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

APN VE DÜZLEMSEL FONKSİYONLAR İLE TANIMLANAN LİNEER KODLARIN BAZI PARAMETRELERİ

DAMLA ÖZDEMİR

YÜKSEK LİSANS TEZİ

Jüri Üyeleri : **Doç. Dr. Seher TUTDERE KAVUT (Tez Danışmanı)**
Prof. Dr. Müge KANUNİ ER
Doç. Dr. Pınar METE

BALIKESİR, AĞUSTOS- 2022

ETİK BEYAN

Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak tarafımca hazırlanan "**APN ve Düzlemsel Fonksiyonlar İle Tanımlanan Lineer Kodların Bazı Parametreleri**" 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.

Damla ÖZDEMİR

ÖZET

APN VE DÜZLEMSEL FONKSİYONLAR İLETANIMLANAN LİNEER KODLARIN BAZI PARAMETRELERİ
YÜKSEK LİSANS TEZİ
DAMLA ÖZDEMİR
BALIKESİR ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
(TEZ DANIŞMANI: DOÇ. DR. SEHER TUTDERE KAVUT)
BALIKESİR, AĞUSTOS-2022

Kodlama teorisinde hemen hemen mükemmel lineer olmayan (APN) fonksiyonlar ve düzlemsel fonksiyonlar ile tanımlanan lineer kodlar önemli bir yere sahiptirler. Bu tezde, bu fonksiyonlar ile tanımlanan lineer kodlar ele alınmıştır. Özel olarak, bu kodların örtme yarıçapı, minimum mesafesi ve boyutları ile ilgili literatürde bilinen sonuçlar incelenerek bir derleme olarak sunulmuştur.

KELİMELER: APN fonksiyonlar, düzlemsel fonksiyonlar, lineer kodlar, minimum mesafe, örtme yarıçapı

Bilim Kod / Kodları: 20401 Sayfa Sayısı: 56

ABSTRACT

SOME PARAMETERS OF LINEAR CODES FROM APN AND PLANAR FUNCTIONS
MSC THESIS
DAMLA ÖZDEMİR
BALIKESIR UNIVERSITY INSTITUTE OF SCIENCE MATHEMATICS
(SUPERVISOR: ASSOC. PROF. DR. SEHER TUTDERE KAVUT)
BALIKESİR, AUGUST-2022

The linear codes defined by almost perfect nonlinear (APN) functions and planar functions play an important role in coding theory. In this thesis, the codes defined by those functions are considered. Specifically, we present a review of the related literature by analyzing some known results on the covering radius, minimum distance and dimension of the mentioned codes.

KEYWORDS: APN functions, planar functions, linear codes, minimum distance, covering radius

Science Code / Codes: 20401 Page Number: 56

İÇİNDEKİLER

Sayfa

TABLO LİSTESİ

Sayfa

SEMBOL LİSTESİ

q : p^m, p bir asal sayı ve m bir pozitif tam sayı
C : n pozitif bir tam sayı olmak üzere, n uzunluklu ve k boyutlu $\mathbb{F}_q$ üzerinde tanımlı kod
|C| : C kodunun büyüklüğü
d(x, y) : x ve y sözcükleri arasındaki mesafe
d(C) : C kodunun minimum mesafesi
e(C) : C kodunun paketleme yarıçapı
G : Üreteç matrisi
H : Eşlik-kontrol matrisi
R(C) : C kodunun örtme yarıçapı
$\boldsymbol{\alpha}$: İlkel kök

ÖNSÖZ

Matematik öğrenmenin ve matematiği anlamanın verdiği mutluluğu yaşam boyu devam ettirmek amacıyla atmaya başladığım bu ilk adımlarımı, üretken bir matematikçi olarak sürdürmek, en büyük arzum ve hayalim.

Bu yolda Matematiğe sadece uzaktan bakan gözlerden, yakından gören gözlere geçişimi sağlayan başta çok değerli hocam ve danışmanım Doç. Dr. Seher TUTDERE KAVUT olmak üzere, hayatlarına girdiğimden bu yana, bana güvenen, cesaretimi güçlendiren ve beni hiçbir zaman yalnız bırakmayan AYDIN ailesinin, tek tek tüm bireylerine, Yüksek Lisans eğitimim boyunca, desteğini esirgemeyen ve her konuda hayatımı kolaylaştırmış olan sevgili M. Ülkü AYDIN KÜÇÜK ablama ve onun değerli arkadaşlarına sonsuz teşekkürlerimi sunarım.

Balıkesir, 2022 **Damla ÖZDEMİR**

1. GİRİŞ

Claude Shannon, 1948 yılında yaptığı çalışmalarla daha önce bazı temel fikirleri anlaşılmış olan bilişim teorisinin daha sağlam temeller üzerine kurulmasını ve popüler hale gelmesini sağlamıştır [1]. Shannon'ın yaptığı çalışmalarda, uygun kodlamanın varlığı söylenmekte, ancak nasıl yapılabileceğine dair herhangi bir açık yöntem verilmemektedir.

Bunun üzerine, uygun kodlamanın nasıl yapılabileceğine ilişkin araştırmalarla birlikte, "Kodlama Teorisi" ortaya çıkmaya başlamıştır. İlk adımı ise Richard W. Hamming, hata düzeltme kodları (e-error-correcting codes) üzerine yaptığı çalışmanın detaylarını yayınlayarak atmıştır [1]. Bundan sonra kodlama teorisi yarım yüzyılı aşan bir süre içinde oldukça hızlı bir şekilde büyümüş ve gelişmiştir.

Hemen hemen mükemmel lineer olmayan (APN) ve mükemmel lineer olmayan (PN) fonksiyonlar, tasarım teorisi, kodlama teorisi ve kriptografide merkezi bir yere sahiptir. Karakteristik $p = 2$ için $\mathbb{F}_{p^m}$ sonlu cismi üzerinde tanımlanan APN fonksiyonlar kriptografik iletişim kurallarının inşasında optimal diferansiyel özelliklere sahiptir. APN fonksiyonlar telekomünikasyon, yani iki ya da daha fazla kişinin teknolojiyi kullanarak bilgi alışverişinde bulunmaları, dışında diğer birçok alanda da kullanılmaktadır.

PN fonksiyonlar içerisinde özel olarak tanımlanmış düzlemsel fonksiyonlar tek karakteristikli cisimler üzerinde APN fonksiyonlarının bir benzeridir. Yani, p nin tek asal olması durumunda sonlu $\mathbb{F}_{p^m}$ cisimleri üzerinde tanımlanır.

Lineer kodlar, cebirsel yapıların analiz edilebilmesi ve donanımsal olarak uygulanmasının kolay olması nedeniyle, veri depolama sistemlerinde, iletişim sistemlerinde ve tüketici elektroniği ürünlerinde geniş bir uygulama alanına sahiptir. Uygulamalı sistemlerin taleplerini karşılamak için mükemmel özelliklere sahip lineer kodların nasıl oluşturulacağı bir araştırma konusu haline gelmiştir. Aynı zamanda lineer kodlar kodlama teorisinde önemli bir kod sınıfıdır ve uygulamalı sistemlerdeki önemleri nedeniyle literatürde kapsamlı bir şekilde çalışılmıştır. Kodlama teorisi fonksiyonlarından APN ve PN fonksiyonlar ile lineer kodlar elde etmenin verimli olduğu yapılan araştırmalarla ortaya çıkarılmıştır.

Bu tezde [1], [2], [15] ve [31] gibi çeşitli yayınlar incelenerek, APN fonksiyonlar ve düzlemsel fonksiyonlar ile tanımlanan lineer kodların bazı parametreleri olan örtme yarıçapı, minimum mesafesi ve boyut ile ilgili sonuçların bir derlemesi sunulmuştur.

Tezin 2. bölümünde, tezde kullanılan temel bilgiler; sonlu cisimler, lineer kodlar, sonlu cisimler üzerine devirli kodlar, APN fonksiyonlar ve düzlemsel fonksiyonlar ile tanımlanan lineer kodlar ile ilgili temel bilgiler verilmiştir.

Tezin 3. bölümünde, bir APN f fonksiyonuyla tanımlanan C_f lineer kodunun k boyutu, $d(C_f)$ minimum mesafesi ve $R(C_f)$ örtme yarıçapı parametrelerinin araştırma sonuçları sunulmuştur.

Tezin 4. bölümünde, düzlemsel f fonksiyonlarıyla tanımlanan C_f lineer kodların $R(C_f)$ örtme yarıçapı ve $d(C_f)$ minimum mesafe parametrelerinin araştırma sonuçları sunulmuştur.

2. TEMEL BİLGİLER

Bu bölümde, bu tezde kullanılan temel tanım ve kavramlar, sonuçlarıyla birlikte [1], [2], [8], [9] ve [10] kaynakları kullanılarak verilmiştir.

2.1 Tanım. $A = \{a_1, a_2, ..., a_q\}$ q-elemanlı bir küme olsun. A kümesine *kod alfabesi* ve kümenin elemanlarına da *kod sembolleri* denir.

(i) $a_1, a_2, ..., a_n \in A$ olmak üzere A kod alfabesi üzerinde uzunluğu n olan bir $a = a_1a_2...a_n$ dizisine n uzunluklu *q-lu sözcük* denir. a dizisi aynı zamanda $a = (a_1, a_2, ..., a_n)$ vektörüyle eşdeğer şekilde düşünülmektedir.
(ii) A kod alfabesi üzerinde aynı n uzunluğa sahip q-lu sözcüklerin boştan farklı bir C kümesine *q-lu blok kod* ya da kısaca *kod* denir.
(iii) C kodunun her bir elemanına *kod sözcüğü* denir.
(iv) C kodu içerisindeki kod sözcüklerin sayısına, yani C kodunun eleman sayısına, kodun *büyüklüğü* denir ve $|C|$ ile gösterilir.
(v) Uzunluğu n olan bir C kodunun *bilgi oranı* $\frac{\left(\log_q|C|\right)}{n}$ ile tanımlanır.
(vi) Uzunluğu n ve büyüklüğü M olan bir C kodu (n, M)-*kodu* olarak tanımlanır.

2.2 Örnek. $\mathbb{F}_2 = \{0, 1\}$ kod alfabesi üzerinde tanımlanan bir koda *ikili kod* denir. İkili kodun kod sembolleri 0 ve 1 dir. Aşağıda bazı ikili kod örnekleri verilmiştir:
(i) $C_1 = \{00, 01, 10, 11\}$ bir $(2, 4)$-kodudur.
(ii) $C_2 = \{000, 011, 101, 110\}$ bir $(3, 4)$-kodudur.
(iii) $C_3 = \{0011, 0101, 1010, 1100, 1001, 0110\}$ bir $(4, 6)$-kodudur.

Richard W. Hamming'in kodlama teorisine katkılarından biri "Hamming mesafesi" kavramının tanımıdır.

2.3 Tanım. Bir A kod alfabesi üzerinde tanımlanan n uzunluklu x ve y sözcükleri verilmiş olsun. $x, y \in A$ için x ve y sözcükleri arasındaki farklı yerlerin sayısına *Hamming mesafesi*

denir ve $d(x,y)$ ile gösterilir. $x = x_1x_2...x_n$ ve $y = y_1y_2...y_n$, q-lu sözcükleri için

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

burada x_i ve y_i kod sembollerinin uzunluğu 1 kabul edilip,

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

olarak tanımlanır.

2.4 Örnek. $\mathbb{F}_2 = \{0,1\}$ kod alfabesi üzerinde $n = 5$ uzunluklu $x = 01010$, $y = 01101$ ve $z = 11101$ sözcükleri için Hamming mesafeleri,

$d(x,y) = d(01010, 01101) = 3$,
$d(y,z) = d(01101, 11101) = 1$,
$d(z,x) = d(11101, 01010) = 4$

olarak bulunur.

2.5 Önerme. Bir A kod alfabesi üzerinde n uzunluğunda x, y ve z q-lu sözcükleri verilmiş olsun. O halde,

(i) $0 \leq d(x,y) \leq n$,
(ii) $d(x,y) = 0 \Leftrightarrow x = y$,
(iii) $d(x,y) = d(y,x)$,
(iv) (Üçgen Eşitsizliği) $d(x,z) \leq d(x,y) + d(y,z)$

metrik olma koşulları, Hamming mesafesi için sağlandığından d bir metriktir.

2.6 Tanım. En az iki kod sözcüğü içeren bir C kodu verilmiş olsun. C kodunun *minimum (Hamming) mesafesi*,

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

olarak tanımlanır.

2.7 Örnek. İkili bir kod alfabesi üzerinde tanımlanan $C = \{00000, 00111, 11111\}$ kodunun minimum mesafesi $d(C) = 2$ dir. Gerçekten,

$d(00000, 00111) = 3,\ d(00000, 11111) = 5$ ve $d(00111, 11111) = 2$

olarak bulunur.

Uzunluğu n, büyüklüğü M ve minimum mesafesi d olan bir C kodu (n, M, d)-*kodu* olarak tanımlanır.

2.1 Sonlu Cisimler

Lineer kodlar sonlu cisimler üzerine tanımlanır, yani $\mathbb{F}_q$ kod alfabesi bir sonlu cisim olarak ele alınmaktadır. Bu yüzden öncelikle sonlu cisimler tanıtılacaktır.

2.8 Tanım. Boştan farklı bir $\mathbb{F}$ kümesi üzerinde tanımlanan $+$ (*toplama*) ve $\cdot$ (*çarpma*) denilen ikili işlemleri için

(i) Her $a, b \in \mathbb{F}$ için $+$ ve $\cdot$ altında sırasıyla, $a + b \in \mathbb{F}$ ve $a \cdot b \in \mathbb{F}$,
(ii) (Değişme özelliği) Her $a, b \in \mathbb{F}$ için $a + b = b + a$ ve $a \cdot b = b \cdot a$,
(iii) (Birleşme özelliği) Her $a, b, c \in \mathbb{F}$ için $(a + b) + c = a + (b + c)$ ve $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
(iv) (Dağılma özelliği) Her $a, b, c \in \mathbb{F}$ için $a \cdot (b + c) = a \cdot b + a \cdot c$

koşulları sağlanır.

Aşağıda verilen özellikleri sağlayan 0 ve 1 elemanlarına sırasıyla $\mathbb{F}$ kümesi üzerinde tanımlanmış olan toplama ve çarpma işlemlerine göre *birim eleman* denir.

(v) Her $a \in \mathbb{F}$ için $a + 0 = a$.
(vi) Her $a \in \mathbb{F}$ için $a \cdot 1 = a$ ve $a \cdot 0 = 0$.
(vii) Her $a \in \mathbb{F}$ için $a + (-a) = (-a) + a = 0$ olacak şekilde bir $-a \in \mathbb{F}$ vardır. $-a$ elemanına, a nın toplama işlemine göre *toplamsal tersi* denir.

(viii) Her $0 \neq a \in \mathbb{F}$ için $a \cdot a^{-1} = a^{-1} \cdot a = 1$ olacak şekilde, bir $a^{-1} \in \mathbb{F}$ vardır. a^{-1} elemanına, a nın çarpma işlemine göre *çarpımsal tersi* denir.

Verilen (i)-(viii) koşullarını sağlayan $\mathbb{F}$ kümesine bir *cisim* denir ve $(\mathbb{F}, +, \cdot)$ üçlüsüyle ifade edilir. Genellikle, $a \cdot b$ yerine ab ve $\mathbb{F} \setminus \{0\}$ yerine kısaca $\mathbb{F}^*$ olarak gösterilmektedir.

2.9 Yardımcı Önerme. Bir $\mathbb{F}$ cismi üzerinde, herhangi iki $a, b \in \mathbb{F}$ için

(i) $(-1) \cdot a = -a$,
(ii) $a \cdot b = 0$ ise $a = 0$ veya $b = 0$

koşulları sağlanır.

2.10 Tanım. Sonlu sayıda eleman içeren bir cisme bir *sonlu cisim* denir.

$a, b \in \mathbb{Z}$ ve $m > 1$ bir pozitif tam sayı olmak üzere, $m|(a - b)$ ise a elemanı, b elemanına m *modülüne göre kongrüent* denir ve $a \equiv b \ (mod\ m)$ olarak yazılır.

$m > 1$ pozitif bir tam sayı olmak üzere, $\mathbb{Z}_m = \mathbb{Z}/(m) = \{0, 1, ..., m - 1\}$ kümesi üzerinde $\oplus$ (*toplama*) işlemi $a \oplus b = a + b \ \ (mod\ m)$ ve $\odot$ (*çarpma*) işlemi $a \odot b = ab \ \ (mod\ m)$ olarak tanımlanır. $(\mathbb{Z}_m, \oplus, \odot)$ üçlüsünün bir halka olduğu açıktır. Bundan sonra, $\mathbb{Z}_m$ kümesi üzerinde $\oplus$ ve $\odot$ işlemleri sırasıyla, $+$ ve $\cdot$ olarak belirtilecektir.

2.11 Örnek. (i) $\mathbb{Z}_2 = \{0, 1\}$ kümesi bilinen toplama ve çarpma işlemleri altında bir halkadır. Kolaylıkla görülebilir ki Tanım 2.8 de verilen özellikler sağlandığından $\mathbb{Z}_2$ bir cisimdir.
(ii) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ kümesi bilinen toplama ve çarpma işlemleri altında bir halkadır. Ancak, çarpma işlemine göre, 2 elemanının çarpımsal tersi $\frac{1}{2}$ bu kümede bulunmadığından $\mathbb{Z}_4$ bir cisim değildir.

Yukarıdaki örneklerden görüldüğü üzere, $\mathbb{Z}_m$ kümesinin bazı m tam sayıları için bir cisim olduğu ancak belirli tam sayılar için yalnızca bir halka olduğu görülmektedir.

2.12 Teorem. $\mathbb{Z}_m$ kümesinin toplama ve çarpma işlemleri altında bir cisim olabilmesi için gerek ve yeter şart m tam sayısının bir asal sayı olmasıdır.

İspat: [1]

2.13 Tanım. Bir $\mathbb{F}$ cismi üzerinde, eğer $p \cdot 1_{\mathbb{F}} = 0_{\mathbb{F}}$ olacak şekilde bir p pozitif tam sayısı varsa, böyle p sayılarının en küçüğüne cismin *karakteristiği* denir. Burada, $1_{\mathbb{F}}$ cismin çarpımsal birimidir.

