T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

KRİPTOGRAFİK FONKSİYONLAR VE İNSİDANS YAPILARI

BÜŞRA YILDIZ ÇAPKAN

YÜKSEK LİSANS TEZİ

Jüri Üyeleri : **Prof. Dr. Seher TUTDERE KAVUT** **(Tez Danışmanı)**
Prof. Dr. Nesrin TUTAŞ
Doç. Dr. Pınar METE

BALIKESİR, OCAK - 2026

ETİK BEYAN

Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak tarafımca hazırlanan "**Kriptografik Fonksiyonlar ve İnsidans Yapıları**" başlıklı tezde;

- Tüm bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Kullanılan veriler ve sonuçlarda herhangi bir değişiklik yapmadığımı,
- Tüm bilgi ve sonuçları bilimsel araştırma ve etik ilkelere uygun şekilde sunduğumu,
- Yararlandığım eserlere atıfta bulunarak kaynak gösterdiğimi,

beyan eder, aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ederim.

Büşra YILDIZ ÇAPKAN

Bu tez çalışması TÜBİTAK-BİDEB 2210-A Yurtiçi Genel Yüksek Lisans Burs Programı tarafından desteklenmiştir.

ÖZET

KRİPTOGRAFİK FONKSİYONLAR VE İNSİDANS YAPILARI
YÜKSEK LİSANS TEZİ
BÜŞRA YILDIZ ÇAPKAN
BALIKESİR ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
(TEZ DANIŞMANI: PROF. DR. SEHER TUTDERE KAVUT)

BALIKESİR, OCAK - 2026

Kriptografide önemli bir role sahip olan Boole ve vektörel fonksiyonların kodlama teorisi ve tasarım teorisinde birçok farklı uygulaması vardır ve bunun tersi de geçerlidir. Son zamanlarda bu fonksiyonların insidans yapıları, özellikle tasarımları üzerine birçok çalışma yapılmıştır. Bu tezde, literatür incelenerek, kriptografik fonksiyonların tanım ve temel özellikleri ile birlikte, bu fonksiyonların insidans yapıları, özellikle kaybolan ve kaybolmayan düzlemleri ile ilgili bilinen sonuçlar, bir derleme olarak sunulmaktadır.

ANAHTAR KELİMELER: Boole fonksiyon, insidans yapı, lineer kod, tasarım, vektörel fonksiyon

Bilim Kod / Kodları : 20401 Sayfa Sayısı : 42

ABSTRACT

CRYPTOGRAPHIC FUNCTIONS AND INCIDENCE STRUCTURES
MSC THESIS
BÜŞRA YILDIZ ÇAPKAN
BALIKESIR UNIVERSITY INSTITUTE OF SCIENCE
MATHEMATICS
(SUPERVISOR: PROF. DR. SEHER TUTDERE KAVUT)

BALIKESİR, JANUARY - 2026

Boolean and vectorial functions, which play an important role in cryptography, have many different applications in coding theory and design theory, and vice versa. Recently, many studies have been conducted on the incidence structures of these functions, especially their designs. In this thesis, by reviewing the literature, together with the definitions and fundamental properties of cryptographic functions, a survey of known results concerning incidence structures of these functions, in particular vanishing and non-vanishing flats, is presented.

KEYWORDS: Boolean function, incidence structure, linear code, design, vectorial function

Science Code / Codes : 20401 Page Number : 42

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

TABLO LİSTESİ

Sayfa

SEMBOL LİSTESİ

$\mathbb{F}_q$	: q elemanlı sonlu cisim
$\mathbb{F}_q^n$	: q elemanlı sonlu cisim üzerinde tanımlı n-boyutlu vektör uzayı
$\boldsymbol{C}$	: Uzunluğu n, boyutu k olan $\mathbb{F}_q$ üzerinde tanımlı kod
$\lvert\boldsymbol{C}\rvert$	: C kodunun büyüklüğü
$\boldsymbol{d}(\boldsymbol{C})$	: C kodunun minimum mesafesi
$\boldsymbol{C}^{\perp}$	: C kodunun dual (ortogonal) kodu
$\boldsymbol{S} = (\boldsymbol{\mathcal{P}}, \boldsymbol{\mathcal{B}})$	: İnsidans yapı, burada $\mathcal{P}$, $\mathcal{S}$' nin nokta kümesi ve $\mathcal{B}$, $\mathcal{S}$' nin blok kümesi
$\boldsymbol{M}(\boldsymbol{S})$	: S insidans yapısının matrisi
$\boldsymbol{W_F}$	: F fonksiyonunun Walsh dönüşümü
$\boldsymbol{\mathcal{VF}}(\boldsymbol{F})$	: F fonksiyonunun kaybolan düzlemleri
$\boldsymbol{\mathcal{NF}_{\mathcal{V}}}(\boldsymbol{F})$	: F fonksiyonunun kaybolmayan düzlemleri
$\boldsymbol{\Delta F}$	: F fonksiyonunun diferansiyel spektrumu
$\boldsymbol{C_F}$	: F ile tanımlanan lineer kod

ÖNSÖZ

Yüksek lisans eğitimim boyunca ve bu tezin hazırlanma sürecinde bana yol gösteren, bilgi ve tecrübelerinden faydalandığım, danışmanım Prof. Dr. Seher TUTDERE KAVUT'a, teşekkürlerimi sunarım.

Eğitimim süresince her konuda desteklerini esirgemeyen başta Sayın Prof. Dr. Sebahattin İKİKARDEŞ olmak üzere diğer bölüm hocalarıma da teşekkür ederim.

Ayrıca çalışmam boyunca yanımda olan matematik yoldaşım Cemile CÜR'e en içten teşekkürlerimi sunarım. Bu süreçteki dostluğu ve sabrı için kendisine minnettarım. Benim matematik sevgimi fark eden ve bu yolda beni destekleyen ortaokul matematik öğretmenim Sevgili Hüseyin Koç'a en içten dileklerimle şükranlarımı sunarım.

Okul sürecim daha başlamadan bana çarpım tablosunu öğretmeye başlayarak matematik temellerimi oluşturan, matematiğe olan merak duygumu hep canlı tutan babam Recep YILDIZ'a ve hayatım boyunca aldığım kararlarda desteğini esirgemeyen her zaman yanımda olan annem Ayşe YILDIZ'a en derin şükranlarımı sunarım. Bana yalnızca akademik anlamda değil, aynı zamanda hayata karşı duruşumda da yol gösterici oldular. Bu süreçte attığım her adımda, verdikleri emek ve gösterdikleri özveri benim için en büyük ilham kaynağı olmuştur. Bu tez çalışmasını tamamlarken, onların varlığının ve desteğinin değerini bir kez daha hissettim. Hayatımın her aşamasında yanımda oldukları için kendimi daima şanslı hissetmekteyim.

Uzun ve meşakkatli bu yolculukta en büyük dayanağım olan sevgili eşim Cihat ÇAPKAN'a duyduğum en derin minnettarlığı ifade etmek isterim. Zorlu ve yorucu geçen bu süreçte, sabrı, sevgisi ve anlayışıyla bana güç verdi; umutsuzluğa kapıldığım her an sözleriyle yeniden ayağa kalkmamı sağladı. Onun sessiz fedakarlıkları ve içten desteği benim için bu yolculuğu katlanabilir kıldı. Yazmış olduğum bu satırlar, ona duyduğum teşekkürün küçük bir ifadesidir. Açıkçası bu tez, yalnızca benim emeğimin değil, aynı zamanda onun sabrının, sevgisinin ve desteğinin de bir ürünüdür.

Son olarak, yüksek lisans eğitimim boyunca maddi desteğinden dolayı "2210-A Yurt İçi Genel Yüksek Lisans Burs Programı'na kayıtlı bursiyer olduğum TÜBİTAK-BİDEB'e saygılarımla teşekkür ederim.

Balıkesir, 2026 **Büşra Yıldız Çapkan**

1. GİRİŞ

Kriptografi, modern bilgi güvenliğinin temel taşlarından biridir ve verilerin gizliliğini, bütünlüğünü ve kimlik doğrulamasını sağlamada önemli rol oynar. Bu sebeple, kriptografik fonksiyonlar özellikle şifreleme algoritmalarının güvenliğini belirleyen en önemli matematiksel araçlardan biridir. Kriptografik fonksiyonlar, kriptografi alanında kullanılan ve güvenlik amaçları için tasarlanmış matematiksel fonksiyonlardır. Bunlar genellikle şifre belirleme, imza oluşturma veya kimlik doğrulama işlemlerinde kullanılmaktadır.

İnsidans yapıları ise matematiksel nesnelerin kombinatorik bir yapısal özelliğini ifade eder. Kriptografide ve özellikle blok şifre tasarımında Boole fonksiyonları temel unsurlar arasında yer almaktadır. Kriptolojik bir fonksiyonun doğrusal saldırılara karşı dayanıklı olabilmesi için doğrusal olmama değerinin yüksek olması gerekmektedir. Mümkün olan en yüksek doğrusal olmama değerine sahip fonksiyonlar bükük (Bent) fonksiyonlardır. Bükük fonksiyonlar, olası en az doğrusallığa sahip olan Boole fonksiyonlardır; yani afin fonksiyonlar kümesine en fazla uzaklığa sahip fonksiyonlardır. Bu kavram ilk olarak 1976 yılında Rothaus tarafından ortaya atılmış [13] ve kriptolojik uygulamalardaki öneminden dolayı geniş ilgi görmüştür.

Kriptografik fonksiyonların incelenmesinde yalnızca fonksiyonel özellikler değil, aynı zamanda bu fonksiyonların ilişkili olduğu insidans yapıları da önemli bir araştırma alanı oluşturur. İnsidans yapıları, noktalar ve bloklar arasındaki düzenli ilişkileri tanımlayan kombinatorik sistemlerdir. Bu yapılar, hem tasarım teorisi hem de kodlama teorisi ile doğrudan bağlantılıdır. Dolayısıyla, kriptografik fonksiyonların insidans yapıları üzerinden incelenmesi, fonksiyonların yapısal özelliklerini anlamada güçlü bir yöntem sunmaktadır. Ayrıca, bu tezde insidans yapılardan, özellikle tasarımlardan bahsedilecektir.

Bu tezde, kriptografik fonksiyonların insidans yapıları ayrıntılı olarak ele alınmış ve literatürdeki güncel çalışmalar derlenmiştir. Çalışmanın amacı, hem kriptografik fonksiyonların matematiksel özelliklerini hem de bu fonksiyonların tasarım ve kodlama teorisi bağlamındaki uygulamalarını bütüncül bir şekilde ortaya koymaktır.

Tezin 2. bölümünde, tez boyunca kullanılacak olan temel kavramlar ve tanımlar verilmiştir. Bu kapsamda sonlu cisimler, lineer kodlar ve insidans yapılar ayrıntılı olarak açıklanmış ayrıca, kriptografik fonksiyonların temel özellikleri ve örnekleri sunulmuştur. Devamında fonksiyonların plato özellikleri ve Walsh spektrumları üzerinden elde edilen yapılar tartışılmıştır.

Tezin 3. bölümünde kriptografik fonksiyonların insidans yapıları incelenmiştir. Bu bağlamda, kaybolan ve kaybolmayan düzlemler kodlama teorisi ve tasarım teorisi açısından ele alınmıştır. Özellikle bükük fonksiyonlar ve bunların genellemeleri tasarım teorisi açısından değerlendirilmiştir. Grup etkileri aracılığıyla tanımlanan geçişli (transitivite) kavramı ile kodların otomorfizma grupları arasındaki ilişki incelenerek, insidans yapıların nasıl ortaya çıktığı gösterilmiştir. Böylece, kodlama teorisi ile tasarım teorisi arasındaki geçişler matematiksel olarak ele alınarak kriptografik fonksiyonların insidans yapıları derinlemesine ortaya konmuştur.

Tezin 4. bölümünde, tez kapsamında ulaşılan sonuçlar değerlendirilmiş ve gelecekte yapılabilecek çalışmalara yönelik öneriler sunulmuştur.

2. TEMEL BİLGİLER

Bu bölümde, tez boyunca başvurulacak temel tanım ve teoremler ile bunlara ilişkin sonuçlar, [1], [3], [4], [6] numaralı kaynaklardan yararlanılarak derlenmiştir.

2.1 Sonlu Cisimler

Sonlu cisimler, cebirsel yapıların en temel örneklerinden birisidir ve kriptografi ile kodlama teorisinde önemli uygulamalara sahiptir. Bu yüzden, ilk olarak sonlu cisimleri ele alacağız.

2.1 Tanım Boştan farklı bir $\mathbb{F}$ kümesi alalım. $\mathbb{F}$ kümesi üzerinde aşağıdaki özellikleri sağlayan *toplama* $(+)$ ve *çarpma* $(\cdot)$ işlemlerinin tanımlandığını varsayalım:
(i) Kapalılık özelliği: Her $x, y \in \mathbb{F}$ için hem toplama hem de çarpma işlemleri altında kapalılığı sağlar; yani $+$ ve $\cdot$ altında sırasıyla, $x + y \in \mathbb{F}$ ve $x \cdot y \in \mathbb{F}$,
(ii) Değişme özelliği: Her $x, y \in \mathbb{F}$ için $x + y = y + x$ ve $x \cdot y = y \cdot x$,
(iii) Birleşme özelliği: Her $x, y, z \in \mathbb{F}$ için $(x + y)+z = x+(y + z)$ ve $x\cdot(y \cdot z) = (x \cdot y)\cdot z$,
(iv) Dağılma özelliği: Her $x, y, z \in \mathbb{F}$ için $x \cdot (y + z) = x \cdot y + x \cdot z$
(v) Birim elemanların varlığı: $\mathbb{F}$ 'de öyle $0, 1$ elemanları vardır ki her $x \in \mathbb{F}$ aldığımızda $x + 0 = x,\ x \cdot 1 = x$ ve $x \cdot 0 = 0$.
(vi) Alınan her $x \in \mathbb{F}$ için $x + (-x) = (-x) + x = 0$ eşitliğini sağlayan bir $-x \in \mathbb{F}$ bulunur. Bu elemana, x 'in toplama işlemine göre *toplamsal tersi* denir.
(vii) Her $x \in \mathbb{F}$ ve $0 \neq x$ için $x \cdot x^{-1} = x^{-1} \cdot x = 1$ eşitliğini sağlayan bir $x^{-1} \in \mathbb{F}$ bulunur. Bu elemana, x 'in çarpma işlemine göre *çarpımsal tersi* denir.
(i)-(vii) numaralı maddelerde belirtilen tüm yapısal özellikleri karşılayan $(\mathbb{F}, +, \cdot)$ yapısı bir *cisim* olarak tanımlanır.
Yazım kolaylığı açısından, çarpma işlemi için $x \cdot y$ yerine doğrudan xy biçimi tercih edilir. Ayrıca, sıfır dışındaki elemanlardan oluşan $\mathbb{F} \setminus \{0\}$ kümesi ise yaygın olarak $\mathbb{F}^*$ simgesiyle gösterilmektedir.

2.2 Tanım $\mathbb{F}$ bir cisim olsun. $\mathbb{F}$ 'nin sonlu sayıda elemanı varsa $\mathbb{F}$ 'ye, *sonlu cisim* denir.

2.3 Teorem [3] Herhangi bir p asal sayısı ve pozitif bir n tam sayısı verildiğinde, eleman sayısı $q = p^n$ olan bir sonlu cisim tanımlanabilir. Bu biçimde olan bir cisim, cebirsel yapı içerisinde genellikle $\mathbb{F}_q$ biçiminde gösterilir. Özellikle $n = 1$ durumunda, yani $q = p$ olduğunda, bu sonlu cisim $\mathbb{F}_p = \mathbb{Z}_p$ ile ifade edilir.

