (ikili düzende ifadelerle) gösterileceği anlamına gelmektedir.

Hata düzeltme kodlamalarında bazı kabuller yapılmaktadır (Kuş, 2002);

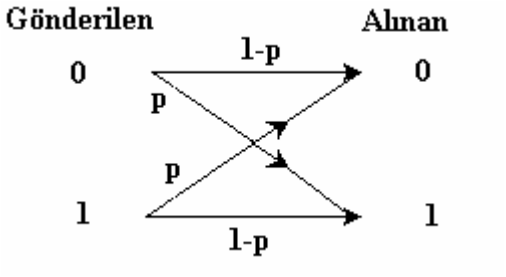
a. Kanal aracılığıyla göndericiden alıcıya gönderilen 0 ve 1'lerden oluşan n uzunluğundaki her kelime, göndericide yine 0 ve 1'lerden oluşan n uzunluğundaki kelime olarak alınacaktır (Bir bitin kanal boyunca kaybolma ihtimali sıfır kabul edilmektedir).

b. Bir bitte oluşacak olan hata diğer bitleri etkilemeyecektir. Yani her bir bitte hata oluşması birbirinden bağımsız olarak gerçekleşir.

c. Mesajın iletildiği ortam, *ikili simetrik kanal* davranışını gösterir.

3.1. İkili Simetrik Kanal

"Simetrik kanal", hatanın oluşma ihtimalinin gönderilen karakterden bağımsız olduğu anlamına gelmektedir. Ayrıca sıfır hafızalı bir kanaldır; hata oluşma olasılığı, önceki bitte hata oluşup oluşmadığına bağlı değildir. İkili simetrik kanal, Şekil 3.2'de gösterilmektedir (http://www-theory.dcs.st-and.ac.uk/~sal/school/CS2010 /Lectures/forhtml/node3.html).

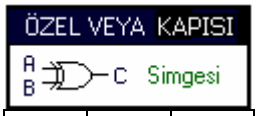


Şekil 3.2. İkili simetrik kanal

p (≤0.5) hata olasılıklı bir ikili simetrik kanal, ikili verinin gönderildiği bir kanaldır. 1-p, iletimde hatanın oluşmama ihtimali olup, "ikili simetrik kanalın güvenilirliği" olarak tanımlanır. Buna göre, gönderilen mesajdaki 0'ın, alıcıda 0 olarak alınması ihtimali (1- p=q), 1 olarak alınması ihtimali ise p'dir.

3.2 Özel veya Kapısı (XOR gate)

Özel veya kapısında; giriş uçları aynıyken (örneğin; 00) çıkış 0, giriş uçları farklıyken (örneğin, 01) çıkış 1'dir. Hesaplamalardaki formülü Q = (A ⊕ B)'dir. Şekil 3.3'te, özel veya kapısının sembolü ve iç yapısı görülmektedir (http://www.bilimveteknoloji.com/elektronik/elektronik/dijital/dijital_elektroniknik_7.htm).



A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

Şekil 3.3. Özel veya kapısı

Şekil 3.3'ten; 0⊕0=0 , 0⊕1=1 , 1⊕0=1 ve 1⊕1=0'dır. Özel veya kapısına göre, a ⊕ b=c ise, a⊕c=b ve b⊕c =a'dır (http://www.cs.mu.oz.au/353/notes/node58.html).

Aynı uzunluktaki iki bloğun bitlerinin toplamı özel veya kapısı işlemiyle bulunur.

Örneğin, iki blok (1100110) ve (1010101) olsun.

$$A = 1100110$$
$$B = 1010101$$
$$A \oplus B = 0110011$$

dir. Bundan sonra kod kelimeleri arasındaki toplama işlemi söz konusu olduğunda, (+) işlemi özel veya kapısı olarak kullanılacaktır. Genel olarak kod kelimeleri, iki elemanlı cisimde vektörler olarak değerlendirilirler.

3.3. Denklik (parity) Kavramı

Bir tamsayının denkliği, çift ya da tek olabilir ve sayısal bir değerle gösterilebilir (Arazi, 1988).

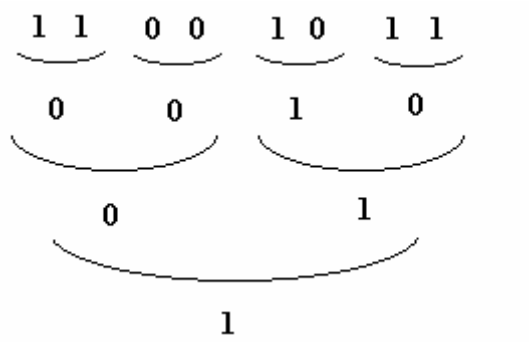
Tanım 3.1. Çift bir denklik; denklik 0 ve tek bir denklik; denklik 1 olarak adlandırılır (Tek sayılar 1 denkliğine, çift sayılar 0 denkliğine sahiptir).

Bitlerin belli bir grubunun denkliği söz konusu olduğunda, gruptaki 1 değerlerinin sayısı denkliği gösterir. (11001011) bloğu için incelersek; örneğin, bloğun ilk dört elemanının denkliği 0, son dört elemanının denkliği 1'dir.

Temel sayılabilecek bir özellik; iki bloğun toplamının denkliğinin, bunların denklikleri toplamına eşit olmasıdır. A ve B iki blok ve C de toplamları ise, blokların denkliklerinin sırasıyla a,b ve c olması varsayımıyla, c = a+b'dir.

Verilen bir bit grubunun denkliği, mantık kapıları kullanılarak hesaplanabilir. Örneğin, 7 girişli bir özel veya kapısında; 6 girişin değeri 1 ise, çıkış 0; 3 girişin değeri 1 ise, çıkış 1'dir.

Örneğin, (11001011) bloğu göz önüne alınsın. Bloğun denkliği 1'dir (1'lerin sayısı 5'tir) ve bu sonuca nasıl ulaşıldığı Şekil 3.4'ten de görülebilir.



Şekil 3.4. (11001011) Bloğunun çoklu özel veya kapısı

Sonuç 3.1. k bitli bir blok, 0 denkliğine sahip k+1 bitli bir bloğa dönüştürülebilir: Bu bloğun denkliğine eşit bir bit bloğa eklenirse; blok, k+1 bitli ve 0 denkliğine sahip bir blok olacaktır (Arazi,1988).

3.4. Blok Kodları Kavramı

Bir *kelime,* sayılardan oluşan bir diziyi gösterdiğinde (burada 0 ve 1'ler), örneğin (01); bir *kod kelimesi* (codeword), sayılardan oluşan daha uzun bir diziyi gösterir; örneğin (01010101) vb. gibi (www.southwestern.edu/~shelton/ REU02 /papers/ douglasc.doc)…

Bir *blok kodu*, aynı uzunlukta olup, kod kelimeleri olarak adlandırılan ikili blokların birleşimi olarak tanımlanmıştır. "ikili blok", "ikili vektör", ve "ikili kelime" terimleri, kullanıldıkları yere göre, yer değiştirebilirler. Çizelge 3.1'de belli bir kodun kod kelimeleri listelenmiştir (Arazi,1988).

Çizelge 3.1'deki kod, 0 denkliğine sahip (Bkz. Tanım 3.1), 4 uzunluğundaki blokların toplamından oluşur. Bu tür her bir blok bir kod kelimesidir ve kodda toplam 8 kod kelimesi vardır. Bunlar, 3 uzunluklu olası tüm ikili blokların (bilgi bitlerinin) seçimiyle ve her bir bloğa denklik bitinin eklenmesiyle oluşturulmuştur.

Çizelge 3.1. Bir koda ait kod kelimeleri

0000	1001
0011	1010
0101	1100
0110	1111

Bir blok kodundaki n uzunluklu her bir kod kelimesi, genel olarak k uzunluklu bir bilgi vektörünün genişletilmesiyle oluşturulur. Genişletme, değerleri bilgi bitlerinden

hesaplanan denklik bitlerinin, bilgi vektörüne eklenmesiyle yapılır. Bu nedenle, koddaki kod kelimelerinin sayısı, rastgele seçilmiş olası k bitlerinin sayısıyla, 2^k ile, belirlenir (http://www-theory.dcs.st-and.ac.uk/~sal/school/CS2010/Lectures/forhtml/node3.html).

Bir (n,k) blok kodu, her bir kod kelimesinin n uzunluğunda ve k tane bitin bilgi biti olduğu (denklik biti sayısı bu yüzden n-k'dır) bir koddur.

Çizelge 3.1'deki kodda; k=3, n=4, kod kelimesi sayısı 2^3 tür ve bu kod, bir (4,3) blok kodudur.

3.5. Hamming Ağırlığı

Hamming ağırlığını tanımlamadan önce, doğrusal kod kavramının, basit bir tanımı verilecektir.

Tanım 3.2. *Bir doğrusal kod*, herhangi iki kod kelimesinin toplamının, yine bir kod kelimesi olduğu koddur (Arazi,1988).

Çizelge 3.1'deki kod, bu tanıma göre doğrusal bir koddur. Örneğin; (0011) ve (0101) kod kelimelerinin toplamı olan (0110); kod kelimesi olup, koddaki 8 kod kelimesinden biridir.

Tanım 3.3. Bir kod kelimesinin *Hamming ağırlığı*, 1 değerine sahip elemanlarının sayısıdır (http://web.syr.edu/~rrosenqu/ecc/main. htm).

Örneğin, (010101) kod kelimesinin Hamming ağırlığı 3'tür ve w(010101)=3 şeklinde gösterilir.

3.6. Hamming Uzaklığı

Tanım 3.4. Aynı uzunluktaki İki kod kelimesi arasındaki *Hamming uzaklığı*, bitlerde farklı olan rakamların sayısıdır.

Uzaklık fonksiyonu d(x,y);d(x,y)= x ve y arasındaki uzaklık olarak tanımlanırsa; uzaklık fonksiyonu, kod kelimeleri kümesi üzerinde metriktir ve aşağıdaki koşulları sağlar (Vanstone and Oorschot, 1989):

$$d(x,y) \geq 0 \text{ ve } d(x,y) = 0 \Leftrightarrow x=y$$

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

$d(x,y) \leq d(x,y) + d(y,z)$

Örneğin, d(0,1)=1, d(001, 011)=1, d(000, 111)=3, d(111,111)=0'dır.

A ve B iki kod kelimesi ve C de toplamları ise, A ve B'nin farklı rakamlara sahip oldukları bitlerde, C, 1 değerine sahip olacaktır. Bu durumda C'deki 1 elemanı, A ve B arasındaki Hamming uzaklığıdır. Öte yandan bu sayı, C'nin Hamming ağırlığıdır.

Sonuç 3.2. İki kod kelimesinin toplamının Hamming ağırlığı, bu iki kelime arasındaki Hamming uzaklığıdır (Arazi,1988).

Örneğin (1010111) ve (1111010) kelimelerinin ikisinin de Hamming ağırlığı 5; Hamming uzaklığı d(1010111,1111010)=4'tür. Bu iki kelimenin toplamı olan (0101101) kelimesinin Hamming ağırlığı 4 olup, iki kelime arasındaki Hamming uzaklığına eşittir.

Bir kodun en kısa uzaklığı ise, farklı kod kelimeleri arasındaki bütün uzaklıkların en kısasıdır: C'nin en kısa uzaklığı, d= min { d(x,y) | x, y $\in$ C }'dir.

k uzunluğundaki olası tüm 2^k vektörlerinden oluşan (k,k) kodunun, en kısa Hamming uzaklığı 1 olduğunda, en kısa Hamming uzaklığını artırmak için bu vektörlerin her birine denklik bitleri eklenebilir. Bu denklik bitleri rastgele bitlerden hesaplanır. Kod kelime sayısını sabit tutarak, en kısa Hamming uzaklığını artırmak mümkündür. Bu süreç Çizelge 3.2'de gösterilmektedir (Arazi,1988).

Çizelge 3.2. Denklik bitleri eklenerek en kısa Hamming uzaklığının artırılması

Sütun (a)			**Sütun (b)**			**Sütun (c)**	
0000	1000		00000	10001		0000000	1000110
0001	1001		00011	10010		0001101	1001011
0010	1010		00101	10100		0010111	1010001
0011	1011		00110	10111		0011010	1011100
0100	1100		01001	11000		0100011	1100101
0101	1101		01010	11011		0101110	1101000
0110	1110		01100	11101		0110100	1110010
0111	1111		01111	11110		0111001	1111111

Çizelge 3.2'nin (a) sütunu, 4 bitlik yapıları listeler. Buradaki en kısa Hamming uzaklığı 1'dir. (b) sütunu, kod kelimelerini 0 denklikli (Bkz. Böl. 3.3) yapacak şekilde yeni bir denklik biti eklenmesiyle elde edilmiştir. Buradaki en kısa Hamming uzaklığı 2'dir. (c) sütunu, ilk kodun kelimelerine, 3 denklik bitinin eklenmesiyle elde edilmiştir. Buradaki en kısa Hamming uzaklığı,d, 3'tür.

3.7. Bir Kodun Hata Bulma ve Düzeltme Kapasitesi

A=(10110011) gönderilen bir vektör olsun. Alıcıya gelene kadar hataya maruz kalan vektörün hata yapısı E=(11001001) ve B vektörü, A+E=(01111010)'dir. A'da oluşan hata sayısı ve E'nin Hamming ağırlığı 4'tür. Bu sayı aynı zamanda, A ve B arasındaki Hamming uzaklığıdır.

Genel olarak, gönderilen ve alınan vektörler arasındaki Hamming uzaklığının, hata yapısının Hamming ağırlığı olduğu söylenir (Arazi,1988).

Tanım 3.5. Bir C blok kodu; her bir c kelimesi, en az 1, en çok t sembolün değiştirilmesiyle c'den elde edilen $\mathbf{c}'$ için; $\mathbf{c}'$ kod kelimesi değilse, t hata bulur.

Önerme 3.1. Bir kod, ancak ve ancak en kısa uzaklığı t'den büyükse t hata bulur (http://www-theory.dcs.st-and.ac.uk/~sal/school/CS2010/Lectures/forhtml/node3.html).

Tanım 3.6. Bir kodun *hata düzeltme kapasitesi,* alıcının orijinal mesajı düzeltme olasılığı olduğu durumlarda, iletilen kod kelimesinde meydana gelebilecek en fazla hata sayısıdır.

Sonuç 3.3. Bir kodun hata düzeltme kapasitesi, [(d-1)/2] 'dir (Arazi,1988).

Teorem 3.1. Bir C kodu, yalnız ve yalnız, $d(C) \geq 2t+1$ ise, t hata-düzeltme kodudur (Vanstone and Oorschot, 1989).

3.8. Doğrusal Kodlar

Bir kodun matematiksel bir yapıya sahip olması gerekmez. Uygulamada, kodlama ve çözmeyi olanaklı kılmak için kodlar kullanıldığında, pek çok matematiksel yapı göz önüne alınır.

q, bir asal sayının kuvveti ise, q sembollü bir kümeden, {0,1,…,q-1}, n uzunluklu

tüm kelimelerin kümesi, V(n,q) vektör uzayı olarak değerlendirilebilir. Bu yüzden, bu sembolleri kullanan n uzunluğundaki bir kod, V(n,q)'nun alt kümesidir.

Bütün kod kelimelerinin kümesi bir V(n,q)'nun alt uzayını oluşturuyorsa ve kod kelimeleri farklıysa, GF(q) üzerindeki böyle bir kod, doğrusal koddur.

Tanım 3.7. Bir C blok kodu, a) 0'lardan oluşan kelime C'de ve b) v ve w, v,w$\in$C olmak üzere, v+w$\in$C ise doğrusal bir koddur (http://www-theory.dcs.st-and.ac.uk/~sal/school/CS2010/Lectures/ forhtml/node3. html).

Teorem 3.2. Bir doğrusal kodun uzaklığı, 0 olmayan kod kelimelerinin ağırlığına eşittir.

Bir doğrusal kodun parametreleri: Doğrusal kodlar, n uzunluğuna (bir kod kelimesindeki hane sayısı), d uzaklığına ve k boyutuna sahiptir. Bu parametrelere sahip bir doğrusal kod, (n,k,d) doğrusal kodu olarak gösterilir (Pretzel,1992).

V(n,q) vektör uzayı, q^n vektörlüdür. k boyutlu bir alt uzayı ise q^k vektöre sahiptir (http://www.mcs.vuw.ac.nz/courses/MATH314/2003T2/Notes/314_notes2003_04. pdf).

Tanım 3.8. F üzerindeki bir doğrusal (n,k,d) kodu, $V_n(F)$=V(n,q)'nun k-boyutlu bir alt uzayıdır.

Tanım 3.9. v$\in V_n(F)$ vektörünün Hamming ağırlığı, w(v), v'deki 0 olmayan koordinatların sayısıdır.

Tanım 3.10. Bir (n,k,d) C kodunun Hamming ağırlığı,

$$w(C)=\min\{w(x): x \in C, x\neq 0\}\text{'dır.}$$

Örnek 3.1. S_1 ={(0000),(1000),(0100),(1100)}

S_2 ={(0000),(1100),(0011),(1111)}

Kümelerinin ikisi de, $V_4(Z_2)$'nin 2-boyutlu alt uzayıdır. S_1'in ağırlığı ve uzaklığı 1, S_2'nin ağırlığı ve uzaklığı 2'dir.

Teorem 3.3. d, bir (n,k,d) kodunun uzaklığı olsun. Bu durumda d;

$\mathbf{d = \min_{w \in C, x \neq 0} w(x)}$ 'dir (Hedeyat, Sloane; and Stufken,1999).

3.8.1. Üreteç matrisleri

Bir (n,k,d) doğrusal kodu, Ü.M.ne göre tanımlanabilir.

Tanım 3.11. Bir (n,k) kodu için G Ü.M., satırları C için temel (Bkz.Önerme 2.4.) olarak seçilen vektörlerden oluşan k×n boyutlu bir matristir (http://www-theory.dcs.st-and.ac.uk/~sal/school/CS2010/Lectures/forhtml/node3.html).

Üreteç matrisi G,

$$G = [I_k \;\; A] \tag{3.1}$$

olarak tanımlanır ve rankı k'dır. Burada, I_k, k×k birim matris ve A, k×(n-k) boyutlu bir matristir. Böylelikle bilgi bitleri, bir kod kelimesinin ilk k elemanında görünecektir. Böyle bir G matrisi, *standart biçimde* olarak adlandırılır. Bir doğrusal kod, pek çok temele (hepsi aynı büyüklükte) ve pek çok Ü.M.ne sahip olabilir. Ü.M.nin önemli özelliklerinden biri de kodun en az Hamming ağırlığının, G Ü.M.nin satırlarının ağırlığından bulunabilmesidir.

