

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



GRÖBNER TABANLARI VE
LİNEER KODLARIN
TEMEL PARAMETRELERİ

CEMİLE CÜR

YÜKSEK LİSANS TEZİ

Jüri Üyeleri : **Prof. Dr. Seher TUTDERE KAVUT** **(Tez Danışmanı)**
 Prof. Dr. Mesut ŞAHİN
 Prof. Dr. Sebahattin İKİKARDEŞ

BALIKESİR, TEMMUZ - 2026

ETİK BEYAN

Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak tarafımda hazırlanan “**Gröbner Tabanları ve Lineer Kodların Temel 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.

Cemile CÜR

ÖZET

GRÖBNER TABANLARI VE LİNEER KODLARIN TEMEL PARAMETRELERİ
YÜKSEK LİSANS TEZİ
CEMİLE CÜR
BALIKESİR ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
(TEZ DANIŞMANI: PROF. DR. SEHER TUTDERE KAVUT)
(EŞ DANIŞMAN: DOÇ. DR. PINAR METE)
BALIKESİR, TEMMUZ - 2026

Değişmeli cebirin polinom halkaları, idealler, varyeteler ve Gröbner tabanları gibi temel kavram ve araçları, kodlama teorisindeki lineer kodların yapısını ve parametrelerini belirlemede önemli bir rol oynamaktadır. Bu tezde amaç, kodlama teorisinin bazı alanlarında uygulanabilecek olan Gröbner teoriye ait temel kavram ve yöntemleri tanıtmak, afin varyete ve afin kartezyen kodların temel özelliklerini incelemek, ve Gröbner tabanları kullanılarak elde edilen ayak izi (footprint) yönteminin, afin varyete kodlarının temel parametreleri olan uzunluk, boyut ve minimum uzaklığın belirlenmesindeki kullanımını ortaya koymaktır. Ayrıca, afin kartezyen kodların temel parametrelerine ilişkin, bahsi geçen yöntemin kullanılmasıyla literatürde elde edilen bazı sonuçlar incelenmektedir.

ANAHTAR KELİMELELER: Afin kartezyen kodlar, afin varyeteler, afin varyete kodlar, Gröbner tabanları, lineer kodlar

ABSTRACT

GROBNER BASES AND BASIC PARAMETERS OF LINEAR CODES

MSC THESIS

CEMİLE CÜR

BALIKESİR UNIVERSITY INSTITUTE OF SCIENCE

MATHEMATICS

(SUPERVISOR: PROF. DR. SEHER TUTDERE KAVUT)

(CO-SUPERVISOR: ASSOC. PROF. DR. PINAR METE)

BALIKESİR, JULY - 2026

The fundamental concepts and tools of commutative algebra, such as polynomial rings, ideals, varieties, and Gröbner bases, play an important role in determining the structure and parameters of linear codes in coding theory. The aim of this thesis is to introduce the fundamental concepts and methods of Gröbner theory that can be applied to certain areas of coding theory, to examine the basic properties of affine variety codes and affine cartesian codes, and to demonstrate the use of the footprint method, based on Gröbner bases, in determining the fundamental parameters of affine variety codes, namely length, dimension, and minimum distance. Furthermore, some results reported in the literature concerning the fundamental parameters of affine cartesian codes, obtained by means of the aforementioned method, are examined.

KEYWORDS: Affine cartesian codes, affine varieties, affine variety codes, Gröbner bases, linear codes

Science Code / Codes : 20401

Page Number : 40

İÇİNDEKİLER

Sayfa

ÖZET	i
ABSTRACT	ii
İÇİNDEKİLER.....	iii
ŞEKİL LİSTESİ	iv
TABLO LİSTESİ	v
SEMBOL LİSTESİ	vi
ÖNSÖZ.....	vii
1. GİRİŞ	1
2. TEMEL BİLGİLER.....	3
2.1 Cisimler ve Cisim Genişlemeleri.....	3
2.2 Sonlu Cisimler	4
2.3 Lineer Kodlar	6
3. GRÖBNER TABANLARI	10
4. AFİN VARYETELER VE AFİN VARYETE KODLARI.....	20
4.1 Afın Varyeteler.....	20
4.2 Afın Varyete Kodları	25
5. AFİN KARTEZYEN KODLARI	32
6. KAYNAKLAR.....	39
ÖZGEÇMİŞ	40