2.4 Örnek $\mathbb{F}_p = \mathbb{Z}_p = \{\, 0, 1, 2, \ldots, p - 1 \,\}$ sonlu cisminde toplama ve çarpma işlemleri

$mod\ p$ 'ye göre yapılır.

2.5 Teorem [3] $\mathbb{Z}_p$ kümesi toplama ve çarpma işlemleri altında bir cisim oluşturur ancak ve ancak p bir asal sayıdır.

2.6 Tanım $\mathbb{E}$ ve $\mathbb{F}$ iki cisim olsun. $\mathbb{E}$ 'den $\mathbb{F}$ 'ye birebir ve örten bir $f : \mathbb{E} \to \mathbb{F}$ dönüşümü tanımlansın. Eğer her $x, y \in \mathbb{E}$ için

$$f(x+y) = f(x) + f(y) \quad \text{ve} \quad f(xy) = f(x)f(y)$$

eşitlikleri sağlanıyorsa, $\mathbb{E}$ ve $\mathbb{F}$ cisimlerine *eşyapılı cisimler* denir.

2.7 Önerme [3] $\mathbb{F}$, karakteristiği p olan bir cisim olsun. Buna göre $\mathbb{F}$ 'nin p elemanlı bir altcismi vardır ve bu altcisim $\mathbb{Z}_p$ ile eşyapılıdır.

2.2 Lineer Kodlar

Lineer kodlar, kodlama teorisinin en önemli konularından birisidir. Hata tespit ve düzeltme amacıyla kullanılan bu kodlar, sonlu cisimler üzerinde tanımlanır ve cebirsel yapıları sayesinde güçlü matematiksel özellikler taşımaktadır.

2.8 Tanım $A = \{a_1, a_2, ..., a_q\}$ kümesini ele alalım.

(i) $v_1, ...v_n \in A$ olmak üzere $v = v_1v_2...v_n$ şeklindeki bir diziye n-uzunluklu bir q-*lu sözcük* denir. v aynı zamanda $(v_1, v_2, ..., v_n)$ vektörü ile eşdeğer şekilde de düşünülebilir.

(ii) Aynı n uzunlukluğuna sahip q-lu sözcüklerin boş olmayan bir C kümesine q-*lu blok kodu* veya kısaca q-*lu kod* denir. C kümesinin her elemanına ise *kod sözcüğü* adı verilir. C içindeki kod sözcüklerinin sayısına C'nin büyüklüğü denir ve $|C|$ ile gösterilir.
Bu durumda, A kümesine *kod alfabesi* (code alphabet) ve bu kümenin elemanlarına ise *kod simgeleri* denilmektedir.

2.9 Tanım Bir sonlu A kümesi üzerinde tanımlı, uzunluğu n olan x ve y sözcükleri arasındaki farklı yerlerin sayısı *Hamming mesafesi* olarak adlandırılır ve $d(x, y)$ ile ifade edilir. Her $x = x_1x_2...x_n$ ve $y = y_1y_2...y_n$ olmak üzere $x, y \in A^n$ için

$$d(x, y) = \sum_{i=1}^{n} d(x_i, y_i)$$

şeklinde bulunabilir, burada x_i ve y_i 'nin uzunluğu 1 olduğundan

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

olarak tanımlanır.

2.10 Tanım $\mathbb{F}_q^n$ uzayında tanımlı bir x vektörünün kaç adet sıfırdan farklı bileşen içerdiği, o vektörün *Hamming ağırlığı* olarak adlandırılır. Bu ağırlık $wt(x)$ ile gösterilir ve aynı zamanda x ile sıfır vektörü arasındaki Hamming mesafesine eşittir. Bu durumda,

$$wt(x) = d(x, 0).$$

2.11 Uyarı Bir q-lu sözcük $x = x_1x_2...x_n$ için Hamming ağırlığı, her bir bileşenin ayrı ayrı değerlendirilmesiyle elde edilir. Bu durumda toplam ağırlık, bileşenlerin bireysel ağırlıklarının toplamına eşittir:

$$wt(x) = wt(x_1) + wt(x_2) + ... + wt(x_n),$$

burada $x_i \in \mathbb{F}_q$ bileşeni için ağırlık değeri şu şekilde belirlenir:

$$wt(x_i) = d(x_i, 0) = \begin{cases} 1 & x_i \neq 0 \text{ ise,} \\ 0 & x_i = 0 \text{ ise.} \end{cases}$$

2.12 Tanım Sonlu cisim $\mathbb{F}_q$ üzerinde tanımlı $\mathbb{F}_q^n$ vektör uzayının herhangi bir C alt uzayı, uzunluğu n olan bir *lineer kod* olarak adlandırılır.

Eğer bir $C \subseteq \mathbb{F}_q^n$ kodu için, kod sözcüklerinin toplamı ve bir skaler sayı ile çarpımı yine kod sözcüğünü veriyorsa, bu kodu lineer olarak adlandırırız. Dolayısıyla lineer kodlar vektör uzayının cebirsel yapısını koruyan özel alt kümelerdir. $\mathbb{F}_q^n$ uzayına ise ayrıca *q-lu Hamming uzayı* denir.

Lineer kodlardan t-tasarımları elde edilmektedir. Bununla ilgili daha detaylı bilgiler ileriki bölümlerde verilecektir.

2.13 Tanım V, $\mathbb{F}_q$ sonlu cismi üzerinde tanımlanan bir vektör uzayı olsun. V uzayını üreten ve lineer bağımsız olan bir B alt kümesi varsa bu kümeye, V 'nin bir *bazı (tabanı)* denir.

Her vektör uzayının en az bir bazı vardır. Ayrıca bir vektör uzayının farklı bazları bulunabilir. Bir vektör uzayında seçilen her baz aynı sayıda eleman içerir. Buradaki sabit sayı, söz konusu vektör uzayının boyutu olarak adlandırılır. Dolayısıyla, k-boyutlu bir vektör uzayı için boyut ifadesi $boy_{\mathbb{F}_q}(V) = k$ biçiminde gösterilir.

2.14 Tanım C bir lineer kod olsun. Satırları C 'nin bir bazı olan bir matrise C kodunun *üreteç matrisi* denir.

2.15 Örnek $C = \{0000,\ 1010,\ 0101,\ 1111\} \subseteq \mathbb{F}_2^4$ kümesi, $\mathbb{F}_2$ üzerinde bir lineer koddur. Öncelikle, C için bir baz bulmamız gerekir. $B = \{1010,\ 0101\}$ kümesinin C için bir baz olduğunu gösterelim:

(i) $1111 = 1010 + 0101$,

(ii) Şimdi $a_1, a_2 \in \mathbb{F}_2$ olmak üzere:

$$a_1 \cdot (1010) + a_2 \cdot (0101) = 0000 \Rightarrow a_1 = a_2 = 0.$$

Bu durumda, 1010 ve 0101 vektörleri lineer bağımsızdır. Sonuç olarak, B, C için bir tabandır. O halde, C için bir üreteç matris

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

olarak yazılabilir.

2.16 Tanım En az iki sözcük içeren bir C kodu için *minimum mesafe*

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

olarak tanımlanır.

Sonlu cisim olan $\mathbb{F}_q$ üzerinde vektör uzayı yapısına sahip olan C kodunun boyutu, bu lineer *kodun boyutu* olarak adlandırılmakta ve $boy(C)$ sembolüyle gösterilmektedir.

$C \subseteq \mathbb{F}_q^n$ biçiminde tanımlanan bir lineer kodun uzunluğu n, boyutu k ve minimum mesafesi d olmak üzere, bu kod bir $[n, k, d]_q$-kodu şeklinde gösterilir. Bu üçlü (n, k, d), kodun *parametreleri* olarak adlandırılmaktadır.

2.17 Örnek $\mathbb{F}_2$ cismi üzerinde tanımlanan $C = \{000, 001, 010, 011\}$ kümesi bir lineer koddur. Bu kodun minimum mesafesi $d(C) = 1$ 'dir, çünkü,

$d(000, 001) = 1 \quad d(000, 010) = 1$

$d(000, 011) = 2 \quad d(001, 010) = 2$

$d(001, 011) = 1 \quad d(010, 011) = 1.$

Burada kodun uzunluğu $n = 3$, kodun boyutu $k = 2$ 'dir. Böylece C bir $(3, 2, 1)$-üçlü kodu olduğu elde edilir.

2.18 Örnek $\mathbb{F}_2$ sonlu cismi üzerinde tanımlı $C = \{0000,\ 1000,\ 0100,\ 1100\}$ lineer kodunu ele alalım. Bu kod dört adet kod sözcüğünden oluşmaktadır ve her sözcük dört bileşenli bir vektördür. Kod sözcüklerinin Hamming ağırlıkları ayrı ayrı incelendiğinde:

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

elde edilir. Burada 1000 ve 0100 sözcükleri yalnızca tek bir sıfırdan farklı bileşen içerdiğinden ağırlıkları 1 'dir; 1100 ise iki bileşeni sıfırdan farklı olduğu için ağırlığı 2 'dir. Dolayısıyla kodun minimum Hamming ağırlığı 1 olarak bulunur. Lineer kodlar için minimum mesafe $d(C)$, sıfırdan farklı kod sözcüklerinin en küçük Hamming ağırlığına eşittir. Bu örnekte, $d(C) = wt(C) = 1$ sonucu elde edilir.

2.19 Tanım Uzunluğu n olan, $\mathbb{F}_q$ cismi üzerinde tanımlanan C lineer kodu için

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid \text{her } c \in C \text{ için } \langle x, c\rangle = 0\}$$

altuzayı C 'nin *dual kodu* olarak adlandırılır, burada $\langle x, c\rangle$ standart iç çarpımı ifade eder.

2.20 Teorem [3, Theorem 4.2.4] C, $\mathbb{F}_q$ üzerinde uzunluğu n olan bir lineer kod olsun.

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

(ii) $C^{\perp}$ bir lineer koddur ve $boy(C) + boy(C^{\perp}) = n$.

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

2.21 Örnek $q = 2$ olsun. Aşağıdaki kodu ele alalım:

$$C = \{0000,\ 1010,\ 0101,\ 1111\}.$$

Bu durumda kodun boyutu aşağıdaki şekilde hesaplanır:

$$\text{boy}(C) = \log_2 |C| = \log_2 4 = 2.$$

Ayrıca, kodun duali aşağıdaki şekilde elde edilir:

$$C^{\perp} = \{x \in \mathbb{F}_2^4 \mid \text{her } c \in C \text{ için } \langle x, c\rangle = 0\}.$$

Verilen kodun tüm elemanları birbirine dik olduğundan, iç çarpım her durumda sıfırdır. Örneğin:

$$\langle 1010,\ 0101\rangle = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 0.$$

Benzer şekilde diğer tüm çiftler için de iç çarpım sıfırdır. Bu nedenle:

$$C^{\perp} = C.$$

Yani bu kod kendi dualidir.

2.22 Örnek $q = 3$ olsun. Aşağıdaki kodu ele alalım:

$$C = \{000,\ 001,\ 002,\ 010,\ 020,\ 011,\ 012,\ 021,\ 022\}.$$

Bu kodun boyu, eleman sayısının q tabanındaki logaritması ile hesaplanır:

$$\text{boy}(C) = \log_3 |C| = \log_3 9 = 2.$$

Şimdi $C^{\perp}$ dual kodunu bulalım. Verilen C kodunun tüm elemanları $(0, *, *)$ biçimindedir. Dolayısıyla her $x = (x_1, x_2, x_3) \in C$ için

$$\langle x, (0, a, b)\rangle = x_1 \cdot 0 + x_2 \cdot a + x_3 \cdot b = x_2 a + x_3 b$$

şeklindedir. Bu ifadenin her $a, b \in \mathbb{F}_3$ için sıfır olabilmesi için $x_2 = x_3 = 0$ olmalıdır.
Sonuç olarak dual kod;

$$C^{\perp} = \{(0,0,0),\ (1,0,0),\ (2,0,0)\}$$

şeklinde elde edilir. Bu kodun boyutu ise

$$\text{boy}(C^{\perp}) = \log_3 |C^{\perp}| = \log_3 3 = 1.$$

Dolayısıyla C kodunun boyutu 2, dual kodunun boyutu ise 1 'dir.

2.3 İnsidans Yapılar

Kombinatorik tasarım teorisinin temel kavramlarından biri insidans yapılarıdır. Genel olarak bir insidans yapısı, belirli bir nokta kümesi ile bu noktaların alt kümelerinden oluşan blokların birlikte ele alınmasıyla tanımlanır. Bu nedenle insidans yapılar, noktalar ve bloklar arasındaki düzenli ilişkileri inceleyen matematiksel ifadelerdir.

İnsidans yapıların, özellikle t-(v, k, λ) tasarımlarının tanımlanmasında önemli bir rolü vardır. Burada v nokta sayısını, k blokta yer alan her kümenin eleman sayısını, λ ise her t

elemanlı alt kümesinin kaç tane bloktaki kümede yer aldığını belirtir. Bu tür yapılar, hem kombinatorik tasarım teorisinde hem de kriptografide fonksiyonların özelliklerini incelemek için güçlü bir araçtır.

Bu tezde ise insidans yapıları (n, m)-fonksiyonların plato (plateaued) özellikleriyle ilişkilendirilerek ele alınacaktır. Özellikle, fonksiyonların Walsh spektrumları ve kaybolan düzlem kavramları üzerinden elde edilen insidans yapılar, fonksiyonların plato olup olmadığını karakterize eden tasarımlar oluşturmaktadır. Böylece insidans yapılar, fonksiyonların yapısal özelliklerini anlamada yardımcı olmaktadır.

2.23 Tanım Sonlu bir insidans yapısı $\mathcal{S} = (\mathcal{P}, \mathcal{B})$, sonlu bir $\mathcal{P}$ noktalar kümesi ve $\mathcal{B}$, blok adı verilen altkümelerin bir koleksiyonundan oluşmaktadır.

2.24 Örnek $\mathcal{P} = \{1, 2, 3, 4, 5\}$ sonlu noktalar kümesi olsun ve bu kümenin 4 elemanlı alt kümeleri: $\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{1, 2, 4, 5\}, \{1, 3, 4, 5\}, \{2, 3, 4, 5\}$
5 elemanlı alt küme: $\{1, 2, 3, 4, 5\}$
Burada bloklar kümesini $\mathcal{B}$ ile tanımlayalım ve $\mathcal{P}$ 'nin tüm 4 ve 5 elemanlı alt kümelerinden oluşsun. Böylece $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ insidans yapıdır.

İnsidans yapı en genel tanımdır; noktalar ve bloklardan oluşan bir sistemdir. Tasarım ise insidans yapının özel bir türüdür; noktalar ve bloklar arasında belirli koşulları sağlar (bkz. Tanım 2.27).

2.25 Tanım $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ bir insidans yapı olsun. $\mathcal{S}$ ile ilgili tüm bilgiler, onun insidans matrisi olan $\mathbf{M}(\mathcal{S}) = (m_{i,j})$ ile ifade edilir. Bu matris, $b \times v$ boyutunda ikili (binary) bir matristir ve $m_{i,j} = 1$ ise $p_j \in B_i$ olur; yani p_j noktası $\mathcal{P}$ kümesinden ve B_i bloğu $\mathcal{B}$ kümesinden olmak üzere, p_j noktası B_i bloğunda yer alıyorsa $m_{i,j} = 1$ olur. Aksi takdirde $m_{i,j} = 0$ olur.