Tanım 3.12. F cismi üzerindeki (n,k,d) C ve C' kodları; eğer, C ve C' için G ve G' Ü.M.leri varsa ve n×n P permütasyon matrisi olduğunda, G'=GP ise, eşit kodlardır (Pless,1998).

Örneğin, (4,2) kodu için, v_1 = [1000] ve v_2 = [0110] temel vektörler olsun. Ü.M. bu vektörlerden oluşacağından, bu örnek için Ü.M.;

$$G = [I_k \;\; A] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}_{2\times 4}$$

dir.

3.8.2. Denklik kontrol matrisleri

Bir doğrusal kodu tanımlamanın seçenek bir yolu, D.K.M.ni vermektir. D.K.M, satırları dik uzayı koda ayıran, (n-k)×n boyutlu bir matristir ve en kısa uzaklığın hesaplanmasında kullanılabilir (http://www-theory.dcs.st-and.ac.uk/~sal/school

/CS2010/Lectures/forhtml/node3.html).

Tanım 3.13. Bir C kodu için, v∈C olmak üzere, Bir H matrisi, yalnız ve yalnız $\mathbf{v}\mathbf{H} = \mathbf{0}$ ise, bir D.K.M.'dir.

G, C için Ü.M. ve H de C için D.K.M. ise, G'nin satırları kod kelimeleri olduğundan, G.H=0'dır.

Önerme 3.2. G= [I_k A] ise, buna karşılık gelen D.K.M n-k×n boyutlu; **H= [-A^T I_{n-k}]**'dır. H'nin rankı n-k'dır (Macwilliams and Sloane,1977).

{00000,11111} kod kelimelerine sahip kod için D.K.M,

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \qquad (3.2)$$

dir.

3.8.3. Bir kodun duali

C, F cismi üzerinde bir (n,k,d) kodu ise, C'nin $C^{\perp}$ (C dual) dik tümleyeni; $C^{\perp}$ = { x ∈ $V_n(F)$: x.y = 0 bütün y ∈ C için }'dir. Bunun anlamı, $C^{\perp}$'in C'deki her vektöre dik, F üzerindeki n-haneli küme olduğudur.

Tanım 3.14. x = (x_1,x_2,…,x_n) ve y = (y_1,y_2,…,y_n) $V_n(F)$'de vektörler olsun. x ve y'nin içsel çarpımı;

$$x.y = \sum^{n} x_i\, y_i$$

dir ve toplamlar F üzerinden hesaplanır (Vanstone and Oorschot , 1989).

İçsel çarpım değişmelidir (commutative).

1. x,y,z ∈ $V_n(F)$, (x+y)z = x.z+y.z

2. x,y ∈ $V_n(F)$ ve λ ∈ F, (λ.x)y = λ(x.y)

3. x.y = 0 ise, x ve y, birbirine diktir denir.

Teorem 3.4. C, bir (n,k,d) doğrusal kodu olsun. Bu durumda; n uzunluğuna, n-k boyutuna ve bazı $\mathbf{d}^{\perp}$ (C'nin dual uzaklığı) sayıları için $\mathbf{d}^{\perp}$ en kısa uzaklığına sahip

a) $\mathbf{C}^{\perp}$ dual kodu; bir (n,n-k, $\mathbf{d}^{\perp}$) kodudur.

b) C için Ü.M., $\mathbf{C}^{\perp}$ için D.K.M.dir. C için bir D.K.M., $\mathbf{C}^{\perp}$ için bir Ü.M.dir.

c) $(\mathbf{C}^{\perp})^{\perp} = \mathbf{C}$'dir (Hedeyat et al.,1999).

Sonuç 3.4. G=[I_k A], C için Ü.M. ise, H = [$-A^T$ I_{n-k}] da $\mathbf{C}^{\perp}$'in üretecidir (Pless,1998).

3.8.3.1. Self-dual kodlar

Bir C kodu, $\mathbf{C}^{\perp}$=C ise, self-dual-duali kendisine eşit-bir koddur.

a) Bir kodun duali kendisiyse, kelime uzunluklarının çift olması gerekir.

b) Duali kendisine eşit bir kodun bütün kelimeleri çift ağırlıktadır ve bütün ağırlıklar 4 ile bölünebiliyorsa, n, 8'in çarpanıdır.

c) Duali kendisine eşit kodlar, (n, n/2) doğrusal kodlarıdır (Sloane and Thompson,1983).

Önerme 3.3. Herhangi bir (2k, k, d) self-dual kodu için, G=[I_k A] ile oluşturulan ve d ağırlıklı bir satır içeren, denk bir C kodu vardır (Bilous and Rees,2003).

3.8.4. Kodlama Sınırları

Bir (n,A,d) kodu, d uzunluğuna sahip, A tane kod kelimesi içeren n uzunluğunda bir koddur.

Üç parametreli bu kodların, hangisinin daha iyi olduğuna iki değişken sabitken karar verilebilir. n ve d sabit, A değişebilir olsun. Bir (n,A_1,d) kodu, (n,A_2,d) kodundan yalnız ve yalnız $A_1 > A_2$ ise iyidir.

Bir (n,k,d) ikili kodu, (n,2^k,d) kodudur (http://www.mcs.vuw.ac.nz/courses/MATH314/ 2003T2/Notes/314_notes2003_03.pdf).

Teorem 3.5. (Hamming ya da küre-paketi sınırı) Bir q-dizini (n, A, 2t+1) kodu,

$$A\left(\binom{n}{0}+(q-1)\binom{n}{1}+...+(q-1)^t\binom{n}{t}\right)\leq q^n$$'yi sağlar.

Bir (n,A,2t+1) kodu için;

$A\leq\dfrac{q^n}{\left\{\binom{n}{0}+...\binom{n}{t}(q-1)^t\right\}}$ ya da başka bir deyişle;

$$\sum_{\mathbf{i}=0}^{\mathbf{t}}\binom{\mathbf{n}}{\mathbf{i}}\leq 2^{\mathbf{n-k}} \qquad (3.3)$$

dir (Nguyen,1997).

Hamming sınırı, verilen bir n uzunluklu, 2t+1 uzaklıklı kodda, kod kelimelerinin sayısı için bir üst sınırdır.

Örnek 3.2. d=3, n=7 olan en büyük doğrusal C kodu nedir?

d=2t+1, t=1'dir. Hamming sınırı;

$|C|\leq\dfrac{2^7}{\binom{7}{0}+\binom{7}{1}}=\dfrac{2^7}{2^3}$ 'dir. C doğrusalsa, $|\boldsymbol{C}|$, 2'nin kuvveti olmalıdır. $|\boldsymbol{C}|\leq 2^4$'tür

ve bu nedenle, kodun boyutu 4'ten küçük ya da eşittir.

Teorem 3.6. (Griesmer Sınırı) C, GF(q) üzerinde bir [n,k,d] koduysa,

$$\mathbf{n}\geq\sum_{\mathbf{i}=0}^{\mathbf{k-1}}\left\lceil\frac{\mathbf{d}}{\mathbf{q^i}}\right\rceil \qquad (3.4)$$

dır. Griesmer sınırı, verilen bir n,k,d için alt sınırdır.

Hamming kodlarının dualleri, Griesmer sınırını sağlayan kodlar ailesindendir (Gulliver and Bhargava,2000).

Teorem 3.7. (Singleton sınırı) n-k ≥ d-1'dir.

Teorem 3.8. (Varshamov-Gilbert Sınırı). Aşağıdaki eşitsizliği sağlayan en kısa d uzaklıklı, en fazla r denklik bitli, n uzunluklu, 2 elemanlı bir cisim üzerinde doğrusal bir kod vardır (MacWilliams and Sloane,1977).

$$\sum_{i=0}^{d-2} \binom{n-1}{i} < 2^r \qquad (3.5)$$

3.8.4.1. Mükemmel kodlar

Bir q-dizini (n,A,2t+1) kodu, Hamming sınırını (Eş. 3.3) sağlarsa, mükemmeldir.

Teorem 3.9. Mükemmel bir t-hata düzeltme ikili (n,k) kodunun var olabilmesi için; n,k ve t sayılarının aşağıdaki eşitliği sağlaması gerekir.

$$\left(\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{t}\right)2^k = 2^n$$

i) d=1 ise, t=0'dır ve bir (n,A,1) ikili kodu, $2^n / \binom{n}{0} = 2^n$ kod kelimesine sahip olacaktır.

ii) n=2t+1 ve d=2t+1 olsun. Bu parametrelere sahip mükemmel bir kodun

kod kelimesi sayısı, $A = \dfrac{2^{2t+1}}{\binom{2t+1}{0}+\ldots+\binom{2t+1}{t}}$ 'dır.

Burada, $\binom{2t+1}{0}+\ldots+\binom{2t+1}{t} = 2^{2t}$'dir. Bu durumda, A=2'dir ve bu tür kodlar vardır (http://www.mcs.vuw.ac.nz/courses/MATH314/2003T2/Notes/314_notes2003_08.pdf).

Örneğin, {000...0,111...1} bir {2t+1, 2, 2t+1} kodudur. Bu tür kodlar önemsiz (trivial) mükemmel kodlar olarak adlandırılırlar.

3.9. Hamming Kodları

Teorem 3.1'den, bir kodun tek hata düzeltebilmesi için en kısa uzaklığının 3 olması gerektiği bilinmektedir. Buna göre,

a) D.K.M.nin hiçbir satırı 0 olmamalı,

b) D.K.M.nin hiçbir iki satırının toplamı 0 olmamalıdır (http://www-theory.dcs.st-and.ac.uk/~sal/ school /CS2010/Lectures/forhtml/node3.html).

İkili bir H_r Hamming kodu, $n=2^r-1$ uzunluğunda ($r \geq 2$); sütunları r uzunluklu sıfır olmayan ikili vektörlerden oluşan H D.K.M.li doğrusal bir ($n=2^r-1, k=2^r-r-1, d=3$) kodudur. Hamming kodları mükemmel (perfect) tek hata-düzeltme kodlarıdır (http://www.mathworld.wolfram.com/HammingCode.html).

Hata düzeltme kodlamalarında, kod üretiminde kullanılan D.K.M., $(n-k)\times n$ boyutlarına sahiptir (Bkz. Önerme 3.2). Bu matrisin doğrusal bağımsızlık şartını sağlaması için, n – k uzunluğunda n adet sütunundan hiç birinin sıfırdan oluşmaması gerekir. n - k uzunluğunda olabilecek en fazla sütun sayısı = 2^{n-k}, sıfırdan farklı olanları ise 2^{n-k}–1'dir. Matrisin sütun sayısı için aşağıdaki eşitliği yazmak mümkündür.

$$n \leq 2^{n-k} - 1 \qquad (3.6)$$

$n = 2^{n-k} - 1$ eşitliğini sağlayan kodlara Hamming Kodu veya ideal kodlar (perfect codes) denilmektedir Hamming kodu için $n = 2^{n-k} - 1$ eşitliği göz önünde tutulursa, (n,k) için (3,1), (7,4), (15,11),(31,26) gibi değerler kullanılabilir (Kuş,2002).

Örneğin, r=2 için, H(3,1) kodunun D.K.M;

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad (3.7)$$

ve Önerme 3.2.'den, G Ü.M.;

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \qquad (3.8)$$

dir.

Bir tane denklik biti eklemek koşuluyla, ($n=2^r-1$, $k=2^r-r-1$, $d=3$) mükemmel kodu, ($n=2^r$, 2^r-r-1, 4) genişletilmiş mükemmel kodu üretir (Nguyen,1997).

3.9.1. Hamming kodlarının oluşturulması

Bir Hamming kodunu oluşturmanın yolu; bilgi bitlerinden hesaplanan n-k tane denklik bitini, bilgi vektörüne ekleyerek; k uzunluğundaki bilgi vektörünü, n uzunluğundaki kod kelimesine dönüştürmektir.

k uzunluğundaki bilgi vektörü abcd ve n-k tane denklik biti p0,p1,p2 ile gösterilmiştir. Hamming (1950), bilgi vektöründen kod kelimesine ulaşılmasını denklik kontrolü olarak adlandırmış ve ilk denklik kontrolünün en sağında bir olan noktaları kullanacağını belirtmiştir (1,3,5,7..). Aynı şekilde, ikinci denklik kontrolü, sağdan ikinci 1'lere sahip noktaları (2,3,6,7..) ve 3. denklik kontrolü de 4,5,6,7,... noktalarını kullanmalıdır.

(0011) bilgi vektörü alınsın. Bilgi bitlerinin pozisyonu 3,5,6,7'dir.

		0		0	1	1

1,3,5,7 pozisyonları üzerindeki ilk denklik kontrolü; $0+0+1 \equiv 1 \pmod 2$ olduğundan; 1, 1. pozisyona yerleşir.

1		0		0	1	1

2,3,6,7 üzerindeki ikinci denklik kontrolü, $0+1+1 \equiv 0 \pmod 2$. Böylece 0, ikinci pozisyona yerleşir.

1	0	0		0	1	1

Son kontrol, 4,5,6,7 üzerindedir ve $0+1+1 \equiv 0 \pmod 2$'dir ve kodlanan kod kelimesi,

1	0	0	0	0	1	1

olarak bulunur.

Bu durumda, denklik bitleri aşağıdaki n-k=7-4=3 eşitlikten yararlanarak elde edilir.

$$p2 + b + c + d = 0 \Rightarrow p2 = b + c + d$$

$$p1 + a + c + d = 0 \Rightarrow p1 = a + c + d \qquad (3.9)$$

$$p0 + a + b + d = 0 \Rightarrow p0 = a + b + d$$

Bu eşitliklerden yararlanarak oluşturulan Hamming(7,4) ya da H_3 Çizelge 3.3'te gösterilmektedir.

Çizelge 3.3'ten (1100) bilgi vektörünün alındığı varsayılsın. Bu durumda, a=1,b=1,c=0 ve d=0'dır. Bu değerler Eş. 3.9'da yerine konulursa;

$$p2 + 1 + 0 + 0 = 1 \Rightarrow p2 = 1$$

$$p1 + 1 + 0 + 0 = 1 \Rightarrow p1 = 1 \qquad (3.10)$$

$$p0 + 1 + 1 + 0 = 0 \Rightarrow p0 = 0$$

bulunur. Kod kelimesi **p0 p1 a p2 b c d** sırasıyla yerleştirildiğinde, elde edilen (0111100) kod kelimesi Çizelge 3.3'te bulunmaktadır.

Çizelge 3.3. Hamming (7,4) kodunun oluşturulması

Ondalık sistem	**İkilik sistem Bilgi bitleri (abcd)**	**Hamming(7,4) p0p1ap2bcd 1 2 3 4 5 6 7**
0	0000	0000000
1	0001	1101001
2	0010	0101010
3	0011	1000011
4	0100	1001100
5	0101	0100101
6	0110	1100110
7	0111	0001111
8	1000	1110000
9	1001	0011001
10	1010	1011010
11	1011	0110011
12	1100	0111100
13	1101	1010101
14	1110	0010110
15	1111	1111111

Çizelge 3.3'te gösterilen H(7,4) kodunun D.K.M. aşağıda gösterildiği gibidir:

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \qquad (3.11)$$

3.10. Döngüsel Kodlar

GF(q) üzerindeki doğrusal bir koda;

$$(c_0, c_1, \ldots, c_{n-2}, c_{n-1})$$

kod kelimesi iken,

$$(c_1, c_2, \ldots, c_{n-1}, c_0)$$

de kod kelimesiyse, döngüsel kod denir (Hedeyat et al.,1999).

Bir kod, temel olarak bir kod kelimeleri kümesidir. Kodun türüne bağlı olarak, bir kod kelimesi bir vektör ya da polinom olarak yorumlanabilir. Bilindiği gibi, doğrusal bir kod D.K.M. ya da Ü.M. ile tanımlanabilir. Bir kod, elemanlarının döngüsel değişimleri (cyclic shifts) yine bir kod kelimesi ise döngüsel olarak adlandırılır ve üreteç polinomu ya da denklik kontrol polinomuna göre tanımlanır. Döngüsel bir kod, aynı zamanda doğrusaldır.

Döngüsel kodlar sonlu cisimler üzerindeki polinomlara dayanırlar ve basit kodlama işlemleri, halka teorisi yardımıyla yapılabilir (Pretzel,1992).

Teorem 3.10. g(x), ancak ve ancak x^n-1'i bölerse, n uzunluklu bir döngüsel kod için üreteç polinomudur (ikili döngüsel kodlar söz konusu olduğunda n tektir).

Teorem 3.11. Döngüsel bir (n,k,d) kodu için g(x) üreteç polinomu, her zaman aşağıdaki özelliklere sahip olacak şekilde seçilebilir.

a) g(x)'in derecesi n-k'dir

b) Baştaki g_{n-k}'nın katsayısı 1'dir.

c) g(x), GF(q) üzerinde x^n-1'i böler.

Bütün kelimelerin kümesi a(x)g(x) polinomlarından yararlanılarak gösterilir. Buradaki a(x), katsayıları GF(q)'dan olan bütün polinomlardır ve dereceleri k-1'i geçmez.

Bu özelliklere sahip tek bir üreteç polinomu vardır (Hedeyat et al.,1999).

Üreteç vektörünün;

$$g=(1110100) \tag{3.12}$$

olduğu varsayılsın. Bu durumda Ü.M. aşağıdaki gibi oluşturulur.

$$\mathbf{G}=\left|\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right| \begin{array}{l} \longrightarrow g_0+g_1x+g_2x^2+g_3x^3+g_4x^4+g_5x^5+g_6x^6 \\ \longrightarrow g_6x^6+g_0+g_1x+g_2x^2+g_3x^3+g_4x^4+g_5x^5 \\ \longrightarrow g_5x^5+g_6x^6+g_0+g_1x+g_2x^2+g_3x^3+g_4x^4 \end{array}$$

Teorem 3.12. C, g(x) üreteç polinomlu bir ikili döngüsel kodsa,

$$\mathbf{g(x)\ h(x)=x^n-1} \tag{3.13}$$

eşitliğini sağlar. h(x) polinomu, C'nin denklik kontrol polinomu olarak adlandırılır (Pretzel, 1992).

Bir kod döngüselse, duali de döngüseldir.