ŞEKİL LİSTESİ

	<u>Sayfa</u>
Şekil 3.1: $\Delta(I)$ 'nın (ayak izinin) şekli.....	18
Şekil 4.1: $V(I)$ 'nin grafiği.....	21
Şekil 4.2: $V(I)$ 'nin grafiği.....	21

TABLO LİSTESİ

	<u>Sayfa</u>
Tablo 5.1: Polinomlar ve kod sözcükleri.....	33

SEMBOL LİSTESİ

$\mathbb{F}_q$	: q elemanlı sonlu cisim
$\mathbb{F}_q^n$	: q elemanlı sonlu cisim üzerinde tanımlı n -boyutlu vektör uzayı
$\mathbb{R}$	: Reel sayılar kümesi
$\mathbb{Q}$	: Rasyonel sayılar kümesi
$\mathbb{C}$	: Kompleks sayılar kümesi
$\mathcal{C}^\perp$	: $\mathcal{C}$ kodunun dual (ortogonal) kodu
$\mathbf{F}[X]$	: Çok değişkenli polinom halkası
$\sqrt{I}$	: I idealinin radikali
R / I	: Bölüm halkası
$\mathcal{M}$	: Tekterimliler kümesi
$\Delta(I)$	: I idealinin ayak izi (footprint)
$V(I)$	: I idealinin varyetesi
$I(V)$	: V varyetesinin ideali
$\mathbf{d}(\mathcal{C})$	: $\mathcal{C}$ kodunun minimum mesafesi
$ A $	: A kümesinin eleman sayısı
$\mathbf{wt}(x)$	: x sözcüğünün hamming ağırlığı
$\mathbf{d}(a, b)$	: a ile b arasındaki hamming mesafe
$\mathbf{lm}(f)$	: f polinomunun baş tek terimlisi
$\mathbf{lc}(f)$	: f polinomunun baş tek terimlisinin katsayısı
$\mathbf{lt}(f)$	: f polinomunun baş terimi

ÖNSÖZ

Bu tez çalışmasının hazırlanmasında bana yol gösteren, değerli katkılarıyla sürecin her aşamasında destek olan danışmanım Prof. Dr. Seher TUTDERE KAVUT'a ve eş danışmanım Doç. Dr. Pınar METE'ye teşekkür ederim.

Akademik yolculuğumun en başından beri yanımda olan, bu yoğun süreçte dostluğunu ve desteğini her zaman hissettiren arkadaşım Büşra YILDIZ ÇAPKAN'a teşekkür ederim.

Hayatımın her anında olduğu gibi, lisansüstü eğitimim ve tez yazım sürecim boyunca da bana her koşulda inanan, maddi ve manevi desteklerini hiçbir zaman esirgemeyen sevgili annem Havva CÜR'e, canım babam Erden CÜR'e ve varlığıyla bana her zaman güç veren ablam Ferhan Kübra KESER'e sevgi ve şükranlarımı sunarım.

Son olarak, bu uzun ve sabır gerektiren yolculuğun getirdiği tüm zorlukları benimle birlikte göğüsleyen, en yorgun anlarımda motivasyon kaynağım olan, anlayışı, sabrı ve sonsuz sevgisiyle her zaman yanımda yürüyen nişanlım Fatih DURMUŞLUOĞLU'na yürekten teşekkür ederim.

Balıkesir, 2026

Cemile Cür

1. GİRİŞ

Matematiksel yapıların sistematik biçimde incelenmesi, günümüzde hem teorik hem de uygulamalı matematik açısından büyük önem taşımaktadır. Özellikle cebirsel yöntemler, karmaşık problemlerin çözümünde güçlü araçlar sunmakta; kodlama teorisi, cebirsel geometri ve değişmeli cebir gibi farklı disiplinler arasında önemli ilişkilerin kurulmasına olanak sağlamaktadır. Bu nedenle cebirsel yapıların incelenmesi ve bu yapıların farklı alanlardaki uygulamalarının ortaya konulması, modern matematiğin temel araştırma konularından biri hâline gelmiştir.