2.26 Örnek $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ insidans yapısının nokta kümesi $\mathcal{P} = \{p_1, p_2, p_3\}$ olsun ve blok kümesi $\mathcal{B} = \{B_1, B_2, B_3\}$ şu şekilde tanımlansın:

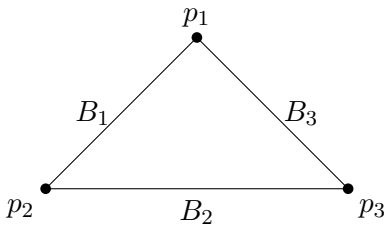
$$B_1 = \{p_1, p_2\}, \quad B_2 = \{p_2, p_3\}, \quad B_3 = \{p_1, p_3\}.$$

Bu durumda her nokta (yani $t = 1$) tam olarak $\lambda = 2$ blokta yer alır. Ayrıca $v = |\mathcal{P}| = 3$ ve her $i = 1, 2, 3$ için $k = |B_i| = 2$ 'dir. Dolayısıyla bu yapı bir $t - (v, k, \lambda) = 1 - (3, 2, 2)$ tasarımdır (bkz. Tanım 2.27).

İnsidans matrisi şu şekilde yazılır:

$$M(\mathcal{S}) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Burada satırlar blokları, sütunlar noktaları temsil eder.



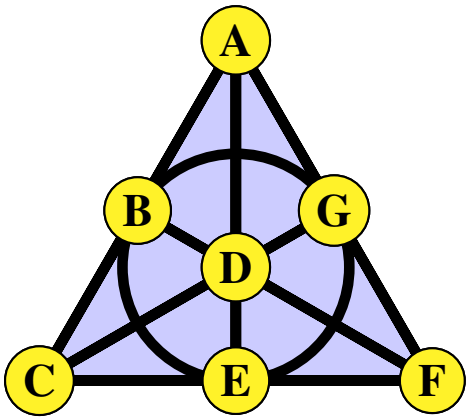
2.27 Tanım $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ bir insidans yapı olsun. Eğer aşağıdaki koşullar sağlanıyor ise $\mathcal{S}$ insidans yapısına bir $t-(v,k,\lambda)$ *tasarımı* denir:

(i) $|\mathcal{P}| = v$,

(ii) Her $B_i \in \mathcal{B}$ için $|B_i| = k$,

(iii) $\mathcal{P}$ 'nin her t elemanlı altkümesi tam olarak λ tane B_i kümesinde bulunur.

2.28 Örnek Bir 2-(7,3,1) tasarımı şu şekilde gösterilebilir:



2-(7,3,1) Tasarımı

Şekil 2.1: 2-(7,3,1) Tasarımı

Burada, $\mathcal{P} = \{A, B, C, D, E, F, G\}$, $\mathcal{B} = \{B_1, B_2, B_3, B_4, B_5, B_6, B_7\}$,

$B_1 = \{A, B, C\}$ $B_2 = \{A, D, E\}$

$B_3 = \{A, F, G\}$ $B_4 = \{B, D, F\}$

$B_5 = \{B, E, G\}$ $B_6 = \{C, D, G\}$

$B_7 = \{C, E, F\}$

2-(7,3,1) Tasarımı

	A	B	C	D	E	F	G
B_1	1	1	1	0	0	0	0
B_2	1	0	0	1	1	0	0
B_3	1	0	0	0	0	1	1
B_4	0	1	0	1	0	1	0
B_5	0	1	0	0	1	0	1
B_6	0	0	1	1	0	0	1
B_7	0	0	1	0	1	1	0

Yukarıda verilen $2\text{-}(7, 3, 1)$ blok tasarımı, her biri üç eleman içeren yedi bloktan oluşur ve herhangi iki nokta yalnızca bir blokta birlikte yer alır. Tasarımın geometrik gösterimi, noktalar arasındaki ilişkileri sezgisel olarak sunarken; ilişki matrisi ise her bloğun hangi noktaları içerdiğini ifade eder.

2.29 Tanım $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ bir $t - (v, k, \lambda)$ tasarımı olsun. Eğer, bir $t' - (v', k, \lambda')$ tasarımı $\mathcal{S}' = (\mathcal{P}', \mathcal{B}')$ için $\mathcal{P}' \subseteq \mathcal{P}$ ve $\mathcal{B}' \subseteq \mathcal{B}$ koşulları sağlanıyorsa, $\mathcal{S}'$, $\mathcal{S}$ 'nin *alt tasarımı* olarak adlandırılır.

Son olarak, eğer bir $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ tasarımı için,

$$\mathcal{B} = \bigsqcup_{i=1}^{n} \mathcal{B}_i$$

olmak üzere n tane alt tasarım $\mathcal{S}_i = (\mathcal{P}, \mathcal{B}_i)$ mevcutsa, bu durumda $\mathcal{S}$ tasarımı $\mathcal{S}_1, \ldots, \mathcal{S}_n$ alt tasarımlarına *bölünmüş (parçalanmış)* olarak adlandırılır ve şu şekilde gösterilir:

$$\mathcal{S} = \bigsqcup_{i=1}^{n} \mathcal{S}_i$$

2.4 Kriptografik Fonksiyonlar

Kriptografik fonksiyonlar, modern bilgi güvenliğinin temelini oluşturur. Verilerin gizliliğini, bütünlüğünü ve kimlik doğrulamasını sağlamaktadır. Matematiksel olarak karmaşık yapıları sayesinde saldırılara karşı dayanıklıdır ve pratikte kırılması çok zordur. Bu nedenle bankacılık, e-ticaret, blok zincir ve kişisel veri güvenliği gibi birçok alanda kritik rol oynamaktadır. Bu bölümde genel olarak [1] numaralı kaynaktan yararlanılmıştır.

2.30 Tanım $\mathbb{A}$ herhangi bir küme ve k herhangi bir pozitif tam sayı olsun. $f : \mathbb{A}^k \to \mathbb{F}_2$ ile tanımlanan fonksiyonlara *Boole fonksiyonları* denir.

2.31 Örnek $A = \mathbb{F}_2$ ve $k = 2$ olsun. Bu durumda $f : \mathbb{F}_2^2 \to \mathbb{F}_2$ biçiminde tanımlanan bir Boole fonksiyonu şu şekilde verilebilir:

$$f(x_1, x_2) = x_1 \cdot x_2$$

Bu fonksiyon, ikili sistemdeki çarpmayı temsil eder. Doğruluk tablosunu ise aşağıdaki gibi gösterebiliriz:

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	0
1	0	0
1	1	1

2.32 Örnek $A = \mathbb{F}_2$ ve $k = 2$ olsun. Bu durumda $f : \mathbb{F}_2^2 \to \mathbb{F}_2$ biçiminde tanımlanan bir Boole fonksiyonu şu şekilde verilebilir:

$$f(x_1, x_2) = x_1 \oplus x_2$$

Bu fonksiyon, ikili sistemdeki toplama işlemini temsil eder. Doğruluk tablosu ise aşağıdaki gibidir:

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	0

2.33 Tanım [1] $\mathbb{F}_2 = \{0, 1\}$ iki elemanlı sonlu cisim, n, m pozitif tam sayı ve $\mathbb{F}_2^n, \mathbb{F}_2$ üzerinde n boyutlu vektör uzayı olsun. $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ ye olan fonksiyonlara (n, m)-fonksiyonlar denir. Özel olarak $(n, 1)$-fonksiyonları Boole fonksiyonlarıdır ve $m \geq 2$ iken (n, m)-fonksiyonlara *vektörel fonksiyonlar* denir. Herhangi bir (n, m)-vektörel fonksiyon F, m koordinat Boole fonksiyonu $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $(1 \leq i \leq m)$ için benzersiz bir şekilde ($\mathbb{F}_2^m$ baz biçimine kadar) sütun vektörü olarak ilişkilendirilebilir:

$$F(x) := (f_1(x), ..., f_m(x))^T,$$

burada T ile transpoz gösterilmektedir.

Dejenere olmayan (non-degenerate) tanımına geçmeden önce aşağıda sunulan ön bilgilere ihtiyaç duyulmaktadır.

Bir F cismi üzerinde tanımlı sonlu boyutlu V ve W vektör uzayları ele alındığında, V 'den F 'ye giden tüm lineer fonksiyonlar kümesi $V^* = L(V, F)$ uzayına V'nin *dual uzayı* denilir. Eğer $\psi : V \times W \to F$ biçiminde tanımlı bir çifte doğrusal biçim (bilinear form) ise aşağıdaki iki doğrusal dönüşüm elde edilir:

$$\psi_L : V \to W^*; \quad v \mapsto (w \mapsto \psi(v, w))$$
$$\psi_R : W \to V^*; \quad w \mapsto (v \mapsto \psi(v, w))$$

Burada, ψ 'nin ikinci argümana göre doğrusal olması, her $v \in V$ için $\psi_L(v)$ 'nin $W \to F$ biçiminde tanımlı bir lineer fonksiyon olduğunu ve dolayısıyla W^*'nin bir elemanı olduğunu gösterir. Benzer şekilde, ψ 'nin birinci argümana göre doğrusal olması, ψ_L 'nin kendisinin de doğrusal bir dönüşüm olduğunu ortaya koyar. (Aynı şekilde, ψ_R dönüşümü için de benzer çıkarımlar yapılabilir; yalnızca argümanların yerleri değiştirilerek yorumlanmalıdır.)

2.34 Teorem [14] Aşağıdaki ifadelerden herhangi ikisi üçüncüsünü gerektirir:

(i) Çek($\psi_{\mathbb{L}}$)= $\{0\}$, yani $\psi(v, w) = 0$ ifadesi tüm $w \in W$ için geçerli ise, $v = 0$ olduğu anlamına gelir.

(ii) Çek($\psi_{\mathbb{R}}$)= $\{0\}$, yani $\psi(v, w) = 0$ ifadesi tüm $v \in V$ için geçerli ise, $w = 0$ olduğu anlamına gelir.

(iii) $boyV = boyW$.

Burada Çek terimi, "çekirdek" (kernel) kavramının kısaltılmasıdır ve bir doğrusal dönüşümün sıfıra götürdüğü öğelerin kümesini ifade eder.

2.35 Tanım Bir çifte doğrusal biçim $\psi : V \times W \longrightarrow F$, Teorem 2.34 'ün koşullarını sağlıyorsa *dejenere olmayan (non-degenerate)* olarak adlandırılır.

2.36 Tanım [1] Bir (n, m)-fonksiyonu olan F 'nin bileşen fonksiyonları (component functions), $F_{\mathbf{b}} : \mathbf{x} \in \mathbb{F}_2^n \mapsto \langle \mathbf{b}, F(\mathbf{x}) \rangle_m$ şeklinde tanımlanan Boole fonksiyonlarıdır. Burada $\mathbf{b} \in \mathbb{F}_2^m$ ve $\langle ., . \rangle_m$, $\mathbb{F}_2^m$ üzerinde tanımlı bir dejenere olmayan çifte doğrusal biçim, yani $\langle \mathbf{b}, F(\mathbf{x}) \rangle_m : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ dir.

2.37 Tanım $a_0, a_1, ..., a_{12...n} \in \mathbb{F}_2$ olmak üzere $f : \mathbb{F}_2^n \to \mathbb{F}_2$ bir Boole fonksiyonu olsun.

$$f(x) = a_0 \oplus a_1 x_1 \oplus ... \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus ... \oplus a_{12...n} x_1 x_2 ... x_n$$
$$= \left(\bigoplus_{k=1}^{n} \bigoplus_{i_1,...,i_k} a_{i_1,...,i_k} x_{i_1} \cdots x_{i_k} \right) \oplus a_0$$

polinom gösterimine f 'nin *cebirsel normal formu (Algebraic Normal Form-ANF)* denir, burada $\oplus$, mod 2 'ye göre toplama işlemini ifade eder. Bu gösterimde, toplamın bir parçası olarak ortaya çıkan her değişken çarpımına bir *terim* denir. Her terimdeki değişkenlerin sayısına, o terimin *derecesi* denir. Bir fonksiyonun derecesi ise, en büyük dereceye sahip terimin derecesidir ve $deg(f)$ ile gösterilir.

2.38 Tanım [1] Bir vektörel (n, m)-fonksiyonun cebirsel derecesi $\deg(F)$, onun bileşen fonksiyonlarının cebirsel derecelerinin maksimumu olarak tanımlanır, yani

$$\deg(F) := \max_{1 \le i \le m} \deg(f_i).$$

Açıkça görülmektedir ki, herhangi bir (n, m)-fonksiyonun cebirsel derecesi en fazla n olabilir.

2.39 Tanım [5] $F_n = \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$ (tüm Boole fonksiyonlarının kümesi) ve $\mathcal{V}_n = \mathbb{F}_2^n$ alalım. Bir $f \in F_n$ fonksiyonu, tüm $\alpha, \beta \in \mathcal{V}_n$ için

$$f(\alpha \oplus \beta) = f(\alpha) \oplus f(\beta)$$

eşitliği sağlanıyorsa, lineer olarak adlandırılır. Böyle bir fonksiyon ise şu şekilde ifade edilir:

$$f(x) = a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n, \;\; a_i \in \mathbb{F}_2.$$

Tüm lineer fonksiyonların kümesi $\mathcal{L}_n$ ile gösterilir.

Bir $f \in F_n$ fonksiyonu, tüm $\alpha, \beta \in \mathcal{V}_n$ ve $a \in \{0,1\}$ için

$$f(\alpha \oplus \beta) = f(\alpha) \oplus f(\beta) \oplus a$$

eşitliği sağlanıyorsa, afin olarak adlandırılır. Böyle bir fonksiyon şu şekilde ifade edilir:

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n, \;\; a_i \in \mathbb{F}_2.$$

Tüm afin fonksiyonların kümesi $\mathcal{A}_n$ ile gösterilir. Açıkça görülüyor ki $\mathcal{L}_n < \mathcal{A}_n$ ve $|\mathcal{A}_n| = 2|\mathcal{L}_n| = 2^{n+1}$.

2.40 Tanım [1] $\mathbb{F}_2^n$ üzerindeki Boole fonksiyonlarının kümesi $\mathcal{B}_n$, $(\mathcal{B}, d)$ metrik uzayı yapısıyla donatılmıştır, burada

$$d(f,g) := |\{\mathbf{x} \in \mathbb{F}_2^n : f(\mathbf{x}) \neq g(\mathbf{x})\}|$$

$f, g \in \mathcal{B}_n$, Boole fonksiyonları arasındaki *Hamming mesafeyi* ifade eder.

2.41 Tanım [1] Bir $\mathbb{F}_2^n$ üzerindeki Boole fonksiyon f'nin *doğrusal olmama ölçüsü (nonlinearity)*, f ile tüm afin fonksiyonlar kümesi $\mathcal{A}_n$ arasındaki mesafenin bir ölçüsüdür ve $nl(f)$ ile gösterilir, yani

$$nl(f) := \min_{a \in \mathcal{A}_n} d(f,a).$$

Doğrusal olmama tanımı, bileşen fonksiyonları tanımı kullanılarak vektörel durumda da genişletilebilir. Vektörel bir (n,m)-fonksiyon *F'nin doğrusal olmama ölçüsü* şu şekilde ifade edilir:

$$nl(F) := \min_{a \in \mathcal{A}_n, \mathbf{b} \in \mathbb{F}_2^m \setminus \{0\}} d(F_{\mathbf{b}}, a), \text{burada } F_{\mathbf{b}}(x) = \langle \mathbf{b}, F(x) \rangle_m.$$

Bir (n,m)-fonksiyonu F 'nin doğrusal olmama ölçüsü $nl(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ dir.

2.42 Tanım [1] Bir (n,m)-fonksiyonu F için $nl(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$ ise *mükemmel doğrusal olmayan (perfect nonlinear)* fonksiyon olarak adlandırılır.

2.43 Örnek Eğer p tek bir asal sayı ise $\mathbb{F}_{p^m}$ sonlu cisminde $f(x) = x^2$ ile tanımlanan (m,m)-fonksiyonu mükemmel doğrusal olmayan bir fonksiyondur.