Teorem 3.13. C, GF(q) üzerinde n uzunluklu döngüsel bir kodsa ve üreteç polinomu da g(x) ise; $\mathbf{C}^{\perp}$ de döngüseldir ve Eş. 3.14'teki üreteç polinomuna sahiptir.

$$\mathbf{x^{n-1}/\tilde{g}(x)} \tag{3.14}$$

Burada,

$$\mathbf{\tilde{g}(x)=x^{deg(g)}\ g(x^{-1})} \tag{3.15}$$

g(x)'e karşılık gelen (reciprocal) polinomdur (Hedeyat et. al.,1999).

Eş.3.12'de verilen g üreteç polinomunun, $g(x)=1+x+x^2+x^4$, karşılık gelen polinomu; Eş.3.15'ten; $1+x^2+x^3+x^4$ olarak bulunur. Bu durumda dual kodun üreteç polinomu da Eş. 3.14'ten,

$$\frac{\mathbf{x^7-1}}{\mathbf{1+x^2+x^3+x^4}}=\mathbf{1+x^2+x^3}$$

dir.

3.11. Ağırlık Dağılımları ve Ağırlık Sayıları

Tanım 3.15. C bir (n,k,d) kodu ve A_i, C'de i ağırlıklı kod kelimelerinin sayısı ise, n+1 haneli $(A_0,A_1,...,A_n)$ vektörü, C'nin ağırlık dağılımı olarak adlandırılır. A_0 her zaman 1'e eşittir (Vanstone and Oorschot,1989).

C'nin ağırlık sayıları (enumerators) ise,

$$W_C(x,y) = \sum_{i=0}^{n} A_i \, x^{n-i} \, y^i \qquad (3.16)$$

dir. Bu, derecesi kodun uzunluğuna eşit, homojen bir polinomdur.

Uzaklığı d olan herhangi bir doğrusal kod için,

$$\sum_{i=0}^{n} A_i = n \text{ ve}$$

$$A_0 = 1$$

$$A_i = 0, \quad 1 \le i \le d-1 \text{ için}$$

dir (Vanstone and Oorschot,1989).

Kod doğrusalsa, dual kodun ağırlık sayıları için, Teorem 3.14'teki formül kullanılır.

Teorem 3.14. Bir (n,k,d) doğrusal C kodu için,

$$W_{C^\perp}(x,y) = \frac{1}{N} W_C(x+y, x-y) \qquad (3.17)$$

dir (Hedeyat et al.,1999).

4. DİKEY DİZİMLER VE KODLAR

Simetrik çok etkenliler için, kesirli çok etkenli tasarımlar, dikey dizimlerle yakından ilişkilidir. Elemanları q sembollü bir kümeye ait, k×N boyutlu B matrisi; B'nin her bir t×N alt matrisinde, her bir t×1 q sembollü sütun vektörü eşit sayıda görünüyorsa; k etkenli, N denemeli, q sembollü ve t güçlü bir dikey dizimdir.

k etkenli bir dikey dizimin k satırı tanımlanırsa; dikey dizimin sütunları, N denemeli bir q^k çok etkenlisinin denemelerini oluşturur (Dey, 1985).

Tanım 4.1. Bir dikey dizimin denemeleri farklıysa, basit (simple) olarak adlandırılır.

Tanım 4.2. q bir asal kuvvet olsun. Düzeyleri GF(q)'da olan bir OA(N,n,q,t) dikey dizimi basitse ve GF(q)'dan alınan n-haneli N denemesi, GF(q) üzerinde bir vektör uzayı oluşturuyorsa, doğrusaldır.

Doğrusal dikey dizimler, dikey dizimlerin sahip olmadığı 2 avantaja sahiptir:

i) Basit bir tanıma sahiptirler: Satırlarından oluşturulan vektör uzayı için bir temel vermek yeterlidir. Bu temel genellikle, satırları temel olan k×n boyutlu Ü.M. (Bkz. Eş. 3.1) biçiminde verilir.

ii) $u_1,u_2,\ldots,u_k$ Ü.M.nin satırları olduğunda, doğrusal birleşimlerin bütün kümesi,

$$c_1,\ldots,c_k \in GF(q) \qquad c_1u_1,\ldots,c_ku_k$$

dikey dizimin denemelerini oluşturur.

Bir dikey dizim doğrusalsa, doğrusal bir hata düzeltme kodundaki kod kelimelerini denemelerin birleşimi olarak değerlendirmek mümkündür (Hedeyat et al,1999).

Teorem 4.1. Bir kodla ilişkili dikey dizim, yalnız ve yalnız kod doğrusalsa, doğrusaldır.

Teorem 4.2. C, GF(q) üzerinde $\mathbf{d}^{\perp}$ dual uzaklıklı bir (n,k,d) doğrusal kodu ise, C'nin kod kelimeleri, elemanları GF(q)'dan olan bir OA($N=q^k$,n,q,$\mathbf{d}^{\perp}-\mathbf{1}$) dikey diziminin satırlarını oluşturur. Sonuç olarak, GF(q) üzerindeki doğrusal bir OA($N=q^k$,n,q,t)'nin satırları, $\mathbf{d}^{\perp} \geq \mathbf{t}+\mathbf{1}$ dual uzaklıklı bir (n,k,$\mathbf{d}^{\perp}$) kodu oluşturur.

Dikey dizimin gücü t ise, $\mathbf{d^{\perp} = t + 1}$'dir (Brouwer et al.,2003; Hedeyat et al.,1999).

Kodlar ve dikey dizimler arasındaki ilişki aşağıdaki cümleyle özetlenebilir: İyi bir hata düzeltme kodu, birbirlerinden uzaklıkları mümkün olduğunca büyük olan, verilen uzunluktaki vektörlerin büyük bir kümesidir. İyi bir dikey dizim, dual uzaklığı mümkün olduğunca büyük olan, verilen uzunluktaki vektörlerin küçük bir kümesidir (Pless 1998,Hedeyat et al.,1999).

5. KESİRLİ ÇOK ETKENLİ TASARIMLAR VE KODLAR

Dikey dizimlerle kesirli çok etkenli tasarımlar ve dikey dizimlerle kodlar arasındaki ilişki bilinmektedir. Kesirli çok etkenli tasarımlarla kodlar arasında ilişki olduğunu düşündüren çalışma, Franklin(1984)'in en az sapma ve optimal moment tasarımlarına ilişkin makalesidir. Burada, bir p^{n-m} tasarımı için; m=3 ve n [4-7] arasında olduğunda, aşağıdaki tam Ü.M. önerilmiştir. Ancak Ü.M. olarak adlandırılmasına karşın, H(7,4) Hamming kodunun D.K.M.ne eşittir (Bkz.Eş. 3.11).

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

Hamming kodlarının incelenmesi sırasında (Bkz. Bölüm 3.9.1), n-k tane denklik bitinin, kesirli çok etkenli tasarımları oluştururken kullandığımız ek etkenler ve k tane bilgi bitinin de temel etkenler olarak düşünülebileceği görülmüştür. Önerme 3.2'den D.K.M.nin boyutunun $(n-k)\times n$ olduğu bilinmektedir. Bu durumda, kodu oluşturan n-k eşitliğin katsayılarını veren bu matris; kesirli çok etkenli tasarımlar söz konusu olduğunda, tasarımın tanımlayıcı bağıntılarını gösteren matris olarak düşünülebilir.

Rao(1946), N denemeli, k etkenli, q sembollü ve (t+m+1) güçlü bir dikey dizimin, m etkileşime kadar tüm etkileşimlerin dik olarak tahmin edilebildiği (daha fazla etkenli etkileşimlerin sıfır olduğu varsayımı altında) bir kesirli çok etkenli tasarıma eşit olduğunu kanıtlamıştır. Bu nedenle, 2 güçlü bir dikey dizim simetrik çok etkenliler için dik ana-etki tasarımlarına; 3 güçlü bir dikey dizim Ç-IV tasarımlarına eşittir.

Dikey dizimin gücüyle, bir (n,k,d) kodunun dualinin en kısa uzaklığı, $d^{\perp}$, arasında ilişki olduğu bilinmektedir (Bkz. Teorem 4.2). Dikey dizimin gücüyle, $d^{\perp}$ arasında kurulan ilişki, kesirli çok etkenli tasarımın çözümü ile $d^{\perp}$ arasında da kurulabilmektedir.

Teorem 3.4 (b)'den, C için D.K.M.nin, $\mathbf{C}^{\perp}$ için Ü.M. olduğu bilinmektedir. D.K.M., kesirli çok etkenli tasarım için tanımlayıcı bağıntıları gösteriyorsa, bu matrisin satırları temel olarak alındığında; elde edilen kod kelimelerinin, tasarım için tanımlayıcı bağıntı yapısını vermesi gerekir.

Bölüm 2.2.'de en az sapma ölçütüne göre tasarımları karşılaştırırken kullanılan kelime uzunlukları yapıları, kodlar söz konusu olduğunda Tanım 3.15'te verilen ağırlık dağılımlarıdır.

Kod kelimelerinin bulunması ve en kısa uzaklıkların hesaplanmasında, MATLAB 6.5'da var olan fonksiyon ve komutlardan yararlanılmıştır.

Hangi tasarımların inceleneceği konusunda, Box, Hunter ve Hunter (1978) tarafından oluşturulan ve en yüksek çözüme sahip tasarımları gösteren çizelge (Bkz. Ek-1) temel olarak alınmış ve sadece, bazı tasarımlar için ayrıntıya girilmiştir.

5.1. 2_{III}^{3-1} Tasarımı

Tanımlayıcı bağıntısı I=ABC olan 2_{III}^{3-1} kesirli çok etkenli tasarımı Çizelge 5.1'de gösterilmektedir.

Çizelge 5.1. 2_{III}^{3-1} Tasarımı (I=ABC)

a	b	c=a+b	Denemeler
0	0	0	000
0	1	1	011
1	0	1	101
1	1	0	110

Çizelge 5.1'deki denemeleri kod kelimeleri olarak düşünürsek; örneğin, 011 kod kelimesi iken, 101 de kod kelimesi olduğundan, denemelere karşılık gelen kodun, döngüsel olduğu görülmektedir (Bkz. Bölüm 3.10).

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{matrix} \Rightarrow \begin{matrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{matrix} \Rightarrow \text{döngüsel}$$

Kod kelimeleri arasındaki en kısa Hamming uzaklığı d=2'dir (Bkz. Tanım 3.4). Döngüsel bir koda karşılık geldiklerine göre, kod kelimelerinin üreteç polinomundan oluşturulması ve Eş. 3.12'den, üreteç polinomu ile denklik kontrol polinomunun çarpımının x^n-1'e eşit olması gerekmektedir.

2_{III}^{3-1} tasarımı söz konusu olduğunda;

$$\mathbf{H} = [1 \quad 1 \quad 1]_{1\times 3} \qquad \rightarrow \ 1+x+x^2 \tag{5.1}$$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{2\times 3} \rightarrow \ 1+x \tag{5.2}$$

dir. Görüldüğü gibi, H D.K.M, I=ABC tanımlayıcı bağıntısının polinom olarak gösterimidir. Eş. 3.12'den;

$$\mathbf{x}^3 - 1 = (1+\mathbf{x})(1+\mathbf{x}+\mathbf{x}^2)$$

dir. Tanım 3.11'den, G Ü.M.inin satırları, C'nin temelleridir. Bu temeli X ile gösterirsek;

X= { (101),(011) }

olarak yazabiliriz. Bu temellerden elde edilen kod kelimeleri; aynı zamanda, tasarımın denemeleridir:

0(101)+0(011)=000

0(101)+1(011)=011

1(101)+0(011)=101

1(101)+1(011)=110

Denemeleri elde etmek için diğer bir yol, Örnek 2.1'de (Bkz. Bölüm 2.4.1) GF(2^2) için oluşturulan güç döngüsü ile, G Ü.M.ni çarpmaktır.

$$\mathbf{P} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \times \mathbf{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

G Ü.M., k×n, 2×3 boyutlu olduğundan ve kodun döngüsel olduğu bilindiğinden, denemelerin karşılık geldiği kod; döngüsel (3,2) kodudur.

(3,2) döngüsel kodunun duali, Teorem 3.4. (a)'dan (3,1,3) döngüsel kodudur. Teorem 3.13'ten, üreteç polinomu; $\tilde{\mathbf{g}}(\mathbf{x}) = \mathbf{x}^{\deg(\mathbf{g})}\,\mathbf{g}(\mathbf{x}^{-1})$ iken $\mathbf{x}^{\mathbf{n}-1} / \tilde{\mathbf{g}}(\mathbf{x})$'dir.

Buradan, $\tilde{\mathbf{g}}(\mathbf{x}) = \mathbf{x}.\mathbf{g}(\mathbf{x}^{-1}) = \mathbf{x}\left(1+\frac{1}{\mathbf{x}}\right) = \mathbf{x}+1$ ve üreteç polinomu da

$\mathbf{x}^{n-1} / \bar{\mathbf{g}}(\mathbf{x}) = \mathbf{x}^3 - 1 / \mathbf{x} + 1 = 1 + \mathbf{x} + \mathbf{x}^2$'dir.

Teorem 3.4 (b)'den, C için D.K.M., $\mathbf{C}^{\perp}$ için Ü.M. olduğundan; dual kodun, (3,1) döngüsel kodunun, Ü.M.; Eş. 5.1'deki H D.K.M.'dir.

$$\mathbf{G_{dual}} = [1 \quad 1 \quad 1]_{1\times 3}$$

Dual kodun Ü.M.nden elde edilen kod kelimeleri, 0.111=000 ve 1.111=111 olduğundan; (2^2-1,2^2-2-1,3) Hamming (3,1) kodudur (Bkz. Bölüm 3.9).

$$\mathbf{C}^{\perp} = \{(000), (111)\} \rightarrow H(3,1) \qquad (5.3)$$

Teorem 3.3'ten en kısa Hamming uzaklığı, $d^{\perp}$=3 olduğundan, 2^{3-1} tasarımının çözümü III'tür (Bkz. Teorem 4.2). Dual kodun 0'lardan oluşan kod kelimesi dışındaki kelimesi 111'dir ve I=ABC tanımlayıcı bağıntı yapısına karşılık gelir. Bir tasarım, çözümü ile ifade edildiğinden, 2^{3-1}_{III} tasarımının kod olarak karşılığı, (3,2,$d^{\perp}$=3)'tür.

Dual kodun ağırlık dağılımı, Tanım 3.15'ten,

$$\{1,0,0,1\}^{\perp} \qquad (5.4)$$

dir.

Dual kodun tanımı gereği (Bkz. Bölüm 3.8.3), dualin kod kelimelerinin, (3,2) döngüsel kodunun kod kelimelerine dik olması gerekmektedir. Dualdeki kod kelimelerini, koddaki kelimelerle tek tek çarpmak yerine, matris gösterimi tercih edilirse; dualin kod kelimelerini gösteren matrisin, denemelerin devriği ile çarpımı, diklik koşulunun sağlanıp sağlanmadığını gösterecektir.

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}^{\mathbf{T}} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Görüldüğü gibi, diklik koşulu sağlanmaktadır.

Tasarımların eşdeş yapısı da bulunmak istenirse; bu durumda, tahmin edilecek etkilerin vektörlerle ifade edilmesi, örneğin A etkisi için (100), ve Eş. 5.1'deki

D.K.M. ile toplanması gerekmektedir.

Önerme 2.7'den, (3,2) kodunun Ü.M.ndeki temeller ile H(3,1) kodunun Ü.M.ndeki temellerin birleşimi U vektör uzayının temellerini oluşturursa, tümleyendirler.

(3,2) kodunun Ü.M. $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{2\times 3}$ ve duali H(3,1) kodunun Ü.M. $\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}_{1\times 3}$'in temellerinin birleşimi;

$$\mathbf{G_{birleşim}} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

dir ve bu matrisin temellerinden oluşan denemeler 2^3 tamamlanmış çok etkenli tasarımının denemeleridir.

Teorem 2.9'dan C ve $C^{\perp}$'in tümleyen olabilmesi için, boyutlarının toplamının U'nun boyutları toplamına eşit olması ve C ve $C^{\perp}$'in kesişimlerinin {0} vektörü olması gerektiği bilinmektedir.

Bir vektör uzayının ya da alt uzayının boyutu Önerme 2.3'ten temelindeki vektör sayısıdır. C'nin temelindeki vektör sayısı 2 ve $C^{\perp}$'in temelindeki vektör sayısı 1 olduğuna göre, U uzayının üreteç matrisi $G_{birleşim}$'de 3 temel olmalıdır. Görüldüğü gibi koşul sağlanmaktadır. Ayrıca, $C \cap C^{\perp} = \{0\}$'dır.

Sonuç olarak (3,2) ve H(3,1) kodunun temellerinin birleşimleri 2^3 tamamlanmış çok etkenli tasarımını oluşturur.

5.2. 2_{IV}^{4-1} Tasarımı

Çizelge 5.2'de gösterilen 2_{IV}^{4-1} tasarımı, kod kelimeleri döngüsel kod tanımına uymasına karşın, n=4 çift olduğundan, (Bkz. Teorem. 3.10), üreteç polinomundan oluşturulamamaktadır. Döngüsel kodlar, aynı zamanda doğrusal olduklarından, bu durum sorun çıkarmamaktadır.

Artık H D.K.M.nin tasarımın tanımlayıcı bağıntı yapısını verdiği bilinmektedir. Bu durumda H;

$$\mathbf{H} = [1 \quad 1 \quad 1 \quad 1]_{1\times 4} \tag{5.5}$$

olacaktır.

Çizelge 5.2. 2_{IV}^{4-1} Tasarımı (I=ABCD)

a	b	c	d=a+b+c	Denemeler
0	0	0	0	0000
0	0	1	1	0011
0	1	0	1	0101
0	1	1	0	0110
1	0	0	1	1001
1	0	1	0	1010
1	1	0	0	1100
1	1	1	1	1111

Önerme 3.2'den, G= [I_k A] ve H= [$-A^T$ I_{n-k}]'dır. Eş. 5.5'teki H matrisinden elde edilen G Ü.M.;

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}_{3\times 4}$$

dir. G ve H matrislerinin boyutlarına bakarak denemelerin (4,3) doğrusal koduna karşılık geldiğini söyleyebiliriz. G Ü.M.nden elde edilen kod kelimeleri;

0 0 0 0

0 0 1 1

0 1 0 1

0 1 1 0

1 0 0 1

1 0 1 0

1 1 0 0

1 1 1 1

2_{IV}^{4-1} tasarımının denemelerine karşılık gelmektedir. Tanım 3.4 (b)'den, (4,3) doğrusal kodunun dualinin Ü.M., Eş. 5.5'teki D.K.M.'dir.

$$\mathbf{G_{dual}} = [1 \quad 1 \quad 1 \quad 1] \tag{5.6}$$

Dualin,(4,1,4) doğrusal kodunun kod kelimeleri:

0.1111=0000

1.1111=1111 $\rightarrow$ $\mathbf{d^{\perp}=}$ 4 ve I=ABCD'dir.