Bir $\mathbb{F}$ cisminin p karakteristiği yoksa cisminin karakteristiği 0 dır.

2.14 Örnek. (i) Rasyonel $\mathbb{Q}$ sayılar, reel $\mathbb{R}$ sayılar ve kompleks $\mathbb{C}$ sayılar cisimlerinin karakteristiği 0 dır.
(ii) p bir asal sayı ise, $\mathbb{Z}_p$ cisminin karakteristiği p dir.

2.15 Teorem. Bir $\mathbb{F}$ cisminin karakteristiği 0 ya da bir p asal sayısıdır.

İspat: 1 in karakteristik olmadığı $1 \cdot 1_{\mathbb{F}} = 1_{\mathbb{F}} \neq 0_{\mathbb{F}}$ den açıktır.
Varsayalım ki $\mathbb{F}$ cisminin karakteristiği 1 den büyük ve asal olmayan bir p sayısı olsun. O halde, $p = nm$ için $1 < n, m < p$ olacak şekilde bazı n ve m pozitif tam sayıları vardır. $1_{\mathbb{F}}$ sayısı $\mathbb{F}$ cisminin çarpımsal birimi olmak üzere, $a = n \cdot 1_{\mathbb{F}}$ ve $b = m \cdot 1_{\mathbb{F}}$ olsun. O zaman,

$$a \cdot b = (n \cdot 1_{\mathbb{F}})(m \cdot 1_{\mathbb{F}}) = \left(\sum_{i=1}^{n} 1_{\mathbb{F}}\right)\left(\sum_{j=1}^{m} 1_{\mathbb{F}}\right) = (m \cdot n) \cdot 1_{\mathbb{F}} = p \cdot 1_{\mathbb{F}} = 0_{\mathbb{F}}.$$

Yardımcı Önerme 2.9(ii) maddesinden $a = 0$ veya $b = 0$ dır. Yani $m \cdot 1_{\mathbb{F}} = 0_{\mathbb{F}}$ veya $n \cdot 1_{\mathbb{F}} = 0_{\mathbb{F}}$ olmalıdır. Bu durumsa karakteristik tanımıyla çelişir. O halde p bir asal sayıdır.

□

2.16 Teorem. Karakteristiği p olan bir $\mathbb{F}$ sonlu cismi, $n \geq 1$ bir tam sayı olmak üzere, p^n tane eleman içerir.

İspat: [1]

2.17 Tanım. Bir $\mathbb{F}$ cismi üzerinde tanımlanan

$$\mathbb{F}[x] := \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in \mathbb{F}, n \geq 0 \right\}$$

kümesi *polinom halkası* olarak adlandırılır. $\mathbb{F}[x]$ polinom halkasının elemanlarına $\mathbb{F}$ cismi üzerinde tanımlanan bir *polinom* denir. $a_0, a_1, ..., a_n$ elemanlarına $f(x)$ polinomunun *katsayıları* denir. Sıfırdan farklı bir $f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + ... + a_n x^n$ polinomu için, eğer $a_n \neq 0$ ise n tam sayısına $f(x)$ in *derecesi* denir ve $der(f(x)) = n$ ile ifade edilir.

Her $i = 0, ..., n$ için $a_i = 0$ olarak tanımlanan sıfır polinomunun derecesi, $der(0) = -1$ ya da $der(0) = -\infty$ olarak tanımlanmaktadır.

2.18 Tanım. Bir $\mathbb{F}$ cismi üzerinde tanımlanan $f(x) \in \mathbb{F}[x]$ polinomu ve $c \in \mathbb{F}$ için, eğer c nin $f(x)$ polinomundaki değeri 0, yani $f(c) = 0_{\mathbb{F}}$ ise c ye $f(x)$ polinomunun bir *kökü* ya da bir *sıfırı* denir.

2.19 Tanım. Sıfırdan farklı bir $f(x) = \sum_{i=0}^{n} a_i x^i$ polinomu ve $der(f(x)) = n$ için $f(x) = a_0 + a_1 x + ... + x^n$ olmak üzere, yani $a_n = 1$ ise $f(x)$ polinomuna bir *monik polinom* denir.

2.20 Tanım. Bir $\mathbb{F}$ cismi üzerinde tanımlanan $f(x)$ polinomu için $der(f(x)) > 1$ olmak üzere,

$$f(x) = g(x)h(x) \quad \text{ve} \quad der(g(x)) < der(f(x)), \quad 1 \leq der(h(x)) < der(f(x))$$

olacak şekilde $g(x)$ ve $h(x)$ polinomları varsa, $f(x)$ polinomuna *indirgenebilir polinom* denir. Aksi taktirde, $f(x)$ polinomuna *indirgenemez polinom* denir.

2.21 Örnek. (i) $\mathbb{Z}_3[x]$ polinom halkası üzerinde tanımlanan $f(x) = x^4 + 2x^6$ polinomu için $der(f(x)) = 6$ ve $f(x) = x^4(1 + 2x^2)$ olacak şekilde $g(x) = x^4$ ve $h(x) = 1 + 2x^2$ polinomları var olduğundan $f(x)$ indirgenebilir bir polinomdur.
(ii) $\mathbb{Z}_2[x]$ polinom halkası üzerinde tanımlanan $f(x) = 1+x+x^2$ polinomu için, $der(f(x)) =$

2 dir; ancak $g(x) = 1+x+x^2 = (x+a)(x+b) = x^2+x(a+b)+ab$ olmak üzere $a+b = 1$ ve $ab = 1$ olacak şekilde $a, b \in \mathbb{Z}_2$ var olmadığından $f(x)$ indirgenemez bir polinomdur.

2.22 Teorem. p herhangi bir asal sayı ve $n \geq 1$ pozitif bir tam sayı olmak üzere p^n elemanlı bir sonlu cisim vardır ve biriciktir.

İspat: [1]

Bir $\mathbb{F}$ cismi üzerinde $der(f(x)) = n \geq 1$ olan bir $f(x)$ polinomu için $\mathbb{F}[x]/(f(x))$ halkası derecesi n den küçük olan $\mathbb{F}$ üzerinde tanımlanmış tüm polinomlardan oluşur. Yani,

$$\mathbb{F}[x]/(f(x)) = \left\{a_0 + a_1x + ... + a_{n-1}x^{n-1} : a_0, a_1, ..., a_{n-1} \in \mathbb{F}\right\}. \tag{2.1}$$

$\mathbb{Z}$ tam sayılar halkası ve $\mathbb{F}[x]$ polinom halkası Tablo 2.1 de karşılaştırılarak verilmiştir.

$m > 1$ için $\mathbb{Z}_m = \mathbb{Z}/(m)$ ve $n > 1$ dereceli bir $f(x)$ polinomu için $\mathbb{F}[x]/(f(x))$ halkaları elde edilmiştir. Tablo 2.2 oluşturularak, $\mathbb{Z}_m$ ile $\mathbb{F}[x]/(f(x))$ halkaları karşılaştırılmıştır.

Tablo 2.1: $\mathbb{Z}$ ve $\mathbb{F}[x]$ arasındaki benzerlikler

$\mathbb{Z}$ kümesi	$\mathbb{F}[x]$ kümesi
$\mathbb{Z}$ bir halka	$\mathbb{F}[x]$ bir polinom halkası
m bir tam sayı	$f(x)$ bir polinom
p bir asal sayı	$p(x)$ bir indirgenemez polinom

Tablo 2.2: $\mathbb{Z}_m$ ve $\mathbb{F}[x]/(f(x))$ arasındaki benzerlikler

$\mathbb{Z}_m$ kümesi, $m > 1$	$\mathbb{F}[x]/(f(x)$ kümesi, $der(f(x)) = n$
$\mathbb{Z}_m = \{0, 1, ..., m-1\}$	$\mathbb{F}[x]/(f(x)) = \left\{\sum_{i=0}^{n-1} a_i x^i : a_i \in \mathbb{F}, n \geq 1\right\}$
$a \oplus b = a + b \pmod m$	$g(x) \oplus h(x) = g(x) + h(x) \pmod{f(x)}$
$a \odot b = ab \pmod m$	$g(x) \odot h(x) = g(x)h(x) \pmod{f(x)}$
$\mathbb{Z}_m$ bir halka	$\mathbb{F}[x]/(f(x))$ bir halka
$\mathbb{Z}_m$ bir cisim $\Leftrightarrow$ m bir asal sayı	$\mathbb{F}[x]/(f(x))$ bir cisim $\Leftrightarrow$ $f(x)$ bir indirgenemez polinom

Bir $\mathbb{F}$ cismi üzerinde $f(x)$ indirgenemez bir polinom ve $der(f(x)) = n$ olsun. $f(x)$ polinomu için α, $f(x)$ polinomunun bir kökü, öyle ki (2.1) de tanımlanan kümede x yerine α verilirse, $\mathbb{F}[x]/(f(x))$ cismi yeniden,

$$\mathbb{F}[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_0, a_1, ..., a_{n-1} \in \mathbb{F}\}$$

olarak tanımlanır. Bunun en temel amacı ise $\mathbb{F}[x]/(f(x))$ cisminin elemanlarıyla $\mathbb{F}$ üzerindeki polinomlar arasındaki karışıklığı önlemektir.

$\mathbb{F}_q$ sonlu cismi üzerinde, derecesi m olan bir indirgenemez polinomun bir α kökü olmak üzere, eğer $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$ cisminin bir elemanıysa,

$$\mathbb{F}_q[\alpha] = \{a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1} : a_0, a_1, ..., a_{m-1} \in \mathbb{F}\} = \left\{0, \alpha, \alpha^2, \alpha^3, ..., \alpha^{q^m-1}\right\}$$

olacağından $\mathbb{F}_{q^m}$ cisminin her bir elemanı, hem α nın bir polinomu hem de α nın bir kuvveti olarak yazılabilir.

2.23 Tanım. $\mathbb{F}_q$ sonlu cisminin bir α elemanı için $\mathbb{F}_q = \{0, \alpha, \alpha^2, ..., \alpha^{q-1}\}$ olarak yazılabiliyorsa α elemanına $\mathbb{F}_q$ cisminin bir *ilkel kökü (üreteci)* denir.

2.24 Örnek. Bir α elemanı, $1 + x + x^2 \in \mathbb{F}_2[x]$ indirgenemez polinomun bir kökü olsun. O halde $\mathbb{F}_2[\alpha] = \{a_0 + a_1\alpha : a_0, a_1 \in \mathbb{F}_2\} = \{0, 1, \alpha, \alpha + 1\}$ olmak üzere $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ cismini göz önünde bulundurarak,

$$\alpha^2 = -(1 + \alpha) = 1 + \alpha \Rightarrow \alpha^3 = \alpha(\alpha^2) = \alpha(\alpha + 1) = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1$$

elde edilir. Böylece, $\mathbb{F}_4 = \{0, \alpha, \alpha^2, \alpha^3\} = \{0, 1, 1 + \alpha, \alpha\}$ olduğundan α, $\mathbb{F}_4$ cisminin bir ilkel köktür.

2.25 Tanım. $\mathbb{F}_q$ sonlu cisminin sıfırdan farklı bir β elemanı için $\beta^k = 1$ olacak şekilde en küçük pozitif k tam sayısına β elemanının *mertebesi* denir ve $m(\beta)$ ile gösterilir.

2.26 Örnek. Bir $f(x) = 1 + x^2$ polinomunun $\mathbb{F}_3$ sonlu cismi üzerinde lineer çarpanları olmadığından $f(x)$ polinomu $\mathbb{F}_3$ üzerinde indirgenemezdir. β elemanı $f(x)$ polinomunun

bir kökü ve $\mathbb{F}_9 = \mathbb{F}_3[\beta]$ cisminin bir elemanı olsun. O halde,
$\beta^2 = -1$,
$\beta^3 = \beta(\beta)^2 = \beta(-1) = -\beta$,
$\beta^4 = (\beta^2)^2 = (-1)^2 = 1$
böylece, $m(\beta) = 4$ bulunur.

Bundan böyle $q = p^m$, p bir asal sayı, $m \geq 1$ tam sayı olmak üzere, $\mathbb{F}_q$ ile q elemanlı sonlu cisim gösterilecektir.

2.27 Yardımcı Önerme. (i) Her $\beta \in \mathbb{F}_q^*$ için mertebe $m(\beta)$, $q-1$' i böler; yani, $m(\beta)|q-1$.
(ii) $\beta, \gamma \in \mathbb{F}_q^*$ için $gcd(m(\beta), m(\gamma)) = 1$ ise, $m(\beta\gamma) = m(\beta)m(\gamma)$ olur.

İspat: [1]

2.28 Önerme. (i) $\mathbb{F}_q$ sonlu cisminin sıfırdan farklı bir α elemanının ilkel kök olması için gerek ve yeter şart mertebesinin $m(\alpha) = q - 1$ olmasıdır.
(ii) Her sonlu cismin en az bir ilkel kökü vardır.

İspat: [1]

2.29 Tanım. $m \geq 1$ bir tam sayı olmak üzere, bir $\alpha \in \mathbb{F}_{q^m}$ elemanının $f(\alpha) = 0$ olacak şekilde, $\mathbb{F}_q[x]$ deki en küçük dereceli sıfır olmayan monik bir $f(x)$ polinomuna α elemanının $\mathbb{F}_q$ cismi üzerinde bir *minimal polinomu* denir.

2.30 Teorem. (i) $\mathbb{F}_{q^m}$ nin her elemanının $\mathbb{F}_q$ üzerinde bir minimal polinomu vardır ve biriciktir. Ayrıca, bu polinom $\mathbb{F}_q$ üzerinde indirgenemezdir.
(ii) $\alpha \in \mathbb{F}_{q^m}$, eğer bir monik indirgenemez $M(x) \in \mathbb{F}_q[x]$ polinomunun bir kökü ise, o zaman $M(x)$ polinomu, α nın $\mathbb{F}_q$ üzerinde minimal polinomudur.

İspat: [1]

Bir $\alpha \in \mathbb{F}_{q^m}$ ilkel elemanın minimal polinomu biliniyorsa, herhangi bir i için de α^i nin de minimal polinomu bulunabilir. Bunun bulunabilmesi için dairesel koset tanımına ihtiyaç vardır.

2.31 Tanım. i ve m aralarında asal olsun.

$C_i = \{(i \cdot q^j (mod\ m)) \in \mathbb{Z}_m : j = 0, 1, 2, ...\}$
ile tanımlanan kümeye q nun m modülüne göre i yi içeren *dairesel koseti* veya *q-dairesel koset* denir.

Şimdiyse, $\mathbb{F}_{p^m}$ sonlu cismi üzerinde tanımlanan temel tanım ve kavramlar verilecektir.

Her i için $a_i \in \mathbb{F}_{p^m}$ olmak üzere, *tek değişkenli* bir $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ fonksiyonu $f(x) = \sum_{i=0}^{p^m-1} a_i x^i$ olarak tanımlanır.

2.32 Tanım. $d \in \mathbb{N}^+$ olmak üzere, $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$, $f(x) = x^d$ ile tanımlanan fonksiyona *kuvvet fonksiyonu* denir.

$\mathbb{F}_{p^m}$ cismi üzerinde tanımlanan $f(x) = x^d$ fonksiyonu birebir ve örten bir fonksiyondur ancak ve ancak d ile $p^m - 1$ aralarında asaldır.

2.33 Tanım. p bir asal sayı ve n tam sayısının p-genişlemesi, $0 \leq a_i < p$ olmak üzere $n = a_0 + a_1 p + a_2 p^2 + ... + a_s p^s$ olsun. $\sigma_p(n) = \sum_{i=0}^{s} a_i$ toplamına n nin *p-ağırlığı* denir.

Eğer, bir $f(x) = x^d$ fonksiyonu $x^d := x_1^{d_1} x_2^{d_2} ... x_n^{d_n}$ ise *p-ağırlık derecesi*,

$wt_p(x^d) := \sigma_p(d_1) + \sigma_p(d_2) + ... + \sigma_p(d_n)$

olarak tanımlanır.

Bir $f(x_1, x_2, ..., x_n) = \sum_d a_d x^d$ polinomunun *p-ağırlık derecesi*,

$w_p(f) := \max_{x^d, a_d \neq 0} w_p(x^d)$

olarak tanımlanır.

$p = 2$ için sonlu bir $\mathbb{F}_{p^m}$ cismi üzerinde lineer fonksiyon tanımı şu şekilde verilmektedir:

2.34 Tanım. m pozitif bir tam sayı ve $a_i \in \mathbb{F}_{2^m}$ olmak üzere, $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$ fonksiyonu için, $f(x) = \sum_{i=0}^{m-1} a_i x^{2^i}$ olarak tanımlanan fonksiyona bir *lineer fonksiyon* denir.

Her $x, y \in \mathbb{F}_{2^m}$ için

$$(x+y)^{2^i} = x^{2^i} + y^{2^i} \tag{2.2}$$

olduğundan

$$f(x+y) = \sum_{i=0}^{m-1} a_i (x+y)^{2^i} = \sum_{i=0}^{m-1} a_i x^{2^i} + \sum_{i=0}^{m-1} a_i y^{2^i} = f(x) + f(y)$$

elde edilir.

Tüm $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ lineer fonksiyonları, $a_i \in \mathbb{F}_{p^m}$ için $f(x) = \sum_{i=0}^{m-1} a_i x^{p^i}$ tek değişkenli lineerleştirilmiş polinomlardır.

2.2 Lineer Kodlar

$n \geq 1$ bir tam sayı olmak üzere, sonlu bir $\mathbb{F}_q$ cismi üzerinde n uzunluğundaki bir kod, basitçe $\mathbb{F}_q^n$ vektör uzayının bir alt uzayıdır. Lineer kodlar vektör uzayları olduğundan, cebirsel yapıları genellikle onları tanımlamayı ve kullanmayı, lineer olmayan kodlardan daha kolay hale getirir. Bu tezde lineer kodlara odaklanılmıştır.