2.44 Tanım $f : \mathbb{F}_2^n \to \mathbb{F}_2$ ' ye bir Boole f fonksiyonunun *Walsh dönüşümü* $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ aşağıdaki gibi tanımlanmaktadır:

$$W_f(\mathbf{a}) := \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \langle \mathbf{a}, \mathbf{x} \rangle}, \quad \mathbf{a} \in \mathbb{F}_2^n,$$

burada $\langle \mathbf{a}, \mathbf{x} \rangle = \sum_{i=1}^{n} a_i \cdot x_i$ toplamı $\mathbb{F}_2^n$ 'de standart iç çarpımı göstermektedir.
Bir (n,m)-fonksiyonu F 'nin doğrusal olmamasını hesaplamak için kullanılan standart araç $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ *Walsh dönüşümü* şu şekilde tanımlanır:

$$W_F(\mathbf{a},\mathbf{b}) := W_{F_\mathbf{b}}(\mathbf{a}) \quad \text{ve} \quad W_{F_\mathbf{b}}(\mathbf{a}) := \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F_\mathbf{b}(\mathbf{x})\oplus\langle \mathbf{a},\mathbf{x}\rangle_n}, \ \mathbf{a} \in \mathbb{F}_2^n \quad \text{ve} \quad \mathbf{b} \in \mathbb{F}_2^m,$$

burada F_b Boole fonksiyonları F 'nin bileşenleridir. Walsh dönüşümü kullanılarak, bir (n,m)-fonksiyonu F 'nin doğrusal olmaması şu şekilde hesaplanabilir:

$$nl\left(F\right) = 2^{n-1-\frac{1}{2}} \cdot \max_{\mathbf{a}\in\mathbb{F}_2^n, \mathbf{b}\in\mathbb{F}_2^m\setminus\{0\}} \left|W_F(\mathbf{a},\mathbf{b})\right|.$$

Çoklu küme $\Lambda_F := \{*W_F(\mathbf{a},\mathbf{b}) : \mathbf{a} \in \mathbb{F}_2^n, \mathbf{b} \in \mathbb{F}_2^m \setminus \{0\} *\}$, bir (n,m)-fonksiyonu F 'nin *Walsh spektrumu* olarak adlandırılır.

Bir (n,m)-fonksiyonu F 'nin *birinci mertebeden* türevi $D_\mathbf{a}F : \mathbf{x} \mapsto F\left(\mathbf{x} \oplus \mathbf{a}\right) \oplus F\left(\mathbf{x}\right)$ şeklinde tanımlanmaktadır.

2.45 Tanım Herhangi bir (n,m)-fonksiyonu F için F 'nin *diferansiyel tekdüzeliğ*i $\delta(F)$ değeri aşağıdaki gibi

$$\delta\left(F\right) := \max_{\mathbf{a}\in\mathbb{F}_2^n\setminus\{\mathbf{0}\}, \mathbf{b}\in\mathbb{F}_2^m} \delta_F\left(\ \mathbf{a},\mathbf{b}\right), \text{ burada } \delta_F\left(\mathbf{a},\mathbf{b}\right) := \left|\{\mathbf{x} \in \mathbb{F}_2^n : D_\mathbf{a}F(x) = \mathbf{b}\}\right|,$$

tanımlanmaktadır. $\Delta_F := \{*\delta_F(\mathbf{a},\mathbf{b}) : \mathbf{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}, \mathbf{b} \in \mathbb{F}_2^m *\}$ çoklu kümesine F fonksiyonunun *diferansiyel spektrumu* denir.

Not: Bir (n, m)-fonsksiyonu F 'nin diferansiyel tekdüzeliği $\delta_F \geq 2^{n-m}$ 'dir.

Genel olarak, en yüksek doğrusal olmamaya sahip (n, m)-fonksiyonları ile en düşük diferansiyel tekdüzeliğe sahip (n, m)-fonksiyonları iki farklı fonksiyon kümesidir. Ancak, aşağıdaki sonuçta gösterildiği gibi, bazı durumlarda bu kümeler aynı olabilir.

2.46 Sonuç [1, Result 1.2] n çift ve $m < \frac{n}{2}$ olmak üzere F bir (n, m)-fonksiyonu olsun. Aşağıdaki ifadeler birbirine denktir:

(i) F mükemmel doğrusal olmayan (perfect nonlinear) bir fonksiyondur, yani
$nl(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

(ii) F'nin diferansiyel tekdüzeliği $\delta_F = 2^{n-m}$ dir.

(iii) Her $\mathbf{a} \in \mathbb{F}_2^n$ ve $\mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ için Walsh dönüşümü $|W_F(\mathbf{a},\mathbf{b})| = 2^{n/2}$ eşitliğini sağlar.

2.47 Tanım Eğer $f : \mathbb{F}_2^n \to \mathbb{F}_2$ biçiminde tanımlanan bir fonksiyonun Walsh dönüşümünün tüm bileşenleri eşit büyüklükte, yani tüm $\mathbf{a} \in \mathbb{F}_2^n$ için

$$|W_f(\mathbf{a})| = 2^{n/2}$$

ise f 'ye *bükük fonksiyon* denir.

Bir bükük fonksiyon, $f : \mathbb{F}_2^n \to \mathbb{F}_2$ biçiminde tanımlanan ve yalnızca çift sayıda değişken için var olan özel bir Boole fonksiyonudur. Bükük fonksiyonlar, lineer ve afin fonksiyonlara karşı *maksimum doğrusal olmayanlığa* sahip olup, çıktıları ile herhangi bir lineer fonksiyonun çıktısı arasındaki Hamming uzaklığı en büyük değeri alır. Bu özellikleri nedeniyle bükük fonksiyonlar kriptografi ve kodlama teorisinde önemli bir rol oynar.

2.48 Örnek $n = 2$ için tanımlı bir bükük fonksiyon aşağıdaki gibi verilebilir:

$$f(x_1, x_2) = x_1 \cdot x_2 \oplus x_1$$

Fonksiyonun doğruluk tablosu:

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	0
1	0	1
1	1	0

elde edilir. Şimdi ise Walsh dönüşümünü kullanarak katsayıları bulalım. Walsh dönüşümü

$$W_f(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^2} (-1)^{f(\mathbf{x}) \oplus \langle \mathbf{a}.\mathbf{x} \rangle},$$

şeklindeydi. Bunu kullanarak Walsh katsayıları aşağıdaki gibi elde edilir,

$$W_f(0,0) = (-1)^0 + (-1)^0 + (-1)^1 + (-1)^0 = 2,$$
$$W_f(1,0) = (-1)^{0\oplus 0} + (-1)^{0\oplus 0} + (-1)^{1\oplus 1} + (-1)^{0\oplus 1} = 2,$$
$$W_f(0,1) = (-1)^{0\oplus 0} + (-1)^{0\oplus 1} + (-1)^{1\oplus 0} + (-1)^{0\oplus 1} = -2,$$
$$W_f(1,1) = (-1)^{0\oplus 0} + (-1)^{0\oplus 1} + (-1)^{1\oplus (1\oplus 0)} + (-1)^{0\oplus (1\oplus 1)} = 2.$$

Sonuç olarak,

$$W_f(a) \in \{\pm 2\} = \{\pm 2^{n/2}\} \quad \text{dir.}$$

Tüm değerler eşit büyüklükte olduğundan f fonksiyonu bir bükük fonksiyondur.

2.49 Tanım [1] Bir (n,m)-bükük fonksiyonu F için $f : \mathbb{F}_2^n \to \mathbb{F}_2$ şeklinde tanımlanmış bir Boole bükük f fonksiyonu mevcutsa öyle ki $G : \mathbf{x} \in \mathbb{F}_2^n \mapsto (F(\mathbf{x}), f(\mathbf{x}))^T$ fonksiyonu bir (n, m+1)-bükük fonksiyon ise, F 'ye *genişletilebilir (extendable) fonsiyon* denilir. Eğer böyle bir bükük f fonksiyonu mevcut değilse, F, *genişletilemez (non-extendable*) ya da *yalnız (lonely)* olarak adlandırılır (bkz. [16]).

n çift ve $m \leq n/2$ olduğunda (n,m)-fonksiyonlarının mükemmel doğrusal olmaması (perfect nonlinearity), Walsh dönüşümünün değer kümesinin minimalitesi veya diferansiyel spektrumun minimalitesi ile karakterize edilir. Mükemmel doğrusal olmayan fonksiyonların daha genel biçimleri, bu minimalite koşullarının hafifçe gevşetilmesiyle elde edilebilir.

2.50 Tanım [1] Bir Boole fonksiyonu $f : \mathbb{F}_2^n \to \mathbb{F}_2$, eğer Walsh dönüşümünün mutlak değeri tüm $\mathbf{a} \in \mathbb{F}_2^n$ için yalnızca iki değer alıyorsa, yani $|W_f(a)| \in \left\{0, 2^{\frac{n+s}{2}}\right\}$ ise *s-plato (s-plateaued)* olarak adlandırılır. $2^{(n+s)/2}$ değeri, s-plato bir Boole fonksiyonun *genişliği (amplitude)* olarak adlandırılır.

(i) Bir (n,m)-fonksiyonu F, eğer $\mathbf{b} \neq \mathbf{0}$ olan tüm bileşen fonksiyonları $F_{\mathbf{b}}$, s-plato ise, *s-plato* olarak adlandırılır.

(ii) Eğer bir (n,m)-fonksiyonu F'nin tüm bileşen fonksiyonları F_b, s_b-plato ise (genişlikleri aynı olmak zorunda değildir), bu durumda F bir *(n,m)-plato* fonksiyonu olarak adlandırılır.

(iii) $\mathbb{F}_2^n$ üzerinde n tek olduğunda 1-plato Boole fonksiyonları ve n çift olduğunda 2-plato Boole fonksiyonları *yarı-bükük (semi-bükük)* olarak adlandırılır.

2.51 Tanım [1] Bir (n,m)-fonksiyonu F, diferansiyel spektrumunda yalnızca iki farklı değer varsa, yani $\Delta_F = \{0, 2^s\}$ (çokluklar göz ardı edilerek), diferansiyel olarak *iki değerli* olarak adlandırılır. Özellikle, $\Delta_F = \{0, 2\}$ olan (m,m)-fonksiyonları *neredeyse mükemmel doğrusal olmayan (almost perfect nonlinear)* veya kısaca *APN fonksiyonları* olarak adlandırılır.

Not: $\mathbb{F}_{2^n}$ sonlu cisminin elemanları, aynı zamanda aşağıdaki polinom gösterimiyle yazılabilir:

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \quad a_i \in \mathbb{F}_2,$$

burada polinomlar, derecesi n olan indirgenemez bir polinom modunda alınır. Bu şekilde, $(a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n$ ile $\mathbb{F}_{2^n}$ cismi arasında bire bir eşleme kurulabilir.

Daha açık bir şekilde ifade etmek gerekirse, $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$ şeklinde tanımlı bir f fonksiyonu için

$$\max_{a \in \mathbb{F}_{2^m}^*} \max_{b \in \mathbb{F}_{2^m}} |\{x \in \mathbb{F}_{2^m} : f(x+a) - f(x) = b\}|$$

şeklinde tanımlanan maksimum değer 2 çıkarsa fonksiyona *hemen hemen mükemmel doğrusal olmayan (APN) fonksiyon* adı verilir.
$p = 2$ olduğunda $f(x+a) + f(x) = b$ denklemini, $\mathbb{F}_{2^m}$ sonlu cismi üzerinde bir x_0 elemanı sağlıyorsa, aynı zamanda $x_0 + a$ elemanı da bu denklemi sağlar. Fonksiyon f yalnızca her $0 \neq a \in \mathbb{F}_{2^m}$ için x_0 ve $x_0 + a$ elemanlarının $\tilde{f}(x) = f(x+a) + f(x)$ için $\tilde{f}(x_0) = \tilde{f}(x_0 + a)$ durumunda APN olur. Diğer bir ifade ile,

$\tilde{f}(x_0) = f(x_0 + a) + f(x_0) = b$,
$\tilde{f}(x_0 + a) = f(x_0 + a + a) + f(x_0 + a) = f(x_0 + 2a) + f(x_0 + a) = f(x_0) + f(x_0 + a) = b$

eşitlikleri sağlanır.
APN fonksiyonları, kriptografi ve hata düzeltme gibi geniş uygulama alanlarına sahip olduklarından özellikle $p = 2$ karakteristikte çalışılmıştır.

2.52 Örnek [2] $f(x) = x^3$ fonksiyonu bütün $\mathbb{F}_{2^m}$ sonlu cisimlerinde APN özelliğini sağlamaktadır. Denklemi inceleyelim:

$f(x+a) + f(x) = b \Rightarrow (x+a)^3 + x^3 = b$

burada açılım yapıldığında,

$x^3 + 3x^2a + 3xa^2 + a^3 + x^3 = b$

elde edilir. $3 \equiv 1 \pmod 2$ olduğundan

$x^2a + xa^2 + a^3 = b$

biçiminde kuadratik denklem ortaya çıkar. Bu denklemin çözüm sayısı 0, 1 veya 2 olabilir. Ancak, f fonksiyonu APN olduğundan, tanım gereği bu denklemin yalnızca 0 veya 2 çözümü bulunur.

Tablo 3.1: x^d biçimindeki $\mathbb{F}_{2^m}$ üzerinde tanımlı kuadratik olmayan APN kuvvet fonksiyonları

$f(x)$ fonksiyon	Şartlar
$x^{2^{2^i}-2^i+1}$	$(i,m)=1$, $1 \leq i \leq \frac{m-1}{2}$, Kasami
x^{2^m-2}	m tek, Inverse
$x^{2^t+2^{\frac{t}{2}}-1}$	t çift, $m=2t+1$, Niho
$x^{2^t+2^{\frac{3t+1}{2}}-1}$	t tek, $m=2t+1$, Niho
x^{2^t+3}	$m=2t+1$, Welch
$x^{2^{4t}+2^{3t}+2^{2t}+2^t-1}$	$m=5t$, Dobbertin

Tablo 3.1 'de [4], $f(x)$ başlığı altında çeşitli kuvvet fonksiyonları sıralanmakta; karşılık gelen "Şartlar" sütununda ise, bu fonksiyonların APN özelliği taşıyabilmesi için sağlanması gereken koşulları ve bu sonuçların dayandığı ilgili koşulları sunulmaktadır.

Gold ve Dobbertin kuvvet fonksiyonları, $\mathbb{F}_{2^m}$ üzerinde tanımlı ve diferansiyel kriptanalize karşı güçlü olan *neredeyse mükemmel doğrusal olmayan (APN)* fonksiyonlardır. Her iki fonksiyon ailesi de APN özelliğine sahip olmakla birlikte, yapısal özellikleri ve literatürdeki rolleri bakımından önemli farklılıklar gösterir.

Gold Fonksiyonları: Gold fonksiyonları en klasik ve en çok incelenmiş kuadratik APN fonksiyonlardır. Yapıları basittir:

$$f(x) = x^{2^i+1}, \quad \text{obeb}(i,m) = 1.$$

Walsh spektrumları tamamen bilinmektedir ve çift boyutlarda bükük fonksiyon olabilme özelliğine sahiptirler. Bu nedenle hem kriptografi hem de kodlama teorisinde temel örnek olarak değerlendirilirler.

Dobbertin Fonksiyonları: Dobbertin tarafından tanıtılan bu fonksiyonlar daha karmaşık üs yapısına sahiptir:

$$f(x) = x^{2^{4t}+2^{3t}+2^{2t}+2^t-1}, \quad m = 5t.$$

Kuadratik olmayan APN fonksiyon oldukları gösterilmiş olsa da, Walsh spektrumları tam olarak bilinmemektedir. Literatürde hâlâ açık bir problem olarak değerlendirilen bu fonksiyonlar, APN fonksiyonların yapısal sınırlarını anlamada kritik bir örnek teşkil eder.