Kodlama teorisi, bilgi iletimi ve depolanması sırasında oluşabilecek hataların tespit edilmesi ve düzeltilmesi amacıyla geliştirilen matematiksel yöntemleri inceleyen bir bilgi kuramı dalıdır. Özellikle sonlu cisimler ve polinom halkaları üzerine kurulan cebirsel kodlar, kodlama teorisinin en önemli araştırma alanlarından birini oluşturmaktadır.

Değişmeli cebir ise polinom halkaları, idealler ve bunlara bağlı cebirsel yapıları inceleyen matematiğin temel dallarından biridir. Bu alanda geliştirilen kuramsal sonuçlar ve algoritmik yöntemler, özellikle cebirsel geometri ve kodlama teorisinde geniş uygulama alanı bulmaktadır. Gröbner tabanları, polinom sistemlerinin çözümünde, ideallerin analizinde ve cebirsel problemlerin etkin biçimde ele alınmasında önemli araçlar arasında yer almaktadır.

Bu tez çalışmasının amacı, lineer kodlar, Gröbner tabanları, afin varyeteler ve afin kartezyen kodlarını değişmeli cebirin sunduğu yöntemler çerçevesinde sistematik bir yaklaşımla incelemektir. Bu kapsamda ilgili literatürde yer alan temel sonuçlar ele alınarak değişmeli cebirin kodlama teorisindeki bazı uygulamaları incelenmektedir. Özellikle, Gröbner tabanları kullanılarak elde edilen ayak izi (footprint) kavramına dayanan, afin varyete kodlarının temel parametreleri olan uzunluk, minimum uzaklık ve boyutunun belirlenmesinde kullanılan bir yöntem ele alınmaktadır. Tez beş bölümden oluşmaktadır. İkinci bölümde, çalışmanın ilerleyen kısımlarında kullanılacak temel kavramlar verilmekte; cisimler ve cisim genişlemeleri, sonlu cisimler ile lineer kodlara ilişkin temel tanım ve sonuçlar sunulmaktadır.

Üçüncü bölümde, çok değişkenli polinom halkalarında ideallerin yapısının incelenmesinde kullanılan Gröbner tabanları ele alınmaktadır. Bu kapsamda tek terim sıralamaları, Buchberger algoritması ve ayak izi (footprint) kavramı açıklanmakta; ayrıca Hilbert Baz Teoremi Gröbner tabanlarının cebirsel problemlerin çözümündeki önemi ortaya konulmaktadır.

Dördüncü bölümde, cebirsel geometrinin temel kavramlarından biri olan afin varyeteler ve bunlardan elde edilen afin varyete kodları incelenmektedir. Çok değişkenli polinomların sıfır kümeleri olarak tanımlanan varyetelerin ideallerle olan ilişkisi açıklanmakta; bunların yardımıyla afin varyete kodları incelenmektedir. Ayrıca, afin varyete kodlarının temel parametrelerini elde etmek için ayak izi kavramına dayanan yöntemden bahsedilmektedir. Bir sonraki bölümde bu yöntemle, afin varyete kodların özel bir hali olan afin kartezyen kodların temel parametrelerinin nasıl elde edildiği açıklanmaktadır.

Beşinci bölümde ise afin varyete kodların özel bir hali olan afin kartezyen kodlar incelenmektedir. Bu kodların yapısı, tek terim sıralamaları ve ayak izi kavramı çerçevesinde açıklanmakta; son olarak kodların temel parametrelerine ilişkin [3] ve [5]'te elde edilen sonuçlar, tez boyunca sunulan cebirsel yöntemler kullanılarak sunulmaktadır.

2. TEMEL BİLGİLER

Bu bölümde tez kapsamında kullanılacak başlıca tanım ve sonuçlar [1], [2] ve [3] numaralı kaynaklardan yararlanılarak sunulmaktadır. Bu bölüm, ilerleyen kısımlarda kullanılacak cebirsel altyapının anlaşılması için gerekli teorik zemini sağlamaktadır.