Dolayısıyla 2_{IV}^{4-1} tasarımı, (4,3,$d^{\perp}$=4) koduna karşılık gelmektedir. Dual kodun ağırlık dağılımı, $\{1,0,0,1\}^{\perp}$'dir. Dualin kod kelimeleri ile kod kelimeleri arasında diklik koşulu sağlanmaktadır.

5.2.1. 2_{III}^{4-1} Tasarımı

Çizelge 5.3. 2_{III}^{4-1}Tasarımı (I=BCD)

a	b	c	d=b+c	Denemeler
0	0	0	0	0000
0	0	1	1	0011
0	1	0	1	0101
0	1	1	0	0110
1	0	0	0	1000
1	0	1	1	1011
1	1	0	1	1101
1	1	1	0	1110

2_{III}^{4-1} tasarımının tanımlayıcı bağıntısı I=BCD olduğuna göre, denemelerin karşılık geldiği kodun kod kelimeleri Eş. 5.7 ve Eş. 5.8'deki D.K.M. ve Ü.M.nden oluşturulabilir.

$$\mathbf{H}=\begin{bmatrix}0 & 1 & 1 & 1\end{bmatrix}_{1\times 4} \tag{5.7}$$

$$\mathbf{G}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\end{bmatrix}_{3\times 4} \tag{5.8}$$

H ve G matrislerinin boyutlarına bakarak, temsil ettikleri kodun (4,3) kodu olduğunu; denemelere bakarak da bunun doğrusal bir kod olduğunu söyleyebiliriz (Bkz. Tanım 3.7).

Bölüm 2.4.1, Örnek 2.2'deki GF(2^3) için oluşturulan güç döngüsü kullanılarak kod kelimelerine ulaşılabilir.

$$\mathbf{P}=\begin{bmatrix}0&0&0\\0&0&1\\0&1&0\\0&1&1\\1&0&0\\1&0&1\\1&1&0\\1&1&1\end{bmatrix}\times\mathbf{G}=\begin{bmatrix}1&0&0&0\\0&1&0&1\\0&0&1&1\end{bmatrix}=\begin{bmatrix}0&0&0&0\\0&0&1&1\\0&1&0&1\\0&1&1&0\\1&0&0&0\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix}$$

Kod kelimeleri (4,3) doğrusal koduna karşılık gelmektedir ve en kısa Hamming uzaklığı d=2'dir.

Tasarımın çözümünü bulmak için, (4,3)'ün dualini bulmamız gerekmektedir. Tanım 3.4 (b)'den, dualin Ü.M.;

$$\mathbf{G_{dual}}=\begin{bmatrix}0&1&1&1\end{bmatrix}_{1\times4} \qquad (5.9)$$

ve kod kelimeleri de $\{1,0,0,1,0\}^{\perp}$ ağırlık dağılımına sahiptir.

0.0111=0000

1.0111=0111

$\mathbf{d^{\perp}=}3$ ve I=BCD olduğundan; 2_{III}^{4-1} tasarımının kod olarak karşılığı, (4,3, $\mathbf{d^{\perp}=}3$)'tür. Dualin kod kelimeleri ile kod kelimeleri arasında diklik koşulu sağlanmaktadır.

5.3. 2_V^{5-1} Tasarımı

2_V^{5-1} tasarımı, I=ABCDE tanımlayıcı bağıntılı bir yarı tekrardır. Şimdiye kadar oluşturulan iki yarı tekrardan anlaşıldığı üzere; n=5 tek olduğundan, 2_V^{5-1} tasarımının döngüsel bir koda karşılık geleceği söylenebilir.

Eş. 3.12'den;

$$x^{5-1}=(1+x)(1+x+x^2+x^3+x^4)$$

dir ve üreteç polinomu ile denklik kontrol polinomunun çarpımından oluşmaktadır.

Çizelge 5.4. 2_V^{5-1} Tasarımı (I=ABCDE)

a	b	c	d	e=a+b+c+d	Denemeler
0	0	0	0	0	00000
0	0	0	1	1	00011
0	0	1	0	1	00101
0	0	1	1	0	00110
0	1	0	0	1	01001
0	1	0	1	0	01010
0	1	1	0	0	01100
0	1	1	1	1	01111
1	0	0	0	1	10001
1	0	0	1	0	10010
1	0	1	0	0	10100
1	0	1	1	1	10111
1	1	0	0	0	11000
1	1	0	1	1	11011
1	1	1	0	1	11101
1	1	1	1	0	11110

Denemelerin karşılık geldiği kodun kod kelimeleri Eş. 5.10 ve Eş. 5.11'deki D.K.M. ve Ü.M.nden oluşturulabilir.

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}_{1\times 5} \qquad \rightarrow (1+x+x^2+x^3+x^4) \tag{5.10}$$

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \rightarrow 1+x \Rightarrow \mathbf{G}_{\mathbf{I_k A}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{4\times 5} \tag{5.11}$$

Eş. 5.10'daki iki matris kullanılarak da kod kelimelerine ulaşılabilir ve iki matristen elde edilecek kod kelimeleri aynıdır; ancak, gösterim olarak standart biçim benimsenmiştir.

Standart biçime getirilmiş Ü.M.inin satırlarından yararlanılarak bulunan (5,4) kodunun kod kelimeleri döngüseldir ve en kısa uzaklık d=2'dir.

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

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

$C^{\perp}$ için $\frac{x^5-1}{1+x} = 1+x+x^2+x^3+x^4$ üreteç polinomu ve Ü.M. de

$$\mathbf{G_{dual}} = [1 \quad 1 \quad 1 \quad 1 \quad 1] \tag{5.12}$$

dir. Dualin kod kelimeleri:

0.11111 =00000

1.11111=11111

ve ağırlık dağılımı $\{1,0,0,0,0,1\}^{\perp}$ 'dir.

$d^{\perp}=5$ ve I=ABCDE olduğundan; 2_V^{5-1} tasarımının kod olarak karşılığı, (5,4, $d^{\perp}=5$)'dir. Kod kelimeleri 2 ve 4 ağırlığındaki kelimelerden oluştuğuna göre, dualin kod kelimeleri ile kod kelimeleri arasında diklik koşulunun sağlandığını doğrudan söyleyebiliriz.

5.4. 2_{III}^{5-2} Tasarımı

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{2\times 5} \tag{5.13}$$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}_{3\times 5} \tag{5.14}$$

D.K.M. ve Ü.M.ne sahip kod, Çizelge 5.5'teki 2_{III}^{5-2} tasarımının denemelerine karşılık gelmektedir.

Çizelge 5.5. 2_{III}^{5-2} Tasarımı (I=ABD=ACE)

a	b	C	d=a+b	e=a+c	Denemeler
0	0	0	0	0	00000
0	0	1	0	1	00101
0	1	0	1	0	01010
0	1	1	1	1	01111
1	0	0	1	1	10011
1	0	1	1	0	10110
1	1	0	0	1	11001
1	1	1	0	0	11100

G Ü.M.nden elde edilen kod kelimeleri:

0 0 0 0 0

0 0 1 0 1

0 1 0 1 0

0 1 1 1 1

1 0 0 1 1

1 0 1 1 0

1 1 0 0 1

1 1 1 0 0

Çizelge 5.5'teki denemelerle aynıdır ve kod olarak karşılıkları, en kısa uzaklığı d=2 olan (5,3) doğrusal kodudur.

Tanım 3.4 (b)'den, Dualin Ü.M.i (5,3) kodunun D.K.M. olacaktır.

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{2\times 5} \tag{5.15}$$

Dualdeki kod kelimeleri de

$$\begin{aligned} &0(11010)+0(10101)=0\ 0\ 0\ 0\ 0 \\ &0(11010)+1(10101)=1\ 0\ 1\ 0\ 1 \rightarrow \text{I=ACE} \\ &1(11010)+0(10101)=1\ 1\ 0\ 1\ 0 \rightarrow \text{=ABD} \\ &1(11010)+1(10101)=0\ 1\ 1\ 1\ 1 \rightarrow \text{=BCDE} \end{aligned} \tag{5.16}$$

dir. Dualin ağırlık dağılımı;

$$\{1,0,0,2,1,0\}^{\perp} \tag{5.17}$$

ve $\mathbf{d^{\perp}=3}$'tür. I=ACE=ABD=BCDE tanımlayıcı bağıntı yapısına sahip 2_{III}^{5-2} tasarımının kod olarak karşılığı, (5,3, $\mathbf{d^{\perp}=3}$)'tür.

5.5. 2_{VI}^{6-1} Tasarımı

Tasarımın tanımlayıcı bağıntısı I=ABCDEF olduğunda, kodun D.K.M.;

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}_{1\times 6} \tag{5.18}$$

ve Ü.M.;

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{5\times 6} \tag{5.19}$$

dir.

Ü.M.inden yararlanılarak bulunan kod kelimeleri:

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

dir ve (6,5) doğrusal koduna karşılık gelmektedir. $C^{\perp}$ için Ü.M.;

$$\mathbf{G_{dual}} = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] \tag{5.20}$$

dir. Dual kodun, (6,1), kod kelimeleri:

0.111111=000000

1.111111=111111

ve $d^{\perp}$=6'dır. Dualin kod kelimelerinden I=ABCDEF olduğu görülmektedir. Bu durumda 2_{VI}^{6-1} tasarımının kod olarak ifadesi; (6,5, $d^{\perp}$=6)'dır. Ağırlık dağılımı ise, $\{1,0,0,0,0,0,1\}^{\perp}$'dir. Bütün tasarımlar için olduğu gibi, burada da dualin kod kelimeleri ile kod kelimeleri arasındaki diklik koşulu sağlanmaktadır.

5.6. 2_{IV}^{6-2} Tasarımı

Çizelge 5.6 2_{IV}^{6-2} Tasarımı (I=ABCE=BCDF)

a	b	c	d	e=a+b+c	f=b+c+d	Denemeler
0	0	0	0	0	0	000000
0	0	0	1	0	1	000101
0	0	1	0	1	1	001011
0	0	1	1	1	0	001110
0	1	0	0	1	1	010011
0	1	0	1	1	0	010110
0	1	1	0	0	0	011000
0	1	1	1	0	1	011101
1	0	0	0	1	0	100010
1	0	0	1	1	1	100111
1	0	1	0	0	1	101001
1	0	1	1	0	0	101100
1	1	0	0	0	1	110001
1	1	0	1	0	0	110100
1	1	1	0	1	0	111010
1	1	1	1	1	1	111111

Tasarımın tanımlayıcı bağıntıları H D.K.M.nin satırlarına karşılık geldiğine göre;

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}_{2\times 6} \tag{5.21}$$

ve Ü.M. de

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}_{4\times 6} \tag{5.22}$$

dir. P=[0 0 0 0;0 0 0 1;0 0 1 0;0 0 1 1;0 1 0 0;0 1 0 1;0 1 1 0;0 1 1 1;1 0 0 0;1 0 0 1;1 0 1 0;1 0 1 1;1 1 0 0;1 1 0 1;1 1 1 0;1 1 1 1], GF(2^4)'ün güç döngüsünü göstermek üzere (Bkz. Örnek 2.3), P×G'den elde edilen kod kelimeleri;

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

d=2 olan (6,4) doğrusal koduna karşılık gelmektedir.

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}_{2\times 6} \tag{5.23}$$

ve Pdual=[0 0;0 1;1 0;0 1], GF(2^2)'nin güç döngüsünü olmak üzere (Bkz. Örnek 2.1);

Eş. 5.23'teki Ü.M.nden elde edilen dual kodun kod kelimeleri:

$$\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1\rightarrow \text{I=BCDF} \\ 1 & 1 & 1 & 0 & 1 & 0\rightarrow \text{ =ABCE} \\ 1 & 0 & 0 & 1 & 1 & 1\rightarrow \text{ =ADEF} \end{array} \qquad (5.24)$$

$d^{\perp}$=4 ve ağırlık dağılımı;

$$\{1,0,0,0,3,0,0\}^{\perp} \qquad (5.25)$$

olan (6,2,4) doğrusal koduna karşılık gelmektedir. Tasarımın karşılık geldiği kod ise, (6,4, $d^{\perp}$=4)'tür ve diklik koşulu sağlanmaktadır.

5.6.1. 2_{III}^{6-2} Tasarımı: en az sapma ölçütüne göre I. en iyi tasarım

2^{6-2}, literatürde en az sapma ölçüte göre sıralanmış tasarımlardan biridir (Wu and Chen,1992). Öncelikle, en az sapma ölçütüne göre sıralanmış tasarımların kod olarak karşılıkları bulunmuştur.

Çizelge 5.7. 2_{III}^{6-2} Tasarımı (I=ABE=BCDF)

a	b	c	d	e=a+b	f=b+c+d
0	0	0	0	0	0
0	0	0	1	0	1
0	0	1	0	0	1
0	0	1	1	0	0
0	1	0	0	1	1
0	1	0	1	1	0
0	1	1	0	1	0
0	1	1	1	1	1
1	0	0	0	1	0
1	0	0	1	1	1
1	0	1	0	1	1
1	0	1	1	1	0
1	1	0	0	0	1
1	1	0	1	0	0
1	1	1	0	0	0
1	1	1	1	0	1

Tasarımın tanımlayıcı bağıntılarından elde edilen D.K.M. Eş. 5.26'da verilmektedir.

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}_{2\times 6} \tag{5.26}$$

ve Önerme 3.2'den yararlanarak H'den elde edilen Ü.M.;

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}_{4\times 6} \tag{5.27}$$

dir. GF(2^4) cisminin güç döngüsü ile G'nin çarpımından elde edilen kod kelimeleri;

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

en kısa uzaklığı, d=2, olan (6,4) doğrusal koduna karşılık gelmektedir.

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}_{2\times 6} \tag{5.28}$$

ve dualin kod kelimeleri de;

0	0	0	0	0	0
0	1	1	1	0	$1\rightarrow$ I=BCDF
1	1	0	0	1	$0\rightarrow$ =ABE
1	0	1	1	1	$1\rightarrow$ =ACDEF

(5.29)

dir.

Dualin karşılık geldiği kod; ağırlık dağılımı;

$$\{1,0,0,1,1,1,0\}^{\perp} \tag{5.30}$$

olan (6,2,$d^{\perp}$=3) doğrusal kodudur. Bu durumda, 2_{III}^{6-2} 1. en iyi tasarım(en az sapma ölçütüne göre), aynı zamanda, (6,4, $d^{\perp}$=3) doğrusal kodudur.

Duallik için gereken diklik koşulu sağlanmaktadır.

5.6.2. 2_{III}^{6-2} Tasarımı: en az sapma ölçütüne göre II. en iyi tasarım

En az sapma ölçütüne göre III. en iyi tasarımın tanımlayıcı bağıntıları;

I=ABE=CDF ve D.K.M.;

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{2\times 6} \tag{5.31}$$

dir. Önerme 3.2'den yararlanarak, H D.K.M.nden bulunan Ü.M.;

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}_{4\times 6} \tag{5.32}$$

dir. G'nin satırlarındaki temellerden yararlanarak elde edilen kod kelimeleri;

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

d=2 uzaklıklığına sahip bir (6,4) doğrusal koduna aittir. Kodun Ü.M., dualin D.K.M. olduğuna göre;

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \tag{5.33}$$

Ü.M.nden elde edilen kod kelimeleri tasarımın tanımlayıcı bağıntı yapısıdır:

$$
\begin{array}{cccccc}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 \rightarrow \text{ I=CDF} \\
1 & 1 & 0 & 0 & 1 & 0 \rightarrow \text{ =ABE} \\
1 & 1 & 1 & 1 & 1 & 1 \rightarrow \text{ =ABCDEF}
\end{array}
\tag{5.34}
$$

2_{III}^{6-2} III. en iyi tasarımı;

$$\{1,0,0,2,0,0,1\}^{\perp} \tag{5.35}$$

ağırlık dağılımına sahip, bir (6,2, $d^{\perp}$=3) kodudur ve diklik koşulu sağlanmaktadır.

5.6.3. 2_{III}^{6-2} Tasarımı: en az sapma ölçütüne göre III. en iyi tasarım

I=ABE=ABDF olmak üzere, H D.K.M ve G Ü.M.;

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{2\times 6} \tag{5.36}$$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}_{4\times 6} \tag{5.37}$$

dir. G Ü.M.nden yararlanarak elde edilen kod kelimeleri;

$$
\begin{array}{cccccc}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

1 0 0 1 1 0

1 0 1 0 1 1

1 0 1 1 1 0

1 1 0 0 0 0

1 1 0 1 0 1

1 1 1 0 0 0

1 1 1 1 0 1

d=1 olan (6,4) doğrusal koduna karşılık gelmektedir. Teorem 3.4(b)'den,

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{2\times 6} \tag{5.38}$$

ve dualin kod kelimeleri de;

0 0 0 0 0 0

1 1 0 1 0 $1\rightarrow$ I=ABDE

1 1 0 0 1 $0\rightarrow$ =ABE (5.39)

0 0 0 1 1 $1\rightarrow$ =DEF

$d^{\perp}$=3 ve ağırlık dağılımı;

$$\{1,0,0,2,1,0,0\}^{\perp} \tag{5.40}$$

olan, bir (6,2,3) doğrusal koduna karşılık gelmektedir. Tasarım ise, (6,4, $d^{\perp}$=3) kodudur ve diklik koşulu sağlanmaktadır.

5.6.4. 2_{III}^{6-2} Tasarımlarının karşılaştırılması

Bilindiği gibi, en az sapma ölçütüne göre en iyi tasarımı belirlemek için tanımlayıcı bağıntı yapısındaki kelime uzunluklarına bakılır ve en yüksek çözümü en az yapan tasarım, en az sapma tasarımı olarak seçilir.