Bu iki fonksiyon ailesi, APN fonksiyonların sınıflandırılması ve doğrusal olmayanlık analizleri açısından birbirini tamamlayıcı niteliktedir. Gold fonksiyonları temel yapı taşlarını

sunarken, Dobbertin fonksiyonları daha ileri düzey araştırmalar için zengin bir inceleme alanı sağlar.

2.4.1 Kriptografik Fonksiyonların İnsidans Yapıları

Li ve diğerleri [6], (n,n)-fonksiyonlarının CCZ-eşdeğersizliği çalışmasından ilham alarak, (n,n)-fonksiyonu F 'nin kaybolan düzlemleri olarak adlandırılan kısmi dörtlü sistem $\mathcal{VF}(F)$' yi tanıttı. Bu yapı, verilen fonksiyon hakkında ayrıntılı kombinatoryal bilgiyi sağlar. Bu yapı şu şekilde tanımlanır:

2.53 Tanım [1] $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ şeklinde tanımlı bir fonksiyon olsun. $P = \{x : x \in \mathbb{F}_2^n\}$ noktalar kümesi ve

$$\mathcal{VF}_F = \left\{ \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\} \;\middle|\; \begin{array}{l} x_1 + x_2 + x_3 + x_4 = 0 \text{ ve} \\ \\ F(x_1) + F(x_2) + F(x_3) + F(x_4) = 0,\ \mathbf{x}_i \in \mathbb{F}_2^n \text{ için} \end{array} \right\}.$$

blok kümesi olmak üzere, $\mathcal{VF}(F) = (\mathcal{P}, \mathcal{VF}_F)$ insidans yapısına F 'nin *kaybolan düzlemleri* denir.

$(\mathbb{F}_2^n, \mathcal{VF}_F)$ yapısıyla ilişkili özellikle dikkat çekici nicelik, blok kümesi $\mathcal{VF}_F$'nin büyüklüğüdür; başka bir deyişle, F 'nin kaybolan düzlemlerinin sayısıdır.

Not: Kaybolan düzlemlerin sayısı, yalnızca F'nin APN olması durumunda sıfırdır. Bu anlamda, kaybolan düzlemlerin sayısı F ile APN fonksiyonlar kümesi arasındaki mesafeyi ölçer. Aslında, $\mathcal{VF}_F$'nin boyutu F'nin diferansiyel spektrumundan elde edilir.

2.54 Örnek $n \geq 2$ için $\mathbb{F}_{2^n}$ içindeki tüm 2-boyutlu düzlemlerin kümesi aşağıdaki şekilde tanımlanır:

$\mathcal{B}_n = \{\{x_1, x_2, x_3, x_4\} | x_1 + x_2 + x_3 + x_4 = 0$ ve $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^n}$ birbirinden farklıdır.$\}$

$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ bir fonksiyonu F ancak ve ancak $\mathcal{B}_n$'deki her bir $\{x_1, x_2, x_3, x_4\}$ için:

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq 0$$

ise APN'dir.(Almost Perfect Nonlinear-Neredeyse Mükemmel Doğrusal Olmayan)

Yani, F'nin her 2-boyutlu düzlem üzerindeki toplamı sıfır değildir (non-vanishing).

Her bir kaybolan düzlem $x_1, x_2, x_3, x_4 \in \mathcal{VF}_F$, üç farklı kritik yön $a_1 = x_1 + x_2,\ a_2 = x_1 + x_3,\ a_3 = x_1 + x_4$ oluşturur. Bu kritik yönler için $F(x + a_i) + F(x), 1 \leq i \leq 3$ olmak

üzere 2'ye 1 değildir. Dolayısıyla, kritik yönler kümesi D_F doğrudan $\mathcal{VF}_F$ 'den elde edilir. $\mathcal{B}_n$ dört elemanlı ve toplamları sıfır olan tüm alt kümeleri içeren blok kümesini ifade eder ve $\mathcal{VF}_F \subset \mathcal{B}_n$ olduğundan $(\mathbb{F}_{2^n}, \mathcal{VF}_F)$ küme sistemine kısmi dörtlü sistem adını veriyoruz. Aslında, bir kısmi dörtlü sistem, çok daha genel bir yapı olan dizilimler (packings) sınıfının bir örneğidir. Genel Steiner sistemleri ve dizilimler hakkında kapsamlı çalışmalar için [8] ve [9] çalışmalarına başvurulabilir.

f ve g, $\mathbb{F}_{2^n}$'den $\mathbb{F}_{2^n}$'ye tanımlı iki polinom olsun. Eğer $\mathbb{F}_2^n \times \mathbb{F}_2^n$ üzerinde bir afin permütasyon A varsa öyle ki

$$\left\{ \begin{pmatrix} x \\ g(x) \end{pmatrix} \mid x \in \mathbb{F}_2^n \right\} = \left\{ A \begin{pmatrix} x \\ f(x) \end{pmatrix} \mid x \in \mathbb{F}_2^n \right\} \tag{2.1}$$

olacak şekilde bir ilişki kurulabiliyorsa, CCZ-eşdeğer olarak adlandırılır. Burada, $\mathbb{F}_{2^n}$'nin $\mathbb{F}_2$ üzerinde bir tabanı seçildiğinde, polinomlar f ve g, $\mathbb{F}_2^n$ 'den $\mathbb{F}_2^n$ 'ye iki farklı eşleme olarak düşünülebilir. Bilindiği üzere, CCZ-eşdeğerlik, diferansiyel tekdüzeliği korur ve dolayısıyla APN (Hemen hemen mükemmel doğrusal olmayan) özelliğini de korur [10,Proposition 2]. Ayrıca hatırlatmak gerekir ki, iki kısmi dörtlü sistem, eğer noktalar kümesi arasında bir birebir eşleme bulunabiliyor ve bu eşleme blok kümeleri arasında da birebir bir dönüşüm sağlıyorsa, izomorfik olarak adlandırılır. Şimdi, CCZ-eşdeğerliğin kısmi dörtlü sistemleri izomorfizm açısından koruduğunu göstereceğiz. Bu bağlamda, iki izomorfik kısmi dörtlü sistemi temsil etmek için $\cong$ notasyonu kullanılacaktır.

2.55 Teorem [6, Theorem 2.1] f ve g, $\mathbb{F}_{2^n}$' den $\mathbb{F}_{2^n}$'ye tanımlı ve

$$\left\{ \begin{pmatrix} x \\ g(x) \end{pmatrix} : x \in \mathbb{F}_{2^n} \right\} = \left\{ \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} x \\ f(x) \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} : x \in \mathbb{F}_{2^n} \right\}$$

şartını yerine getiren CCZ-eşdeğer iki fonksiyon olsun. Bu durumda, $(x_1, x_2, x_3, x_4) \in \mathcal{VF}_f$ ancak ve ancak $(y_1, y_2, y_3, y_4) \in \mathcal{VF}_g$ 'dir. Burada,
$y_i = A_{11}x_i + A_{12}f(x_i) + u$ olarak tanımlanmıştır. Sonuç olarak $(\mathbb{F}_{2^n}, \mathcal{VF}_f) \cong (\mathbb{F}_{2^n}, \mathcal{VF}_g)$ eşitliği sağlanır ve CCZ-eşdeğerlik altında kaybolan düzlemlerin sayısı değişmezdir.

3. KRİPTOGRAFİK FONKSİYONLAR VE İNSİDANS YAPILARI

Bükük fonksiyonlar, hem kriptografik güvenlik hem de kombinatorik yapıların analizi açısından özel bir öneme sahiptir. Bu bölümde, bükük fonksiyonların tasarım teorisi bağlamında nasıl yorumlandığı ve bu fonksiyonların oluşturduğu lineer kodlarla olan ilişkisi ele alınacaktır. Böylece, kod parametreleri ve ağırlık dağılımları üzerinden tasarım özelliklerinin nasıl türetilebildiği gösterilecektir.

Kriptografik fonksiyonların yapısal özellikleri, yalnızca güvenlik açısından değil, aynı zamanda kombinatorik ve cebirsel bağlamda da önemli sonuçlar sunar. Öncelikle, grup etkileri aracılığıyla tanımlanan geçişli (transitivite) kavramı ile kodların otomorfizma grupları arasındaki ilişkisi incelenerek, insidans yapılarının nasıl ortaya çıktığı gösterilecektir. Böylece, kodlama teorisi ile tasarım teorisi arasındaki geçişler matematiksel bir çerçevede ele alınacaktır.

3.1 Tanım Bir (n, m)-fonksiyonu $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ için *F ile tanımlanan C_F lineer kodu*, $\mathbf{x} \in \mathbb{F}_2^n$ olmak üzere

$$G_F = \begin{bmatrix} 1 \\ \mathbf{x} \\ F(\mathbf{x}) \end{bmatrix}$$

matrisinin satırları tarafından üretilen lineer kod olarak tanımlanır.

Bu C_F kodunun üreteç matrisini daha açık biçimde verecek olursak,

$$G_F = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_{1,1} & x_{2,1} & \cdots & x_{2^n,1} \\ x_{1,2} & x_{2,2} & \cdots & x_{2^n,2} \\ \vdots & \vdots & & \vdots \\ x_{1,n} & x_{2,n} & \cdots & x_{2^n,n} \\ F_1(x_1) & F_1(x_2) & \cdots & F_1(x_{2^n}) \\ \vdots & \vdots & & \vdots \\ F_m(x_1) & F_m(x_2) & \cdots & F_m(x_{2^n}) \end{bmatrix}_{(1+n+m) \times 2^n}$$

Burada, ilk satır n tane sabit 1 değerlerinden oluşur, sonraki n satır giriş vektörlerinin $x_i \in \mathbb{F}_2^n$ bileşenlerini içerir, son m satır ise fonksiyonun çıktı bileşenlerini içerir.

Bu kod ve onun duali $C_F^{\perp}$, ilgili fonksiyonun Walsh ve diferansiyel spektrumları hakkında tüm bilgileri içerir. Ayrıca, eşdeğer olmayan fonksiyonları ayırt etmek için de kullanılabilir.

3.2 Tanım Uzunluğu v olan bir lineer kod $\mathcal{C}$ verilsin. $A_w \neq 0$ olacak şekilde bir w tam sayısı seçilsin. Kodun tüm koordinat pozisyonlarını içeren küme,

$$\mathcal{P}(\mathcal{C}) := \{1, 2, \ldots, v\}$$

ve sabit ağırlıklı kod sözcüklerinin destek kümelerinden oluşan,

$$\mathcal{B}_w(\mathcal{C}) := \{\text{supp}(c) \mid \text{wt}(c) = w,\ c \in \mathcal{C}\}$$

kümesi tanımlansın, burada supp(c), c 'nin sıfırdan farklı koordinatlarının kümesidir. Eğer $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ çifti sabit bir w için bir t-tasarım oluşturuyorsa, $\mathcal{C}$ kodunun ağırlığı w olan kod sözcüklerinin bir t-tasarımı taşıdığı söylenir. Eğer $0 \leq w \leq v$ aralığındaki her w için kod sözcükleri bir t-tasarımı taşıyorsa, bu durumda $\mathcal{C}$ kodunun t-tasarımları desteklediği ifade edilir. Bu tanım, $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ çifti aşikar bir tasarım (trivial design) olsa dahi geçerlidir.

(n,n)-fonksiyonlarının C_F ve $C_F^{\perp}$ lineer kodlarından elde edilen insidans yapılar üzerinde yapılan [6, 17] gibi son çalışmalar [1] 'de genişletilmektedir. Aslında, bir (n, n) fonksiyonu F 'nin $\mathcal{VF}(F)$ kaybolan düzlemleri, $(\mathcal{P}(C_F^{\perp}), \mathcal{B}_4(C_F^{\perp}))$ insidans yapısıdır. (n, m)- bükük F fonksiyonların kaybolan düzlemleri $\mathcal{VF}(F)$, tanım gereği $C_F^{\perp}$ kodundaki ağırlığı 4 olan kod sözcüklerin destekleridir. Böylelikle F 'nin kaybolan düzlemlerinin sayısı $C_F^{\perp}$ kodunun ağırlığı 4 olan kod sözcüklerinin sayısına eşittir (bkz. Sonuç 3.21).

Lineer kodlardan t-tasarımlar (designs) oluşturmak oldukça karmaşık bir problemdir. Bu konuda yaygın olarak kullanılan yöntemlerden biri, sabit ağırlığa sahip kod sözcüklerinin destek kümelerini incelemektir. Bu yaklaşımda, kodun otomorfizma grubunun t-geçişli olup olmadığına veya aşağıda verilen Assmus-Mattson teoreminin koşullarını sağlayıp sağlamadığına bakılır. Bir grup etkisinin t-geçişli olması şu şekilde tanımlanır:

3.3 Tanım G bir grup, S bir küme ve $\cdot : G \times S \to S$ bir grup etkisi olsun. Bu grup etkisi, S kümesinden seçilen herhangi iki sıralı t-li $(x_1, x_2, \ldots, x_t)$ ve $(y_1, y_2, \ldots, y_t)$ ayrık eleman dizisi için, her $i \in \{1, \ldots, t\}$ için $g \cdot x_i = y_i$ olacak şekilde bir $g \in G$ elemanı varsa *t-geçişli (t- transitive)* olarak adlandırılır.

3.4 Teorem [1] $(Transitivity\ Theorem)$ $\mathbb{F}_2$ üzerinde uzunluğu v olan bir C kodu verilsin ve $Aut(C)$(Otomorfizma grubu), t-geçişli olsun. O zaman, ağırlığı $w \geq t$ olan kod sözcükleri (code words) bir t-tasarımı oluşturur.

3.5 Sonuç [17, Theorem 5.3] [Genişletilmiş Assmus - Mattson Teoremi] C kodu, uzunluğu v olan ve minimum mesafesi d olan $\mathbb{F}_2$ üzerinde tanımlı bir lineer kod olsun. $C^{\perp}$, minimum mesafesi $d^{\perp}$ olan C 'nin dual kodunu göstersin. s ve t pozitif tam sayılar olmak üzere, $t < \min\{d, d^{\perp}\}$ koşulunu sağlasın. S, $\{d, d+1, \ldots, v-t\}$ kümesinin s-altkümesi olsun. Varsayalım ki $(\mathcal{P}(C), \mathcal{B}_{\ell}(C))$ ve $(\mathcal{P}(C^{\perp}), \mathcal{B}_{\ell}(C^{\perp}))$ yapıları, $\ell \in \{d, d+1, \ldots, v-t\} \setminus S$ ve $0 \leq \ell \leq s+t-1$ için t-tasarımlardır.
O hâlde, $(\mathcal{P}(C), \mathcal{B}_{k}(C))$ ve $(\mathcal{P}(C^{\perp}), \mathcal{B}_{k}(C^{\perp}))$ yapıları, her $t \leq k \leq v$ için t-tasarımdır.

3.6 Tanım $\mathbb{F}_q$ üzerinde tanımlı iki adet (n, M)-koddan biri, diğerinden aşağıdaki işlemlerin bir dizisi uygulanarak elde edilebiliyorsa, bu iki kod *eşdeğerdir*:

(i) Kod sözcüklerinin koordinatlarının permütasyonu;

(ii) Sabit bir konumdaki koordinatın sıfırdan farklı bir skaler ile çarpılması.