2.1 Cisimler ve Cisim Genişlemeleri

Bu kısımda matematiğin en temel yapılarından biri olan cisim kavramı ele alınmaktadır. Ayrıca, cisim genişlemeleri ile ilgili temel tanım ve sonuçlar sunulmaktadır.

2.1 Tanım F , üzerinde toplama (+) ve çarpma ($\cdot$) işlemleri tanımlı olan boştan farklı bir küme olsun. Aşağıdaki özellikler sağlanıyorsa $(F, +, \cdot)$ yapısına bir *cisim* denir:

$x, y, z \in F$ olmak üzere,

(i) Kapalılık özelliği: $x + y \in F$ ve $x \cdot y \in F$,

(ii) Değişme özelliği: $x + y = y + x$, $x \cdot y = y \cdot x$,

(iii) Birleşme özelliği: $(x + y) + z = x + (y + z)$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(iv) Dağılım özelliği: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$,

(v) Birim elemanlar: $0, 1 \in F$ vardır öyle ki her $x \in F$ için $x + 0 = x$ ve $x \cdot 1 = x$,

(vi) Toplamsal ters elemanın varlığı: Her $x \in F$ için $-x \in F$ vardır öyle ki

$$x + (-x) = (-x) + x = 0,$$

(vii) Çarpımsal ters elemanın varlığı: Her $0 \neq x \in F$ için $x^{-1} \in F$ vardır öyle ki

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

Yukarıdaki tanımda (i)-(vi) özellikleri sağlanıyorsa $(F, +, \cdot)$ yapısına *değişmeli halka* denir.

Bu tezde sadece değişmeli halkalar kullanılacaktır.

2.2 Örnek $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ ve $(\mathbb{C}, +, \cdot)$ birer cisimdir.

2.3 Tanım F bir cisim olmak üzere $\emptyset \neq S \subseteq F$ altkümesini alalım. S kümesi bir altcisimdir ancak ve ancak her $a, b, c \in S$, $c \neq 0$ için

(i) $a - b \in S$,

(ii) $a \cdot c^{-1} \in S$.

2.4 Tanım F bir cisim olsun. Eğer F cismi, E cisminin bir altcismi ise E 'ye F 'nin bir *cisim genişlemesi* denir.

2.5 Örnek

(i) $\mathbb{Q} \subseteq \mathbb{R}$ olduğundan $\mathbb{R}$, $\mathbb{Q}$ 'nun bir cisim genişlemesidir.

(ii) $\mathbb{R} \subseteq \mathbb{C}$ olduğundan $\mathbb{C}$, $\mathbb{R}$ 'nin bir cisim genişlemesidir.

2.6 Teorem (Kronecker) F bir cisim ve $f(x) \in F[x]$ sabit olmayan bir polinom olsun. Bu durumda, $f(x)$ 'in bir kökünü içeren F 'nin bir E cisim genişlemesi vardır.

2.7 Örnek $x^2 - 2 \in \mathbb{Q}[x]$ polinomunu ele alalım.

$x^2 - 2 = 0$ ise $x = \pm\sqrt{2} \notin \mathbb{Q}$ olduğundan $x^2 - 2$ polinomunun $\mathbb{Q}$ 'da kökü yoktur. Fakat $\mathbb{R}$ 'de iki tane kökü vardır. Benzer şekilde, $x^2 + 1 \in \mathbb{R}[x]$ polinomunu ele alalım.

$x^2 + 1 = 0$ ise $x = \pm i \notin \mathbb{R}$ olduğundan $x^2 + 1$ polinomunun $\mathbb{R}$ 'de kökü yoktur. Fakat $\mathbb{C}$ 'de iki tane kökü vardır.

2.8 Tanım F bir cisim ve E , F 'nin bir cisim genişlemesi olsun. Bir $\alpha \in E$ için eğer $f(\alpha) = 0$ olacak şekilde bir $0 \neq f(x) \in F[x]$ polinomu varsa α 'ya F üzerinde *cebirsel* denir. Eğer α cebirsel bir eleman değilse, α 'ya bir *transandant (aşkın) eleman* denir.