Çizelge 5.8'de, Wu ve Chen(1992)'in 2_{III}^{6-2} tasarımı için I. en iyi tasarım dedikleri tasarımın kelime uzunluğu yapısı, {3,4,5}'tir. Diğer iki tasarımla karşılaştıracak olursak; yalnızca 1. en iyi tasarımda, en yüksek çözüm 3 uzunluğunda 1 kelime

vardır. Diğer iki tasarımda 3 uzunluğunda 2 kelime olduğundan, 1. en iyi tasarım, en yüksek çözüm uzunluğundaki kelime sayısını en az yapmıştır; dolayısıyla, en az sapma ölçütü söz konusu olduğunda, diğer iki tasarıma göre **daha iyi** bir tasarım ve üç tasarım arasında **en iyi** tasarımdır.

Buradaki amacımız, kodlardan yararlanarak en iyi tasarıma karar verebilmektir. Çizelge 5.8'de tasarımların kodlarla ifade edildiği satırlara baktığımızda, bütün tasarımların (6,4) koduna karşılık geldiğini ve parametrelerinin; n,k,d,$d^{\perp}$, eşit olduğu görülmektedir.

Çizelge 5.8. 2^{6-2}_{III} Tasarımlarının karşılaştırılması

	I. En İyi Tasarım	**II. En İyi Tasarım**	**III. En İyi Tasarım**
T.B. yapısı	I=ABE=BCDF =ACDEF	I=ABE=CDF =ABCDEF	I=ABE=ABDF =DEF
Kelime uzunluğu yapısı	{3,4,5}	{3,3,6}	{3,3,4}
(n,k) kodu	(6,4)	(6,4)	(6,4)
Rank G	4	4	4
d	2	2	2
Rank $G^{\perp}$	2	2	1
$d^{\perp}$	3	3	3
Ağırlık dağılımı	{1,0,4,6,3,2,0}	{1,0,6,0,9,0,0}	{1,1,2,6,5,1,0}
$A^{\perp}_i$ dağılımı- i=Çmax,...,6	{1,1,1,0}	{2,0,0,1}	{2,1,0,0}

Tasarımların ağırlık dağılımları söz konusu olduğunda, üç tasarımın da kendilerinin ve duallerinin dağılımları farklı olduğundan; en iyi tasarıma karar verebilmek için bu sayıların kullanılabileceği düşünülmüştür.

Dual kodun en kısa uzaklığı tasarımın çözümünü verdiğine göre, Çizelge 5.8'de dual kodun ağırlık dağılımında, ağırlık değerleri ≥$Ç_{max}$ olmalıdır (2^{6-2} için 3). Aynı mantıkla, dual kod, en az sapma tasarımına karar verirken de belirleyici olmalıdır. Bilindiği gibi, dual koddaki kod kelimeleri, tasarımın tanımlayıcı bağıntı yapısını vermektedir. Çizelge 5.8'de 1. en iyi,…,3.en iyi olarak sınıflandırılan tasarımlarla, karşılık geldikleri kodların dualleri arasındaki ilişki Çizelge 5.9'da gösterilmiştir.

Çizelge 5.9. 2^{6-2}_{III} –(6,4) Kodlarının duallerine göre karşılaştırılması

	I. En İyi Tasarım	**II. En İyi Tasarım**	**III. En İyi Tasarım**
T.B. yapısı	I=ABE=BCDF =ACDEF	I=ABE=CDF =ABCDEF	I=ABE=ABDF =DEF
(n,k) kodu	(6,4)	(6,4)	(6,4)
$d^{\perp}_{min}$	3	3	3
$A^{\perp}_i$ dağılımı-i=Çmax,...,6	{1,1,1,0}	{2,0,0,1}	{2,1,0,0}
Dual kodu	(6,2)	(6,2)	(6,2)
Dualdeki kod kelimeleri-{0}	011101 :BCDF 110010 :ABE 101111:ACDEF	001101 :CDF 110010 :ABE 111111:ABCDEF	110101 :ABDF 110010 :ABE 000111 :DEF

Görüldüğü gibi, kodun dualindeki kod kelimelerinden yararlanarak tasarımların tanımlayıcı bağıntı yapısına ulaşabilir; dualin ağırlık dağılımlarından, $A^{\perp}_i$, yararlanarak tasarımlar 1. en iyi, 2. en iyi vb. olarak sıralanabilmektedir.

I. En iyi tasarım	**II. En iyi tasarım**	**III. En iyi tasarım**
$A^{\perp}_3=1$, $A^{\perp}_4=1$,	$A^{\perp}_3=2$, $A^{\perp}_4=0$,	$A^{\perp}_3=2$, $A^{\perp}_4=1$,
$A^{\perp}_5=1$, $A^{\perp}_6=0$	$A^{\perp}_5=0$,$A^{\perp}_6=1$	$A^{\perp}_5=0$, $A^{\perp}_6=0$

$A^{I}_3=1<A^{II}_3=2$ olduğundan; I, II'den daha iyi bir tasarımdır.

$A^{I}_3=1<A^{III}_3=2$ olduğundan; I, III'ten daha iyi bir tasarımdır.

$A^{II}_4=0>A^{III}_4=1$ olduğundan, II, III'ten daha iyi bir tasarımdır.

5.7. 2^{6-3}_{III} Tasarımı

2_{III}^{6-3} Tasarımının tanımlayıcı bağıntıları I=ABD=ACE=BCF'dir. H D.K.M.ne bu tanımlayıcı bağıntılardan ve G Ü.M.ne de H D.K.M.nden ulaşılabilir.

Çizelge 5.10. 2^{6-3}_{III} Tasarımı(I=ABD=ACE=BCF)

a	**b**	**c**	**d=a+b**	**e=a+c**	**f=b+c**	**Denemeler**
0	0	0	0	0	0	000000
0	0	1	0	1	1	001011
0	1	0	1	0	1	010101
0	1	1	1	1	0	011110
1	0	0	1	1	0	100110
1	0	1	1	0	1	101101
1	1	0	0	1	1	110011
1	1	1	0	0	0	111000

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 6} \tag{5.41}$$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{3\times 6} \tag{5.42}$$

G Ü.M.nin satırları temeller olarak alınarak bulunan kod kelimeleri:

0 0 0 0 0 0

0 0 1 0 1 1

0 1 0 1 0 1

0 1 1 1 1 0

1 0 0 1 1 0

1 0 1 1 0 1

1 1 0 0 1 1

1 1 1 0 0 0

d=3 olan doğrusal bir (6,4) kodudur. Kodun D.K.M., dualinin Ü.M. olarak alındığında;

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 6} \tag{5.43}$$

dir ve dualin Ü.M.nden elde edilen kod kelimeleri, yine doğrusal bir (6,3) kodudur:

0 0 0 0 0 0

0 1 1 0 0 1 →I=BCF

1 0 1 0 1 0 →=ACE

1 1 0 0 1 1 →=ABEF (5.44)

1 1 0 1 0 0 →=ABD

1 0 1 1 0 1 →=ACDF

0 1 1 1 1 0 →=BCDE

0 0 0 1 1 1 →=DEF

Dual kodun ağırlık dağılımı;

$$\{1,0,0,4,3,0,0\}^{\perp} \tag{5.45}$$

ve en kısa uzaklığı, $d^{\perp}=3$'tür. Tasarımın karşılık geldiği kod, (6,4, $d^{\perp}=3$)'tür.

5.8. 2_{IV}^{7-2} Tasarımı

I=ABCDF=ABDEG tanımlayıcı bağıntılarına sahip 2_{IV}^{7-2} tasarımı, Eş. 5.46 ve Eş. 5.47'de gösterilen D.K.M ve Ü.M. yoluyla tanımlanabilir.

$$\mathbf{H}=\begin{bmatrix}1&1&1&1&0&1&0\\1&1&0&1&1&0&1\end{bmatrix}_{2\times7} \tag{5.46}$$

$$\mathbf{G}=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&0&1&1\\0&0&1&0&0&1&0\\0&0&0&1&0&1&1\\0&0&0&0&1&0&1\end{bmatrix}_{5\times7} \tag{5.47}$$

G Ü.M.nden elde edilen kod kelimleri en kısa uzaklığı d=2 olan doğrusal bir (7,5) koduna aittir.

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

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

Dual kodun Ü.M.;

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{2\times 7} \tag{5.48}$$

dir. Dualin kod kelimeleri;

0	0	0	0	0	0	0
1	1	0	1	1	0	$1\rightarrow$I=ABDEG
1	1	1	1	0	1	$0\rightarrow$ =ABCDF
0	0	1	0	1	1	$1\rightarrow$ =CEFG

(5.49)

$d^{\perp}$=4 en kısa uzaklıklı;

$$\{1,0,0,0,1,2,0,0\}^{\perp} \tag{5.50}$$

ağırlık dağılımlı bir (7,2) doğrusal koduna karşılık gelmektedir ve diklik koşulu sağlanmaktadır. Bu durumda 2_{IV}^{7-2} tasarımının kod olarak karşılığı; (7,5, $d^{\perp}$=4)'tür.

5.9. 2_{III}^{7-4} Tasarımı

Çizelge 5.11. 2_{III}^{7-4} Tasarımı (I=ABD=ACE=BCF=ABCG)

a	b	c	d=a+b	e=a+c	f=b+c	g=a+b+c
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	0	1	1
0	1	1	1	1	0	0
1	0	0	1	1	0	1
1	0	1	1	0	1	0
1	1	0	0	1	1	0
1	1	1	0	0	0	1

Çizelge 5.11'de verilen 2_{III}^{7-4} tasarımı, Eş. 5.51 ve Eş. 5.52'de verilmiş olan H D.K.M. ve G Ü.M. ile ifade edilebilir. Satırları tasarımın tanımlayıcı bağıntılarından oluşan H matrisi;

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}_{4\times 7} \tag{5.51}$$

ve H'dan elde edilen G matrisi de;

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}_{3\times 7} \tag{5.52}$$

dir. G Ü.M. nin satırları temel olarak alındığında, (7,3,4) doğrusal koduna ulaşılır.

X= { (1001101),(0101011),(0010111) }

0(1001101)+0(0101011)+0(0010111)= 0000000

0(1001101)+0(0101011)+1(0010111)= 0010111

0(1001101)+1(0101011)+0(0010111)= 0101011

0(1001101)+1(0101011)+1(0010111)= 0111100

1(1001101)+0(0101011)+0(0010111)= 1001101

1(1001101)+0(0101011)+1(0010111)= 1011010

1(1001101)+1(0101011)+0(0010111)= 1100110

1(1001101)+1(0101011)+1(0010111)= 1110001

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{4\times 7} \tag{5.53}$$

dir ve dualin Ü.M.nden elde edilen kod kelimeleri:

0000000	1000111→ =AEFG		
0001101→ I=DEG	1001010→ =ADF		
0010011→ =CFG	1010100→ =ACE	Ağırlık dağılımı:	
0011110→ =CDEF	1011001→ =ACDG	$\{1,0,0,7,7,0,0,1\}^{\perp}$	(5.54)
0100110→ =BEF	1100001→ =ABG		
0101011→ =BDFG	1101100→ =ABDE		
0110101→ =BCEG	1110010→ =ABCF		
0111000→ =BCD	1111111→ =ABCDEFG		

Sonuç olarak 2_{III}^{7-4} tasarımı, bir (7,3,$d^{\perp}$=3) doğrusal kodudur.

5.9.1. 2_{III}^{7-4}'ten 2_{III}^{6-3} Tasarımının oluşturulması

Deney tasarımında, 2_{III}^{7-4} tasarımından, daha az etken içeren Ç-III tasarımlarının oluşturulabileceği bilinmektedir. 2_{III}^{7-4} tasarımı için D.K.M.;

$$\mathbf{H}=\begin{bmatrix}1&1&0&1&0&0&0\\1&0&1&0&1&0&0\\0&1&1&0&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}_{4\times 7}$$

ve tanımlayıcı bağıntıları I=ABD=ACE=BCF=ABCG'dir.

H D.K.M.nin son satır ve sütunu silinirse; 2_{III}^{6-3} için D.K.M. Eş. 5.41'deki D.K.M.'dir.

$$\mathbf{H}=\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}_{3\times 7}$$

Tasarımın tanımlayıcı bağıntıları I=ABD=ACE=BCF'dir (Bkz. Çizelge 5.10).

5.10. 2_{IV}^{7-3} Tasarımı

Çizelge 5.12'de verilen 2_{IV}^{7-3} tasarımı, Eş. 5.55 ve Eş. 5.56'da verilmiş olan H D.K.M. ve G Ü.M. ile ifade edilebilir.

Çizelge 5.12. 2_{IV}^{7-3} Tasarımı (I=ABCE=BCDF=ACDG)

a	b	c	d	e=a+b+c	f=b+c+d	g=a+c+d	Deneme
0	0	0	0	0	0	0	0000000
0	0	0	1	0	1	1	0001011
0	0	1	0	1	1	1	0010111
0	0	1	1	1	0	0	0011100
0	1	0	0	1	1	0	0100110
0	1	0	1	1	0	1	0101101
0	1	1	0	0	0	1	0110001
0	1	1	1	0	1	0	0111010
1	0	0	0	1	0	1	1000101
1	0	0	1	1	1	0	1001110
1	0	1	0	0	1	0	1010010
1	0	1	1	0	0	1	1011001
1	1	0	0	0	1	1	1100011
1	1	0	1	0	0	0	1101000
1	1	1	0	1	0	0	1110100
1	1	1	1	1	1	1	1111111

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 7} \tag{5.55}$$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{4\times 7} \tag{5.56}$$

G'nin satırları temeller olarak alınıp, kod kelimeleri bulunur.

X= { (1000101), (0100110),(0010111), (0001011) }

0	0	0	0	0	0	0	
0	0	0	1	0	1	1	
0	0	1	0	1	1	1	
0	0	1	1	1	0	0	
0	1	0	0	1	1	0	(7,4,3) Hamming kodu
0	1	0	1	1	0	1	
0	1	1	0	0	0	1	
0	1	1	1	0	1	0	
1	0	0	0	1	0	1	

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

H(7,4,3) koduna karşılık gelen kod kelimeleri, Çizelge 5.12'deki denemelerle aynıdır. D.K.M, dualinin üreteç matrisi olduğundan;

$$\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 7} \tag{5.57}$$

Dualin kod kelimeleri:

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \times \mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 7}$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & & \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & \rightarrow & \text{ACDG} \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & \rightarrow & \text{BCDF} \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & \rightarrow & \text{ABFG} \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & \rightarrow & \text{ABCE} \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & \rightarrow & \text{BDEG} \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & \rightarrow & \text{ADEF} \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & \rightarrow & \text{CEFG} \end{bmatrix} \qquad \{1,0,0,0,7,0,0,0\}^{\perp} \tag{5.58}$$

(7, 4, $\mathbf{d^{\perp} = 4}$) kodunu oluşturmakta ve diklik koşulu sağlanmaktadır.

n=7 olduğuna göre, x^7-1, indirgenemez polinomların çarpımı şeklinde ifade edilebilir. Çizelge 2.3'te, n=3 için verilen indirgenemez polinomlar, $1+x+x^3$,

$1+x^2+x^3$'tür ve Tanım 2.10'dan aynı zamanda monik polinomlardır. Bu polinomlar Örnek 2.5 ve 2.6'da gösterildiği gibi GF(2^3)'ü oluşturmak için de kullanılmışlardır.

$$\begin{aligned}\mathbf{x}^7-1&=(1+\mathbf{x})(1+\mathbf{x}+\mathbf{x}^3)(1+\mathbf{x}^2+\mathbf{x}^3)\\&=(1+\mathbf{x}+\mathbf{x}^2+\mathbf{x}^4)(1+\mathbf{x}+\mathbf{x}^3)\\&=(1+\mathbf{x}^2+\mathbf{x}^3+\mathbf{x}^4)(1+\mathbf{x}^2+\mathbf{x}^3)\end{aligned} \tag{5.59}$$

üreteç polinomu, $g(x)=1+x+x^3$ alındığında, elde edilecek Ü.M. Eş. 5.60'da verilmiştir.

$$\mathbf{G}=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{bmatrix}_{4\times7} \tag{5.60}$$

X= { (1101000),(0110100),(0011010) (0001101) } temel olarak alınıp kod kelimeleri bulunduğunda,

0(1101000)+0(0110100)+0(0011010)+0(0001101)=0000000
0(1101000)+0(0110100)+0(0011010)+1(0001101)=0001101
0(1101000)+0(0110100)+1(0011010)+0(0001101)=0011010
0(1101000)+0(0110100)+1(0011010)+1(0001101)=0010111
0(1101000)+1(0110100)+0(0010110)+0(0001101)=0110100
0(1101000)+1(0110100)+0(0011010)+1(0001101)=0111001
0(1101000)+1(0110100)+1(0011010)+0(0001101)=0101110
0(1101000)+1(0110100)+1(0011010)+1(0001101)=0100011
1(1101000)+0(0110100)+0(0011010)+0(0001101)=1101000
1(1101000)+0(0110100)+0(0011010)+1(0001101)=1100101
1(1101000)+0(0110100)+1(0011010)+0(0001101)=1110010
1(1101000)+0(0110100)+1(0011010)+1(0001101)=1111111
1(1101000)+1(0110100)+0(0011010)+0(0001101)=1011100
1(1101000)+1(0110100)+0(0011010)+1(0001101)=1010001
1(1101000)+1(0110100)+1(0011010)+0(0001101)=1000110
1(1101000)+1(0110100)+1(0011010)+1(0001101)=1101011

Çizelge 5.12'deki denemelerle aynı olmadığı görülmüştür. Eş. 5.60'daki Ü.M.ni standart hale getirmek için, 2. satırı 1'le çarpıp son satıra eklersek;

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

3. sütunla, son sütun yer değiştirilirse,

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

6. sütunla, 7. sütun yer değiştirildiğinde;

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \qquad (5.61)$$

elde edilir ve satırları temel olarak kullanılırsa, Çizelge 5.12'deki denemelere ulaşılır.