3.7 Örnek $\mathbb{F}_3$ üzerinde tanımlı

$$C = \{000,\ 011,\ 001,\ 002,\ 010,\ 020,\ 012,\ 021,\ 022\}$$

kodunun her kod sözcüğündeki 3. koordinat, sabit bir skaler olan 2 ile çarpılsın. Ardından koordinatlar $2, 3, 1$ sırasına göre yeniden düzenlensin. Bu işlemler sonucunda C 'ye eşdeğer olan aşağıdaki kod elde edilir:

$$C' = \{000,\ 120,\ 020,\ 010,\ 100,\ 200,\ 110,\ 220,\ 210\}.$$

Dolayısıyla, C ve C' kodları, eşdeğer kodlardır.

3.8 Tanım Tüm (n,m)-fonksiyonları kümesi üzerinde aşağıdaki eşdeğerlik (denklik) ilişkileri tanımlanmaktadır.

(i) Genişletilmiş-afin eşdeğerlik (EA-eşdeğerlik): Eğer $\mathbb{F}_2^m$ 'nin bir lineer permütasyonu A_1, $\mathbb{F}_2^n$ 'nin bir afin permütasyonu, A_2, bir afin fonksiyon, $A_3 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ varsa ve bu fonksiyonlar $F = A_1 \circ F' \circ A_2 \oplus A_3$ eşitliğini sağlıyorsa;

(ii) Carlet-Charpin-Zinoviev eşdeğerlik (CCZ-eşdeğerlik): Eğer $\mathbb{F}_2^n \times \mathbb{F}_2^m$ 'nin bir afin permütasyonu $\mathcal{L}$ varsa ve $\mathcal{L}(\mathcal{G}_{\mathcal{F}}) = \mathcal{G}_{\mathcal{F}'}$ eşitliğini sağlıyorsa, burada,

$\mathcal{G}_{\mathcal{F}} := \{(x, F(x)) \mid x \in \mathbb{F}_2^n\}$ bir (n,m)-fonksiyonun grafiği olarak tanımlanır.

Not: Boole fonksiyonlar ve (n,m)-bükük fonksiyonlar için bu iki eşdeğerlik çakışır [11, 12].

3.9 Teorem [19, Theorem 9] $F_1 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ biçiminde tanımlı bir fonksiyon verilsin. O hâlde, F_1 fonksiyonu, $F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ biçiminde tanımlı bir başka fonksiyon ile *CCZ eşdeğerliğe* sahiptir ancak ve ancak C_{F_1} ve C_{F_2} kodları *eşdeğerdir*.

Not: CCZ-eşdeğer fonksiyonların yalnızca ağırlık polinomları (weight enumerators) değil, aynı zamanda sabit ağırlığa sahip kod sözcükleri tarafından desteklenen insidans yapıları da değişmezdir (invariant) (bkz. Sonuç 3.12).

Sonuç 3.12 'yi vermeden önce aşağıdaki tanıma ihtiyaç vardır. Öncelikle, hatırlayalım ki bir *insidans yapı*, $S = (\mathcal{P}, \mathcal{B})$, burada $\mathcal{P}$, S 'nin *nokta kümesi* olarak adlandırılan sonlu bir kümedir ve $\mathcal{B}$, $\mathcal{P}$ 'nin alt kümelerinden oluşan ve *blok kümesi* olarak adlandırılan bir koleksiyondur.

3.10 Tanım İki insidans yapı S ve S', eğer öyle permütasyon matrisleri P ve Q varsa ki:

$$M(S) = P \cdot M(S') \cdot Q,$$

oluyorsa *izomorfik* olarak adlandırılır, burada $M(S)$ ve $M(S')$, sırasıyla S ve S' insidans yapılarının insidans matrisleridir.

3.11 Örnek Nokta kümesi $\mathcal{P} = \{p_1, p_2, p_3\}$ ve blok kümesi $\mathcal{B} = \{B_1, B_2\}$, öyle ki $B_1 = \{p_1, p_2\}$, $B_2 = \{p_2, p_3\}$ olsun. $S = (\mathcal{P}, \mathcal{B})$ insidans yapının insidans matrisi

$$M(S) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

şeklindedir.

Şimdi ikinci bir insidans yapı S' tanımlayalım: $\mathcal{P}' = \{p_2, p_1, p_3\}$ ve blok sırasını $\mathcal{B}' = \{B_2, B_1\}$, $B_1 = \{p_1, p_2\}$, $B_2 = \{p_2, p_3\}$ olarak alalım. Bu durumda

$$M(S') = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Aşağıdaki permütasyon matrislerini tanımlayalım:

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Q = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Burada P satırları (blokları), Q ise sütunları (noktaları) permüte (yer değiştirir) eder. Kolayca doğrulanır ki

$$M(S) = P \cdot M(S') \cdot Q,$$

dolayısıyla S ve S' izomorfiktir.

3.12 Sonuç [1, Result 1.11] F ve F', CCZ-eşdeğer iki (n, m)-fonksiyon olsun. O zaman aşağıdaki yapılar birbirine izomorfiktir: her $0 \leq k, l \leq 2^n$ için

$$(\mathcal{P}(C_F), \mathcal{B}_k(C_F)) \cong (\mathcal{P}(C_{F'}), \mathcal{B}_k(C_{F'})) \quad \text{ve} \quad \left(\mathcal{P}(C_F^{\perp}), \mathcal{B}_l(C_F^{\perp})\right) \cong \left(\mathcal{P}(C_{F'}^{\perp}), \mathcal{B}_l(C_{F'}^{\perp})\right).$$

3.13 Tanım $(G, +)$ yapısının $\mu \cdot \nu$ mertebesinde sonlu bir grup olduğunu ve N, G'nin ν mertebesinde normal bir alt grubu olduğunu varsayalım. G kümesinin bir alt kümesi olan $R \subseteq G$ için, eğer $|R| = k$ ve $r, r' \in R$ için farklar listesi $r - r'$, $G \setminus N$ kümesindeki her elemanı tam olarak λ kez içerirse, R 'ye N alt grubuna göre *göreli bir* (μ, ν, k, λ)*-fark kümesi* denilir. Ayrıca, *yasak alt grup* olarak adlandırılan N'nin sıfır olmayan hiçbir elemanı bu farklar listesinde yer almaz.

3.14 Tanım Bir fonksiyonun çizgesi (graph), tüm girdi-çıktı çiftlerinden oluşan kümedir. Yani $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ için çizge

$$G_F = \left\{ \begin{pmatrix} \mathbf{x} \\ F(\mathbf{x}) \end{pmatrix} : \mathbf{x} \in \mathbb{F}_2^n \right\}$$

şeklinde tanımlanır. Burada x fonksiyonun girdisini, $F(x)$ ise çıktısını ifade eder.
Fonksiyonun çıktılarının oluşturduğu küme ise *görüntü* (image) olarak adlandırılır:

$$\text{Im}(F) = \left\{ \Big(F(x) \Big) : x \in \mathbb{F}_2^n \right\} \subseteq \mathbb{F}_2^m.$$

Dolayısıyla çizge, girdi-çıktı eşleşmelerinin kümesi iken; görüntü yalnızca çıktılar kümesidir.

3.15 Sonuç [15, Theorem 1] n çift bir sayı olmak üzere, aşağıdaki ifadeler birbirine denktir:

(i) Bir (n, m)-fonksiyonu F büküktür.

(ii) $G_F \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m$ çizgesi, $N = \{(0, y) : y \in \mathbb{F}_2^m\}$ alt grubuna göre $\mathbb{F}_2^n \times \mathbb{F}_2^m$ içinde bir göreli $(2^n, 2^m, 2^n, 2^{n-m})$-fark kümesidir.

3.16 Teorem [1, Theorem 3.3] F bir (n, m)-fonksiyonu olsun. Aşağıdaki ifadeler birbirine denktir:

(i) F bir (n,m)-bükük fonksiyonudur.

(ii) $\mathcal{VF}(F)$, bir $2-(2^n,4,2^{n-m-1}-1)$ tasarımdır.

İspat: (1) $\Rightarrow$ (2): F bir (n,m)-bükük fonksiyonu olsun ve $\mathcal{VF}(F)=(\mathcal{P},\mathcal{B})$ bu fonksiyonun kaybolan düzlemler yapısı olsun. Herhangi iki farklı $\mathbf{x}_1,\mathbf{x}_2\in\mathcal{P}$ noktalarının, $\mathcal{B}$ kümesinde tam olarak $2^{n-m-1}-1$ adet blokta birlikte yer aldığını göstereceğiz.
Öncelikle,

$$\mathbf{a}:=\mathbf{x}_1\oplus\mathbf{x}_2 \qquad \text{ve} \qquad \mathbf{v}:=F(\mathbf{x}_1)\oplus F(\mathbf{x}_2)$$

olsun. Fonksiyonun grafiği

$$G_F:=\left\{\begin{pmatrix}\mathbf{x}\\ F(\mathbf{x})\end{pmatrix}:\mathbf{x}\in\mathbb{F}_2^n\right\}$$

grubu $G=\mathbb{F}_2^n\times\mathbb{F}_2^m$ içinde, yasak altgrup $N=\{(0,\mathbf{y}):\mathbf{y}\in\mathbb{F}_2^m\}$ 'ye göre bir $(2^n,\ 2^m,\ 2^n,\ 2^{n-m})$-fark kümesidir. Bu durumda,

$$\mathbf{g}:=\begin{pmatrix}\mathbf{a}\\ \mathbf{v}\end{pmatrix}\in G\setminus N$$

elemanı şu şekilde $2^{n-m}-2$ farklı biçimde gösterilebilir:

$$\begin{pmatrix}\mathbf{x}_1\\ F(\mathbf{x}_1)\end{pmatrix}\oplus\begin{pmatrix}\mathbf{x}_2\\ F(\mathbf{x}_2)\end{pmatrix}=\mathbf{g}=\begin{pmatrix}\mathbf{x}_3\\ F(\mathbf{x}_3)\end{pmatrix}\oplus\begin{pmatrix}\mathbf{x}_4\\ F(\mathbf{x}_4)\end{pmatrix}, \tag{3.1}$$

burada $\{\mathbf{x}_3,\mathbf{x}_4\}\neq\{\mathbf{x}_1,\mathbf{x}_2\}$.
Dolayısıyla her iki elemanlı altküme $\{\mathbf{x}_1,\mathbf{x}_2\}$, tam olarak $2^{n-m-1}-1$ adet blokta yer alır, öyle ki

$$\begin{pmatrix}\mathbf{x}_1\\ F(\mathbf{x}_1)\end{pmatrix}\oplus\begin{pmatrix}\mathbf{x}_2\\ F(\mathbf{x}_2)\end{pmatrix}\oplus\begin{pmatrix}\mathbf{x}_3\\ F(\mathbf{x}_3)\end{pmatrix}\oplus\begin{pmatrix}\mathbf{x}_4\\ F(\mathbf{x}_4)\end{pmatrix}=\begin{pmatrix}0\\ 0\end{pmatrix}. \tag{3.2}$$

Bu nedenle $\mathcal{VF}(F)$ yapısı, bir $2-(2^n,4,2^{n-m-1}-1)$ tasarımıdır.
(2) $\Rightarrow$ (1): Elde edilen $2-(2^n,4,2^{n-m-1}-1)$ tasarımın toplam blok sayısı (bkz.(3.3)), lineer kod $C_F^{\perp}$ içinde ağırlığı 4 olan kod sözcüklerinin sayısı A_4 'ün minimum değeri olan (3.9) ile örtüşür. Bu minimum değer yalnızca F fonksiyonu bir (n,m)-bükük fonksiyonu olduğunda elde edilir. Dolayısıyla, $\mathcal{V}_F(F)$ tasarımı bu özelliği sağladığı için F büküktür.

□

3.17 Uyarı Bir önceki teoreme ait ispat, bir F fonksiyonunun kaybolan düzlemlerinin sayısını $|\mathcal{VF}_F|$ hesaplamak için şu şekilde bir kombinatorik yöntem sunar:

(i) Grup farkı $G \setminus N$ içinden bir $\mathbf{g}$ elemanı seçmek için $2^{n+m} - 2^m$ farklı yol vardır.

(ii) Seçilen $\mathbf{g}$ için, eşitlik (3.1) 'in sol tarafını seçmek üzere 2^{n-m} farklı yol bulunur; bu da sağ taraf için $2^{n-m} - 2$ kalan seçim anlamına gelir.

(iii) Bu şekilde, eşitlik (3.2) 'yi sağlayan $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)$ biçiminde sıralı dörtlüler yani,

$$(2^{n+m} - 2^m) \cdot 2^{n-m} \cdot (2^{n-m} - 2)$$

adet sıralı kaybolan düzlemler elde edilir.

Bu sayı 24 'e bölündüğünde, blok sayısı şu şekilde bulunur:

$$|\mathcal{VF}_F| = \frac{(2^{n+m} - 2^m) \cdot 2^{n-m} \cdot (2^{n-m} - 2)}{24}. \tag{3.3}$$

Bu ifade açılıp sadeleştirildiğinde, eşitlik (3.9) 'daki değerle örtüşür.

Sonuç 3.12 'de belirtildiği gibi, kaybolan düzlemler yapısı (n, m)-fonksiyonlar için CCZ-denklik altında değişmezdir. Ancak, iki fonksiyon F ve F' için $\mathcal{VF}(F) \cong \mathcal{VF}(F')$ olması, her zaman CCZ-denkliği anlamına gelmez. Örneğin, APN fonksiyonlar için elde edilen insidans yapıları aşikar (trivial) olduğundan bu geçerli değildir. Bununla birlikte, yapılan hesaplamalara göre, bu ters yönlü ifade $(6, m)$-bükük fonksiyonlar için geçerlidir (bkz. [1]).

3.18 Uyarı Bükük fonksiyonlar, maksimum doğrusal olmayanlık özellikleri nedeniyle hem kriptografi hem de kombinatorik tasarım teorisinde önemli bir yere sahiptir. Sonuç 3.21, bükük fonksiyonların lineer kodlarla nasıl karakterize edilebildiğini göstermektedir. Özellikle, bükük fonksiyonun çizgesinden elde edilen C_F lineer kodu belirli parametrelere sahip olup, ağırlık sayacı (weight enumerator) kod sözcüklerinin dağılımını verir. Dual kod $C_F^{\perp}$ ise minimum mesafesi 4 olan bir lineer koddur ve ağırlığı 4 olan kod sözcüklerinin sayısı A_4, (bkz.(3.9)) değeri bükük fonksiyonların karakterizasyonu için bir kriter olarak kullanılmaktadır. Ayrıca hatırlamak gerekirse, (n, m)- bükük F fonksiyonların kaybolan düzlemleri $\mathcal{VF}(F)$, tanım gereği $C_F^{\perp}$ kodundaki ağırlığı 4 olan kod sözcüklerin destekleridir, böylelikle F 'nin kaybolan düzlemlerinin sayısı, $C_F^{\perp}$ kodunun ağırlığı 4 olan kod sözcüklerinin sayısına eşittir

Şimdi de bir (n, m)-fonksiyonu F 'nin lineer kodu $C_F^{\perp}$ 'de ağırlığı 4 olan kod sözcüklerinin sayısı ile Walsh dönüşümünün dördüncü momentleri arasında bir bağlantı (bkz. Teorem 3.20) vermeden önce aşağıdaki tanım ve sonuçlara ihtiyaç vardır.

Bir ikili lineer kodda her kod sözcüğü, sıfır ve birlerden oluşan bir vektördür. Bu vektörün ağırlığı, sıfır olmayan bileşenlerinin sayısıdır. Ağırlığı w olan bir kod sözcüğü, tam olarak w adet 1 içeren bir vektördür. Bu tür kod sözcüklerinin sayısı, kodun ağırlık dağılımını belirler ve kodun yapısal özelliklerinin analizinde önemli rol oynar.