2.9 Tanım E , F 'nin bir cisim genişlemesi olsun. Eğer her $\alpha \in E$, F üzerinde cebirsel ise E 'ye F 'nin bir *cebirsel genişlemesi* denir.

2.10 Örnek (i) $\mathbb{C}$, $\mathbb{R}$ 'nin bir cebirsel genişlemesidir. Çünkü her $a + bi \in \mathbb{C}$ elemanı $x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$ polinomunun bir köküdür.

(ii) $\mathbb{R}$, $\mathbb{Q}$ 'nun bir cebirsel genişlemesi değildir. Çünkü Euler sayısı $e \in \mathbb{R}$, ancak $f(e) = 0$ olacak şekilde bir $f(x) \in \mathbb{Q}[x]$ polinomu yoktur, yani e bir transandant elemandır.

2.11 Teorem E , F 'nin bir cisim genişlemesi olsun. Eğer $\alpha, \beta \in E$ elemanları F üzerinde cebirsel ise,

$$\alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta \quad \text{ve} \quad \frac{\alpha}{\beta} \quad (\beta \neq 0)$$

elemanları da F üzerinde cebirsel olur.

2.12 Tanım E , F 'nin bir cisim genişlemesi olsun. F 'nin E içindeki *cebirsel kapanışı* şu şekilde tanımlanır:

$$\overline{F} := \{\alpha \in E \mid \alpha, F \text{ üzerinde cebirseldir}\}.$$

Teorem 2.11'e göre $\overline{F}$ kümesi bir cisimdir.

2.2 Sonlu Cisimler

Bu bölümde sonlu sayıda elemana sahip cisimlerin bazı temel özellikleri ele alınmaktadır.

2.13 Tanım Sonlu sayıda elemanı olan cisimlere *sonlu cisim* denir.

2.14 Örnek p bir asal sayı olmak üzere $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ bir sonlu cisimdir.

2.15 Örnek $\mathbb{Z}_6$ bir cisim değildir, çünkü $2 \cdot 3 = 6 \equiv 0 \pmod{6}$ olduğundan 2 ve 3 sıfır bölen elemanlarının çarpımsal tersi yoktur.

2.16 Tanım F bir cisim olsun. F cisminin karakteristiği, $p \cdot 1_F = 0_F$ eşitliğini sağlayan en küçük p pozitif tam sayısıdır, burada 1_F , F cisminin çarpma işlemine göre birim elemanını ve 0_F de toplama işlemine göre birim elemanını ifade eder. Eğer böyle bir p bulunmuyorsa, cismin karakteristiği 0 olarak tanımlanır.

2.17 Örnek (i) $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ cisimlerinde $p \cdot 1 = 0$ eşitliğini sağlayan bir p pozitif tam sayısı bulunmadığından, bu cisimlerin karakteristiği 0'dır.

(ii) p asal sayı olmak üzere, $\mathbb{Z}_p$ cisminin karakteristiği p 'dir.

2.18 Teorem [1, Theorem 3.3.3] p bir asal sayı ve $0 \neq n \in \mathbb{N}$ olmak üzere eleman sayısı $q = p^n$ olan bir sonlu cisim vardır. Bu cisim $\mathbb{F}_q$ ile gösterilir. Özellikle $n = 1$ durumunda, yani $q = p$ için, elde edilen sonlu cisim $\mathbb{F}_p$ olup bu yapı $\mathbb{Z}_p$ ile özdeştir.

2.19 Tanım Bir $\alpha \in \mathbb{F}_q$ için $\mathbb{F}_q = \{0, \alpha, \alpha^2, \dots, \alpha^{q-1}\}$ yazılabiliyorsa, α elemanına $\mathbb{F}_q$ cisminin bir *ilkel elemanı* denir.