0(1101000)+0(0100110)+0(0001011)+0(0111010)=0000000
0(1101000)+0(0100110)+0(0001011)+1(0111010)=0111010
0(1101000)+0(0100110)+1(0001011)+0(0111010)=0001011
0(1101000)+0(0100110)+1(0001011)+1(0111010)=0110001
0(1101000)+1(0100110)+0(0001011)+0(0111010)=0100110
0(1101000)+1(0100110)+0(0001011)+1(0111010)=0011100
0(1101000)+1(0100110)+1(0001011)+0(0111010)=0101101
0(1101000)+1(0100110)+1(0001011)+1(0111010)=0010111
1(1101000)+0(0100110)+0(0001011)+0(0111010)=1101000
1(1101000)+0(0100110)+0(0001011)+1(0111010)=1010010
1(1101000)+0(0100110)+1(0001011)+0(0111010)=1100011
1(1101000)+0(0100110)+1(0001011)+1(0111010)=1011001
1(1101000)+1(0100110)+0(0001011)+0(0111010)=1001110
1(1101000)+1(0100110)+0(0001011)+1(0111010)=1110100
1(1101000)+1(0100110)+1(0001011)+0(0111010)=1000101
1(1101000)+1(0100110)+1(0001011)+1(0111010)=1111111

Tanım 3.12'den G Ü.M.leri birbirinden elde edilebilen kodların eşit olduğu

bilinmektedir. Ancak kod anlamında eşit olan bu kodlar, tasarım olarak eşit değilllerdir.

5.10.1. 2_{III}^{7-3} Tasarımı: en az sapma ölçütüne göre I. en iyi tasarım

Tanımlayıcı bağıntıları I=ABCE=ABDF=CDG olan 2_{III}^{7-3} tasarımı; Eş. 5.62'deki H ve G matrisleriyle ifade edilebilmektedir.

$$\mathbf{H}=\begin{bmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\0&0&1&1&0&0&1\end{bmatrix}_{3\times7} \rightarrow \mathbf{G}=\begin{bmatrix}1&0&0&0&1&1&0\\0&1&0&0&1&1&0\\0&0&1&0&1&0&1\\0&0&0&1&0&1&1\end{bmatrix}_{4\times7} \qquad (5.62)$$

G'nin satırları temeller olarak alındığında elde edilen kod kelimeleri aşağıda gösterilmektedir.

0	0	0	0	0	0	0	
0	0	0	1	0	1	1	
0	0	1	0	1	0	1	
0	0	1	1	1	1	0	
0	1	0	0	1	1	0	
0	1	0	1	1	0	1	
0	1	1	0	0	1	1	
0	1	1	1	0	0	0	(7,4) doğrusal kodu
1	0	0	0	1	1	0	
1	0	0	1	1	0	1	
1	0	1	0	0	1	1	
1	0	1	1	0	0	0	
1	1	0	0	0	0	0	
1	1	0	1	0	1	1	
1	1	1	0	1	0	1	
1	1	1	1	1	1	0	

Dualin Ü.M.;

$$\mathbf{G_{dual}}=\begin{bmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\0&0&1&1&0&0&1\end{bmatrix}_{3\times7} \qquad (5.63)$$

ve dualdeki kod kelimeleri;

0	0	0	0	0	0	0			
0	0	1	1	0	0	1→I=CDG			
1	1	0	1	0	1	0→ =ABDF			
1	1	1	0	0	1	1→ =ABCFG	(7,3) doğrusal kodu		(5.64)
1	1	1	0	1	0	0→ =ABCE	$d^{\perp}$ =3, $\{1,0,0,2,3,2,0,0\}^{\perp}$		
1	1	0	1	1	0	1→ =ABDEG			
0	0	1	1	1	1	0→ =CDEF			
0	0	0	0	1	1	1→ =EFG			

tasarımın tanımlayıcı bağıntı yapısını vermektedir.

5.10.2. 2_{III}^{7-3} Tasarımı: en az sapma ölçütüne göre II. en iyi tasarım

I=ABCDE=BCF=ABCG tanımlayıcı bağıntılarına sahip, 2_{III}^{7-3} tasarımı Eş. 5.65'te verilen H D.K.M. ve G Ü.M. ile tanımlanabilmektedir.

$$\mathbf{H}=\begin{bmatrix}1&1&1&1&1&0&0\\0&1&1&0&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}_{3\times7} \rightarrow \mathbf{G}=\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&1\\0&0&0&1&1&0&0\end{bmatrix}_{4\times7} \qquad (5.65)$$

G Ü.M.nden elde edilen kod kelimeleri aynı zamanda tasarımın denemeleridir.

0	0	0	0	0	0	0	
0	0	0	1	1	0	0	
0	0	1	0	1	1	1	
0	0	1	1	0	1	1	
0	1	0	0	1	1	1	
0	1	0	1	0	1	1	
0	1	1	0	0	0	0	
0	1	1	1	1	0	0	d=2, doğrusal (7,4) kodu
1	0	0	0	1	0	1	
1	0	0	1	0	0	1	
1	0	1	0	0	1	0	
1	0	1	1	1	1	0	
1	1	0	0	0	1	0	

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

H D.K.M, Ü.M. alınarak elde edilen dualin kod kelimeleri;

0	0	0	0	0	0	0		
1	1	1	0	0	0	1→ I=ABCG		
0	1	1	0	0	1	0→ =BCF		
1	0	0	0	0	1	1→ =AFG	Ağırlık dağılımı:	
1	1	1	1	1	0	0→ =ABCDE	{1,0,0,3,2,1,1,0}	(5.66)
0	0	0	1	1	0	1→ =DEG		
1	0	0	1	1	1	0→ =ADEF		
0	1	1	1	1	1	1→ =BCDEFG		

$d^{\perp}$ =3, en kısa uzaklıklı (7,3) doğrusal koduna karşılık gelmektedir.

5.10.3. 2_{III}^{7-3} Tasarımı: en az sapma ölçütüne göre III. en iyi tasarım

I=ABCE=ABDF=ABG tanımlayıcı bağıntılı 2_{III}^{7-3} tasarımı Eş. 5.67'deki matrisler yoluyla tanımlanabilir.

$$\mathbf{H}=\begin{bmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\1&1&0&0&0&0&1\end{bmatrix}_{3\times7} \rightarrow \mathbf{G}=\begin{bmatrix}1&0&0&0&1&1&1\\0&1&0&0&1&1&1\\0&0&1&0&1&0&0\\0&0&0&1&0&1&0\end{bmatrix}_{4\times7} \qquad (5.67)$$

G matrisinden elde edilen kod kelimeleri:

0	0	0	0	0	0	0	
0	0	0	1	0	1	0	
0	0	1	0	1	0	0	
0	0	1	1	1	1	0	
0	1	0	0	1	1	1	
0	1	0	1	1	0	1	
0	1	1	0	0	1	1	d=2, (7,4) doğrusal kodu
0	1	1	1	0	0	1	
1	0	0	0	1	1	1	
1	0	0	1	1	0	1	
1	0	1	0	0	1	1	
1	0	1	1	0	0	1	
1	1	0	0	0	0	0	

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

ve Ü.M. $\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{3\times 7}$ olarak alındığında dualdeki kod kelimeleri:

0	0	0	0	0	0	0		
1	1	0	0	0	0	1→I=ABG		
1	1	0	1	0	1	0→ =ABDF		
0	0	0	1	0	1	1→ =DFG		
1	1	1	0	1	0	0→ =ABCE	$\{1,0,0,3,3,0,0,1\}^{\perp}$	(5.68)
0	0	1	0	1	0	1→ =CEG		
0	0	1	1	1	1	0→ =CDEF		
1	1	1	1	1	1	1→ =ABCDEFG		

$d^{\perp}$ =3, en kısa uzaklıklı (7,3) doğrusal koduna karşılık gelmektedir.

5.10.4. 2_{III}^{7-3} Tasarımı: en az sapma ölçütüne göre IV. en iyi tasarım

Tanımlayıcı bağıntıları I=ABE=ABDF=BDG olan 2_{III}^{7-3} tasarımı Eş. 5.69'daki matrisler yoluyla tanımlanabilir.

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 7} \rightarrow \mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{4\times 7} \qquad (5.69)$$

G'den elde edilen kod kelimeleri:

0	0	0	0	0	0	0	
0	0	0	1	0	1	1	
0	0	1	0	0	0	0	
0	0	1	1	0	1	1	
0	1	0	0	1	1	1	
0	1	0	1	1	0	0	
0	1	1	0	1	1	1	d=1, (7,4) doğrusal kodu
0	1	1	1	1	0	0	
1	0	0	0	1	1	0	
1	0	0	1	1	0	1	
1	0	1	0	1	1	0	

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

dir. Dualin Ü.M.i $\mathbf{G_{dual}} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 7}$ alındığında ulaşılan kod kelimeleri;

0	0	0	0	0	0	0	
0	1	0	1	0	0	1→ I=BDG	
1	1	0	1	0	1	0→ =ABDF	
1	0	0	0	0	1	1→ =AFG	
1	1	0	0	1	0	0→ =ABE	$\{1,0,0,4,3,0,0,0\}^{\perp}$ (5.70)
1	0	0	1	1	0	1→ =ADEG	
0	0	0	1	1	1	0→ =DEF	
0	1	0	0	1	1	1→ =BEFG	

$d^{\perp}$ =3 en kısa uzaklıklı (7,3) doğrusal kodudur.

5.10.5. 2_{III}^{7-3} Tasarımlarının Karşılaştırılması

Görüldüğü gibi, Wu ve Chen(1992)'in en az sapma ölçütüne göre oluşturdukları listede 1. en iyi…4.en iyi olarak sıralanmış 4 tane 2_{III}^{7-3} tasarımı vardır. Çizelge 5.13'te bu 4 tasarımın kod parametreleri gösterilmiştir.

Çizelge 5.13. 2_{III}^{7-3} –(7,4) Kodlarının duallerine göre karşılaştırılması

	I. En İyi Tasarım	**II. En İyi Tasarım**	**III. En İyi Tasarım**	**IV. En İyi Tasarım**
T.B.	I=ABCE=ABDF =CDG	I=ABCDE=BCF =ABCG	I=ABCE=ABDF =ABG	I=ABE=ABDF =BDG
Dual kod kelimeleri- { I,0 }	1110011:ABCFG 1101101:ABDEG 0011110:CDEG 0000111:EFG	1000011:AFG 0001101:DEG 1001110:ADEF 0111111:BCDEFG	0001011:DFG 0010101:CEG 0011110:CDEF 1111111:ABCDEFG	1000011:AFG 1001101:ADEG 0001110:DEF 0100111:BEFG
(n,k) kodu	(7,4)	(7,4)	(7,4)	(7,4)
$d^{\perp}$	3	3	3	3
$A^{\perp}_i$ dağılımı- i=Çmax,...,7	{2,3,2,0,0}	{3,2,1,1,0}	{3,3,0,0,1}	{4,3,0,0,0}

I. En iyi tasarım **II. En iyi tasarım**

$A^{\perp}_3=2$, $A^{\perp}_4=3$, $A^{\perp}_3=3$, $A^{\perp}_4=2$,

$A^{\perp}_5=2$, $A^{\perp}_6=0$, $A^{\perp}_7=0$ $A^{\perp}_5=1$, $A^{\perp}_6=1$, $A^{\perp}_7=0$

III. En iyi tasarım **IV. En iyi tasarım**

$A^{\perp}_3=3$, $A^{\perp}_4=3$, $A^{\perp}_3=4$, $A^{\perp}_4=3$,

$A^{\perp}_5=0$,$A^{\perp}_6=0$, $A^{\perp}_7=1$ $A^{\perp}_5=0$,$A^{\perp}_6=0$, $A^{\perp}_7=0$

$A^{I}_3=2<A^{II}_3=3$, $A^{III}_3=3$, $A^{III}_3=4$, olduğundan;

I. tasarım, II,III ve IV'ten daha iyi bir tasarımdır(daha az sapmaya sahiptir).

$A^{II}_4=2<A^{III}_4=3$, $A^{IV}_4=3$ olduğundan;

II. tasarım, III ve IV'ten daha iyi bir tasarımdır.

$A^{III}_3=3<A^{IV}_3=4$ olduğundan, III, IV'ten daha iyi bir tasarımdır.

Bu karşılaştırma, Çizelge 5.13'ten de yapılabilir.

5.11. 2^{8-4}_{IV} Tasarımı

I=BCDE=ACDF=ABCG=ABDH tanımlayıcı bağıntılı 2_{IV}^{8-4} tasarımı, Eş. 5.71'deki matrislerle tanımlanabilmektedir.

$$\mathbf{H}=\begin{bmatrix}0&1&1&1&1&0&0&0\\1&0&1&1&0&1&0&0\\1&1&1&0&0&0&1&0\\1&1&0&1&0&0&0&1\end{bmatrix}_{4\times8} \rightarrow \mathbf{G}=\begin{bmatrix}1&0&0&0&0&1&1&1\\0&1&0&0&1&0&1&1\\0&0&1&0&1&1&1&0\\0&0&0&1&1&1&0&1\end{bmatrix}_{4\times8} \qquad (5.71)$$

G Ü.M.ndeki satırlardan elde edilen kod kelimeleri;

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

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

d=4 en kısa uzaklıklı, (8,4) doğrusal kodudur. Dualin Ü.M.:

$$\mathbf{G_{dual}} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}_{4\times 8} \tag{5.72}$$

dir. Dualin kod kelimeleri:

0	0	0	0	0	0	0	0
1	1	0	1	0	0	0	1→I=ABDH
1	1	1	0	0	0	1	0→ =ABCG
0	0	1	1	0	0	1	1→CDGH
1	0	1	1	0	1	0	0→ =ACDF
0	1	1	0	0	1	0	1→ =BCFH
0	1	0	1	0	1	1	0→ =BDFG
1	0	0	0	0	1	1	1→ =AFGH
0	1	1	1	1	0	0	0→ =BCDE
1	0	1	0	1	0	0	1→ =ACEH
1	0	0	1	1	0	1	0→ =ADEG
0	1	0	0	1	0	1	1→ =BEFH
1	1	0	0	1	1	0	0→ =ABEF
0	0	0	1	1	1	0	1→ =DEFH
0	0	1	0	1	1	1	0→ =CEFG
1	1	1	1	1	1	1	1→ =ABCDEFGH

(5.73)

(8,4) doğrusal kodu olup, $d^{\perp}=4$ ve ağırlık dağılımı;

$$\{1,0,0,0,14,0,0,0,1\}^{\perp} \tag{5.74}$$

dir. Dualin kod kelimeleriyle, kodun kod kelimeleri aynı olduğundan, (8,4) kodu

self-dual bir koddur. Yani, duali kendisine eşittir (Bkz. Bölüm 3.8.3.1).

5.11.1. 2_{III}^{7-4}'ten 2_{IV}^{8-4} tasarımının oluşturulması

2_{III}^{7-4} tasarımı, I=ABD=ACE=BCF=ABCG, için Eş 5.51'de verilen D.K.M.ne satırlardaki 1 sayısını çift yapacak şekilde 1 veya 0 eklenirse, elde edilecek H_2 D.K.M., 2_{IV}^{8-4} tasarımının D.K.M.

$$\mathbf{H}_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

dir ve tanımlayıcı bağıntıları I=ABDH=ACEH=BCFH=ABCG olacaktır.

6. UYGULAMA

Bölüm 5'ten, kesirli çok etkenli tasarımlarla, kodlar arasında ilişki olduğu görülmektedir. Burada incelenen tasarımlar ışığında; denemeler kod kelimeleri, tasarımın çözümü $d^{\perp}$, dual kodun ağırlık dağılımı kelime uzunluğu yapısı ve dual kodun kod kelimeleri de tanımlayıcı bağıntı yapısı olarak yorumlanabilmektedir.

Tasarımlar kodlarla ifade edilirken, $(n,k,d^{\perp}_{min})$ gösterimi kullanılırsa; Bölüm 5.6'daki 2_{IV}^{6-2} tasarımının (6,4,4); Bölüm 5.6.1, Bölüm 5.6.2, Bölüm 5.6.3'te verilen, en az sapma ölçütüyle sıralanmış 2_{III}^{6-2} tasarımlarının (6,4,3) kodu olması; aynı n,k, hatta aynı $d^{\perp}$ değerlerine sahip olmalarına karşın, kodların farklı olduğunu ve farklı tasarımlara ulaşıldığını göstermektedir.

Bu farklılığı yaratan dual koddur ve burada, örneğin bir (8,4,3) kodu söz konusu olduğunda, dual ağırlık dağılımları farklı kaç kod; dolayısıyla en az sapma ölçütüne göre sıralanmış kaç tasarım elde edilebileceği sorusu akla gelmektedir.

Bölüm 5'te yardımcı olan MATLAB fonksiyon ve komutları bu soruya çözüm üretmekten uzak olduğundan; MATLAB'ın var olan özelliklerinden de yararlanarak bir program yazılması uygun görülmüştür.

Kesirli çok etkenli tasarımlarla kodlar ve en az sapma ölçütüyle dual ağırlık dağılımları arasındaki ilişki belirlendikten sonra; ağırlık dağılımlarının hesaplanması; en iyi tasarıma karar verilebilmesi; tasarımların en az sapma ölçütüne göre sıralanabilmesi için, bazı fonksiyonlar yaratılmış ve iki farklı program (1. program, en iyi tasarım; 2. program belli bir tasarım/kod içindir) çalıştırılarak; tasarımlar karşılık geldikleri kod parametreleriyle birlikte elde edilmiştir.

Program girdileri; 1. program için n ve k değerleri; 2. program içinse, $G=[I_k\ A]$'deki A matrisidir. Başlangıçta D.K.M ya da Ü.M. kullanılması düşünülmüş; ancak, hızı etkileyebileceği endişesiyle A'da karar kılınmıştır. A matrisleri, en düşük çözüm 3 olacak ve birbirinin aynı olan matrisler elenecek şekilde belirlenmiştir.

Program çıktıları, özellikle etken sayısı arttığında çok uzun olduğundan; etken sayısının az olduğu örneklerin verilmesi uygun görülmüş ve gerektiğinde çıktılarda kısaltmaya gidilmiştir.

Örnek 6.1. 2_{III}^{3-1} tasarımı (I=ABC) (Bkz. Çizelge 5.1) için, n=3,p=1 ve k=2'dir. n=3, k=2 için en iyi tasarımı bulmaya yönelik 1. programın verdiği çıktı:

```
**************************************************
        As = (Bkz. Eş.5.2)
             1
             1
        Rs =    3
        ADs =    1    0    0    1 (Bkz. Eş.5.4)
**************************************************
```

dir. Burada;

As: G=[I_k A] Ü.M.ndeki k×(n-k) boyutlu A matrisi (Bkz. Tanım 3.11);

Rs: Dual kodun en kısa uzaklığı ya da tasarımın çözümü;

ADs: Dual kodun ağırlık dağılımı;

dır. 2_{III}^{3-1} tasarımı için Eş. 5.3'te verilen G Ü.M. A'yı da içermektedir. Program çıktı olarak birden fazla A vermediğinden; (3,2,3) kodu tek bir tasarıma karşılık gelmektedir.