2.35 Tanım. $\mathbb{F}_q$, q elemanlı sonlu cisim olmak üzere, boştan farklı bir V kümesi üzerinde $+$ (*toplama*) ve $\cdot$ (*çarpma*) işlemleri için,

(i) Her $u, v \in V$ için $u + v \in V$,
(ii) Her $u, v, w \in V$ için $(u + v) + w = u + (v + w)$,
(iii) Her $v \in V$ için $0 + v = v + 0 = v$ olacak şekilde $0 \in V$ vardır,

(iv) Her $u \in V$ için $u + (-u) = (-u) + u$ olacak şekilde $-u \in V$ vardır,
(v) Her $u, v \in V$ için $u + v = v + u$,
(vi) $\lambda \in \mathbb{F}_q$ ve her $u \in V$ için $\lambda v \in V$,
(vii) $\lambda, \mu \in \mathbb{F}_q$ ve her $u, v \in V$ için $\lambda(u + v) = \lambda u + \lambda v$, $(\lambda + \mu)u = \lambda u + \mu u$,
(viii) $\lambda, \mu \in \mathbb{F}_q$ ve her $u \in V$ için $(\lambda\mu)u = \lambda(\mu u)$,
(xi) $\mathbb{F}_q$ sonlu cisminin çarpımsal birimi 1 ve her $u \in V$ için $1u = u$,

koşulları sağlanıyorsa, V kümesine $\mathbb{F}_q$ cismi üzerinde bir *vektör uzayı* denir. Vektör uzayının her bir elemanına *vektör* adı verilir.

Böylece, bir $V = \mathbb{F}_q^n$ vektör uzayı, $\mathbb{F}_q$ sonlu cismi üzerinde vektör elemanlarının uzunluğu n olan bir kümedir. Yani, $\mathbb{F}_q^n = \{(v_1, v_2, ..., v_n) : v_i \in \mathbb{F}_q\}$.

Bir $\mathbb{F}_q^n$ vektör uzayında $v = (v_1, v_2, ..., v_n), w = (w_1, w_2, ..., w_n) \in \mathbb{F}_q^n$ ve $\lambda \in \mathbb{F}_q$ için,

(i) (*Vektör toplama*) $v + w = (v_1 + w_1, v_2 + w_2, ..., v_n + w_n) \in \mathbb{F}_q^n$,
(ii) (*Skaler çarpma*) $\lambda v = \lambda(v_1, v_2, ..., v_n) = (\lambda v_1, \lambda v_2, ..., \lambda v_n) \in \mathbb{F}_q^n$,

olarak bileşen bazında tanımlanır.

Bir $\mathbb{F}_q^n$ vektör uzayında, n uzunluklu *sıfır vektörü* $0 = (0, 0, ..., 0)$ olarak tanımlanır.

2.36 Örnek. Bir $\mathbb{F}_q$ sonlu cismi üzerinde, aşağıdaki kümelerin vektör uzayı olduğu açıktır. Gerçekten,
(i) $(q = 2, n = 4)$ $C_1 = \{(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\}$,
(ii) $(q = 3, n = 3)$ $C_2 = \{(0, 0, 0), (0, 1, 2), (0, 2, 1)\}$.

2.37 Tanım. Bir V vektör uzayının, boştan farklı bir C alt kümesi, eğer V vektör uzayıyla, aynı vektör toplama ve skaler çarpma işlemleri altında, Tanım 2.35 i sağlıyorsa, C ye bir *alt vektör uzay* denir.

Diğer bir ifadeyle, bir V, $\mathbb{F}_q$ sonlu cismi üzerinde vektör uzayı ve C, boştan farklı bir alt

kümesi olsun. O zaman,

(i) $0 \in C$,
(ii) her $u, v \in C$ için $u + v \in C$,
(iii) her $u \in C$ ve her $\lambda \in \mathbb{F}_q$ için $cu \in C$

koşulları sağlanıyorsa, C alt kümesi V vektör uzayının bir *alt vektör uzayıdır* denir.

Bir V vektör uzayının, sıfır vektörü C kümesinin bir elemanı değilse, C kümesinin bir alt vektör uzayı olamayacağına dikkat ediniz.

2.38 Örnek. Örnek 2.36 de verilen vektör uzayları için,
(i) C_1 kümesi, $\mathbb{F}_2^4$ vektör uzayının bir alt vektör uzayıdır, yani $C_1 \subseteq \mathbb{F}_2^4$.
(ii) C_2 kümesi, $\mathbb{F}_3^3$ vektör uzayının bir alt vektör uzayıdır, yani $C_2 \subseteq \mathbb{F}_3^3$.

V, $\mathbb{F}_q$ sonlu cisminin bir vektör uzayı ve $B = \{v_1, v_2, ..., v_k\}$ kümesi V için bir *taban* ise V nin her elemanı B'nin elemanlarıyla yalnızca bir kez lineer birleşim olarak yazılabilir, yani her $v \in V$ için $v = \lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_k v_k$ olacak şekilde tek türlü belirli $\lambda_1, \lambda_2, ..., \lambda_k \in \mathbb{F}_q$ elemanları bulunabilir.

Her V vektör uzayının, en az bir B tabanı mevcuttur. Ayrıca, çok sayıda farklı tabanı da bulunabilir. Ancak vektör uzayının tüm tabanları aynı k sayıda eleman içerir. Bu sayıya, V vektör uzayının *boyutu* denir ve $boy(V) = k$ ile gösterilir.

2.39 Teorem. Bir $\mathbb{F}_q$ sonlu cismi üzerinde V vektör uzayı olmak üzere, $boy(V) = k$ ise,
(i) V vektör uzayında q^k eleman vardır.
(ii) V vektör uzayında $\frac{1}{k!} \prod_{i=0}^{k-1} (q^k - q^i)$ farklı taban mevcuttur.

İspat: [1]

2.40 Tanım. $\mathbb{F}_q$ sonlu cismi üzerinde, $\mathbb{F}_q^n$ vektör uzayının bir C alt vektör uzayına n uzunluklu bir *lineer kod* denir.

Diğer bir deyişle, bir $C \subseteq \mathbb{F}_q^n$ kodu, eğer kod sözcüklerinin vektör toplamları ve skalerle çarpımları yine bir kod sözcüğü ise, C koduna *lineer* denir. Bu ise, C kodunun $\mathbb{F}_q^n$ nin bir lineer alt uzayı olduğu anlamına gelir. Aynı zamanda, $\mathbb{F}_q^n$ vektör uzayına *q-lu Hamming uzayı* denir.

$\mathbb{F}_q$ sonlu cismi üzerinde bir vektör uzayı olarak C kodunun boyutu, C lineer kodunun boyutu olarak adlandırılır ve $boy(C)$ ile gösterilir.

Kod uzunluğu n, boyutu k ve minimum mesafesi d olan bir $C \subseteq \mathbb{F}_q^n$ lineer kodu bir $[n, k, d]_q$-kodu olarak tanımlanır. n, k ve d sayılarına kodun *parametreleri* denir.

2.41 Örnek. Aşağıda verilen C kodların birer lineer kod olduğu açıktır:
(i) $(q = 2)$ $C = \{000, 001, 010, 011\}$.
(ii) $(q = 3)$ $C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$.

2.42 Tanım. $C \subseteq \mathbb{F}_q^n$ bir lineer kod olmak üzere, $C^\perp$ ile gösterilen C nin ortogonal tümleyeni $\mathbb{F}_q^n$ deki her vektöre dik olan vektörlerin kümesidir. Bu kümeye C nin *dual kodu* denir.

2.43 Teorem. $C \subseteq \mathbb{F}_q^n$ bir lineer kod ve C kodunun büyüklüğü $|C|$ olmak üzere,
(i) $|C| = q^{boy(C)}$ yani, $boy(C) = \log_q |C|$,
(ii) $C^\perp$ dual kodu bir lineer kod ve $boy(C) + boy(C^\perp) = n$.

İspat: [1]

2.44 Örnek. $\mathbb{F}_2$ sonlu cismi üzerinde $C \subseteq \mathbb{F}_2^4$ olmak üzere,
(i) $C = \{0000, 1010, 0101, 1111\}$ lineer kodu için $boy(C) = \log_q |C| = \log_2 4 = 2$ dir.
(ii) $C^\perp = \{0000, 1010, 0101, 1111\}$ liner kodu için $C^\perp = C$ olduğundan, $boy(C^\perp) = 2$ dir.
Buradan $boy(C) + boy(C^\perp) = 2 + 2 = 4$ olduğu görülür.

Richard W. Hamming'in kodlama teorisine diğer katkılarından biri de "Hamming ağırlığı" kavramının tanımıdır.

2.45 Tanım. Bir $x \in \mathbb{F}_q^n$ sözcüğünün sıfırdan farklı koordinatlarının sayısına *Hamming ağırlığı* denir ve $wt(x)$ ile gösterilir. Yani,

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

Burada, $0 = 00...0$ sözcüğü n uzunluklu *sıfır sözcüğü* olarak tanımlanır.

2.46 Uyarı. Bir $x = x_1x_2...x_n$, q-lu sözcüğü için

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

burada her $x_i \in \mathbb{F}_q$ için

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

şeklinde tanımlanır.

2.47 Yardımcı Önerme. $x, y \in \mathbb{F}_q^n$ için $d(x, y) = wt(x - y)$ dir.

İspat: $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n) \in \mathbb{F}_q^n$ olsun. Önerme 2.5 (ii) koşulundan, $d(x, y) = 0 \Leftrightarrow x = y$ dir. Tanım 2.3 ve Uyarı 2.46 den,
$d(x, y) = \sum_{i=1}^{n} d(x_i, y_i)$ ve $wt(x - y) = d(x - y, 0) = \sum_{i=1}^{n} d(x_i - y_i, 0)$
Her $i = 1, ..., n$ için $d(x_i, y_i) = d(x_i - y_i, 0)$ olduğu açıktır. O halde, $d(x, y) = wt(x - y)$ dir.

□

2.48 Sonuç. q çift olsun. $x, y \in \mathbb{F}_q^n$ için $d(x, y) = wt(x + y)$ dir.

2.49 Tanım. C bir kod olmak üzere (lineer kod olması şart değil), C kodunun, $wt(C)$ *minimum (Hamming) ağırlığı*, sıfırdan farklı kod sözcüklerinin ağırlıklarının en küçüğüdür.

2.50 Teorem. Bir $\mathbb{F}_q$ sonlu cismi üzerinde, C bir lineer kod olmak üzere, $d(C) = wt(C)$ dir.

İspat: [1]

2.51 Örnek. Bir $\mathbb{F}_q$ sonlu cismi üzerinde, $C = \{0000, 1000, 0100, 1100\}$ bir lineer kod olmak üzere, $wt(1000) = 1$, $wt(0100) = 1$ ve $wt(1100) = 2$ olduğundan, $d(C) = wt(C) = 1$ dir.

Lineer bir kod, bir vektör uzayı olduğu için tüm elemanları bir taban ile tanımlanabilir. Lineer bir kod için bir taban bilmenin faydası, onun kod sözcüklerinin açıkça tanımlanmasını sağlar. Kodlama teorisinde, lineer bir kodun tabanı, genellikle bir matris şeklinde temsil edilir ve buna kodun üreteç matrisi denir. Daul kod için bir tabanı temsil eden bir matrise ise kodun eşlik-kontrol matrisi denir. Aynı zamanda bir lineer kod, üreteci veya eşlik-kontrol matrisleri ile tanımlanabilmektedir. Bundan dolayıdır ki, bu matrisler kodlama teorisinde önemli bir rol oynamaktadır.

2.52 Tanım. (i) Bir $B = \{v_1, v_2, ..., v_k\}$ kümesi C kodunun bir tabanı olmak üzere,

$$G = G(C) = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}_{k \times n}$$

olarak tanımlanan $k \times n$ matrisine C kodunun bir *üreteç matrisi* denir. Yani satırları C için bir taban oluşturan matristir.
(ii) $C^{\perp}$ dual kodu için tanımlanan $(n-k) \times n$ üreteç matrisine C kodu için bir *eşlik-kontrol matrisi* denir.

Bir üreteç matrisinin ve eşlik-kontrol matrisinin satırları lineer bağımsızdır. Bir $k \times n$ lik G matrisinin, bir C, $[n, k]$-lineer kodu için üreteç matrisi olduğunu göstermek için G nin satırlarının C nin kod sözcükleri olduğunu ve bunların lineer bağımsız olduklarını göstermek yeterlidir.

2.53 Yardımcı Önerme. $C \subseteq \mathbb{F}_q^n$ için C bir $[n,k]$-lineer kod ve G üreteç matrisi olmak üzere $v \in C^{\perp}$ olabilmesi için gerek ve yeter şart v elemanın G nin her satırına ortogonal olmasıdır; yani, $v \in C^{\perp} \Leftrightarrow vG^T = 0$ dır. Verilen bir $(n-k) \times n$ matrisi H, C nin bir eşlik-kontrol matrisidir ancak ve ancak H nin satırları lineer bağımsızdır ve $HG^T = O$ dur.

2.54 Teorem. C bir lineer kod ve H, C için bir eşlik-kontrol matrisi olmak üzere,
(i) $d(C) \geq d$ dir gerek ve yeter şart H nin herhangi $d-1$ sütunu lineer bağımsızdır.
(ii) $d(C) \leq d$ dir gerek ve yeter şart H nin herhangi d sütunu lineer bağımlıdır.

İspat: [1]

Bu teoremin doğrudan bir sonucu olarak aşağıdaki sonuç elde edilir.

2.55 Sonuç. C bir lineer kod ve H, C için bir eşlik-kontrol matrisi olmak üzere aşağıdaki ifadeler eşdeğerdir:
(i) $d(C) = d$,
(ii) H nin herhangi $d-1$ sütunu lineer bağımsızdır ve H nin lineer bağımlı d tane sütunu vardır.

2.56 Tanım. Bir C kodunun d minimum mesafesi, e-hata düzeltme kapasitesini hesaplar, yani,

$$e(C) = \left\lfloor \frac{d(C)-1}{2} \right\rfloor$$

değerine *paketleme yarıçapı* denir.

Kod sözcüklerin etrafındaki $e(C)$ paketleme yarıçaplı küreler ayrıktır. Öyle ki, $e(C)$ nin en büyük tam sayı olduğu kolayca görülür.

2.57 Tanım. Bir $C \subseteq \mathbb{F}_q^n$ kodunun elemanları etrafındaki t yarıçaplı kürelerin tüm $\mathbb{F}_q^n$ cismini örtecek şekilde mümkün olan en küçük t tam sayıya, yani,

$$R(C) = \max\left\{\min\left\{d(x,c) : c \in C\right\} : x \in \mathbb{F}_q^n\right\}$$

değerine, C nin *örtme yarıçapı* denir.

Bir $x \in \mathbb{F}_q^n$ vektörü etrafındaki t yarıçaplı bir küre, $\left\{x \in \mathbb{F}_q^n : d(x,c) \leq t\right\}$ olarak tanımlanır.

O halde, her $x \in \mathbb{F}_q^n$ vektörü, C kodunun bir kod sözcüğünde R-örtünür, yani

$$R = R(C) = \max_{x \in \mathbb{F}_q^n} d(x, C).$$

Kısaca, kod sözcükleri etrafındaki $R(C)$ örtme yarıçaplı küreler $\mathbb{F}_q^n$ cisminin tamamını örter, öyle ki $R(C)$ bu özelliği sağlayan en küçük tam sayıdır.

C bir lineer kod ve H, C nin bir eşlik-kontrol matrisi olsun. $c \in C$ ve e, $\mathbb{F}_q^n$ de en fazla $R(C)$ ağırlıklı bir vektör için $x \in \mathbb{F}_q^n$ vektörü, $x = c + e$ olarak ifade edilir. O zaman,

$$H.x^T = H.(c+e)^T = H.e^T$$

olduğundan C kodunun örtme yarıçapı, eşlik-kontrol matrisi cinsinden, aşağıda verilen şekilde de tanımlanabilmektedir:

2.58 Tanım. Bir C kodu, eşlik-kontrol matrisi H olarak verilen $[n,k]_q$-kodu olsun. C kodunun örtme yarıçapı, mümkün olan en küçük r tam sayıdır öyle ki her q-lu $(n-k)$-lı sütun vektörü, H den en fazla r sütununun bir lineer kombinasyonu olarak yazılabilir.

H, C kodunun eşlik-kontrol matrisiyse, C kodu $C = \left\{x \in \mathbb{F}_q^n : Hx^T = 0\right\}$ şeklinde tanımlanır. Burada, her $x \in \mathbb{F}_q^n$ için $Hx^T \in \mathbb{F}_q^{n-k}$ vektörüne x *in sendromu (syndrome)* denir. Dolayısıyla C kodu 0 a eşit sendromlu vektörlerden oluşur.

Yardımcı Önerme 2.47 ile lineer bir kodun minimum mesafesi, bir kod sözcüğünün sıfır olmayan en küçük ağırlığıdır; yani, sıfırdan farklı bir kod sözcüğün en küçük ağırlığıdır. Özellikle ikili durum için aşağıdaki teorem elde edilmiştir:

2.59 Teorem. [10, Theorem 2.1.8] C bir ikili $[n, k]$ kodu ve H eşlik-kontrol matrisi olsun. C nin minimum mesafesi, H nin bazı d sütunlarının toplamı 0 olacak şekilde en küçük pozitif d tam sayısıdır.

Büyüklüğü $|C| \geq 2$ olan herhangi bir kodun $d(C)$ minimum uzaklığı ve $R(C)$ örtme yarıçapı şu şekilde ilişkilidir [11, 12]:
$d(C) \leq 2R(C) + 1$

2.60 Önerme. [13] C lineer bir $[n, k]$-kodu ise, $R(C) \leq n - k$ dir.

İspat: H matrisinin rankı $n - k$ olduğundan örtme yarıçapının tanımından istenilen sonuç elde edilir.

2.61 Tanım. (i) Örtme yarıçapı en az paketleme yarıçapı kadar büyükse, yani $R(C) = e(C)$ eşitliği sağlanıyorsa C koduna *mükemmel kod* denir.
(ii) Örtme yarıçapı paketleme yarıçapından bir fazlaysa, yani $R(C) = e(C) + 1$ eşitliği sağlanıyorsa C koduna *yarı-mükemmel kod* denir.