3.19 Önerme [20, Proposition 1.5] Her $a \in \mathbb{F}_2^n$ için aşağıdaki eşitlik geçerlidir:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} = \begin{cases} 0 & \text{eğer } a \neq 0, \\ 2^n & \text{eğer } a = 0. \end{cases}$$

İspat: Öncelikle $a = 0$ ele alalım. İç çarpım $a \cdot x = 0$ olur ve her terim $(-1)^0 = 1$ olur. Dolayısıyla:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} = \sum_{x \in \mathbb{F}_2^n} 1 = 2^n.$$

Şimdi $a \neq 0$ olduğunu varsayalım. Bu durumda, aşağıdaki iki küme tanımlanır:

$$H_1 = \{x \in \mathbb{F}_2^n \mid a \cdot x = 0\}, \quad H_2 = \{x \in \mathbb{F}_2^n \mid a \cdot x = 1\}.$$

Açıkça görülüyor ki H_1 ve H_2, $\mathbb{F}_2^n$ uzayının ayrık bir bölümlenmesidir. Her $x \in H_1$ için $(-1)^{a \cdot x} = 1$, her $y \in H_2$ için $(-1)^{a \cdot y} = -1$ olur. Her iki kümenin eleman sayıları eşittir ve 2^{n-1} eleman içerir.

Bu durumda, toplamı şu şekilde hesaplayabiliriz:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} = \sum_{x \in H_1} 1 + \sum_{x \in H_2} (-1) = 2^{n-1} - 2^{n-1} = 0.$$

Böylece, her $a \in \mathbb{F}_2^n$ için

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} = \begin{cases} 2^n & \text{eğer } a = 0, \\ 0 & \text{eğer } a \neq 0 \end{cases}$$

eşitliği sağlanmış olur.

□

3.20 Teorem [20, Theorem 2.5.] $m \leq n$ olacak şekilde $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ fonksiyonu verilsin. Bu fonksiyona karşılık gelen $C_F^{\perp}$ dual kodunda ağırlığı 4 olan vektörlerin sayısı $\lambda(f_1, \ldots, f_m)$ aşağıdaki şekilde verilir:

$$\lambda(f_1, \ldots, f_m) = \frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{\substack{a\in\mathbb{F}_2^n \\ b\in\mathbb{F}_2^m \\ b\neq 0}} (W_F(a,b))^4 + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right]. \tag{3.4}$$

İspat: Daha önce de verildiği gibi, Walsh dönüşümü $W_F(a,b)$ aşağıdaki şekilde tanımlanır:

$$W_F(a,b) = \sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x + b\cdot F(x)}, \quad a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m.$$

Bu Walsh dönüşümde her iki tarafın da dördüncü kuvvetini aldığımızda ise aşağıdaki şekilde gösterilir:

$$(W_F(a,b))^4 = \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x + b\cdot F(x)}\right)^4, \quad a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m.$$

Şimdi, şu durumu ele alıyoruz:

$$\sum_{a\in\mathbb{F}_2^n,\, b\in\mathbb{F}_2^m} (W_F(a,b))^4 = \sum_{a\in\mathbb{F}_2^n,\, b\in\mathbb{F}_2^m} \left(\sum_{x,y,z,w\in\mathbb{F}_2^n} (-1)^{a\cdot(x+y+z+w)+b\cdot(F(x)+F(y)+F(z)+F(w))}\right) \tag{3.5}$$

Dolayısıyla,

$$\begin{aligned}\sum_{a\in\mathbb{F}_2^n,\, b\in\mathbb{F}_2^m} (W_F(a,b))^4 \;=\; & \sum_{x,y,z,w\in\mathbb{F}_2^n} \left[\sum_{a\in\mathbb{F}_2^n} (-1)^{a\cdot(x+y+z+w)}\right] \\ & \cdot \left[\sum_{b\in\mathbb{F}_2^m} (-1)^{b\cdot(F(x)+F(y)+F(z)+F(w))}\right].\end{aligned} \tag{3.6}$$

(3.5), (3.6) eşitlikleri ve Önerme 3.19 kullanılarak aşağıdaki sonuç elde edilir:

$$\sum_{a\in\mathbb{F}_2^n,\, b\in\mathbb{F}_2^m} (W_F(a,b))^4 = 2^{n+m}\cdot\Gamma,$$

buradaki Γ (dört elemanlı vektör toplamlarının sıfır olduğu ve fonksiyon değerlerinin de toplamda sıfır olduğu durumların sayısı) ise şu şekilde tanımlanır:

$$\Gamma = \#\left\{(x,y,z,w) \in (\mathbb{F}_2^n)^4 \;\middle|\; \begin{array}{l} x+y+z+w = 0 \\ F(x)+F(y)+F(z)+F(w) = 0 \end{array}\right\}. \tag{3.7}$$

Şimdi ise (3.7) numaralı eşitliği sağlayan dörtlü $(x, y, z, w) \in (\mathbb{F}_2^n)^4$ değerleri için olabilecek durumları inceleyelim:

Durum 1: İlk olarak tüm değerler eşit yani $x = y = z = w$ olsun. Böylece $F(x) = F(y) = F(z) = F(w)$ eşitlikleri de olur. Bu durumda her $x \in \mathbb{F}_2^n$ için tek bir çözüm elde edilmiş olur. Dolayısıyla bu durumda tam olarak 2^n farklı dörtlü vardır.

Durum 2: İkinci olarak dörtlüdeki tüm elemanlar birbirinden farklı olsun. Bu şekilde olan dörtlüler, $\mathcal{C}_{f_1,\ldots,f_m}$ lineer kodunun içindeki ağırlığı 4 olan kod sözcüklerini temsil eder. Ağırlığı 4 olan her kod sözcüğünü sıralamanın yolları $4! = 24$ olur bu da 24 farklı dörtlü üretir. Bu nedenle bu durumda $24 \cdot \lambda(f_1, \ldots, f_m)$ adet dörtlü vardır.

Durum 3: Son durum olarak ise dörtlüdeki herhangi iki eleman eşit olsun (örneğin $x = y$, $x = z$, vb.). Bu durumda $x+y+z+w = 0$ eşitliğinin sağlanabilmesi için diğer iki elemanın da birbirine eşit olması gerekir. Ancak bu durumun, durum 1 kapsamına girmemesi için iki farklı eleman seçilerek oluşturulmalıdır. Bu da

$$\binom{2^n}{2}$$

farklı seçimle yapılabilir. Toplamda 6 farklı eşleşme durumu olduğundan bu türden elde edilen dörtlü sayısı ise

$$6 \cdot \binom{2^n}{2} = 3(2^{2n} - 2^n)$$

şeklinde hesaplanır.

Yukarıda incelediğimiz üç farklı durumun toplamı, Walsh dönüşümünün dördüncü kuvvetlerinin toplamını verir:

$$\sum_{a \in \mathbb{F}_2^n,\, b \in \mathbb{F}_2^m} (W_F(a,b))^4 = 2^{n+m} \left[2^n + 24 \cdot \lambda(f_1, \ldots, f_m) + 3(2^{2n} - 2^n)\right].$$

Bu eşitlikten yola çıkılarak ağırlığı 4 olan kod sözcüklerinin sayısını şu şekilde verebiliriz:

$$\lambda(f_1, \ldots, f_m) = \frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{a \in \mathbb{F}_2^n,\, b \in \mathbb{F}_2^m,\, b \neq 0} (W_F(a,b))^4 + 2^{4n}\right) - 3 \cdot 2^{2n} + 2^{n+1}\right],$$

burada, $W_F(a, 0) = 2^n$ yalnızca $a = 0$ için geçerlidir; $a \neq 0$ olduğunda $W_F(a, 0) = 0$ olur. Sonuç olarak, Önerme 3.19 'dan dolayı,

$$W_F(a, 0) = 0 \quad \text{(eğer } a \neq 0 \text{ ise)}.$$

□

3.21 Sonuç [1, Corollary 1.13] $n = 2k$ olmak üzere, aşağıdaki üç ifade birbirine denktir:

(i) Bir (n, m)-fonksiyonu F büküktür.

(ii) C_F lineer kodu, bir $[2^n,\ n+m+1,\ 2^{n-1}-2^{k-1}]$-lineer koddur ve ağırlık sayacı (weight enumerator) şu şekildedir:

$$W_{C_F}(z) = 1 + (2^m - 1)2^n z^{2^{n-1}-2^{k-1}} + (2^{n+1} - 2)z^{2^{n-1}} + (2^m - 1)2^n z^{2^{n-1}+2^{k-1}} + z^{2^n} \quad (3.8)$$

(iii) $C_F^{\perp}$ dual lineer kodu, bir $[2^n,\ 2^n - n - m - 1,\ 4]$-lineer koddur ve ağırlığı 4 olan kod sözcüklerinin sayısı aşağıdaki gibidir:

$$A_4 = \frac{1}{3}\left(2^{3n-m-3} - 2^{2n-m-3} - 2^{2n-2} + 2^{n-2}\right). \quad (3.9)$$

Bu değer, n çift ve $m \leq n/2$ koşulu altında bir (n, m)-fonksiyonu F için mümkün olan en küçük değerdir.

Yukarıdaki mükemmel ve neredeyse mükemmel doğrusal olmayan fonksiyonların karakterizasyonlarını Teorem 3.20 ile elde etmek zor değildir.

3.22 Sonuç [1, Corollary 1.14] Bir (n, n)-fonksiyonu F, ancak ve ancak aşağıdaki birbirine denk iki koşuldan biri sağlandığında *neredeyse mükemmel doğrusal olmayan (APN)* fonksiyondur:

(i) $C_F^{\perp}$ dual lineer kodu, bir $[2^n,\ 2^n - 2n - 1,\ 6]$-lineer koddur.

(ii) $C_F^{\perp}$ içinde ağırlığı 4 olan kod sözcüklerinin sayısı $A_4 = 0$'dır.

Neredeyse mükemmel doğrusal olmayan (APN) fonksiyonlar, diferansiyel kriptanalize karşı en güçlü doğrusal olmayanlık özelliklerine sahip fonksiyonlardır. Sonuç 3.22, bu fonksiyonların karakterizasyonunu kodlama teorisi açısından sunmaktadır.

3.23 Tanım F, $\mathbb{F}_2^n$ üzerinde tanımlı bir APN (Neredeyse Mükemmel Doğrusal Olmayan) fonksiyonu olsun. Genelliği kaybetmeyecek şekilde $F(0) = 0$ olduğunu varsayalım. Fonksiyon F 'nin klasik Walsh spektrumuna sahip olması aşağıdaki iki durumdan birinin sağlanmasıyla tanımlanır:

(i) n tek sayı ise ve F, AB formundaysa, spektrum şu şekildedir:

$$\Lambda_F = \left\{*2^n[1],\ 0\left[(2^{n-1}+1)(2^n-1)\right],\ \pm 2^{(n+1)/2}\left[(2^n-1)\left(2^{n-2} \pm 2^{(n-3)/2}\right)\right] *\right\}. \quad (3.10)$$

(ii) n çift sayı ise ve F, Gold formundaki APN fonksiyonların spektrumuna sahipse (burada $f : x \mapsto x^{2^i+1}$, $\gcd(i, n) = 1$), spektrum şu şekildedir:

$$\begin{aligned}\Lambda_F \;=\; &\left\{ *2^n[1],\ 0\left[(2^n-1)(2^{n-2}+1)\right],\ \pm 2^{(n+2)/2}\left[\frac{1}{3}(2^n-1)\left(2^{n-3}\pm 2^{(n-4)/2}\right)\right],\right.\\ &\left.\pm 2^{n/2}\left[\frac{2}{3}(2^n-1)\left(2^{n-1}\pm 2^{(n-2)/2}\right)\right] * \right\}. \qquad (3.11)\end{aligned}$$

3.24 Teorem [1, Theorem 2.9] F, $n = 2k$ olmak üzere $\mathbb{F}_2^n$ üzerinde tanımlı bir APN fonksiyon ve klasik Walsh spektrumuna sahip olsun. Eğer F, yalnızca bükük ve yarı-bükük olan sıfır olmayan bileşen fonksiyonlara sahip bir fonksiyon F' ile CCZ-eşdeğerliğe sahipse, o hâlde lineer kodlar $\mathcal{C}_F$ ve $\mathcal{C}_F^{\perp}$, 2-tasarım destekler.

Şimdi de (n, m) fonksiyonların kaybolmayan düzlemlerinden bahsedilecektir.

3.25 Tanım F bir (n, m)-fonksiyonu olsun. Sıfır olmayan bir vektör $v \in \mathbb{F}_2^m$'ye göre tanımlanan (n, m)-fonksiyonunun *kaybolmayan düzlemleri* olarak adlandırılan kısmi dörtlü sistem, aşağıdaki insidans yapısı ile tanımlanır:

$$\mathcal{NF}_v(F) := (\mathcal{P}, \mathcal{NF}_{v,F})$$

burada nokta kümesi

$$\mathcal{P} := \{x : x \in \mathbb{F}_2^n\}$$

ve blok kümesi $\mathcal{NF}_{v,F}$ aşağıdaki şekilde tanımlanır:

$$\mathcal{NF}_{v,F} = \left\{ \{x_1, x_2, x_3, x_4\} : \bigoplus_{i=1}^{4} \begin{pmatrix} x_i \\ F(x_i) \end{pmatrix} = \begin{pmatrix} 0 \\ \mathbf{v} \end{pmatrix}, \quad x_i \in \mathbb{F}_2^n \right\} \qquad (3.12)$$

3.26 Sonuç [1, Result 4.7] F bir (n, m)-fonksiyon olsun. Fonksiyonun $x \in \mathbb{F}_2^n$ noktasında ikinci mertebeden türevi, aşağıdaki şekilde tanımlanır:

$$D_{a,b}F(x) := F(x) \oplus F(x \oplus a) \oplus F(x \oplus b) \oplus F(x \oplus a \oplus b).$$

Her $v \in \mathbb{F}_2^m$ ve $x \in \mathbb{F}_2^n$ için, aşağıdaki kümenin eleman sayısını ifade eden $N_F(v; x)$ şu şekilde tanımlanır:

$$N_F(v; x) := \left|\{(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \ : \ D_{a,b}F(x) = v\}\right|.$$

Bu durumda, her $x \in \mathbb{F}_2^n$ ve $v \in \mathbb{F}_2^m$ için $N_F(v; x)$ değeri aşağıdaki şekilde hesaplanabilir:

$$N_F(v;x) = 2^{-m} \cdot \sum_{u \in \mathbb{F}_2^m} \sum_{a,b \in \mathbb{F}_2^n} (-1)^{\langle u, D_{a,b}F(x)\rangle_m \oplus \langle u,v\rangle_m}.$$

3.27 Teorem [1, Theorem 4.10] F bir (n,m)-fonksiyonu olsun ve $\lambda_v \in \mathbb{N}$ aşağıdaki şekilde tanımlansın:

$$\lambda_0 = \frac{N_F(0;x) - 3 \cdot 2^n + 2}{6}, \quad \lambda_v = \frac{N_F(v;x)}{6} \quad \text{için} \quad v \in \mathbb{F}_2^m \setminus \{0\}.$$

O hâlde, ancak ve ancak tüm $v \in \mathbb{F}_2^m \setminus \{0\}$ için $\mathcal{NF}_v(F)$ insidans yapısı bir 1-$(2^n, 4, \lambda_v)$ tasarımı olduğunda, F fonksiyonu *plato* bir fonksiyondur.

Ayrıca, bir (n,m)-fonksiyonu F 'nin kaybolan düzlemleri olan $\mathcal{VF}(F)$ yapısı bir 1-$(2^n, 4, \lambda_0)$ tasarımıdır.

3.28 Sonuç [1, Corollary 4.12] F bir (n,m)-fonksiyonu olsun. Aşağıdaki ifadeler birbirine denktir:

(i) F fonksiyonu, s-plato (s-plateaued) bir fonksiyondur.