Buradan elde edilen A matrisi girdi olarak kullanılırsa, tasarımın kod olarak özellikleri, 2. program yoluyla bulunabilir. Program çıktısı, R: tasarımın çözümü olmak üzere, aşağıdaki gibidir.

```
**********************************************************************************************
Uretec matrisi (Bkz. Eş. 5.2) =
   1    0    1
   0    1    1
Denklik kontrol matrisi (Bkz. Eş. 5.1) =
   1    1    1
Denemeler/kod kelimeleri (Bkz. Çizelge 5.1) =
   0    0    0
   0    1    1
   1    0    1
   1    1    0
```

Agirlik dagilimi ={1, 0, 3, 0} (Bkz. Tanım 3.15)

Kod kelimeleri arasi en kisa uzaklik d=2

Tanimlayici baginti yapisi (Bkz. Eş.5.3) =

0 0 0

1 1 1

Dual kodun agirlik dagilimi (Bkz. Eş.5.4)={1, 0, 0, 1}

Dual kod kelimeleri arasi en kisa uzaklik d=R=3 (Bkz. Teorem 4.2)

d cift sayi oldugundan Hamming siniri tanimli degil (Bkz. Teorem 3.5)

Kod Griesmer sinirini esitlikle sagliyor: 3 = 3 (Bkz. Teorem 3.6)

Kod Varshamov-Gilbert sinirini sagliyor: 1 < 2 (Bkz. Teorem 3.8)

Dual Kod Hamming sinirini sagliyor: 3 < 4

Dual Kod Griesmer sinirini esitlikle sagliyor: 3 = 3

Dual Kod Varshamov-Gilbert sinirini sagliyor: 3 < 4

****

Görüldüğü gibi program sonuçları, başlangıçta sorduğumuz sorulara yanıt verir niteliktedir.

Örnek 6.2. 2_{III}^{5-2} tasarımı (I=ABD=ACE) söz konusu olduğunda (Bkz. Çizelge 5.5); 1. programın çalıştırılmasıyla bulunan en iyi tasarımlar;

****

As(:,:,1) =

0 1

1 0

1 1

As(:,:,2) =

0 1

1 1

1 1

Rs = 3

3

ADs = 1 0 0 2 1 0 (Bkz. Eş.5.17)

1 0 0 2 1 0

****

dir. Dikkat edileceği üzere, farklı A matrisleri, dual ağırlık dağılımı ve çözümü aynı olan tasarımlar verebilmektedir. Dual kodun ağırlık dağılımları, Bölüm 5.4'te 2_{III}^{5-2} tasarımı için bulunan ağılık dağılımı ile aynıdır. Eş. 5.14'teki G Ü.M.nden elde edilen A matrisi, girdi olarak kullanılır ve 2. program çalıştırılırsa, aşağıdaki çıktı elde edilir.

****

Uretec matrisi (Bkz. Eş.5.14) =

1 0 0 1 1

0 1 0 1 0

0 0 1 0 1

Denklik kontrol matrisi (Bkz. Eş.5.13)=

1 1 0 1 0

1 0 1 0 1

Denemeler/kod kelimeleri (Bkz. Çiz. 5.5)=

0 0 0 0 0

0 0 1 0 1

0 1 0 1 0

0 1 1 1 1

1 0 0 1 1

1 0 1 1 0

1 1 0 0 1

1 1 1 0 0

Agirlik dagilimi ={1, 0, 2, 4, 1, 0}

Kod kelimeleri arasi en kisa uzaklik d=2

Tanimlayici baginti yapisi (Bkz. Eş.5.16)=

0 0 0 0 0

1 0 1 0 1

1 1 0 1 0

0 1 1 1 1

Dual kodun agirlik dagilimi (Bkz. Eş.5.17) ={1, 0, 0, 2, 1, 0}
Dual kod kelimeleri arasi en kisa uzaklık d=R=3 (Bkz. Teorem 4.2)

d cift sayi oldugundan Hamming siniri tanimli degil (Bkz. Teorem 3.5)
Kod Griesmer sinirini sagliyor: 4 < 5 (Bkz. Teorem 3.6)
Kod Varshamov-Gilbert sinirini sagliyor: 1 < 4 (Bkz. Teorem 3.8)

Dual Kod Hamming sinirini sagliyor: 5 < 8
Dual Kod Griesmer sinirini esitlikle sagliyor: 5 = 5
Dual Kod Varshamov-Gilbert sinirini sagliyor: 5 < 8

****

Bölüm 5.4'te, elle alındığı söylenebilecek sonuçlarla program çıktıları tutarlıdır ve daha fazla bilgi, toplu olarak görülebilmektedir.

Etken sayısı arttığında, bulunan A matrislerinin sayısıyla birlikte, 1. programın çalışma süresi de artmaktadır. Bu nedenle n>5 için verilen örnek çıktılarında, sadece tasarımların karşılık geldiği kodların, 5. Bölümde de yer alan çözümlerine ve bunlara karşılık gelen dual ağırlık dağılımlarına yer verilecektir.

Örnek 6.3. 2^{6-2} tasarımları için, 1. program n=6, k=4 parametreleriyle çalıştırılsın. Bu durumda, program çıktısının, bu parametrelerden oluşturulabilecek tasarımları, Bölüm 5.6.4'te gösterildiği şekilde, 1. en iyi, 2. en iyi vb. olarak sıralaması beklenecektir.

Çözüm değerleri ve bunlara karşılık gelen dual kodun ağırlık dağılımları, en az sapma ölçütüne göre sıralı olarak aşağıdaki gibidir.

****

Rs = 4 3 3 3

ADs = 1 0 0 0 3 0 0 (Bkz. Eş.5.25)
1 0 0 1 1 1 0 (Bkz. Eş.5.30)
1 0 0 2 0 0 1 (Bkz. Eş.5.35)
1 0 0 2 1 0 0 (Bkz. Eş.5.40)

****

Görüldüğü gibi, 1. dual ağırlık dağılımı için $d^{\perp}=4$; son 3 dual ağırlık dağılımı içinse $d^{\perp}=3$'tür. Son 3 ağırlık dağılımı, 2_{III}^{6-2} tasarımlarının en az sapma ölçütüne göre

sıralandığı Çizelge 5.8 ve Çizelge 5.9'da verildiği gibidir. İstendiği takdirde, bu tasarımların özellikleri tek tek 2. programın çalıştırılmasıyla elde edilebilir. Örneğin, 1. sırada yer alan 2_{IV}^{6-2} tasarımı için sonuçlar aşağıda verilmiştir.

****

Uretec matrisi (Bkz. Eş.5.22)=

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

Denklik kontrol matrisi (Bkz. Eş.5.21)=

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

Denemeler/kod kelimeleri (Bkz. Çizelge 5.6)=

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

Agirlik dagilimi ={1, 0, 3, 8, 3, 0, 1}

Kod kelimeleri arasi en kisa uzaklik d=2

Tanimlayici baginti yapisi (Bkz. Eş.5.24)=

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

Dual kodun agirlik dagilimi (Bkz. Eş.5.25) ={1, 0, 0, 0, 3, 0, 0}

Dual kod kelimeleri arasi en kisa uzaklık d=R=4

d cift sayi oldugundan Hamming siniri tanimli degil (Bkz. Teorem 3.5)

Kod Griesmer sinirini sagliyor: 5 < 6 (Bkz. Teorem 3.6)

Kod Varshamov-Gilbert sinirini sagliyor: 1 < 4 (Bkz. Teorem 3.8)

dDual cift sayi oldugundan Hamming siniri tanimli degil

Dual Kod Griesmer sinirini esitlikle sagliyor: 6 = 6

Dual Kod Varshamov-Gilbert sinirini saglamiyor: 16 >= 16

****

Görüldüğü gibi, her iki çıktıda da tasarımın dual ağırlık dağılımı ve çözümü aynıdır; ancak burada, kod ve tasarım hakkında daha fazla bilgi vardır.

5. Bölümde gösterilen tasarımlar dışında, Box, Hunter ve Hunter (1978)'ın standart tablosunda (Bkz. Ek-1) yer alan bütün tasarımlar kodlarla oluşturulmuştur.

7. SONUÇLAR

Bilindiği gibi, bir 2^{n-p} kesirli çok etkenli tasarımında;

n: Etken sayısı, **p**: Tanımlayıcı bağıntı sayısı,

$2^{p}-p-1$: Tanımlayıcı bağıntılar arasındaki genelleştirilmiş etkileşim sayısı,

$2^{p}-1$: Tanımlayıcı bağıntı yapısındaki kelime sayısı,

dır. Çalışma süresince elde edilen bilgiler ışığında; bir (n,k) kodu, n-k=p olmak üzere, k temel etken yardımıyla oluşturulan n etkenli bir 2^{n-p} kesirli çok etkenli tasarım olarak düşünülebilir. Tasarımın çözümü, dual kodun en kısa uzaklığından ($d^{\perp}$) ve tanımlayıcı bağıntı yapısı da dualin kod kelimelerinden bulunabilir.

Başlangıçta amaç, sadece kodlar ve tasarımlar arasındaki ilişkiyi göstermek ve her tasarıma bir kod atamak ya da tam tersini yapmakken; en az sapma ölçütünün kodlarda nasıl işlediğinin araştırılması sırasında karşılaşılan sorular; kod parametreleri aynıyken farklı tasarımlara ulaşılması; farklılığı yaratanın dual kod olması vb. sonuçlar; ilgilenilen konu kodlar ve tasarımlar olunca, hali hazırda yararlanılacak bir programın olmaması güçlüğü; istenileni verebilecek bir programın yazımını zorunlu kılmıştır.

6. Bölümde, programların nasıl çalıştığına dair verilen örnekler; verilebilen en kısa çıktı örnekleridir ve anlaşılacağı üzere bu durum, bu kadar verinin nasıl özetleneceği gibi bir sorunu da beraberinde getirmektedir. Bu bağlamda, Çizelge 7.1'de listelenen tasarımlar ve kod olarak karşılıkları, bazı yönlerden eksiktir. Örneğin, 2_{III}^{9-5} için, dual ağırlık dağılımları farklı 5 tasarım bulunmuş ve hepsi çizelgeye dahil edilmişken; 2_{V}^{10-3} tasarımı için, sadece Ç-V olan 2 tasarım gösterilmiş, Ç-IV olan 22 tasarım ve Ç-III olan 40 tasarım göz ardı edilmiştir.

Çizelge 7.1'de tasarımlar; karşılık geldikleri kodlar, bu kodlara ait dual ağırlık dağılımları ve D.K.M.leri ile ifade edilmişlerdir. Doğrusal kod için B, döngüsel kod için C ve Hamming kodları için H gösterimi kullanılmıştır. Kodların sağladıkları sınırlara da bakılmış; ancak, Varshamov-Gilbert ve Griesmer sınırlarını hepsi; Hamming sınırını ise en kısa uzaklığı tek olanlar sağladığı için, çizelgede bu bilgilere yer verilmemiştir.

Tasarımlar kodlarla ifade edilirken, özellikle tanımlayıcı bağıntı yapısının anlaşılması ve yorumlanmasının kodlarla daha kolay olduğu görülmüştür. Bu şekilde, bir tasarımı sadece bir matrisle tanımlayabilmek mümkündür.

Kod parametreleri ile en az sapma ölçütüne göre yapılan sıralamalar, literatürde yer alan, Örneğin; 2_{III}^{6-2} ve 2_{III}^{7-3} için Wu ve Chen(1992)'in yaptığı, tasarımlarla tutarlıdır.

Çizelge 7.1'de yer almamasına karşın, en az sapma ölçütüne göre sıralanmış diğer tasarımlara da ulaşmak mümkündür. Örneğin, 2_{IV}^{9-3} için 3 tasarım verilmiş; ancak, Ç-IV uzunluğunda 9 tasarım bulunmuş ve dual ağırlık dağılımları aşağıdaki gibi sıralanmıştır.

1. $(1,0,0,0,1,4,2,0,0,0)^{\perp}$
2. $(1,0,0,0,2,3,1,1,0,0)^{\perp}$
3. $(1,0,0,0,2,4,0,0,1,0)^{\perp}$
4. $(1,0,0,0,3,0,4,0,0,0)^{\perp}$
5. $(1,0,0,0,3,2,0,2,0,0)^{\perp}$
6. $(1,0,0,0,3,4,0,0,0,0)^{\perp}$
7. $(1,0,0,0,4,0,2,0,1,0)^{\perp}$
8. $(1,0,0,0,5,0,2,0,0,0)^{\perp}$
9. $(1,0,0,0,7,0,0,0,0,0)^{\perp}$

Tasarımlar hali hazırda sıralanmış olduğundan; kodlar hakkında bilgi sahibi olmak gerekmeksizin; uygun tasarımın seçimi, dual ağırlık dağılımlarına bakılarak da yapılabilir. Örneğin, 2_{III}^{8-4} tasarımı söz konusu olduğunda (Bkz. Çizelge 7.1), 2. tasarımda, 2'li etkileşimlerle karışacak ana etki sayısının, 1. tasarıma göre daha çok olduğu görülmektedir.

Tasarımlar ve kodlar bağlamında pek çok bilgi elde edilmiş olmasına karşın; henüz, eşdeş yapısının doğrudan elde edilebildiği bir algoritma geliştirilememiş; çıkış noktası olarak Hamming kodları alınmasına karşın, H_3, (Bkz. Çizelge 3.3) H_4 vb. kodların D.K.M.lerinden yararlanarak hangi tasarımlara ulaşılabileceği, özel olarak araştırılamamıştır. Ancak, iki algoritma üzerinde de çalışılmaktadır.

Çizelge 7.1. Tasarımlar ve kod karşılıkları

Deneme	Tasarım	Kod karşılığı ($n,k,d^{\perp}_{min}$)	Ağırlık dağılımı$^{\perp}$ i=Çmax,...,n	Denklik kontrol matrisleri/Tanımlayıcı bağıntılar
4	2^{3-1}_{III}	C(3,2,3)	{1}	1 1 1
8	2^{4-1}_{IV}	C(4,3,4)	{1}	1 1 1 1
	2^{4-1}_{III}	B(4,3,3)	{1,0}	0 1 1 1
	2^{5-2}_{III}	B(5,3,3)	{2,1,0}	1 1 0 1 0 1 0 1 0 1
	2^{6-3}_{III}	B(6,3,3)	{4,3,0,0}	1 1 0 1 0 0 1 0 1 0 1 0 0 1 1 0 0 1
	2^{7-4}_{III}	B(7,3,3)	{7,7,0,0,1}	1 1 0 1 0 0 0 1 0 1 0 1 0 0 0 1 1 0 0 1 0 1 1 1 0 0 0 1
16	2^{5-1}_{V}	C(5,4,5)	{1}	1 1 1 1 1
	2^{6-2}_{IV}	B(6,4,4)	{3,0,0}	1 1 1 0 1 0 0 1 1 1 0 1
	1. 2^{6-2}_{III}	B(6,4,3)	{1,1,1,0}	1 1 0 0 1 0 0 1 1 1 0 1
	2. 2^{6-2}_{III}	B(6,4,3)	{2,0,0,1}	1 1 0 0 1 0 0 0 1 1 0 1
	3. 2^{6-2}_{III}	B(6,4,3)	{2,1,0,0}	1 1 0 0 1 0 1 1 0 1 0 1
	2^{7-3}_{IV}	H(7,4,4)	{7,0,0,0}	1 1 1 0 1 0 0 0 1 1 1 0 1 0 1 0 1 1 0 0 1
	1. 2^{7-3}_{III}	B(7,4,3)	{2,3,2,0,0}	1 1 1 0 1 0 0 1 1 0 1 0 1 0 0 0 1 1 0 0 1
	2. 2^{7-3}_{III}	B(7,4,3)	{3,2,1,1,0}	1 1 1 1 1 0 0 0 1 1 0 0 1 0 1 1 1 0 0 0 1
	3. 2^{7-3}_{III}	B(7,4,3)	{3,3,0,0,1}	1 1 1 0 1 0 0 1 1 0 1 0 1 0 1 1 0 0 0 0 1
	4. 2^{7-3}_{III}	B(7,4,3)	{4,3,0,0,0}	1 1 0 0 1 0 0 1 1 0 1 0 1 0 0 1 0 1 0 0 1

Çizelge 7.1. (Devam)

Deneme	Tasarım	Kod karşılığı ($n,k, d^{\perp}_{min}$)	Ağırlık dağılımı$^{\perp}$ i=Çmax,...,n	Denklik kontrol matrisleri/Tanımlayıcı bağıntılar
16	2^{8-4}_{IV}	B(8,4,4) (self dual)	{14,0,0,0,1}	0 1 1 1 1 0 0 0 1 0 1 1 0 1 0 0 1 1 1 0 0 0 1 0 1 1 0 1 0 0 0 1
	1. 2^{8-4}_{III}	B(8,4,3}	{3,7,4,0,1,0}	0 1 1 1 1 0 0 0 1 0 0 1 0 1 0 0 1 0 1 0 0 0 1 0 1 1 0 0 0 0 0 1
	2. 2^{8-4}_{III}	B(8,4,3}	{4,5,4,2,0,0}	0 0 1 1 1 0 0 0 0 1 0 1 0 1 0 0 1 1 0 0 0 0 1 0 1 1 1 0 0 0 0 1
	3. 2^{8-4}_{III}	B(8,4,3}	{4,6,4,0,0,1}	0 0 1 1 1 0 0 0 0 1 0 1 0 1 0 0 0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 1
	4. 2^{8-4}_{III}	B(8,4,3}	{5,5,2,2,1,0}	0 0 1 1 1 0 0 0 0 1 1 1 0 1 0 0 1 0 1 1 0 0 1 0 1 1 0 0 0 0 0 1
	5. 2^{8-4}_{III}	B(8,4,3}	{7,7,0,0,1,0}	0 0 1 1 1 0 0 0 0 1 0 1 0 1 0 0 0 1 1 0 0 0 1 0 0 1 1 1 0 0 0 1
	1. 2^{9-5}_{III}	B(9,4,3)	{4,14,8,0,4,1,0}	1 1 1 0 1 0 0 0 0 0 1 1 1 0 1 0 0 0 1 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 0 1 1 1 1 0 0 0 0 1
	2. 2^{9-5}_{III}	B(9,4,3)	{6,9,9,6,0,0,1}	0 0 1 1 1 0 0 0 0 0 1 1 1 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 1 0 0 0 0 0 1 0 1 1 1 0 0 0 0 0 1
	3. 2^{9-5}_{III}	B(9,4,3)	{6,10,8,4,2,1,0}	0 0 1 1 1 0 0 0 0 0 1 1 1 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 1 1 0 0 0 0 1 0 1 1 1 1 0 0 0 0 1