Başka bir deyişle, bir C kodu için $\Delta(C) = R(C) - e(C) \geq 0$ olmak üzere,

(i) C kodu mükemmel bir koddur ancak ve ancak $\Delta(C) = 0$,
(ii) C kodu yarı-mükemmel bir koddur ancak ve ancak $\Delta(C) = 1$ dir.

2.3 Sonlu Cisimler Üzerinde Devirli Kodlar

Devirli kodlar, lineer kodların bir alt sınıfıdır. Ancak, kodların kolayca uygulanabilmesi için, lineerliğin yanında daha fazla yapının tanıtılması gerekmektedir. Daha kolay kodlama ve kod çözmek için verilen C kodundaki bir kod sözcüğünün hala bir kod sözcüğü olmasını, yani doğal olarak devirli bir değişimi gereklidir. Bu gereksinim bir kombinatoryal yapıya benzer. Neyse ki bu yapı cebirsel bir yapıya dönüştürülebilir. Ayrıca, n uzunluğundaki devirli bir kodun, derecesinin n den küçük bir polinom tarafından belirlendiği gösterilecektir.

2.62 Tanım. $S \subseteq \mathbb{F}_q^n$ için eğer $(a_0, a_1, ..., a_{n-2}) \in S$ iken $(a_{n-1}, a_0, a_1, ..., a_{n-2}) \in S$ oluyorsa S kümesine *devirli* denir. Bir C lineer kodu devirli ise, bu koda bir *devirli kod* adı verilir.

2.63 Örnek. Aşağıda verilen kodlar devirli kodlardır:
(i) $\{0\}$ ve $\mathbb{F}_q^n$ aşikar kodları,
(ii) ikili $[3, 2, 2]$-lineer kodu $\{000, 110, 101, 011\}$.

Devirli kodların kombinatoryal yapısını cebirsel bir yapıya dönüştürmek için aşağıdaki eşleme kullanılmaktadır:

$$\begin{aligned} P : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q[x]/\left(x^n - 1\right) \\ (a_0, a_1, ..., a_{n-1}) &\mapsto a_0 + a_1 x + ... + a_{n-1} x_{n-1} \end{aligned} \tag{2.3}$$

Burada P, $\mathbb{F}_q$ üzerindeki vektör uzaylarının bir $\mathbb{F}_q$-lineer dönüşümüdür. Bu yüzden, $\mathbb{F}_q^n$ yi, $\mathbb{F}_q[x]/(x^n - 1)$ olarak ve $u = (u_0, u_1, ..., u_{n-1})$ vektörünü ise $u(x) = \sum_{i=0}^{n-1} u_i x_i$ polinomuyla tanımlayabiliriz.

2.64 Tanım. R bir (değişmeli) halka ve I, R nin boştan farklı bir alt kümesi olsun. O zaman, her $a, b \in I$ ve $r \in R$ için,

(i) $a - b \in I$,
(ii) $ra \in I$

koşulları I kümesi üzerinde sağlanıyorsa I kümesine R nin bir *ideali* denir.

2.65 Tanım. I, R halkasının bir ideali olmak üzere, eğer $I =< g >$ olacak şekilde bir $g \in I$ elemanı varsa, g elemanı tarafından üretilen I idealine *temel ideal* denir. Burada $< g >= \{gr : r \in R\}$ olarak tanımlanır ve g elemanına I nın *üreteci* denir.

2.66 Teorem. P, (2.3) de tanımlanan bir lineer dönüşüm olsun. O zaman, $\mathbb{F}_q^n$ nin boş olmayan bir C alt kümesi devirlidir ancak ve ancak $P(C)$, $\mathbb{F}[x]/(x^n - 1)$ in bir idealidir.

İspat: [1]

2.67 Örnek. (i) $C = \{(0,0,0),(1,1,1),(2,2,2)\}$ kodu, üçlü bir devirli koddur.
$\mathbb{F}_3[x]/(x^n-1)$ de karşılık gelen $P(C) = \{0, 1+x+x^2, 2+2x+2x^2\}$.
(ii) $I = \{0, 1+x^2, x+x^3, 1+x+x^2+x^3\}$ kümesi $\mathbb{F}_2[x]/(x^4-1)$ de bir idealdir. Buna karşılık gelen devirli kod ise $P^{-1}(I) = \{0000, 1010, 0101, 1111\}$ dir.

2.68 Teorem. $\mathbb{F}_q[x]/(x^n-1)$ de I sıfırdan farklı bir ideal ve $g(x)$, I da en küçük dereceli sıfır olmayan monik bir polinom olsun. O zaman $g(x)$, I nın bir üretecidir ve x^n-1 yi böler.

İspat: [1]

2.69 Teorem. $\mathbb{F}_q/(x^n-1)$ nin sıfırdan farklı her I idealinde en küçük derecede biricik bir polinom vardır ve bu polinom, Teorem 2.68 ye göre, I nın bir üretecidir.

İspat: [1]

2.70 Tanım. $\mathbb{F}_q/(x^n-1)$ nin sıfırdan farklı bir idealinin en küçük derecesinin biricik monik polinomu I nın *üreteç polinomu* olarak adlandırılır. C devirli kodu için, $P(C)$ nin üreteç polinomu, C nin üreteç polinomu olarak adlandırılır.

2.71 Örnek. $\{000, 110, 011, 101\}$ devirli kodunun üreteç polinomu, $1+x$ dir.

2.72 Yardımcı Önerme. $\mathbb{F}_q^n$ deki devirli kodlar ile $x^n-1 \in \mathbb{F}_q[x]$ in monik bölenleri arasında bire-bir olan bir eşleme vardır.

2.73 Teorem. $g(x)$, $\mathbb{F}_q[x]/(x^n-1)$ idealinin üreteç polinomu olsun. $g(x)$ in derecesi $n-k$ ise karşılık gelen devirli kod k boyutuna sahiptir.

İspat: [1]

2.74 Örnek. $x^7 - 1 = (1+x)(1+x^2+x^3)(1+x+x^3) \in \mathbb{F}_2[x]$ in çarpanlarına göre iki tane ikili $[7,3]$-devirli kod olduğu biliniyor;

$$< (1+x)(1+x^2+x^3) >= \{0000000, 1110100, 0111010, 0011101,$$
$$1001110, 0100111, 1010011, 1101001\}$$

ve

$$< (1+x)(1+x+x^3) >= \{0000000, 1011100, 0101110, 0010111,$$
$$1001011, 1100101, 1110010, 0111001\}.$$

2.4 Hemen Hemen Mükemmel Lineer Olmayan (APN) ve Düzlemsel Fonksiyonlar ile Tanımlanan Lineer Kodlar

Bir f fonksiyonu, $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$, $f(0) = 0$ ile tanımlanan bir fonksiyon ve α, $\mathbb{F}_{p^m}$ cisminin bir ilkel kökü verilmiş olsun. Matrisin her bir elemanı, $\mathbb{F}_p$-vektör uzayı $\mathbb{F}_{p^m}$ nin bir bazına göre kendi koordinatının sütununu temsil ettiği bir H_f matrisi,

$$H_f = \begin{bmatrix} 1 & \alpha & \alpha^2 & ... & \alpha^{p^{m-2}} \\ f(1) & f(\alpha) & f(\alpha^2) & ... & f(\alpha^{p^{m-2}}) \end{bmatrix} \tag{2.4}$$

şeklinde verilsin. H_f yi eşlik-kontrol matrisi olarak kabul eden lineer kodu C_f ile gösterelim.

2.75 Uyarı. Eğer $f(x) = x^d$ fonksiyonu $\mathbb{F}_{p^m}$ üzerinde bir kuvvet fonksiyonu ise C_f lineer kodu, üreteç polinomu $g(x) = m_1(x)m_d(x)$ olarak verilen bir devirli kod olur. Burada, $m_1(x)$ ve $m_d(x)$, $\mathbb{F}_{p^m}$'deki α ilkel kökü için, sırasıyla α ve α^d nin $\mathbb{F}_p$ üzerindeki minimum polinomlarıdır.

2.76 Tanım. Bir $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ fonksiyonu için,

$$f(x) = \sum_{i,j=0,\, i\leq j}^{m-1} a_{i,j}x^{p^i+p^j} + \sum_{i=0}^{m-1} b_k x^{p^k} + c \in \mathbb{F}_{p^m}[x], \quad a_{i,j}, b_k, c \in \mathbb{F}_{p^m}$$

fonksiyonuna bir *kuadratik fonksiyon* denir.

$p \neq 2$ için bu ifade biriciktir; eğer $p = 2$ ise, bu ifadedeki $x^{2^j+2^j} = x^{2^{j+1}}$ terimleri bir lineer fonksiyon tanımlar. Ayrıca bu terimler $\sum_{i=0}^{m-1} b_k x^{2^k}$ ifadesini oluşturmaktadır.

Burada, kuadratik terimi yanıltıcı olabilmektedir. Çünkü,burada tanımlanan kuadratik bir fonksiyon hiçbir şekilde $ax^2 + bx + c$ formunda değildir.

Kuadratik fonksiyoların en belirgin özelliği, $x \mapsto f(x + a) - f(x) - f(a) + f(0)$ fonksiyonunun her zaman lineer olmasıdır.

2.77 Tanım. Bir $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ fonksiyonu için eğer $p \neq 2$ ise,

$$f(x) = \sum_{i,j=0,\, i \leq j}^{m-1} a_{i,j} x^{p^i+p^j} \in \mathbb{F}_{p^m} \quad a_{i,j} \in \mathbb{F}_{p^m}$$

eğer $p = 2$ ise,

$$f(x) = \sum_{i,j=0,\, i<j}^{m-1} a_{i,j} x^{2^i+2^j} \in \mathbb{F}_{2^m} \quad a_{i,j} \in \mathbb{F}_{2^m}$$

olarak tanımlanan fonksiyona, *Dembowski-Ostrom (DO) polinom* denir. DO polinomlarının p-ağırlığının 2 olduğu açıktır.

Herhangi bir $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ kuadratik fonksiyon bir DO polinomunun, bir sabitin ve bir lineer polinomun toplamı ile ifade edilebilir. APN olma özelliği, bu terimlerin eklenmesiyle bozulmadığı için kuadratik APN fonksiyonlar DO polinomları ile ifade edilebilir.

2.78 Tanım. Bir $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ fonksiyonu için eğer,

$$\max_{a \in \mathbb{F}^*_{p^m}} \max_{b \in \mathbb{F}_{p^m}} |\{x \in \mathbb{F}_{p^m} : f(x + a) - f(x) = b\}| = 1$$

ise *düzlemsel fonksiyon* ve

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

ise *hemen hemen mükemmel lineer olmayan (APN) fonksiyon* denir.

Açıkça görülüyor ki, $p = 2$ durumunda $\mathbb{F}_{p^m}$ sonlu cismi üzerinde bir x_0 elemanı $f(x+a) + f(x) = b$ denklemini sağlıyorsa, ancak ve ancak $x_0 + a$ elemanı da bu denklemi sağlar. Bu yüzden $\mathbb{F}_{2^m}$ üzerinde düzlemsel fonksiyon yoktur ve f fonksiyonu APN dir ancak ve ancak her $0 \neq a \in \mathbb{F}_{2^m}$ için x_0 ve $x_0 + a$ elemanları, $\tilde{f}(x) = f(x+a) + f(x)$ fonksiyonu altında aynı elemanı verir. Yani,

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

APN fonksiyonlar uygulama alanlarının çokluğu nedeniyle, çoğunlukla $p = 2$ karakteristikte incelenmiş olsa da $p > 2$ için p tek karakteristikte yakın zamanda Kuroda ve Tsujie tarafından *GAPN (genelleştirilmiş APN)* fonksiyonlarına genelleştirilmiştir. Dileyen okuyucu GAPN fonksiyonlar için [14] e başvurabilir.

2.79 Uyarı. [9] Düzlemsel bir f fonksiyonu için dikkat edilmesi gereken bazı durumlar aşağıdaki gibidir.
(1) Düzlemsel bir f fonksiyonunu tanımlayan özellik şu şekilde ifade edilebilir: $f(x+a) - f(x) = b$ denklemleminin $\forall a, b \in \mathbb{F}_{p^n}$ ve $a \neq 0$ için tam olarak bir tek çözümü vardır.
(2) Düzlemsel fonksiyonlar, ancak p tek ise var olabilir; çünkü, p çift ise "$+1 = -1$" ve $f(x+a) + f(x) = f((x+a)+a) + f(x+a)$ elde ederiz. Dolayısıyla, $f(x+a) + f(x) = b$ denklemi herhangi bir $a \neq 0$ için çift sayıda çözüme sahiptir.
(3) Düzlemsel fonksiyonlar, mükemmel lineer olmayan (PN) fonksiyonların özel bir durumudur.
(4) Sıfırdan farklı her $a \in \mathbb{F}_{p^m}$ için $x \mapsto f(x+a) - f(x)$ fonksiyonu bir permütasyondur.
(5) Düzlemsel bir fonksiyona lineer veya sabit fonksiyonlar eklemek, yine düzlemsel bir fonksiyon verir. Bu nedenle, tüm kuadratik düzlemsel fonksiyonlar Dembowski-Ostrom polinomları ile tanımlanabilir.

2.80 Örnek. [9] Her p tek sayısı için $\mathbb{F}_{p^m}$ sonlu cismi üzerinde $f(x) = x^2$ fonksiyonu düzlemseldir. Gerçekten de,

$f(x+a) - f(x) = b \Rightarrow (x+a)^2 - x^2 = b$
$\Rightarrow x^2 + 2xa + a^2 - x^2 = b$

$\Rightarrow 2xa + a^2 = b$

denklemi, her $a \neq 0$ için biricik bir çözüme sahiptir. $p = 2$ için iddianın çalışmayacağı unutulmamalıdır. Çünkü $p = 2$ durumu için $a^2 = b$ denklemini elde ederiz ve dolayısıyla, $f(x + a) - f(x) = b$ denkleminin 0 ($a^2 \neq b$ ise) veya 2^m ($a^2 = b$ ise) çözümü vardır. Aynı zamanda $f(x) = x^2$ fonksiyonunun, $\mathbb{F}_{2^m}$ sonlu cismi üzerinde

$$f(x + y) = (x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2 = f(x) + f(y)$$

olduğundan lineer bir fonksiyon olduğu görülmektedir.

2.81 Örnek. [9] $f(x) = x^3$ fonksiyonu bütün $\mathbb{F}_{2^m}$ sonlu cisimleri üzerinde APN dir.

$f(x + a) + f(x) = b \Rightarrow (x + a)^3 + x^3 = b$
$\Rightarrow x^3 + 3x^2a + 3xa^2 + a^3 + x^3 = b$
$\Rightarrow x^2a + xa^2 + a^3 = b$

kuadratik denkleminin 0, 1 veya 2 tane çözümü olduğuna dikkat edelim. f APN olduğundan, tanım gereği, bu denklemin 0 veya 2 tane çözümü vardır.

Burada x^3 eşlemesi m tek için bijektiftir, ancak m çift için bijektif değildir. x^3 eşlemesine lineer fonksiyonlar ekleyerek, örneğin $x^3 + x$ gibi, m çift için bijektif olmayan APN fonksiyonlar elde etmek kolaydır.

2.82 Örnek. [9] m tek ise $f(x) = x^{-1}$ fonksiyonu $\mathbb{F}_{2^m}$ cismi üzerinde APN dir.

2.83 Tanım. p herhangi bir asal sayı olmak üzere, her $x \in \mathbb{F}_{p^m}$ için $\mathrm{tr} : \mathbb{F}_{\mathrm{p^m}} \longrightarrow \mathbb{F}_{\mathrm{p}}$ olmak üzere

$$\mathrm{tr}_{\mathbb{F}_{\mathrm{p^m}}/\mathbb{F}_{\mathrm{p}}}(\mathrm{x}) := \mathrm{x} + \mathrm{x^p} + \mathrm{x^{p^2}} + ... + \mathrm{x^{p^{m-1}}}$$

ile tanımlanan bir fonksiyona, *iz (trace) fonksiyonu* denir.

İz fonksiyonu aşağıdaki özellikleri sağlar:
(i) Her $x, y \in \mathbb{F}_{p^m}$ için $\mathrm{tr}_{\mathbb{F}_{\mathrm{p^m}}/\mathbb{F}_{\mathrm{p}}}(\mathrm{x} + \mathrm{y}) = \mathrm{tr}_{\mathbb{F}_{\mathrm{p^m}}/\mathbb{F}_{\mathrm{p}}}(\mathrm{x}) + \mathrm{tr}_{\mathbb{F}_{\mathrm{p^m}}/\mathbb{F}_{\mathrm{p}}}(\mathrm{y})$.

(ii) Her $x \in \mathbb{F}_{p^m}$ ve c sabiti için $\mathrm{tr}_{\mathbb{F}_{\mathrm{p}^{\mathrm{m}}}/\mathbb{F}_{\mathrm{p}}}(\mathrm{cx}) = \mathrm{c} \cdot \mathrm{tr}_{\mathbb{F}_{\mathrm{p}^{\mathrm{m}}}/\mathbb{F}_{\mathrm{p}}}(\mathrm{x})$.
(iii) tr fonksiyonu lineer ve örtendir.

2.84 Tanım. m tek sayı olmak üzere, bir $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$ fonksiyonu, her $u, v \in \mathbb{F}_{2^m}$ ve $u \neq 0$ olacak şekilde,

$$W_f(u,v) = \sum_{x \in \mathbb{F}_2^m} (-1)^{\mathrm{tr(uf(x))+tr(vx)}}$$

genişletilmiş Walsh dönüşümü, sadace $W_f(u,v) = 0$ veya $W_f(u,v) = \pm 2^{\frac{m+1}{2}}$ değerlerini alıyorsa, f fonksiyonuna *hemen hemen bükük (AB) fonksiyon* denir. Burada tr iz fonksiyonu,

$$\mathrm{tr}_{\mathbb{F}_{2^{\mathrm{m}}}/\mathbb{F}_2}(\mathrm{x}) = \mathrm{x} + \mathrm{x}^2 + \mathrm{x}^4 + ... + \mathrm{x}^{2^{\mathrm{m}-1}}$$

olarak tanımlanır.

m nin çift olduğu durumlarda AB fonksiyonları mevcut değildir. AB fonksiyonları, yalnızca m nin tek olduğu durumlarda mevcuttur.