2.20 Yardımcı Önerme [1, Lemma 3.3.1] Her $\beta \in \mathbb{F}_q$ için $\beta^q = \beta$ olur.

İspat: $\beta = 0$ için durum açıktır. $\beta \neq 0$ olsun. $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} = \{\beta_1, \dots, \beta_{q-1}\}$ olarak yazalım. Buna göre $\mathbb{F}_q^* = \{\beta\beta_1, \dots, \beta\beta_{q-1}\}$ şeklinde yazılabilir. Dolayısıyla

$$\beta_1 \cdots \beta_{q-1} = \beta\beta_1 \cdots \beta\beta_{q-1} = \beta^{q-1} \beta_1 \cdots \beta_{q-1},$$

yani $\beta^{q-1} = 1$ elde edilir. Bu yüzden $\beta^q = \beta$ olur.

□

2.21 Tanım Bir cisim üzerinde tanımlı indirgenemez bir polinomun, cismin cebirsel kapanışı içerisinde katlı köke sahip olmaması, başka bir ifadeyle tüm köklerinin birbirinden farklı olması durumunda bu polinoma *ayrılabilir polinom* denir.

2.22 Tanım Bir F cismi verildiğinde, eğer her indirgenemez $f(x) \in F[x]$ polinomu ayrılabilir ise F 'ye *mükemmel cisim* denir.

2.23 Örnek Karakteristiği 0 olan her cisim mükemmeldir.

F bir cisim ve karakteristiği p olsun. F 'nin mükemmel olması için gerek ve yeter şart $F = F^p$ olmasıdır. Burada $F^p = \{a^p \mid a \in F\}$ şeklindedir yani her eleman, bir elemanın p -inci kuvveti olarak yazılabilmelidir. Dolayısıyla her sonlu cisim mükemmeldir. Ancak $F_p(x)$ cismi mükemmel değildir çünkü x 'in p -inci kökü bu cisimde bulunamaz.

2.24 Tanım p bir asal sayı ve $n \geq 1$ bir tam sayı olmak üzere $\mathbb{F}_{p^n}$ sonlu cismi $\mathbb{Z}_p[x]$ 'deki $x^{p^n} - x$ polinomunun tüm köklerini içeren en küçük cisim olarak inşa edilebilir ve eğer n, m 'yi bölerse, $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ elde edilir (bkz. [1]). Böylece aşağıdaki sonsuz zincir ortaya çıkar:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3} \subseteq \cdots \subseteq \mathbb{F}_{p^n} \subseteq \cdots$$

Dolayısıyla,

$$\mathbb{F}_{p^\infty} := \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$$

şeklinde tanımlanır. $\mathbb{F}_{p^\infty}$ 'un karakteristiği p olan cebirsel olarak kapalı bir cisim olduğu iyi bilinmektedir. Ayrıca her $n \geq 1$ için $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^\infty}$ geçerlidir. Dolayısıyla $\mathbb{F}_{p^\infty}$ her $\mathbb{F}_{p^n}$ 'nin cebirsel kapanışını oluşturur.

2.3 Lineer Kodlar

Kodlama teorisinde önemli bir role sahip olan lineer kodlarla ilgili temel bilgiler bu bölümde sunulmaktadır.

Boştan farklı herhangi bir sonlu kümeye *alfabe* denilmektedir.

2.25 Tanım $n \geq 1$ bir tam sayı olmak üzere, $\mathbb{F}_q^n$ 'nin bir $\mathbb{F}_q$ -alt vektör uzayına alfabeti $\mathbb{F}_q$ ve uzunluğu n olan bir *lineer kod* denir. Bir kodun elemanlarına *kod sözcükleri* denir.

2.26 Tanım $C, \mathbb{F}_q$ üzerinde bir lineer kod olsun. $B = \{v_1, v_2, \dots, v_k\}$, C 'nin boş olmayan bir altkümesi olsun. Eğer $C = \langle B \rangle$, yani C 'deki her eleman B 'deki elemanların bir lineer kombinasyonu şeklinde yazılabiliyorsa ve B 'deki elemanlar $\mathbb{F}_q$ üzerinde lineer bağımsız ise, B kümesine C 'nin bir *bazı* (*tabanı*) denir.

2.27 Tanım $\mathbb{F}_q$ sonlu cismi üzerindeki bir C lineer kodunun birçok bazı olabilir; ancak tüm bazlar aynı sayıda eleman içerir. Bu sayıya C 'nin $\mathbb{F}_q$ üzerindeki *boyutu* denir ve

$$k(C) := \text{boy}(C)$$

ile gösterilir.