Çizelge 7.1. (Devam)

Deneme	Tasarım	Kod karşılığı ($n,k,d^{\perp}_{min}$)	Ağırlık dağılımı$^{\perp}$ i=Çmax,...,n	Denklik kontrol matrisleri/Tanımlayıcı bağıntılar
16	4. 2^{9-5}_{III}	B(9,4,3)	{7,9,6,6,3,0,0}	0 0 1 1 1 0 0 0 0 0 1 0 1 0 1 0 0 0 0 1 1 0 0 0 1 0 0 1 0 1 0 0 0 0 1 0 1 1 1 0 0 0 0 0 1
	5. 2^{9-5}_{III}	B(9,4,3)	{8,10,4,4,4,1,0}	0 0 1 1 1 0 0 0 0 0 1 0 1 0 1 0 0 0 0 1 1 0 0 0 1 0 0 0 1 1 1 0 0 0 1 0 1 1 1 1 0 0 0 0 1
	1. 2^{10-6}_{III}	B(10,4,3)	{8,18,16,8,8,5,0,0}	1 1 1 0 1 0 0 0 0 0 0 1 1 1 0 1 0 0 0 0 1 0 1 1 0 0 1 0 0 0 1 1 0 1 0 0 0 1 0 0 1 1 1 1 0 0 0 0 1 0 1 1 0 0 0 0 0 0 0 1
	2. 2^{10-6}_{III}	B(10,4,3)	{9,16,15,12,7,3,1,0}	0 0 1 1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 1 1 0 0 0 1 0 0 0 1 0 1 1 0 0 0 1 0 0 1 1 0 0 0 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1
	3. 2^{10-6}_{III}	B(10,4,3)	{10,15,12,15,10,0,0,1}	0 0 1 1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 1 1 1 0 0 1 0 0 0 1 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 0 0 1 0 1 1 0 1 0 0 0 0 0 1
	4. 2^{10-6}_{III}	B(10,4,3)	{10,16,12,12,10,3,0,0}	0 0 1 1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 1 1 0 0 0 1 0 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 0 0 0 0 0 1 0 1 1 0 0 0 0 0 0 0 1
	2^{11-7}_{III}	B(11,4,3)	{12, 26, 28, 24, 20, 13, 4, 0, 0}	1 1 1 0 1 0 0 0 0 0 0 0 1 1 1 0 1 0 0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 1 1 0 1 0 0 0 1 0 0 0 1 1 1 1 0 0 0 0 1 0 0 1 1 0 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 1

Çizelge 7.1. (Devam)

Deneme	Tasarım	Kod karşılığı ($n,k,d^{\perp}_{min}$)	Ağırlık dağılımı$^{\perp}$ i=Çmax,...,n	Denklik kontrol matrisleri/Tanımlayıcı bağıntılar
32	2^{6-1}_{VI}	C(6,5,6)	{1}	1 1 1 1 1 1
	1. 2^{7-2}_{IV}	B(7,5,4)	{1,2,0,0}	1 1 1 1 0 1 0 1 1 0 1 1 0 1
	2. 2^{7-2}_{IV}	B(7,5,4)	{2,0,1,0}	0 0 1 1 1 1 0 1 1 0 0 1 0 1
	3. 2^{7-2}_{IV}	B(7,5,4)	{3,0,0,0}	0 0 1 1 1 1 0 0 1 0 1 1 0 1
	1. 2^{8-3}_{IV}	B(8,5,4)	{3,4,0,0,0}	1 1 1 0 0 1 0 0 1 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1
	2. 2^{8-3}_{IV}	B(8,5,4)	{5,0,2,0,0}	0 0 1 1 1 1 0 0 0 1 0 1 1 0 1 0 1 1 1 0 0 0 0 1
	3. 2^{8-3}_{IV}	B(8,5,4)	{6,0,0,0,1}	0 0 1 1 1 1 0 0 0 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1
	1. 2^{9-4}_{IV}	B(9,5,4)	{6, 8, 0, 0, 1, 0}	0 1 1 1 1 1 0 0 0 1 0 1 1 1 0 1 0 0 1 1 0 1 1 0 0 1 0 1 1 1 0 1 0 0 0 1
	2. 2^{9-4}_{IV}	B(9,5,4)	{7, 7, 0, 0, 0, 1}	0 1 1 1 1 1 0 0 0 1 0 0 1 1 0 1 0 0 1 1 1 0 1 0 0 1 0 1 1 1 1 0 0 0 0 1
	3. 2^{9-4}_{IV}	B(9,5,4)	{9, 0, 6, 0, 0, 0}	0 0 1 1 1 1 0 0 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1 0 1 0 0 0 0 1
	4. 2^{9-4}_{IV}	B(9,5,4)	{10, 0, 4, 0, 1, 0}	0 0 1 1 1 1 0 0 0 0 1 0 1 1 0 1 0 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 0 0 0 1
	5. 2^{9-4}_{IV}	B(9,5,4)	{14, 0, 0, 0, 1, 0}	0 0 1 1 1 1 0 0 0 0 1 0 1 1 0 1 0 0 0 1 1 0 1 0 0 1 0 0 1 1 1 0 0 0 0 1
	1. 2^{10-5}_{IV}	B(10,5,4)	{10,16,0,0,5,0,0}	1 1 1 1 0 1 0 0 0 0 1 1 1 0 1 0 1 0 0 0 1 1 0 1 1 0 0 1 0 0 1 0 1 1 1 0 0 0 1 0 0 1 1 1 1 0 0 0 0 1

Çizelge 7.1. (Devam)

Deneme	Tasarım	Kod karşılığı ($n,k,d^{\perp}_{min}$)	Ağırlık dağılımı$^{\perp}$ i=Çmax,...,n	Denklik kontrol matrisleri/Tanımlayıcı bağıntılar
32	2. 2^{10-5}_{IV}	B(10,5,4)	{15,0,15,0,0,0,1}	0 0 1 1 1 1 0 0 0 0 0 1 0 1 1 0 1 0 0 0 1 0 1 0 1 0 0 1 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1
	3. 2^{10-5}_{IV}	B(10,5,4)	{16,0,12,0,3,0,0}	0 0 1 1 1 1 0 0 0 0 0 1 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 1 0 0 1 0 1 1 0 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1
	2^{11-6}_{IV}	B(11,5,4)	{25,0,27,0,10,0,1,0}	1 1 1 0 0 1 0 0 0 0 0 0 1 1 1 0 0 1 0 0 0 0 0 0 1 1 1 0 0 1 0 0 0 1 0 1 1 0 0 0 0 1 0 0 1 0 0 1 1 0 0 0 0 1 0 0 1 0 1 1 0 0 0 0 0 1
64	2^{7-1}_{VII}	C(7,6,7)	{1}	1 1 1 1 1 1 1
	2^{8-2}_{V}	B(8,6,5)	{2, 1, 0, 0}	1 1 1 1 0 0 1 0 1 1 0 0 1 1 0 1
	1. 2^{9-3}_{IV}	B(9,6,4)	{1, 4, 2, 0, 0, 0}	1 1 1 1 0 0 1 0 0 1 0 1 0 1 1 0 1 0 0 0 1 1 1 1 0 0 1
	2. 2^{9-3}_{IV}	B(9,6,4)	{2, 3, 1, 1, 0, 0}	0 0 0 1 1 1 1 0 0 0 1 1 0 1 1 0 1 0 1 0 1 1 0 0 0 0 1
	3. 2^{9-3}_{IV}	B(9,6,4)	{2,4,0,0,0,1,0)	0 0 0 1 1 1 1 0 0 0 1 1 0 1 1 0 1 0 1 0 1 0 1 1 0 0 1
	1. 2^{10-4}_{IV}	B(10,6,4)	{2,8,4,0,1,0,0}	0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0 1 0 0 1 1 0 1 1 0 0 0 1 0 1 1 1 0 1 0 0 0 0 1
	2. 2^{10-4}_{IV}	B(10,6,4)	{3,6,4,2,0,0,0}	0 0 0 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 0 0 1 0 1 0 0 1 0 0 1 0 1 1 1 1 0 0 0 0 0 1
	3. 2^{10-4}_{IV}	B(10,6,4)	{3,7,4,0,0,1,0}	0 0 1 1 1 1 1 0 0 0 0 1 0 1 1 1 0 1 0 0 1 1 1 0 0 1 0 0 1 0 1 1 1 1 1 0 0 0 0 1

Çizelge 7.1. (Devam)

Deneme	**Tasarım**	**Kod karşılığı (n,k, $d^{\perp}_{min}$)**	**Ağırlık dağılımı$^{\perp}$ i=Çmax,...,n**	**Denklik kontrol matrisleri/Tanımlayıcı bağıntılar**
64	2^{11-5}_{IV}	B(11,6,4)	{4, 14, 8, 0, 3, 2, 0, 0}	0 0 1 1 1 0 1 0 0 0 0 1 1 1 1 0 0 0 1 0 0 0 1 1 0 0 0 1 0 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0 1 0 0 1 1 1 0 0 0 0 1
128	2^{8-1}_{VIII}	C(8,7,8)	{1}	1 1 1 1 1 1 1 1
	2^{9-2}_{VI}	B(9,7,6)	{3, 0, 0, 0}	1 0 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1
	1. 2^{9-2}_{V}	B(9,7,5)	{1,1,1,0,0}	0 0 1 1 1 1 1 1 0 1 1 0 0 0 1 1 0 1
	2. 2^{9-2}_{V}	B(9,7,5)	{2,0,0,1,0}	0 0 0 1 1 1 1 1 0 1 1 1 0 0 0 1 0 1
	3. 2^{9-2}_{V}	B(9,7,5)	{2,1,0,0,0}	0 0 0 1 1 1 1 1 0 0 1 1 0 0 1 1 0 1
	1. 2^{10-3}_{V}	B(10,7,5)	{3,3,1,0,0,0}	1 1 1 0 0 0 1 1 0 0 0 1 1 1 1 0 0 0 1 0 1 0 1 1 0 1 0 0 0 1
	2. 2^{10-3}_{V}	B(10,7,5)	{4,2,0,1,0,0}	0 0 0 1 1 1 1 1 0 0 0 1 1 0 0 1 1 0 1 0 1 1 1 0 1 0 0 0 0 1
	2^{11-4}_{V}	B(11,7,5)	{6, 6, 2, 1, 0, 0, 0}	1 1 1 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 1 0 0 1 0 1 1 0 1 0 0 0 1 0 1 1 1 1 1 1 1 0 0 0 1

KAYNAKLAR

Arazi, B., 1988, A Commensense Approach to the Theory of Error Correcting Codes, Computer System Series, MIT Press, 203p.

Bilous, R.T., Rees, G.H.J.,2003, An enumeration of binary self-dual codes of length 32, http://www.cs.umanitoba.ca/~vanrees/bil.pdf.

Box, G.E.P., Hunter, J.S, 1961, The 2^{k-p} fractional factorial designs part I,2000, part II, 1961, Technometrics.

Box, G.E.P.; Hunter, W.G.; and Hunter, J.J., 1978, Statistics for Experiments, John Wiley&Sons, New York, N.Y., 653p.

Brouwer, A.E., Cohen A.M., Neguyen M.V.M,2003,Fractional factorial desingns of strength 3 and small run size, http://win.tue.nl/amc/pub /cbn.pdf.

Chen, H.,1998, Some projective properties of fractional factorial designs, Statistics & Probabilitiy Letters,40,185-188.

Çallıalp, F.,1999, "Sayılar Teorisi", İstanbul, 168s.

Dey, A., 1985, Orthogonal Fractional Factorial Designs, New Delhi, Wiley Eastern,133 p.

Franklin, M.F., 1984, Constructions tables of minimum aberration designs, Technometrics, 236,3,225-232.

Fries, A., Hunter, W.G., 1980, Minimum aberration 2^{k-p} designs, Technometrics, 22, 4, 601-608.

Gallian, J.A., 1986, "Contemporary Abstract Algebra", D.C.Health and Company, 426p.

Gulliver, T.A. , Bhargava V.K.,2000, New linear codes over GF(8), Applied Mathematics Letters,13,17-19.

Hamming, R. W., 1950, Error detecting and error correcting codes, The Bell System Technical Journal, XXVI,2, 147-160.

Hedeyat, A.S.; Sloane, N.J.A.; and Stufken J.,1999, Orthogonal Arrays: Theory and Applications, Springer-Verlag, NY, 363p.

Kaya, A., 1988, Sayılar Kuramına Giriş, İzmir.

Kuş, P., 2002, "Hata düzeltme kodlaması", Kara Harp Okulu Bilim Dergisi, 2,18-34, Kara Harp Okulu Basımevi.

MacWilliams F.J., Sloane N. J.A.,1977, "The Theory of Error-Correcting Codes", North-Holland Mathematical Library, Elsevier Science Publishers,762p.

Montgomery, D.C., 1984, Design and Analysis of Experiments, Second Edition, John Wiley&Sons, New York, 538 p.

Nguyen, G.D.,1997,A polynomial construction of perfect codes, Computers Math. Applic. Vol.33,No.8,127-131.

Pless, V., 1998, Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, Inc., Third Edition, 207p.

Pretzel, O.,1992, Error-Correcting Codes and Finite Fields, Clarendon Press, Oxford, Student Edition,341p.

Raktoe, B.L., Hedeyat, A., Federer, W.T.,1981, Factorial Designs, John Wiley & Sons, New York, N.Y.

Rao, C.R., 1946,On Hypercubes of Strength d and a System of Confounding in Factorial Experiments, Bull. Cal. Math. Soc.,38,67-78.

Sloane, N.J.A.,Thompson, J.G.,1983, Cyclic self-dual codes,IEEE Trans. Information Theory,29,364-366.

Stewart, I.,1973, “Galois Theory”, Chapman and Hall, 226p.

Sun, D.X., Chen, J., Wu, C.F.J., 1993, A catalogue of two-level and three-level fractional factorial designs with small runs, Internal. Statist. Rev.,61,131-145.

Vanstone, S.A; and Oorschot van P.C., 1989, “An Introduction to Error-Correcting Codes with Applications”Kluwer Academic Publishers, 283p.

Wiggert, D., 1978, “Error-Control Coding and Applications, Artech House, 203p.

Wu, C.F.J.; and Chen, Y.Y., 1991, A graph-aided method for planning two-level experiments when certain interactions are important, IIQP Research Report 91-07, University of Waterloo, Dept. of Statistics and Actuarial Science.

Wu, C.F.J., Chen, Y.Y., 1992, A Graph-aided method for planning two-level experiments when certain interactions are important, Technometrics, 34, 162-175.

EK-1. 2^{n-p} Kesirli Çok Etkenli Tasarımları

Deneme Sayısı : 2^{n-p}	Etken Sayısı (n)								
	3	4	5	6	7	8	9	10	11
4	2_{III}^{3-1} ±C=AB								
8	2^3	2_{IV}^{4-1} ±D=ABC	2_{III}^{5-2} ±D=AB ±E=AC	2_{III}^{6-3} ±D=AB ±E=AC ±F=BC	2_{III}^{7-4} ±D=AB ±E=AC ±F=BC ±G=ABC				
16	2^3 2 tekrar	2^4	2_V^{5-1} ±E=ABCD	2_{IV}^{6-2} ±E=ABC ±F=BCD	2_{IV}^{7-3} ±E=ABC ±F=BCD ±G=ACD	2_{IV}^{8-4} ±E=BCD ±F=ACD ±G=ABC ±H=ABD	2_{III}^{9-5} ±E=ABC ±F=BCD ±G=ACD ±H=ABD ±I=ABCD	2_{III}^{10-6} ±E=ABC ±F=BCD ±G=ACD ±H=ABD ±I=ABCD ±J=AB	2_{III}^{11-7} ±E=ABC ±F=BCD ±G=ACD ±H=ABD ±I=ABCD ±J=AB ± K=AC
32	2^3 4 tekrar	2^4 2 tekrar	2^5	2_{VI}^{6-1} ±F=ABCDE	2_{IV}^{7-2} ±F=ABCD ±G=ABDE	2_{IV}^{8-3} ±F=ABC ±G=ABD ±H=BCDE	2_{IV}^{9-4} ±F=BCDE ±G=ACDE ±H=ABDE ±I=ABCE	2_{IV}^{10-5} ±F=ABCD ±G=ABCE ±H=ABDE ±I=ACDE ±J=BCDE	2_{IV}^{11-6} ±F=ABC ±G=BCD ±H=CDE ±I=ACD ±J=ADE ±K=BDE
64	2^3 8 tekrar	2^4 4 tekrar	2^5 2 tekrar	2^6	2_{VII}^{7-1} ±G=ABCDEF	2_V^{8-2} ±G=ABCD ±H=ABEF	2_{IV}^{9-3} ±G=ABCD ±H=ACEF ±I=CDEF	2_{IV}^{10-4} ±G=BCDF ±H=ACDF ±I=ABDE ±J=ABCE	2_{IV}^{11-5} ±G=CDE ±H=ABCD ±I=ABF ±J=BDEF ±K=ADEF
128	2^3 16 tekrar	2^4 8 tekrar	2^5 4 tekrar	2^6 2 tekrar	2^7	2_{VIII}^{8-1} ±H=ABCDEFG	2_{VI}^{9-2} ±H=ACDFG ±I=BCEFG	2_V^{10-3} ±H=ABCG ±I=BCDE ±J=ACDF	2_V^{11-4} ±H=ABCG ±I=BCDE ±J=ACDF ±K=ABCDEFG

ÖZGEÇMİŞ

Adı Soyadı : Nazan DANACIOĞLU

Doğum Yeri : Seydişehir

Doğum Yılı : 1972

Medeni Hali : Bekar

Eğitim ve Akademik Durumu:

Lise 1985-1989 : Ankara Lisesi

Lisans 1989-1994 : H.Ü. Fen Bilimleri Enstitüsü İstatistik Anabilim Dalı

Y.Lisans 1995-1999: H.Ü. Fen Bilimleri Enstitüsü İstatistik Anabilim Dalı

Yabancı Dil :İngilizce

İş Tecrübesi:

2000- H.Ü. Fen Bilimleri Enstitüsü Araştırma Görevlisi