2.85 Teorem. Her AB fonksiyon APN dir, fakat tersi doğru değildir. [16, 17]

3. HEMEN HEMEN MÜKEMMEL LİNEER OLMAYAN (APN) FONKSİYONLAR İLE TANIMLANAN LİNEER KODLAR

Bu bölümde, $m \geq 3$ pozitif bir tam sayı olmak üzere $p = 2$ ve m tek asalı için, yarı-mükemmel kod sınıfları verilecektir.

Aynı zamanda, genel f APN fonksiyonları için C_f lineer kodunun $R := R(C_f)$ örtme yarıçapı, $d := d(C_f)$ minimum mesafesi, n uzunluğu ve k boyutu olmak üzere, yapılan araştırma sonuçları verilecektir.

3.1 Teorem. [18] $m > 3$ olmak üzere bir C_f lineer, $[2^m - 2, 2^m - 2m - 1, 5]$-kodu yoktur.

Şimdi, $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$ olmak üzere,

$$f(x) = \sum_{j=0}^{2^m-1} \delta_j x^j, \quad \delta_j \in \mathbb{F}_{2^m} \tag{3.1}$$

fonksiyonunu, derecesi 2^m den daha küçük ($der(f(x) < 2^m)$) olan biricik bir polinom olarak kabul edelim.

3.2 Teorem. [15, Theorem 5] f fonksiyonu (3.1) formunda olmak üzere, öyle ki $f(0) = 0$, C_f lineer $[n = 2^m - 1, k, d]$-kodu ve (2.4) formunda bir H_f eşlik-kontrol matrisi verilmiş olsun. O halde,
(i) C_f kodu için $3 \leq d \leq 5$ tir.
(ii) f fonksiyonu APN dir ancak ve ancak $d = 5$ tir.

İspat: (i) İlk olarak herhangi bir f fonksiyonu için, C_f nin boyutunun $k \geq 2^m - 1 - 2m$ olduğuna dikkat edelim. H_f nin herhangi iki sütunu farklı olduğundan $d \geq 3$ tür.

Varsayalım ki, $d \geq 6$ olsun. Lineer bir $[n, k, d]$-kodunun varlığı, lineer bir $[n - 1, k, d - 1]$-kodunun varlığını gerektirdiğinden, $[2^m - 1, k, 6]$ için $k \geq 2^m - 1 - 2m$ parametreleriyle C_f kodu, lineer bir $[2^m - 2, k, 5]$-kodu sağlar. Ancak, Teorem 3.1 de böyle bir kod mevcut

değildir. O halde, $d \leq 5$ olmak zorundadır.

(ii) $c = (c_0, c_1, c_2, ..., c_{n-1})$ ikili bir vektör olsun. H_f nin tanımına göre, c ikili vektörü C_f ye aittir ancak ve ancak

$$\sum_{i=0}^{n-1} c_i \alpha^i = 0 \quad \text{ve} \quad \sum_{i=0}^{n-1} c_i f(\alpha^i) = 0. \tag{3.2}$$

(3.2) ye göre, C_f nin minimum ağırlığı 3 veya 4 gerek ve yeter şart $\mathbb{F}_{2^m}$ nin öyle dört farklı elemanı x, y, x', y' vardır ki

$$x + y + x' + y' = 0 \quad \text{ve} \quad f(x) + f(y) + f(x') + f(y') = 0. \tag{3.3}$$

Bu dört elemandan biri 0 ise, minimum ağırlık 3 tür, aksi halde 4 tür. Bu denklem aşağıdaki gibi yeniden yazılabilir:

$$x + y = a \quad \text{ve} \quad f(x) + f(y) = b. \tag{3.4}$$

Burada, $a \neq 0$ ve b elemanları $\mathbb{F}_{2^m}$ nin keyfi elemanlarıdır. Varsayalım ki, (3.4) denklemlerini sağlayan iki farklı (x, y) ve (x_0, y_0) çiftleri olsun. Burada $\mathbb{F}_{2^m}$ nin dört farklı elemana sahip olduğu varsayılmaktadır. Bazı a ve b için bu tür dört elemanın varlığı, (3.3) denklemlerini sağlayan dört elemanın varlığına eşdeğerdir. Dolayısıyla f fonksiyonu APN dir gerek ve yeter şart C_f nin minimum mesafesi $d \geq 5$ dir. (i) madesinden, $d \leq 5$ olduğundan $d = 5$ elde edilir.

□

f fonksiyonu APN ise $d = 5$ olduğundan, $e(C_f) = \left\lfloor \frac{d(C_f)-1}{2} \right\rfloor = 2$' dir. Yani, C_f bir 2-hata düzeltici koddur.

3.3 Önerme. [15, Corollary 1] f fonksiyonu (3.1) formunda herhangi bir polinom ve $f(0) = 0$ olsun. $m \geq 3$ olmak üzere f bir APN fonksiyon ise, C_f kodunun boyutu $2^m - 2m - 1$ e eşittir.

İspat: f herhangi bir APN fonksiyon olsun. Teorem 3.2 ye göre C_f bir $[n, k, d]$-kodudur, öyle ki, $n = 2^m - 1$, $d = 5$ ve $k \geq n - 2m$ dir. Eğer $k = n + 1 - 2m$ ise, elde

olmayan bir lineer $[2^m - 1, 2^m - 2m, 5]$-kodu elde edilir (bkz. Teorem 3.1). Bu nedenle, $k = n - 2m = 2^m - 2m - 1$ dir.

□

C, $\mathbb{F}_q$ sonlu cismi üzerinde n uzunluğunda bir lineer kod ve $u \in \mathbb{F}_q^n$, n uzunluğunda herhangi bir vektör olmak üzere,

$$u + C = \{u + v : v \in C\} = C + u$$

kümesine u *tarafından tanımlanan* C *nin koseti* adı verilir.

3.4 Önerme. [15, Proposition 4] f herhangi bir APN fonksiyon olsun. O halde, C_f nin örtme yarıçapı R olmak üzere, $3 \leq R \leq 4$ tür.

İspat: $n \geq 7$ uzunluğunda ve minimum mesafesi 5 olan ikili mükemmel kodların olmadığı bilinmektedir [19]. f APN olduğundan C_f kodu bir 2-hata düzeltme kodudur. C_f kodunun, uzunluğu 5 olan aşikar bir mükemmel kod olmadığı varsayılarak, örtme yarıçapının en az 3 olduğu elde edilir.

Şimdi, örtme yarıçapının $R = 5$ olduğunu varsayıp, ağırlığı 5 olan C_f kodunun bir D kosetini düşünelim. Önerme 3.3 e göre, C_f nin boyutunun $2^m - 2m - 1$ olduğu biliniyor. Bu nedenle, $D \cup C_f$ kodu $[2^m - 1, 2^m - 2m, 5]$-kodudur. Fakat böyle bir kod yoktur (bkz. Teorem 3.1).

□

3.5 Önerme. [2, Proposition 1] m bir tek sayı olmak üzere, $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$ ve $f(0) = 0$ fonksiyonuyla tanımlanan C_f kodu, bir yarı-mükemmel lineer kodsa, f bir APN fonksiyondur.

İspat: f eşlemesi, C_f yarı-mükemmel bir lineer kod ve α ilkel kökü verilmiş olsun. Teorem 3.2 nin (i) maddesinde C_f nin minimum mesafesi $3 \leq d \leq 5$ tir. C_f lineer kodunun paketleme yarıçapı $1 \leq e \leq 2$ dir. Diğer yandan, herhangi bir $\gamma \neq 0$ için

$s, r \in \{0, 1, ..., 2^m - 2\}$ ve $c_1, c_2 \in \{0, 1\}$ olmak üzere,

$$\begin{bmatrix} 0 \\ \gamma \end{bmatrix} = c_1 \begin{bmatrix} \alpha^s \\ f(\alpha^s) \end{bmatrix} + c_2 \begin{bmatrix} \alpha^r \\ f(\alpha^r) \end{bmatrix} = \begin{bmatrix} c_1\alpha^s + c_2\alpha^r \\ c_1 f(\alpha^s) + c_2 f(\alpha^r) \end{bmatrix}$$

eşitliğinin bir çözümünün olmadığı gösterilecektir.

$x = c_1\alpha^s$ ve $y = c_2\alpha^r$ alındığında,

$$\begin{bmatrix} 0 \\ \gamma \end{bmatrix} = \begin{bmatrix} x + y \\ f(x) + f(y) \end{bmatrix}$$

olur. Buradan, $y = -x$ ve $f(x) + f(y) = \gamma$ olur. O halde,

$f(x) + f(y) = \gamma \Rightarrow f(x) + f(-x) = \gamma$
$\Rightarrow f(x) + f(x) = \gamma$
$\Rightarrow 2f(x) = \gamma$

denkleminin $\gamma \neq 0$ için bir çözümü yoktur. Bu yüzden, C_f kodunun örtme yarıçapı $R(C_f) \geq 3$ tür. C_f bir yarı-mükemmel kod, yani $R(C_f) = e(C_f) + 1$ olduğundan,

$R(C_f) = \left\lfloor \frac{d(C_f)-1}{2} \right\rfloor + 1 \geq 3 \Rightarrow \left\lfloor \frac{d(C_f)-1}{2} \right\rfloor \geq 2 \Rightarrow d(C_f) - 1 \geq 4 \Rightarrow d(C_f) \geq 5$ dir.

O halde, $d(C_f) = 5$ ve Teorem 3.2 nin (ii) maddesinden f bir APN fonksiyondur.

□

Bir C kodunun hata düzeltme kapasitesi $e = \left\lfloor \frac{d(C)-1}{2} \right\rfloor$ dir. Bundan böyle, C kodunun bir e-hata düzeltme kodu, olduğu söylenecektir. $v \in \mathbb{F}_q^n$ ve $0 \leq k \leq n$ için $B(v, k)$ ve $p(v)$ sırasıyla,

$B(v, k) = |\{c \in C : d(v, c) = k\}|$, v sözcüğüne mesafesi k olan kod sözcüklerinin sayısı,

$p(v) = min\,\{0 \leq k \leq n | B(v, k) \neq 0\}$, v sözcüğünün C koduna olan uzaklığı,

olarak tanımlanır [20].

3.6 Tanım. [20] $\mathbb{F}_q^n$ de C bir e-hata düzeltme kodu olmak üzere, tüm $v \in \mathbb{F}_q^n$ için λ ve μ parametreleriyle C ye, *düzgün paketlenmiş (uniformly packed) kod* adı verilir. Öyle ki,

$p(v) = e \Longrightarrow B(v, e+1) = \lambda$,
$p(v) \geq e+1 \Longrightarrow B(v, e+1) = \mu$,

burada $\lambda < \frac{(n-e)(q-1)}{e+1}$ dir.

3.7 Teorem. [15, Theorem 6] f, (3.1) ile verilen herhangi bir polinom ve m tek sayı olmak üzere, f fonksiyonu AB dir ancak ve ancak C_f kodunun minimum mesafesi $d = 2e+1 = 5$, örtme yarıçapı $R = e+1 = 3$ ve uzunluğu $n = 2^m - 1$ olan düzgün paketlenmiş bir koddur.

Teorem 2.85 e göre her AB fonksiyon APN olduğundan, f fonksiyonu APN ise C_f kodu, minimum mesafesi $d = 2e+1 = 5$, örtme yarıçapı $R = e+1 = 3$ ve uzunluğu $n = 2^m - 1$ olan düzgün paketlenmiş bir koddur.

Şimdiyse, kuadratik ve kuadratik olmayan APN kuvvet fonksiyonları, yani $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$,$f(x) = x^d$, ile tanımlanan C_f lineer kodları ele alınacaktır.

Hemen hemen mükemmel lineer olmayan (APN) fonksiyonlar için kontrol edilen ilk polinom sınıfının $f(x) = x^d$ kuvvet fonksiyonları olmasının avantajı, $(x+1)^d + x^d = b$ denkleminin en fazla 2 çözüme sahip olduğunu kontrol etmenin yeterli olmasıdır. Eğer $(x+a)^d + x^d = b$ ise, denklemi a^d ye bölerek $(y+1)^d + y^d = \frac{b}{a^d}$ elde edilir.

Tüm APN kuvvet fonksiyonları, m tek iken bijektiftir. Ancak, m çift iken hiçbiri bijektif değildir. Bu durum, kuvvet fonksiyonlarınnın alt cisimlerde APN olmasından kaynaklanır. Aynı zamanda, bijektif APN fonsiyonların tersi de APN dir. Ters fonksiyonlar Tablo 3.1 ve Tablo 3.2 ye dahil edilmemiştir. Ancak, dileyen okuyucu APN kuvvet fonksiyonlarının ters fonksiyonları açıklaması için [21] ye başvurulabilir.

3.0.1 Kuadratik APN Fonksiyonlar ile Tanımlanan Lineer Kodlar

Bir f kuadratik APN fonksiyonun ve ikili yarı-mükemmel lineer kodların sınıfları verildiğinde, C_f ikili kodların, $R(C_f)$ örtme yarıçapı verilecektir.

Önerme 3.4 den herhangi bir f APN fonksiyonu için, C_f kodunun örtme yarıçapının en az 3 ($R \geq 3$) olduğu bilinmektedir. Aşağıdaki önerme, herhangi bir $m \geq 3$ pozitif tam sayısı için, C_f kodunun örtme yarıçapını belirler.

3.8 Önerme. [2, Proposition 2] Herhangi bir $m \geq 3$ için, $f(x) = \sum_{i,j=0}^{m-1} a_{i,j} x^{2^i+2^j}$, $a_{i,j} \in \mathbb{F}_{2^m}$ kuadratik fonksiyonu olmak üzere, f bir APN fonksiyon ise C_f lineer kodunun örtme yarıçapı $R(C_f) = 3$ tür.

İspat: Önerme 3.4 den C_f kodunun örtme yarıçapı $R(C_f) \geq 3$ olduğu bilinmektedir. Tanım 2.58 den her $(\delta_1, \delta_2) \in \mathbb{F}_{2^m}^2$ için öyle $x_1, x_2, x_3 \in \mathbb{F}_{2^m}^2$ vardır ki,

$$\begin{aligned} x_1 + x_2 + x_3 &= \delta_1 \\ f(x_1) + f(x_2) + f(x_3) &= \delta_2 \end{aligned} \tag{3.5}$$

olduğunu göstermemiz gerekiyor. $N(\delta_1, \delta_2)$, (3.5) de verilen denklemlerin, x_1, x_2, x_3 çözümlerinin sayısını göstersin.

$t = 1, 2, 3$ için $y_t = x_t + \delta_1$ alındığında,

$$f(y_t) = \sum_{i,j=0}^{m-1} a_{i,j}(x_t + \delta_1)^{2^i+2^j}.$$

(2.2) eşitliğinden her $t = 1, 2, 3$ için $(x_t + \delta_1)^{2^i} = x_t^{2^i} + \delta_1^{2^i}$ olacağından,

$$\begin{aligned} f(y_t) &= \sum_{i,j=0}^{m-1} a_{i,j}(x_t + \delta_1)^{2^i}(x_t + \delta_1)^{2^j} \\ &= \sum_{i,j=0}^{m-1} a_{i,j}(x_t^{2^i} + \delta_1^{2^i})(x_t^{2^j} + \delta_1^{2^j}) \\ &= \sum_{i,j=0}^{m-1} a_{i,j}(x_t^{2^i} x_t^{2^j} + x_t^{2^i}\delta_1^{2^j} + \delta_1^{2^i} x_t^{2^j} + \delta_1^{2^i}\delta_1^{2^j}) \end{aligned}$$

$$= \sum_{i,j=0}^{m-1} a_{i,j}(x_t^{2^i+2^j} + x_t^{2^i}\delta_1^{2^j} + \delta_1^{2^i}x_t^{2^j} + \delta_1^{2^i+2^j}).$$

O zaman $x_1 + x_2 + x_3 = \delta_1$ olduğundan,

$$f(y_1)+f(y_2)+f(y_3) = \sum_{i,j=0}^{m-1} a_{i,j}(x_1+\delta_1)^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_2+\delta_1)^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_3+\delta_1)^{2^i+2^j}$$
$$= \sum_{i,j=0}^{m-1} a_{i,j}(x_1+\delta_1)^{2^i}(x_1+\delta_1)^{2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_2+\delta_1)^{2^i}(x_2+\delta_1)^{2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_3+\delta_1)^{2^i}(x_3+\delta_1)^{2^j}$$
$$= \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j} + x_1^{2^i}\delta_1^{2^j} + \delta_1^{2^i}x_1^{2^j} + \delta_1^{2^i+2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}(x_2^{2^i+2^j} + x_2^{2^i}\delta_1^{2^j} + \delta_1^{2^i}x_2^{2^j} + \delta_1^{2^i+2^j})$$
$$+ \sum_{i,j=0}^{m-1} a_{i,j}(x_3^{2^i+2^j} + x_3^{2^i}\delta_1^{2^j} + \delta_1^{2^i}x_3^{2^j} + \delta_1^{2^i+2^j})$$
$$= \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j}+x_2^{2^i+2^j}+x_3^{2^i+2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}\delta_1^{2^i}(x_1^{2^j}+x_2^{2^j}+x_3^{2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}\delta_1^{2^j}(x_1^{2^i}+x_2^{2^i}+x_3^{2^i})$$
$$+ \sum_{i,j=0}^{m-1} a_{i,j}(\delta_1^{2^i+2^j})$$
$$= \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j} + x_2^{2^i+2^j} + x_3^{2^i+2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}(\delta_1^{2^i+2^j})$$
$$= \sum_{i,j=0}^{m-1} a_{i,j}x_1^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}x_2^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}x_3^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(\delta_1^{2^i+2^j})$$

eşitliklerinden de görüleceği üzere buradan,

$$f(y_1) + f(y_2) + f(y_3) = f(x_1) + f(x_2) + f(x_3) + f(\delta_1) = \delta_2 + f(\delta_1) = \delta_2^{'}. \tag{3.6}$$

elde edilir. O halde,

$$y_1 + y_2 + y_3 = (x_1 + \delta_1) + (x_2 + \delta_1) + (x_3 + \delta_1) = x_1 + x_2 + x_3 + 3\delta_1 = \delta_1 + 3\delta_1 = 4\delta_1 = 0$$

olduğundan, x_1, x_2, x_3 elemanları (3.5) i sağlıyorsa, gerek ve yeter şart,

$$\begin{aligned} y_1 + y_2 + y_3 &= 0 \\ f(y_1) + f(y_2) + f(y_3) &= \delta_2^{'} \end{aligned} \tag{3.7}$$

sağlanmasıdır, burada $\delta_2^{'} = \delta_2 + f(\delta_1)$ dir. Demek ki, $N(\delta_1, \delta_2) = N(0, \delta_2^{'})$.