(ii) Tüm $v \in \mathbb{F}_2^m \setminus \{0\}$ için, $\mathcal{NF}_v(F)$ insidans yapısı bir

$$1\text{-}\left(2^n, 4, \frac{2^{n+s-m}\left(2^{n-s}-1\right)}{6}\right)$$

tasarımıdır. Ayrıca, s-plato bir (n,m)-fonksiyonu F'nin kaybolan düzlemleri olan $\mathcal{V}_F(F)$ bir

$$1\text{-}\left(2^n, 4, \frac{2^{n+s-m}\left(2^{n-s}+2^m-1\right) - 3 \cdot 2^n + 2}{6}\right)$$

tasarımıdır.

3.29 Teorem [1, Theorem 4.14] F bir (n,m)-fonksiyonu olsun. Aşağıdaki ifadeler birbirine denktir:

(i) F bir (n,m)-bükük fonksiyondur.

(ii) Her $v \in \mathbb{F}_2^m \setminus \{0\}$ için, $\mathcal{NF}_v(F)$ insidans yapısı bir $2-(2^n, 4, 2^{n-m-1})$ tasarımıdır.

Ayrıca, bir (n,m)-bükük F fonksiyonun bir $v \in \mathbb{F}_2^m \setminus \{0\}$ vektörüne göre kaybolmayan düzlem sayısı aşağıdaki gibi verilir:

$$|\mathcal{NF}_{v,F}| = \frac{(2^{n+m} - 2^m) \cdot 2^{2(n-m)}}{24}. \tag{3.13}$$

İspat: F bir (n,m)-bükük fonksiyonu ve $v \in \mathbb{F}_2^m \setminus \{0\}$ olsun. Fonksiyonun v'ye göre tanımlanan kaybolmayan düzlemlerin yapısını $\mathcal{NF}_v(F) = (\mathcal{P}, \mathcal{B})$ olarak tanımlayalım. Amaç, $\mathcal{P}$ kümesindeki herhangi iki farklı nokta x_1, x_2'nin tam olarak 2^{n-m-1} adet blokta birlikte yer aldığını göstermektir.

Öncelikle $a := x_1 \oplus x_2$, $v' := F(x_1) \oplus F(x_2)$ ve $v'' := v' \oplus v$ olarak tanımlansın. Bu durumda aşağıdaki eşitlik elde edilir:

$$\begin{pmatrix} x_1 \\ F(x_1) \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ F(x_2) \end{pmatrix} = \begin{pmatrix} a \\ v' \end{pmatrix} = \begin{pmatrix} 0 \\ v \end{pmatrix} \oplus \begin{pmatrix} a \\ v'' \end{pmatrix} \tag{3.14}$$

Burada $\mathcal{G}_F$ grafiği, $G = \mathbb{F}_2^n \times \mathbb{F}_2^m$ grubunda, yasak altgrup $N = \{(0,y) : y \in \mathbb{F}_2^m\}$'e göre bir $(2^n, 2^m, 2^n, 2^{n-m})$-fark kümesidir. Buna göre $g := \begin{pmatrix} a \\ v'' \end{pmatrix} \in G \setminus N$ elemanının

$$g = \begin{pmatrix} x_3 \\ F(x_3) \end{pmatrix} \oplus \begin{pmatrix} x_4 \\ F(x_4) \end{pmatrix} \tag{3.15}$$

şeklinde, $\{x_3, x_4\} \neq \{x_1, x_2\}$ koşulunu sağlayan tam 2^{n-m} farklı gösterimi vardır. Bu yapıdan, her iki elemanlı altküme $\{x_1, x_2\}$ 'nin (3.12) biçimindeki bloklardan tam olarak 2^{n-m-1} adet dört elemanlı blokta $\{x_1, x_2, x_3, x_4\}$ yer aldığını gösterir. Dolayısıyla $\mathcal{NF}_v(F)$ yapısı bir 2-$(2^n, 4, 2^{n-m-1})$ tasarımdır. Blok sayısı Uyarı 3.17 ile uyumludur.

Ters yönde, kaybolan ve kaybolmayan düzlemlerin birlikte Afine Steiner Dörtlü Sistemini oluşturduğu ve bu sistemin bir bölüşüm olduğu bilgisi kullanılır. Bu bölüşüm sonucunda elde edilen kaybolan düzlem sayısı, (3.9) 'da verilen değere eşittir ve bu değer tüm (n,m)-fonksiyonlar arasında mümkün olan en küçük değerdir. Bu minimumluk, F 'nin (n,m)-bükük fonksiyon olmasını gerektirir. Böylece iki ifade birbirine denktir.

□

3.30 Uyarı [1, Remark 4.5] Genel olarak, (n,m)-fonksiyonlar için kaybolmayan düzlemlerin hangi özellikleri gösterdiği, CCZ-eşdeğerlik altında korunmaz. Aşağıda verilen örnek ise bu durumu açıkça gösterir.

$\mathbb{F}_2^6$ sonlu cismi, toplama ve çarpma işlemleriyle birlikte $(\mathbb{F}_{2^6}, +, \cdot)$ yapısı altında ele alınır. Bu cismin çarpımsal grubu $\mathbb{F}_{2^6}^*$, ilkel polinom $p(x) = x^6 + x^4 + x^3 + x + 1$ için bir kök olan a tarafından üretilir ve $\mathbb{F}_{2^6}^* = \langle a \rangle$ şeklinde gösterilir.

$\mathbb{F}_{2^6}$ yapısında tanımlı Kim'in APN fonksiyonu: $x \in \mathbb{F}_{2^6} \mapsto K(x)$ ve Dillon'un APN permütasyonu: $x \in \mathbb{F}_{2^6} \mapsto G(x)$ iki fonksiyon incelenmiştir. Bu iki fonksiyon CCZ-eşdeğer olmalarına rağmen EA-eşdeğer değildir. Bu fonksiyonların tek değişkenli gösterimleri [18] numaralı kaynakta yer almaktadır. Bilgisayar destekli hesaplamalar Kim'in APN fonksiyonu için gösterir ki:

(i) $\mathbb{F}_{2^6}$ cisminde 42 farklı v elemanı için $\mathcal{NF}_v(K)$ yapısı bir 1-$(64, 4, 9)$ tasarımıdır.

(ii) Aynı zamanda 21 farklı v elemanı için $\mathcal{NF}_v(K)$ yapısı bir 1-$(64, 4, 13)$ tasarımıdır.

Buna karşılık olarak, Dillon'un APN permütasyonuna ait kaybolmayan düzlemler arasında yalnızca 7 tanesi, yani

$$v \in V = \{1, a^7, a^8, a^{29}, a^{44}, a^{50}, a^{53}\}$$

için $\mathcal{NF}_v(G)$ yapıları 1-$(64, 4, 13)$ tasarımlardır.

4. SONUÇ VE ÖNERİLER

Bu tezde kriptografik fonksiyonların temel tanım ve özellikleri verilmiştir. Özellikle bu fonksiyonların insidans yapılarıyla ilişkilendirilmesi, fonksiyonların daha derinlemesine anlaşılmasına ve tasarım teorisi ile kodlama teorisi arasında güçlü bir bağ kurulmasına imkan sağlamıştır. Çalışmanın sonunda elde edilen bulgular değerlendirilmiş ve gelecekteki araştırmalar için öneriler sunulmuştur.

Bu sonuçlar, CCZ-eşdeğer fonksiyonlar arasında dahi kaybolmayan düzlemlerin sayısal ve yapısal farklılıklar gösterebileceğini ortaya koymaktadır. Dolayısıyla, bu tür geometrik yapılar CCZ-eşdeğerlik altında korunmaz ve fonksiyonların ayrıştırılmasında ayırt edici bir yere sahiptir.

Bükük fonksiyonlar ve genellemeleri tasarım teorisi kapsamında incelendiğinde, farklı (n, m)-fonksiyon sınıflarının kaybolan düzlemleri, kaybolmayan düzlemleri ve kod destekleri bakımından çeşitli tasarımlara karşılık geldiği görülür. Bunun için şimdiye kadar verdiğimiz bazı teorem ve sonuçlardan yararlanarak bazı bilinen sonuçlara geçeceğiz.

4.1 Sonuç (n, m)-bükük fonksiyonların kaybolan düzlemleri 2-tasarım oluşturur ancak ve ancak Teorem 3.16 'nın koşulları sağlanır. Kaybolmayan düzlemleri de 2-tasarım oluşturur ancak ve ancak Teorem 3.29 'un koşulları sağlanır. Ayrıca, kod ve dual kodun destek yapısı da [17, Example 4] den dolayı 2-tasarım oluşturur.

4.2 Sonuç Diferansiyel olarak iki-değerli s-plato (n, n)-fonksiyonların kaybolan düzlemleri 2-tasarım, kaybolmayan düzlemleri ise eşdüzenli (equiregular) 1-tasarım yapısındadır ancak ve ancak [17, Theorem 6.1] ve Sonuç 3.28 'in koşulları sağlanır. Ayrıca, kod ve dual kodun destek yapısı da [17, Theorem 6.4] den dolayı 2-tasarım oluşturur.

4.3 Sonuç Diferansiyel olarak iki-değerli (n, n)-fonksiyonların kaybolan düzlemleri 2-tasarım oluşturur ancak ve ancak [17, Theorem 6.1] koşulları sağlanır. Kaybolmayan düzlemleri ise Uyarı 3.30 'dan dolayı her zaman 1-tasarım olmayabilir.

4.4 Sonuç s-Plato (n, m)-fonksiyonların kaybolmayan düzlemleri eşdüzenli 1-tasarım yapısındadır ancak ve ancak Sonuç 3.28 koşulları sağlanır.

4.5 Sonuç Plato (n, m)-fonksiyonların kaybolmayan düzlemleri 1-tasarım oluşturur ancak ve ancak Teorem 3.27 koşulları sağlanır.

Son olarak aşağıdaki problemler okuyucuya sunulmuştur [1].

4.6 Problem Genellikle, diferansiyel olarak iki-değerli (n, n)-fonksiyon olan F'ler için tanımlanan lineer kodlar C_F ve dual kodlar $C_F^{\perp}$ 'nun hangi koşullar altında 2-tasarım desteklediğini belirlemek kolay değildir. Teorem 3.24 'de, APN fonksiyonlar için fonksiyonun klasik Walsh spektrumuna sahip olması şeklinde koşul ortaya konmuştur. Bu koşulun hem gerekli hem de yeterli olup olmadığını ortaya koymak veya 2-tasarım destekleyen başka APN fonksiyon sınıflarını belirlemek, araştırmaya değer bir konudur.

4.7 Problem Dillon'un listesinde yer alan kuadratik APN fonksiyonlardan bir koordinat fonksiyonunun silinmesiyle elde edilen projeksiyonlardan 1-tasarım yapıları elde edilebilir. Ancak, bu durumun neden gerçekleştiği teorik olarak net değildir; çünkü genişletilmiş Assmus-Mattson Teoremi artık uygulanabilir değildir. Bu nedenle, bu özel durumda daha dikkatli bir analize ihtiyaç vardır. Yine de bu yapının ilginç bir insidans yapısı üretmesi beklenmemektedir; en fazla 1-tasarım elde edilebileceği öngörülmektedir.

5. KAYNAKLAR

[1] **Meidl, W., Polujan, A. A., and Pott, A.** (2023).Linear codes and incidence structures of bent functions and their generalizations. *Discrete Mathematics*. 346(1), Hollanda. 113157.

[2] **Pott, A.** (2016). Almost perfect and planar functions. *Designs, Codes and Cryptography*, 78(1), Almanya, 141–195.

[3] **Ling, S., and Xing, C.** (2004). Coding Theory. Cambridge University Press, İngiltere, 584.

[4] **Özdemir, D.** (2022). APN ve Düzlemsel Fonksiyonlar ile Tanımlanan Lineer Kodların Bazı Parametreleri. Yüksek Lisans Tezi. Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, 64.

[5] **Sulak, F.** (2006). Construction of Bent Function, The Middle East Technical University Graduate School of Applied Mathematics, 59.

[6] **Li, S.**, **Meidl, W.**, **Polujan, A.**, **Pott, A.**, **Riera, C.**, and **Stanica, P.** (2020). Vanishing flats: a combinatorial viewpoint on the planarity of functions and their application. *IEEE Transactions on Information Theory*, 66(11), United States, 7101–7112.

[7] **Oblaukhov, A.** (2021). On metric regularity of Reed-Muller codes. *Designs, Codes and Cryptography*, 89(1), United States, 167–197.

[8] **Colbourn, C. J.**, **and Mathon, R.** (2007). Steiner systems. Handbook of Combinatorial Designs (Discrete Mathematics and Its Applications), 2nd ed., Chapman & Hall/CRC, United States, 102–110.

[9] **Stinson, D. R.**, **Wei, R., and Yin, J.** (2007). Packings. Handbook of Combinatorial Designs (Discrete Mathematics and Its Applications), 2nd ed., Chapman & Hall/CRC, United States, 550–556.

[10] **Budaghyan, L., Carlet, C.**, **and Pott, A.** (2006). New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3), United States, 1141–1152.

KAYNAKLAR DİZİNİ (devam)

[11] **Budaghyan, L., and Carlet, C.** (2009). On CCZ-equivalence and its use in secondary constructions of bent functions. Preproceedings of the International Workshop on Coding and Cryptography, WCC 2009, Norway, 19–36.

[12] **Kyureghyan, G. M., and Pott, A.** (2008). Some theorems on planar mappings. In J. von zur Gathen, J. L. Imana, ve Ç. K. Koç (Eds.), Arithmetic of Finite Fields, Springer, United States, 117–122.

[13] **Sarıyüce, M.** (2011). *On bent and hyper-bent functions*. Sabancı Üniversitesi Mühendislik ve Fen Bilimleri Enstitüsü, 58.

[14] **Fisher, T. A.** (2008). *Linear algebra: Non-degenerate bilinear forms*. Michaelmas Term Notes, United Kingdom, 1–20.

[15] **Pott, A.** (2004). Nonlinear functions in abelian groups and relative difference sets. *Discrete Applied Mathematics*, 138(1–2), United States, 177–193.

[16] **Polujan, A., and Pott, A.** (2021). On design-theoretic aspects of Boolean and vectorial bent functions. *IEEE Transactions on Information Theory*, 67(2), United States, 1027–1037.

[17] **Tang, C., Ding, C., and Xiong, M.** (2020). Codes, differentially δ-uniform functions, and t-designs. *IEEE Transactions on Information Theory*, 66(6), United States, 3691–3703.

[18] **Browning, K. A., Dillon, J. F., McQuistan, M. T., and Wolfe, A. J.** (2010). An APN permutation in dimension six. In McGuire, G., Mullen, G. L., Panario, D., and Shparlinski, I. E. (Eds.), Finite Fields: Theory and Applications-FQ9, *Contemporary Mathematics*, 518, American Mathematical Society, United States, 33-42.

[19] **Edel, Y.**, **Pott, A.** (2009). *On the equivalence of nonlinear functions*. In: *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, pp. 87–103.

[20] **Arshad, R.** (2018). *Contributions to the theory of almost perfect nonlinear functions*. Ph.D. thesis, *Otto-von-Guericke-Universität Magdeburg*, Fakultät für Mathematik.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Büşra YILDIZ ÇAPKAN

Doğum tarihi ve yeri :

e-posta :

Öğrenim Bilgileri

Derece	Okul / Program	Yıl
Lisans	Balıkesir Üniversitesi / Matematik Bölümü	2022
Lise	Farabi Mesleki ve Teknik Anadolu Lisesi / Hemşirelik (Dursunbey/Balıkesir)	2016