Şimdi, f bir APN fonksiyon ise her $\sigma \in \mathbb{F}^*_{2^m}$ için $N(0, \sigma) \geq 1$ olduğu gösterilecektir.

$f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = 0$ ise, buradan $f(x_1) + f(x_1 + x_2 + x_3) = f(x_2) + f(x_3)$ olur. $a = x_2 + x_3$ ve $b = f(x_2) + f(x_3)$ diyelim. O zaman, x_1, x_2, x_3 elemanları,

$$f(x + a) + f(x) = b \tag{3.8}$$

denklemini sağlar. $f(x)$ fonksiyonu APN ise (3.8) denkleminin iki çözümü olduğunu biliyoruz. O halde, f fonksiyonu APN ancak ve ancak $x_1 = x_2$ veya $x_1 = x_3$ veya $x_2 = x_3$ dir.

[16] de Dillon'a atfedilen gözleme göre, f bir APN fonksiyonsa,

herhangi bir $0 \neq \sigma \in \mathbb{F}^*_{2^m}$ için $f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = \sigma$,

denkleminin en az bir çözümü vardır. Gerçekten de,

$\{f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) : x_1, x_2, x_3 \in \mathbb{F}_{2^m}\}$

kümesinde yer almayan, sıfırdan farklı bir σ_0 elemanı olduğunu varsayalım. O zaman, herhangi bir Boolean fonksiyonu $\varphi : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2$ olmak üzere $\tilde{f}(x) = f(x) + \sigma_0\varphi(x)$ bir APN fonksiyon olacaktır. Bunun nedeni, $\tilde{f}(x_1) + \tilde{f}(x_2) + \tilde{f}(x_3) + \tilde{f}(x_1 + x_2 + x_3) = 0$ denkleminin,

$$f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = (\varphi(x_1) + \varphi(x_2) + \varphi(x_3) + \varphi(x_1 + x_2 + x_3))\sigma_0$$

denklemini öne sürmesi ve buradan $f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = 0$ olmasıdır. f fonksiyonu APN dir ancak ve ancak $f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = 0$ denkleminin çözümleri $x_1 = x_2$ veya $x_1 = x_3$ veya $x_2 = x_3$ şeklinde olması gerektiğini biliyoruz. O halde, $\tilde{f}(x_1) + \tilde{f}(x_2) + \tilde{f}(x_3) + \tilde{f}(x_1 + x_2 + x_3) = 0$ denklemi, yalnızca $x_1 = x_2$ veya $x_1 = x_3$ veya $x_2 = x_3$ olduğunda sağlanır ve bu nedenle $\tilde{f}$ fonksiyonu APN dir.

Ayrıca, $\varphi(x) = \mathrm{tr}(\eta_0 \mathrm{f(x)})$ ile $\mathrm{tr}(\eta_0\sigma_0) = 1$ alınırsa,
$\mathrm{tr}(\eta_0\tilde{\mathrm{f}}(\mathrm{x})) = \mathrm{tr}(\eta_0\mathrm{f(x)} + \eta_0\sigma_0\varphi(\mathrm{x})) = \mathrm{tr}(\eta_0\mathrm{f(x)}) + \mathrm{tr}(\eta_0\sigma_0)\varphi(\mathrm{x}) = 0.$
Önerme 3.3 den $m \geq 3$ için bir f fonksiyonu APN ise C_f kodunun boyutu $2^m - 1 - 2m$ olduğundan, $\tilde{f}$ APN fonksiyonu için tanımlanan $C_{\tilde{f}}$ lineer kodunun boyutu da, $2^m - 1 - 2m$

e eşittir. Yani, $tr(\eta_0\tilde{f}(x)) = 0$ yalnızca $\eta_0 = 0$ olduğunda geçerlidir. Bu ise bir çelişkidir. Bu nedenle, $f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = \sigma$ denkleminin en az bir çözümü vardır. Bu denklem, herhangi bir $\sigma \in \mathbb{F}^*_{2^m}$ için,

$x_1 + x_2 + x_3 = x_4$

$f(x_1) + f(x_2) + f(x_3) = f(x_4) + \sigma$

sisteminin en az bir çözümü olduğunu söyler. (3.6)'da olduğu gibi $t = 1, 2, 3$ için $y_t = x_t + x_4$ yazıldığında

$$
\begin{aligned}
&f(y_1)+f(y_2)+f(y_3) = \sum_{i,j=0}^{m-1} a_{i,j}(x_1+x_4)^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_2+x_4)^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_3+x_4)^{2^i+2^j} \\
&= \sum_{i,j=0}^{m-1} a_{i,j}(x_1+x_4)^{2^i}(x_1+x_4)^{2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_2+x_4)^{2^i}(x_2+x_4)^{2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_3+x_4)^{2^i}(x_3+x_4)^{2^j} \\
&= \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j} + x_1^{2^i}x_4^{2^j} + x_4^{2^i}x_1^{2^j} + x_4^{2^i+2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}(x_2^{2^i+2^j} + x_2^{2^i}x_4^{2^j} + x_4^{2^i}x_2^{2^j} + x_4^{2^i+2^j}) \\
&+ \sum_{i,j=0}^{m-1} a_{i,j}(x_3^{2^i+2^j} + x_3^{2^i}x_4^{2^j} + x_4^{2^i}x_3^{2^j} + x_4^{2^i+2^j}) \\
&= \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j}+x_2^{2^i+2^j}+x_3^{2^i+2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}x_4^{2^i}(x_1^{2^j}+x_2^{2^j}+x_3^{2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}x_4^{2^j}(x_1^{2^i}+x_2^{2^i}+x_3^{2^i}) \\
&+ \sum_{i,j=0}^{m-1} a_{i,j}(x_4^{2^i+2^j}) \\
&= \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j} + x_2^{2^i+2^j} + x_3^{2^i+2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}(x_4^{2^i+2^j}) \\
&= \sum_{i,j=0}^{m-1} a_{i,j}x_1^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}x_2^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}x_3^{2^i+2^j} + \sum_{i,j=0}^{m-1} a_{i,j}(x_4^{2^i+2^j}) \\
&= f(x_1) + f(x_2) + f(x_3) + f(x_4)
\end{aligned}
$$

buradan,

$f(y_1) + f(y_2) + f(y_3) = f(x_1) + f(x_2) + f(x_3) + f(x_4)$,

elde edilir. Böylece,

$y_1 + y_2 + y_3 = 0$

$f(y_1) + f(y_2) + f(y_3) = \sigma$

sistemi en az bir çözüme sahiptir. Yani, $N(0, \sigma) \geq 1$ dir. Böylece, istenilen sonuç elde edilir.

□

Önerme 3.5 ve Önerme 3.8 den aşağıdaki teorem ortaya çıkmaktadır.

3.9 Teorem. [2, Theorem 1] $m \geq 3$ olmak üzere $f(x) = \sum_{i,j=0}^{m-1} a_{i,j} x^{2^i+2^j}$, $a_{i,j} \in \mathbb{F}_{2^m}$ kuadratik fonksiyonu olmak üzere C_f lineer kodu yarı-mükemmeldir ancak ve ancak f bir APN fonksiyondur.

$f_i(x) = x^{2^i+1}$, $(i,m) = 1$, $1 \leq i \leq \frac{m-1}{2}$, kuadratik APN kuvvet fonksiyonları, her $m \geq 3$ için, Gold fonksiyonları olarak adlandırılır.

Tablo 3.1 de, sol kısımda "$f(x)$" ile belirtilen kuvvet fonksiyonu, sağ kısımdaki "Şartlar" ile de fonksiyonun APN olması için gerekli olan koşulu referansıyla birlikte verilmiştir.

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

$f(x)$ fonksiyon	Şartlar
x^{2^i+1} Gold fonksiyonu [22]	$(i,m) = 1$, $1 \leq i \leq \frac{m-1}{2}$
$x^3 + tr(x^9)$	[23, Corollary 1]
$x^{2^s+1} + wx^{2^{ik}+2^{nk+s}}$	$m = 3k$ [24, Corollary 8], [25,26]
$x^{2^s+1} + wx^{2^{ik}+2^{nk+s}}$	$m = 4k$ [24, Theorem 2], [25,26]
$bx^{2^s+1}+b^{2^k}x^{2^{k+s}+2^k}+cx^{2^k+1}+\sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}$	$m = 2k$, k, s tek [27, Theorem 1]
$ux^{2^{-k}+2^{k+s}} + u^{2^k}x^{2^s+1} + vx^{2^{k+s}+2^s}$	$m = 3k$, $(s,3k) = 1$ [27, Theorem 3]
$u^{2^k}x^{2^{-k+2^{k+s}}} + ux^{2^s+1} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^{k+s}+2^s}$	$m = 3k$, $(s,3k) = 1$ [28, Theorem 2.1]
$x^{2^{2^i}+2^i} + bx^{2^k+1} + cx^{2^{k(2^{2i}+2^i)}}$	$m = 2k$, $(i,k) = 1$ [29, Corollary 1]
$x(x^{2^i}+x^{2^k}+cx^{2^{i+k}})+x^{2^i}(c^{2^k}x^{2^k}+sx^{2^{i+k}})+x^{2^{i+1}2^k}$	$m = 2k$, $(i,k) = 1$ [29, Corollary 2]

m tek olduğunda herhangi bir kuadratik f fonksiyonunun sadece ve sadece AB olması durumunda, APN olduğuna dikkat ediniz [15]. Bu durumun tersi doğru değildir. Ancak m tek ise, kuadratik APN fonksiyonların AB olması aşağıdaki önerme ile açıklanmaktadır.

3.10 Önerme. [30, Corollary 11] m tek olsun. Her kuadratik APN fonksiyon $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ hemen hemen bükük bir fonksiyondur.

Bu önerme Teorem 3.7 ile birleştiğinde, tek sayıda değişkenli her kuadratik APN fonksiyonun, minimum mesafesi $d = 2e + 1 = 5$, örtme yarıçapı $R = e + 1 = 3$ ve

uzunluğu $n = 2^m - 1$ olan düzgün paketlenmiş bir C_f kodu verdiği anlamına gelir [15].

Şimdi de Gold fonksiyonları tarafından tanımlanan koda eşdeğer kodlar incelenecektir. Öncelikle aşağıdaki teorem ve tanıma ihtiyacımız vardır.

Devirli kodların sözcükleri, polinom gösterimiyle tanımlanır. Herhangi bir k tam sayısı için, uzunluğu $n = 2^k - 1$ olan bir ikili devirli kodun *ilkel* olduğunu hatırlayalım.

3.11 Teorem. [31, Theorem 2.2] C bir ilkel ikili devirli kod ve birbirinden farklı bazı $d_0, d_1, ..., d_t$ pozitif tam sayıları için $\mathbb{Z}(C) = \left\{\alpha^{d_0}, \alpha^{d_1}, ..., \alpha^{d_t}\right\}$ sıfır kümesi olsun. Varsayalım ki bir C' kodu vardır, öyle ki herhangi bir r tam sayısı için $d(C') = r$ ve $C \subset C'$ dır. $\ell := \sum_{i=0}^{t} \sigma(d_i)$ toplamının bir tek tam sayı olduğunu farzedelim. Eğer $d(C) > l$ ise o zaman her $f > (\ell - s) \max \sigma_2(d_i)$ için $r \leq R(C) \leq \ell$ dir, burada s, $2^s | (\ell + 1)$ olacak şekilde en büyük tam sayıdır.

3.12 Tanım. $\mathbb{F}_q$ cismi üzerinde aynı uzunluğa sahip C_1 ve C_2 kodları aşağıdaki işlemlerin bir kombinasyonu uygulanarak, C_1 kodundan C_2 kodu elde edilirse bu kodlar eşdeğer olarak adlandırılır:
(i) C_1 kodunun kod sözcüklerinde belli bir konumda görünen sembollerin, sıfırdan farklı bir skaler ile çarpımı,
(ii) C_1 kodunun tüm kod sözcüklerindeki bitlerin bir permütasyonu.

3.13 Tanım. $r \geq 2$ olsun. $n = 2^r - 1$ uzunluğunda, sütunları $\mathbb{F}_2^r$ nin sıfır olmayan tüm vektörlerinden oluşan eşlik-kontrol matrisi H olan ikili bir lineer koda $2^r - 1$ *uzunluğundaki ikili Hamming kodu* denir ve *Ham*$(r, 2)$ gösterilir.

3.14 Önerme. [31, Proposition 3.1] C kodu, $(d_1, 2^m - 1) = 1$ olacak şekilde $\mathbb{F}_{2^m}$ cismi üzerinde birbirinden farklı bazı d_1 ve d_2 için sıfır kümesi $\left\{\alpha^{d_1}, \alpha^{d_2}\right\}$ olan bir ilkel devirli kod olsun. O halde, C kodu bazı i için Gold fonksiyonu $f(x) = x^{2^i+1}$ tarafından tanımlanan koda eşdeğerdir öyle ki $(i, m) = 1$ ise $d_2 \equiv d_1(2^i + 1) \bmod (2^m - 1)$, dolayısıyla C kodu yarı-mükemmeldir.

İspat: $n = 2^m - 1$ olsun. $(d_1, 2^m - 1) = 1$ ise $\beta = \alpha^{d_1}$ nin aynı zamanda $\mathbb{F}_{2^m}$ cisminin ilkel elemanı olduğu bilinmektedir. Bu nedenle bazı k için $\alpha^{d_2} = \beta^k$ olacak şekilde pozitif bir k tam sayısı vardır. O halde $\beta^k = \alpha^{d_2} = \alpha^{d_1(2^i+1) \ mod \ (2^m-1)}$ ve dolasıyla $k = 2^i + 1$ dir. Bu da C kodunun sıfır kümesi $\left\{\beta, \beta^{2^i+1}\right\}$ olan koda, yani Gold fonksiyonu $f(x) = x^{2^i+1}$ tarafından tanımlanan koda, eşdeğer olduğu anlamına gelir. Sıfır kümesi $\left\{\beta, \beta^{2^i+1}\right\}$ olan bir kodun yarı-mükemmel olduğu bilinmektedir [32]. Burada [32] sonucunu kapsayan [33] sonucu kullanılarak ayrıntılı bir ispat verilecektir. f fonksiyonuna karşılık gelen kodun eşlik-kontrol matrisi aşağıdaki gibidir:

$$H_f = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ f(1) & f(\beta) & f(\beta^2) & \dots & f(\beta^{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^{2^i+1} & \beta^{2(2^i+1)} & \dots & \beta^{(n-1)(2^i+1)} \end{bmatrix}.$$

Teorem 3.2 nin (ii) maddesinden C_f kodunun minimum mesafesinin $d(C) = 5$ olduğu verilmiştir. Sıfır kümesi $\{\beta\}$ olan C' kodunun, Hamming kodu ve $d(C') = 3$ olduğu bilinmektedir. $C \subset C'$ olduğundan, Teorem 3.11, $\{\beta\}, C = C_f, C'$ ve $r = 3$, $d_0 = 1$, $d_1 = 2^i + 1$ parametreleriyle uygulanabilir. Burada, $\ell = 1 + 2 = 3$ elde edilir. $d(C) > l$ koşulunun sağlandığı açıkça görülmektedir. Böylelikle, Teorem 3.11 den tüm $m > (l - s) \max_i \sigma_2(d_i) = (3 - 2) \cdot 2 = 2$, yani $m \geq 3$ için $R(C) = 3$ elde edilir. Daha sonra Tanım 2.61 (ii) den C kodunun yarı-mükemmel olduğu sonucu elde edilir.

□

3.15 Örnek. Sıfır kümesi $\{\alpha^3, \alpha^7\}$ olan $\mathbb{F}_{2^4}$ cismi üzerinde C kodu ele alınsın. Burada α, $\mathbb{F}_{2^4}$ nin bir ilkel köküdür. C kodunun eşlik-kontrol matrisi H aşağıdaki gibi elde edilir:

$$H = \begin{bmatrix} 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^{14} \\ 1 & \alpha^7 & (\alpha^7)^2 & \dots & (\alpha^7)^{14} \end{bmatrix}.$$

$(7, 15) = 1$ olduğu için $\beta = \alpha^7$ de $\mathbb{F}_{2^4}$ cisminin bir ilkel köküdür. O zaman $\beta^k = \alpha^3 = (\alpha^7)^k$ elde edilir. Buradan ise $k = 2^3 + 1 = 9$ bulunur. Bu nedenle $\{\alpha^3, \alpha^7\}$ sıfır kümesine eş değer olarak $\{\beta, \beta^9\}$ kümesi kabul edilir. Bu ise Gold fonksiyonu $f_3(x) = x^{2^3+1}$ tarafından tanımlanan eş değer kodu verir.($(3, 4) = 1$ olduğuna dikkat edilmeli, tanımda verilen koşul sağlanmaktadır.) Bu nedenle, eşlik-kontrol matrisi H aşağıdaki gibi ifade edilebilir:

$$H = \begin{bmatrix} 1 & \beta^9 & (\beta^9)^2 & \dots & (\beta^9)^{14} \\ 1 & \beta & \beta^2 & \dots & \beta^{14} \end{bmatrix} = \begin{bmatrix} 1 & \beta^9 & (\beta^2)^9 & \dots & (\beta^{14})^9 \\ 1 & \beta & \beta^2 & \dots & \beta^{14} \end{bmatrix}.$$

Bir kodun konumlarının değiştirilmesine izin vermek eşdeğer bir kod ürettiğinden, C kodu aşağıda eşlik-kontrol matrisi H' olarak verilen C' koduna eşdeğerdir:

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{14} \\ 1 & \beta^9 & (\beta^2)^9 & \dots & (\beta^{14})^9 \end{bmatrix}$$

[33]' de $\mathbb{F}_{2^4}$ ve $\mathbb{F}_{2^5}$ için farklı sıfır kümelerine sahip ilkel devirli kodların örtme yarıçapı ve minimum mesafeleri Tablo 1 ve Tablo 2 de verilmiştir. [33]'deki Tablo 1'den, $\{\alpha^5\}, \{\alpha, \alpha^3\}$ ve $\{\alpha, \alpha^3\}$ olmak üzere farklı sıfır kümelerine sahip yalnızca üç yarı-mükemmel kod olduğu görülebilir. Sıfır kümesi $\{\alpha, \alpha^3\}$ olan kodun, sıfır kümesi $\{\alpha, \alpha^9\}$ olan koda eşdeğer olduğu gösterilmişti; ancak α^3 ve α^9 dairesel koset olduğundan, yani $i = 3$ için $\alpha^9 = \alpha^{3.2^i \ mod \ 15}$, bu iki kod da eşdeğerdir. Sonuç olarak, $\mathbb{F}_{2^4}$ cismi için kuvvet fonksiyonları tarafından tanımlanan kodlara karşılık gelen, eşdeğerliliğe kadar farklı, sadece bir tane yarı-mükemmel kod vardır, bu da Gold fonksiyonu tarafından tanımlanan koddur.

Şimdi ise k üssünün herhangi bir pozitif tam sayı değeri için, Önerme 3.14 deki koda eşdeğer olma koşulu genişletilecektir. Bu durumda, Önerme 3.14 de olduğu gibi, ilkel devirli C kodunun, $(d_1, 2^m - 1) = 1$ olacak şekilde bazı farklı d_1 ve d_2 için $\left\{\alpha^{d_1}, \alpha^{d_2}\right\}$ sıfır kümesine sahip olduğu varsayılarak, bazı d için $d_2 \equiv d_1 d \ (mod \ 2^m - 1)$ ise, C kodu $f(x) = x^d$ fonksiyonu tarafından tanımlanan koda eşdeğerdir. Bu durum Önerme 3.14 ün daha genel hali olarak düşünülebilir. Bu duruma örnek için bkz [31].

3.0.2 Kuadratik Olmayan APN Fonksiyonlar ile Tanımlanan Lineer Kodlar

[2] makalesinde, tüm f APN fonksiyonları için, $\mathbb{F}_{2^m}$ üzerinde f ile tanımlanan lineer kodlar yarı-mükemmel midir? sorusu açık bir problem olarak ortaya atılmıştır. Bununla birlikte, küçük m değerleri için bu iddianın doğru olduğu söylenmiş, fakat hesaplamaların detayları ve m değerleri [2] verilmemiştir. [31] de, Tablo 3.2 de verilen kuadratik olmayan APN fonksiyonlar için, $m \leq 8$ iken örtme yarıçapının 3 e eşit olduğu Şekil 1 de verilen Sage kodu

kullanılarak hesaplanmıştır, ve böylelikle [2] nin sonucu bağımsız olarak doğrulanmıştır.

3.16 Teorem. [31, Theorem 3.2] Tablo 3.2 de verilen kuadratik olmayan APN fonksiyonlar tarafından tanımlanan kodlar her $m \leq 8$ için yarı-mükemmeldir.

İspat: Bir C_f kodu, Tablo 3.2 de verilen $\mathbb{F}_{2^m}$ sonlu cismi üzerinde tanımlanan kuadratik olmayan bir APN f fonksiyonu tarafından tanımlansın. Teorem 3.2 nin (ii) maddesinden C_f kodunun minimum mesafesi 5 tir. Şekil 1 de verilen Sage kodu kullanılarak C nin örtme yarıçapının 3 olduğu elde edilir. O halde paketleme yarıçapı tanımından C bir yarı-mükemmel koddur.

□

1: m =eval(input('Enter m:'))
2: d = eval(input('Enter d:'))
3: $R. < x >=$ PolynomialRing(GF(2))
4: $\mathbb{F}. < t >=$ GF(2^m)
5: $p = t$.minpoly()
6: q=(t^d).minpoly
7: $g = p * q$
8: $C =$ codes.CyclicCode(generator_pol= g, length= 2^{m-1})
9: print('Covering radius=',C.covering_radius())

Şekil 1: Örtme yarıçapını hesaplamak için kullanılan Sage kodu

Şekil 1 de satır 1 ve satır 2, kullanıcıdan sırasıyla m cisim genişlemesinin derecesini ve d üssünün girilmesini ister. Satır 3, $\mathbb{F}_2$ üzerinde x tek değişkenli bir polinom halkasını ve satır 4, 2^m büyüklüğünde t tek değişkenli bir $\mathbb{F}$ sonlu cismini oluşturur. Satır 5 ve satır 6, t nin minimal polinomunu p ve t^q nun minimal polinomunu q olarak elde eder. Daha sonra bu minimal polinomlar çarpıldığında devirli C kodunun g üreteç polinomu satır 7 de oluşur. Satır 8 de g üreteç polinomu kullanılarak, uzunluğu $2^m - 1$ olan C devirli kodu oluşturulur. Son olarak satır 9 ise kodun örtme yarıçapını hesaplayarak sonucu görüntüler.

Tablo 3.2 de verilen sol kısımda "$f(x)$" ile belirtilen başlık kuvvet fonksiyonunu, sağ kısmındaki "Şartlar" başlığıysa, fonksiyonun APN olması için gerekli olan koşulu referansıyla birlikte verilmiştir.

Tablo 3.2: $\mathbb{F}_{2^m}$ üzerinde x^d 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 [3]
x^{2^t+3}	$m=2t+1$, Welch [34, 35]
$x^{2^t+2^{\frac{t}{2}}-1}$	t çift, $m=2t+1$, Niho [36, 37]
$x^{2^t+2^{\frac{3t+1}{2}}-1}$	t tek, $m=2t+1$, Niho [36, 37]
x^{2^m-2}	m tek, Inverse [5]
$x^{2^{4t}+2^{3t}+2^{2t}+2^t-1}$	$m=5t$, Dobbertin [38]

4. DÜZLEMSEL FONKSİYONLAR İLE TANIMLANAN LİNEER KODLAR

Düzlemsel fonksiyonların, p çift karakteristikte var olmadığı, ancak $p = 2$ için yapılan çalışmalar sonucunda elde edildiğinden daha önce bahsedilmiştir.

Burada bir p tek asalı için, bilinen tüm f düzlemsel fonksiyonlar, $\mathbb{F}_{p^m}$ sonlu cismi üzerinde, q-ary kodlarının C_f örtme yarıçapı incelenecektir.

Yeni bir düzlemsel fonksiyon oluşturmak oldukça zordur. Bilinen tüm düzlemsel f fonksiyonları aşağıda verilen formlardan biriyle tanımlanabilmektedir [39]:

(1) Düzlemsel Dembowski-Ostrom formu (Düzlemsel DO polinomu):

$$\Lambda_1(x) = \sum_{0 \le i \le j \le m-1} a_{ij} x^{p^i+p^j}, \quad a_{ij} \in \mathbb{F}_p$$

özel kısıtlamalar ve ayrıntılar için bkz [40], [41], [42], [43] ve [44].

(2) Coulter-Matthews formu (Düzlemsel CM polinomu):

$$\Lambda_2(x) = x^{\frac{3^k+1}{2}},$$

burada, $p = 3$, k tek ve $(m, k) = 1$ dir (bakınız [45]).

Düzlemsel DO polinomlarının bazı özellikleri [46] numaralı kaynakçada verilmiştir. Aşağıdaki yardımcı önerme Teorem 4.3 ün kanıtında kullanılacaktır :

4.1 Yardımcı Önerme. [46, Proposition 3.6] $\mathbb{F}_{p^m}$ üzerinde f bir düzlemsel DO polinomu ve $Im(f)$, f nin görüntüsü olsun. $D = Im(f) \setminus \{0\}$, $E = \mathbb{F}_{p^m} \setminus Im(f)$ ve $\zeta \in \mathbb{F}_p^*$ için $\zeta D = \{\zeta x | x \in D\}$ tanımları verilsin. O halde aşağıdaki ifadelerden biri olmalıdır;
(i) $\mathbb{F}_{p^m}$ için de m çift ya da m tek ve a, $\mathbb{F}_{p^m}$ de bir kare olmak üzere, $aD = D$ dir.
(ii) m tek ve a bir kare değilse $aD = E$ dir.

Tanım 2.58 e göre C_f lineer kodunun örtme yarıçapı $R(C_f) = r$ dir ancak ve ancak r en küçük pozitif tam sayıdır öyle ki

$$\begin{cases} \lambda_1 x_1 + \lambda_2 x_2 + ... + \lambda_r x_r = \delta \\ \lambda_1 f(x_1) + \lambda_2 f(x_2) + ... + \lambda_r f(x_r) = \beta \end{cases}$$

denklemini sağlayan herhangi bir $(\delta, \beta) \in \mathbb{F}_{p^m}^2$ için $(\lambda_1, \lambda_2, ..., \lambda_r) \in \mathbb{F}_p^r$ ve r farklı $x_1, x_2, ..., x_r \in \mathbb{F}_{p^m}^*$ eleman vardır.

4.2 Uyarı. $f(x) = x^d$ düzlemsel bir kuvvet fonksiyonu olsun. Öncelikle, $f(x)$ in bir çift fonksiyon olduğunu gösterelim. Burada e kuvveti tek ise, $a = d$ ve $b = 1$ iken,

$$f(x + a) - f(x) = b \Rightarrow (x + d)^d - x^d = 1$$

denkleminin d tek ise 0 ve -1 olmak üzere, en az iki çözümü vardır. Bu durum, $f(x)$ in düzlemsel bir fonksiyon olması ile çelişir. O halde, d kuvveti çift olmak zorundadır. Bu yüzden $f(x) = x^d$ fonksiyonu bir çift fonksiyondur; yani $f(-x) = (-x)^d = x^d = f(x)$ dir. Ayrıca, $f(x)$ bir DO fonksiyonuysa da tanım gereği açıkça bir çift fonksiyondur.

4.3 Teorem. [2, Proposition 3] p bir tek asal sayı ve $f(x)$ bir düzlemsel kuvvet fonksiyonu ya da $\mathbb{F}_{p^m}$ üzerinde bir düzlemsel DO polinomu olsun. C_f lineer kodunun örtme yarıçapı R için,

$$\begin{cases} R = 2, & \text{m tek ise} \\ R = 3, & \text{m çift ise.} \end{cases}$$

İspat: C_f liner kodunun örtme yarıçapına R diyelim. Her $(0, \beta) \in \mathbb{F}_{p^m}^2$ ve $\beta \in \mathbb{F}_p^*$ iken,

$$\begin{cases} \lambda x = 0 \\ \lambda f(x) = \beta \end{cases}$$

denklem sistemini sağlayan $\lambda \in \mathbb{F}_p$ ve $x \in \mathbb{F}_{p^m}$ değerlerinin mevcut olmadığı açıktır. Bu yüzden, $R > 1$ dir.

Şimdi de herhangi bir $(\delta, \beta) \in \mathbb{F}_{p^m}^2$ için m tam sayısının eşliğine göre,

$$\begin{cases} \lambda_1 x_1 + \lambda_2 x_2 = \delta \\ \lambda_1 f(x_1) + \lambda_2 f(x_2) = \beta. \end{cases} \tag{4.1}$$

denklem sistemini ele alalım.

$(\delta, \beta) = (0, 0)$ için (4.1) de yerine yazılırsa,
$\lambda_1 x_1 + \lambda_2 x_2 = 0$
$\lambda_1 f(x_1) + \lambda_2 f(x_2) = 0$
olur. Burada $(\lambda_1, \lambda_2) = (0, 0)$ alınırsa, herhangi iki farklı $x_1, x_2 \in \mathbb{F}_{p^m}^*$ elemanları açıkça bu denklemi sağlar.

$\delta \neq 0$ ve $\beta = f(\delta)$ için (4.1) de yerine yazılırsa,
$\lambda_1 x_1 + \lambda_2 x_2 = \delta$
$\lambda_1 f(x_1) + \lambda_2 f(x_2) = f(\delta)$
olur. Burada $(\lambda_1, \lambda_2) = (1, 0)$ ya da $(\lambda_1, \lambda_2) = (0, 1)$ seçilebilir. $(\lambda_1, \lambda_2) = (1, 0)$ seçilir ve (4.1) de yerine yazılırsa,

$$\begin{cases} x_1 = \delta \\ f(x_1) = f(\delta) \end{cases}$$

olur. Buradan $x_1 = \delta$ ve herhangi bir $x_2 \in \mathbb{F}_{p^m}^* \setminus \{\delta\}$ bu sistemi açıkça sağlar.

$\delta \neq 0$ ve $\beta = -f(\delta)$ için (4.1) de yerine yazılırsa,
$\lambda_1 x_1 + \lambda_2 x_2 = \delta$
$\lambda_1 f(x_1) + \lambda_2 f(x_2) = -f(\delta)$
olur. Buradan, $(\lambda_1, \lambda_2) = (-1, 0)$ veya $(\lambda_1, \lambda_2) = (0, -1)$ seçilebilir. $(\lambda_1, \lambda_2) = (-1, 0)$ seçilir ve (4.1) de yerine yazılırsa,

$$\begin{cases} -x_1 = \delta \\ -f(x_1) = -f(\delta) \end{cases}$$

olur. Buradan $x_1 = -\delta$ ve herhangi bir $x_2 \in \mathbb{F}_{p^m}^* \setminus \{-\delta\}$ bu sistemi açıkca sağlar, çünkü Uyarı 4.2 den $f(\delta) = f(-\delta)$ dır.

Şimdi $\beta \neq \pm f(\delta)$ durumları için (4.1) in çözümlerini araştıralım: $\delta \neq 0$ ve herhangi bir $\beta \in \mathbb{F}_{p^m} \setminus \{\pm f(\delta)\}$ için $(\lambda_1, \lambda_2) = (1, -1)$ seçilip ve (4.1) de yerine yazıldığında,

$$\begin{cases} x_1 - x_2 = \delta \\ f(x_1) - f(x_2) = \beta \end{cases} \tag{4.2}$$

elde edilir. $f(x)$ fonksiyonu düzlemsel bir fonksiyon olduğundan Uyarı 2.79 in (4) maddesinden $f(x)$ bir permütasyondur ve bu yüzden $p(x) = f(x+\delta) - f(x)$ permütasyonu elde edilir.

$x = 0$ için $p(0) = f(0+\delta) - f(0) = f(\delta) - 0 = f(\delta)$ ve
$x = -\delta$ için $p(-\delta) = f(-\delta+\delta) - f(\delta) = f(0) - f(-\delta) = 0 - f(\delta) = -f(\delta)$

olduğundan yukarıdaki (4.2) sisteminin $\beta = f(\delta)$ için $(x_1, x_2) = (\delta, 0)$ ve $(x_1, x_2) = (0, -\delta)$ biricik çözümleri elde edilir. Böylece, $\delta \neq 0$ ve $\beta \neq \pm f(\delta)$ için (4.1)'i sağlayan $\mathbb{F}_{p^m}^* \times \mathbb{F}_{p^m}^*$ 'de biricik bir (x_1, x_2) elde ederiz.

$\delta = 0$ ve $\beta \in \mathbb{F}_{p^m}^*$ için ne λ_1 ne de λ_2 sıfır olamayacağından (4.1) in birinci denkleminden,
$\lambda_1 x_1 + \lambda_2 x_2 = 0 \Longrightarrow \lambda_2 x_2 = -\lambda_1 x_1 \Longrightarrow x_2 = -\lambda_1 \lambda_2^{-1} x_1$
alınıp, ikinci denkemde yerine yazılırsa,

$$\lambda_1 f(x_1) + \lambda_2 f(x_2) = \beta \Longrightarrow \lambda_1 f(x_1) + \lambda_2 f\Big(- \lambda_1 \lambda_2^{-1} x_1 \Big) = \beta \tag{4.3}$$

x_1 değişkenli denklemi elde edilir. Bu denklem $f(x) = x^d$ olduğunda, Uyarı 4.2 den d çift olur ve bu yüzden

$$\lambda_1 f(x_1) + \lambda_2 f\Big(- \lambda_1 \lambda_2^{-1} x_1 \Big) = \beta \Longrightarrow \lambda_1 x_1^d + \lambda_2 \Big(- \lambda_1 \lambda_2^{-1} x_1 \Big)^d = \beta$$
$$\Longrightarrow \left(\lambda_1 x_1^d + \lambda_2 \Big(- \lambda_1 \lambda_2^{-1} x_1 \Big)^d \right) = \beta$$
$$\Longrightarrow \left(\lambda_1 x_1^d + \lambda_2 \lambda_1^d \lambda_2^{-d} x_1^d \right) = \beta$$
$$\Longrightarrow \left(\lambda_1 x_1^d + \lambda_2^{1-d} \lambda_1^d x_1^d \right) = \beta$$
$$\Longrightarrow \left(\lambda_1 + \lambda_2^{1-d} \lambda_1^d \right) x_1^d = \beta$$

olur. Yani

$$\left(\lambda_1 + \lambda_1^d \lambda_2^{1-d} \right) f(x_1) = \beta \tag{4.4}$$

elde edilir. $f(x)$ bir düzlemsel DO polinomu olduğunda $f(x) = \sum_{i,j=0}^{m-1} a_{ij} x^{p^i + p^j}$ iken

$$\left(\lambda_1 + \lambda_1^2 \lambda_2^{-1} \right) f(x_1) = \beta \tag{4.5}$$

olur, çünkü herhangi bir $0 \leq i, j \leq m-1$ için $\Big(-\lambda_1\lambda_2^{-1}\Big)^{p^i+p^j} = \lambda_1^2\lambda_2^{-2}$ dir. Burada $i = j$ dir. Bu durum (4.3) ün birleşik bir şekilde ele alınmasını sağlar.

$\mathbb{F}_{p^m}$ üzerinde d bir çift tam sayı ve $f(x)$ düzlemsel bir terimli veya düzlemsel bir DO polinomu iken,

$$S = \left\{ \lambda_1\Big(1 + \lambda_1^{d-1}\lambda_2^{1-d}\Big) \cdot f(x) | \lambda_1, \lambda_2 \in \mathbb{F}_p^*, x \in \mathbb{F}_{p^m}^* \right\} \tag{4.6}$$

kümesi tanımlayalım. Şimdi de,

- m tek ise $S = \mathbb{F}_{p^m}$,
- m çift ise $S = Im(f) = \{f(x) | x \in \mathbb{F}_{p^m}\}$

olduğu gösterilecektir.

$\lambda_1 = \lambda_2$ ise $\lambda_1\Big(1 + \lambda_1^{d-1}\lambda_2^{1-d}\Big) = 2\lambda_1$ ve $\lambda_1 = -\lambda_2$ ise $\lambda_1\Big(1 + \lambda_1^{d-1}\lambda_2^{1-d}\Big) = 0$ dır. λ_1 ve λ_2 elemanları $\mathbb{F}_p^*$ da değiştikçe $\lambda_1\Big(1 + \lambda_1^{d-1}\lambda_2^{1-d}\Big)$ elemanın $\mathbb{F}_p$ de alacağı değerler değişecektir.

Bu yüzden S kümesinde $\mathbb{F}_p$'deki her elemanı $\lambda_1\Big(1 + \lambda_1^{d-1}\lambda_2^{1-d}\Big) = \zeta$ şeklinde yazılarak,

$$S = \left\{ \zeta f(x) | \zeta \in \mathbb{F}_p, x \in \mathbb{F}_{p^m}^* \right\}$$

kümesi yeniden yazılabilir. $\mathbb{F}_{p^m}$ üzerinde düzlemsel bir $f(x) = x^d$ fonksiyonu için $Im(f)$ nin $\mathbb{F}_{p^m}^*$ deki elemanlarının tümü, karelerden ve sıfır elemanından oluşur, çünkü düzlemsel üs d her zaman çifttir. m çift olduğunda, herhangi bir $\zeta \in \mathbb{F}_p$'nin $\mathbb{F}_{p^m}$ de bir kare olduğu ve böylelikle $\zeta Im(f) = Im(f)$ olduğu kolayca görülmektedir. Bu nedenledir ki, Yardımcı Önerme 4.1'deki sonuç, tüm düzlemsel bir terimli $f(x)$ fonksiyonları için de geçerlidir. Bu yüzden herhangi bir düzlemsel bir terimli veya düzlemsel DO polinomu $f(x)$ için,

- m çift ise, herhangi bir $\zeta \in \mathbb{F}_p^*$ için $\zeta Im(f) = Im(f)$,
- m tek ise bir kare $\zeta \in \mathbb{F}_p^*$ için $\zeta Im(f) = Im(f)$ ve her kare olmayan $\zeta \in \mathbb{F}_p^*$ için $\zeta Im(f) = (\mathbb{F}_{p^m} \setminus Im(f)) \cup \{0\}$ durumları vardır. Ayrıca m tek için $S = \mathbb{F}_{p^m}$ ve m çift için $S = Im(f)$'dir.

Herhangi bir $x \in \mathbb{F}_{p^m}^*$ için $p^m - 1$ tane değer mevcuttur. f bir çift fonksiyon olduğundan x ve $-x$ elemanlarının fonksiyonda alacakları değer aynı olacağından birbirinden farklı $f(x)$

değerlerinin sayısıda $\frac{p^m-1}{2}$'dır. Ayrıca, $f(0) = 0$ olduğundan, $|Im(f)| = \frac{p^m-1}{2} + 1 = \frac{p^m+1}{2}$'dir. Sonuç olarak,

(i) m tek ise, herhangi bir $\beta \in \mathbb{F}_{p^m}^*$ için $\lambda_1, \lambda_2 \in \mathbb{F}_p^*$ ve $x_1 \in \mathbb{F}_{p^m}^*$ elemanları vardır ki,

$\lambda_1\left(1 + \lambda_1^{d-1}\lambda_2^{1-d}\right) \cdot f(x_1) = \beta$ denklemi sağlanır.

(ii) m çift ve $\beta \in \mathbb{F}_{p^m}^* \setminus Im(f)$ ise,

$\lambda_1\left(1 + \lambda_1^{d-1}\lambda_2^{1-d}\right) \cdot f(x) = \beta$ denkleminin herhangi bir $\lambda_1, \lambda_2 \in \mathbb{F}_p^*$ için çözümleri yoktur. O zaman, m tek ise $R = 2$ ve m çift ise $R > 2$ dir.

Şimdi m çift ise $R \leq 3$ olduğunu göstermeliyiz. Yani, herhangi bir $(\delta, \beta) \in \mathbb{F}_{p^m}^2$ için,

$$\begin{cases} \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = \delta \\ \lambda_1 f(x_1) + \lambda_2 f(x_2) + \lambda_3 f(x_3) = \beta \end{cases} \tag{4.7}$$

denklem sistemini sağlayan $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_p^3$ ve üç farklı eleman $x_1, x_2, x_3 \in \mathbb{F}_{p^m}^*$ olduğunu göstereceğiz. $\lambda_3 = 0$ alındığında, (4.7) denklem sisteminin (4.1) denklem sistemi ile aynı olduğuna dikkat edelim. $\delta = 0$ ve $\beta \in \mathbb{F}_{p^m}^*$ dışındaki durumlar için (λ_1, λ_2) değişken grubunun ve (4.1) denklem sistemini sağlayan farklı $x_1, x_2 \in \mathbb{F}_{p^m}^*$ elemanlarının varlığını yukarıda göstermiştik. Bu nedenle, $\delta = 0$ ve $\beta \in \mathbb{F}_{p^m}^*$ durumunu göz önünde bulundurmak yeterlidir.

Bu durumda $(\lambda_1, \lambda_2, \lambda_3) = (1, -1, -1)$ alırsak, (4.7) denklem sistemi,

$$\begin{cases} x_1 - x_2 = x_3 \\ f(x_1) - f(x_2) = \beta + f(x_3) \end{cases} \tag{4.8}$$

olur. $f(x)$ fonksiyonu $\mathbb{F}_{p^m}$ üzerinde düzlemsel olduğundan, (4.8) denklem sisteminin herhangi $x_3, \beta \in \mathbb{F}_{p^m}^*$ için biricik bir (x_1, x_2) çözümü vardır. $\beta = -2f(x_3)$ alındığında (4.8) denklem sistemi,

$$\begin{cases} x_1 - x_2 = x_3 \\ f(x_1) - f(x_2) = -f(x_3) \end{cases}$$

şeklinde olur ve biricik $(x_1, x_2) = (0, -x_3)$ çözümene sahiptir, çünkü $f(x)$ bir çift fonksiyondur (bkz. Uyarı 4.2). $\beta = f(2x_3) - 2f(x_3)$ alındığında (4.8) denklem sistemi

$$\begin{cases} x_1 - x_2 = x_3 \\ f(x_1) - f(x_2) = f(2x_3) - f(x_3) \end{cases}$$

şeklinde olur ve biricik bir $(x_1, x_2) = (2x_3, x_3)$ çözümene sahiptir. Bu yüzden, herhangi bir $\beta \in \mathbb{F}_{p^m}^*$ için, $\beta \notin \{-2f(x_3), f(2x_3) - 2f(x_3)\}$ koşulunu sağlayan $x_3 \in \mathbb{F}_{p^m}^*$ elemanını seçersek (4.8) denklem sisteminin biricik (x_1, x_2) çözümünü elde ederiz; öyle ki, x_1, x_2, x_3 elemanları $\mathbb{F}_{p^m}^*$ da birbirinden farklı elemanlardır. Bu nedenle m çift tam sayısı için C_f nin örtme yarıçapı $R \leq 3$ tür. Sonuç olarak $R = 3$ elde edilir.

□

Önerme 3.8, $\mathbb{F}_{p^m}$ üzerinde bilinen tüm düzlemsel fonksiyonlar için C_f lineer kodlarının örtme yarıçapını inceler. [47, Theorem 6] da kanıtlandığı gibi, $\mathbb{F}_{p^m}$ üzerinde f düzlemsel fonksiyonu verildiğinde, C_f lineer kodunun d minimum mesafesi $2 \leq d \leq 4$ ü sağlar. Buna ek olarak $\lambda_1, \lambda_2 \in \mathbb{F}_p^*$ için,

$\lambda_1 x_1 + \lambda_2 x_2 = 0$
$\lambda_1 f(x_1) + \lambda_2 f(x_2) = 0$

denklem sistemini sağlayan iki farklı $x_1, x_2 \in \mathbb{F}_{p^m}^*$ elemanları vardır, gerek ve yeter şart bazı $c \in \mathbb{F}_p \setminus \{0, 1\}$ ve $x \in \mathbb{F}_{p^m}^*$ için $f(cx) = cf(x)$ eşitliği sağlanır.

Bilinen tüm f düzlemsel fonksiyonlar, bu bölümün başında verilen (1) ve (2) formunda ve buna karşılık gelen C_f kodunun minimum mesafesi $d > 2$ olduğundan aşağıdaki teorem elde edilir:

4.4 Teorem. [2, Theorem 2] $f, \mathbb{F}_{p^m}$ üzerinde düzlemsel bir DO polinomu ya da $\mathbb{F}_{3^m}$ üzerinde bir terimli düzlemsel bir CM polinomu olsun. O zaman, C_f lineer kodları m tek ise yarı-mükemmel kodlardır.

Son olarak, aşağıdaki açık problem okuyucuya sunulmuştur:

4.5 Problem. [2] $\mathbb{F}_{p^m}$ üzerinde herhangi bir f düzlemsel fonksiyon ile tanımlanan C_f lineer kodu için R örtme yarıçapı m çift ise 2 ve m tek ise 3 olması durumu doğru mudur?

5. KAYNAKLAR

[1] S. Ling and C. Xing, *Coding Theory*, Cambridge University Press, 2004.

[2] C. Li and T. Helleseth, "Quasi-perfect linear codes from planar and APN function", *Cryptogr. Commun.*, vol. 8, no. 2, pp. 215-227, April 2016.

[3] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes", *Inform. Control.*, vo. 18, no. 4, pp. 369-394, 1971.

[4] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences", Ph.D. Dissertation, University of Southerm California-Los Angeles, California, 1972.

[5] K. Nyberg, "Differentially uniform mappings for cryptography", *Advances ın Cryptology- EUROCRYPT' 93*, Springer-Verlag Berlin Heidelberg, pp. 55-64, 1994.

[6] T. Beth and C. Ding, "On almost perfect nonlinear permutations", *Advances ın Cryptology- EUROCRYPT' 93*, Springer-Verlag Berlin Heidelberg, pp. 65-67, 1994.

[7] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n by 5", *Finite Fields App.*, Springer-Verlag Berlin Heidelberg, pp. 113-121, 2001.

[8] S. Ling and C. Xing, *Coding Theory: A First Course*, Cambridge, UK: Cambridge University Press, 2004.

[9] A. Pott, "Almost perfect and planar functions", *Design. Code. Cryptogr.*, vol. 78, no. 1, pp. 141-195, December 2016.

[10] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland Mathematical Library, North-Holland, 1997.

[11] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes", *IEEE Trans. Inf. Theory*, vol 31., no. 3, pp. 385-401, May 1985.

[12] J. Quistorff, "On codes with given minimum distance and covering radius", *Contributions to Algebra and Geometry*, vol. 42, no. 2, pp. 601-611, 2001.

[13] G.D. Cohen, M.G. Karpovsky , H.F. Mattson and R. Schatz, “Covering Radius- Survey and Recent Results”, *IEEE Trans. Inf. Theory*, vol. 31, no. 3, pp. 328-343, May 1985.

[14] F. Özbudak and A. Salagean, “New generalized almost perfect nonlinear functions”, *Finite Fields App.*, vol 70, February 2020.

[15] C. Carlet, P. Charpin and V. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystems”, *Design. Code. Cryptogr.*, vol. 15, no. 2, pp. 125-156, 1998.

[16] C. Carlet, “Vectorial boolean functions for cyrptography”, in *Boolean Models and Methodsin Mathematics Computer Science, and Engineering*, Y. Crama and P.L. Hammer, Cambridge University Press, New York, 2010, pp. 298-469.

[17] F. Chabaud and S. Vaudenay, “Links between differential and linear cryptanalysis ”, *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 1994.

[18] A.E. Brouwer and L.M.G.M. Tolhuizen, “ A sharpening of the Johnson bound for binary linear nodes and the nonexistence of linear codes with preparata parameters”, *Design. Code. Cryptogr.*, vol. 3, no. 2, pp. 95-98, May 1993.

[19] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, USA: Matematical Library, 1977.

[20] H.C.A. Van Tilborg, “Uniformly Packed Codes”, *Technische Hogeschool Eindhoven*, Juni 1976, https://doi.org/10.6100/IR162111.

[21] G.M. Kanuregatten and V. Suder, “On inversion in $\mathbb{F}_{2^n-1}$”, *Finite Fields Th. App.*, vol. 25, pp. 234-254, January 2014.

[22] R. Gold, “Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions”, *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154-156, January 1968.

[23] L. Budaghyan, C. Carlet and G. Leander, “Constructing new APN functions from known ones”, *Finite Fields Th. App.*, vol. 15, no. 1, pp. 150-159, 2009.

[24] L. Budaghyan, C. Carlet and G. Leander, “Two Classes of Quadratic APN Binomials Inequivalent to Power Functions”, *IEEE Trans. Inf. Theory*, vol. 54, no. 9, September 2008.

[25] J. Bierbrauer, “New semifields, PN and APN functions”, *Design. Code. Cryptogr.*, vol. 54, no. 3, pp. 189-200, August 2010.

[26] J. Bierbrauer, “A family of crooked functions”, *Design. Code. Cryptogr.*, vol. 50, no. 2, pp. 235-241, September 2009.

[27] C. Bracken, E. Byrne, N. Markin and G. McGuire, “New families of quadratic almost perfect nonlinear trinomials and multinomials”, *Finite Fields Th. App.*, vol. 14, no. 3, pp. 703-714, July 2008.

[28] C. Bracken, E. Byrne, N. Markin and G. McGuire, “A few more quadratic APN functions”, *Cryptogr. Commun.*, vol. 3, no. 1, pp. 43-53, November 2011.

[29] L. Budaghyan and C. Carlet, “Classes of Quadratic APN Trinomials and Hexanomials and Related Structures”, *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 2354-2357, May 2008.

[30] Y. Edel, “Quadratic APN functions as subspaces of alternating bilinear forms”, *Proceedings of the Contact Forum Coding Theory and Cryptography III*, Belgium, vol. 2009, 2011.

[31] S. Tutdere, “Some binary quasi-perfect linear codes defined by APN functions”, *Eur. J. Sci. Theol*, Kabul edildi, 2022.

[32] O. Moreno and N. F. Castro, “Divisibility properties for covering radius of certain cyclic codes”, *IEEE Trans. Inf. Theory*, vol. 49, no. 12, 3299-3303, 2003.

[33] S. Tutdere, “On the covering radii of a class of binary primitive cyclic codes”, *Hacet. J. Math. Sta.*, vol. 51, no. 1, 20-26, 2022.

[34] A. Canteaut, P. Charpin and H. Dobbertin, “Binary m-Sequences with Three-Valued Crosscorrelation: A Proof of Welch’s Conjecture”, *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 4-8, January 2000.

[35] H. Dobbertin, "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: The Niho Case", *Inform. Comput.*, vol. 151, no. 1-2, pp. 57-72, May 1999.

[36] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Welch Case", *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271-1275, May 1999.

[37] H.D.L. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences", *Finite Fields Th. App.*, vol. 7, no. 2, pp. 253-286, April 2001.

[38] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5", *Finite Fields Th. App.*, Springer, Berlin, Heidelberg, pp. 113-121, 2001.

[39] N. Li and S. Mesnager, "Recent result and problems on constructions of linear codes from cryptographic functions", *Cryptogr. Commun.*, vol. 12, no. 5, pp. 965-986, May 2020.

[40] L. Budaghyanve and T. Helleseth, "New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p", *International Conference on Sequences and Their Applications*, pp. 403-414, 2008.

[41] R. Coulter, M. Henderson, L. Hu, P. Kosick, Q. Xiang and X. Zeng , "Planar polynomials and commutative semifields two dimensional over their middle nucleus and four dimensional over their nucleus", *Journal der mathematischen Ablehnungen*, no. 14, pp. 1-5, 2007.

[42] P. Dembowski and T. G. Ostrom, "Planes of order n with collineation groups of order n^2", *Math. Zeilschr.*, no. 103, pp. 239-258, June 1968.

[43] C. Ding and J. Yuan, "A family of skew Hadamard difference sets", *Journal of Combinatorial Theory*, vol. 113, no. 7, pp. 1526-1535, November 2006.

[44] Z. Zha, G. M. Kyureghyan and X. Wang, "Perfect nonlinear binomials and their semifields", *Design. Code. Cryptogr.*, vol. 15, no. 2, pp. 125-133, April 2009.

[45] R.S. Coulter and R.W. Matthews, “Planar Functions and Planes of Lenz-Barlotti Class II”, *Design. Code. Cryptogr.*, vol. 10, no. 2, pp. 167-184, February 1997.

[46] G. Weng and X. Zeng, “Further results on planar DO functions and commutative semifields”, *Design. Code. Cryptogr.*, vol. 63, no. 3, 413-423, September 2012.

[47] C. Carlet, C. Ding and S. Member, “Linear Codes From Perfect Nonlinear Mappings and Their Secret Sharing Schemes”,*IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2089-2102, June 2005.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Damla ÖZDEMİR

Doğum tarihi ve yeri : 27.05.1997/ KARS

e-posta : damla.ozdemir2015@hotmail.com

Öğrenim Bilgileri

Derece	**Okul/Program**	**Yıl**
Y. Lisans	Balıkesir Üniversitesi/Matematik Bölümü	2022
Lisans	Balıkesir Üniversitesi/Matematik Bölümü	2020
Lise	Fevzi Çakmak Lisesi	2015