2.28 Örnek $C = \{0000, 1100, 0011, 1111\} \subseteq \mathbb{F}_2^4$ kümesi, $\mathbb{F}_2$ üzerinde tanımlı bir lineer koddur. Şimdi bu kodun bir tabanını belirleyelim. $B = \{1100, 0011\}$ kümesinin C için uygun bir taban olduğunu gösterelim:

(i) 1111 sözcüğü, 1100 ile 0011'in (vektörel) toplamı olarak elde edilir.

(ii) $a_1, a_2 \in \mathbb{F}_2$ için

$$a_1 \cdot (1100) + a_2 \cdot (0011) = 0000 \text{ ise } a_1 = a_2 = 0$$

eşitliği sağlanır.

Bu sonuç, 1100 ve 0011 sözcüklerinin lineer bağımsız olduğunu gösterir. Dolayısıyla B , C 'nin bir tabanıdır. Tabanın eleman sayısı boyutu verdiği için $\text{boy}(C) = 2$ bulunur.

2.29 Tanım $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n) \in \mathbb{F}_q^n$ olmak üzere a ve b arasındaki *Hamming mesafesi (uzaklığı)*,

$$d(a, b) := |\{i \mid a_i \neq b_i, \text{ her } i \in \{1, \dots, n\}\}|$$

olarak tanımlanır.

Eğer $C \subseteq \mathbb{F}_q^n$ bir lineer kod ve $a, b \in C$ ise $a - b \in C$ ve $d(a, b) = d(a - b, 0)$ eşitliği açıkça sağlanmaktadır, burada $0, \mathbb{F}_q^n$ 'deki sıfır vektörüdür.

2.30 Tanım $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ olmak üzere, x sözcüğünde sıfırdan farklı olan bileşenlerin toplam sayısına x 'in *Hamming ağırlığı* denir ve $wt(x)$ ile gösterilir, yani

$$wt(x) := |\{i \mid x_i \neq 0, 1 \leq i \leq n\}|.$$

Başka bir ifadeyle, Hamming ağırlığı bir kod sözcüğündeki sıfır olmayan koordinatların sayısını ifade eder.

2.31 Tanım Bir C lineer kodun *minimum mesafesi*

$$d(C) := \min\{d(a, b) \mid a, b \in C, a \neq b\}$$

olarak tanımlanır.

2.32 Örnek $C = \{0000, 1100, 0011, 1111\} \subseteq \mathbb{F}_2^4$ lineer kodunu ele alalım. Bu kodun minimum mesafesini bulalım. Bunun için ilk olarak kod sözcükleri arasındaki Hamming mesafeyi hesaplayalım:

$$d(0000, 1100) = 2, \quad d(0000, 0011) = 2, \quad d(0000, 1111) = 4$$

$$d(1100, 0011) = 4, \quad d(1100, 1111) = 2, \quad d(0011, 1111) = 2$$

Dolayısıyla $d(C) = 2$ dir.

2.33 Teorem [1, Theorem 4.3.8] $\mathbb{F}_q$ üzerinde bir tanımlı herhangi bir C lineer kodu için $d(C) = wt(C)$ 'dir.

Minimum uzaklığın önemi, kodun hata düzeltme kapasitesiyle olan ilişkisine dayanır. Bir göndericinin C koduna ait bir kod sözcüğü olan a 'yı bir kanal aracılığıyla (örneğin iki bilgisayar veya bir cep telefonu ile yakındaki bir anten arasındaki iletişimde olduğu gibi) ilettiğini varsayalım. Genellikle kanal "gürültülüdür" yani kod sözcüğündeki bazı girdileri değiştirir. Kanalin en fazla t tane girdiyi değiştirdiğini ve $t \leq \frac{d(C) - 1}{2}$ olduğunu varsayalım. Alıcı kodu bildiğinden a değişmişse a' nün bir kod sözcüğü olmadığını görecektir, çünkü $0 < d(a, a') \leq t < d(C)$. Aslında tüm kod sözcükleri arasında sadece a 'nın $d(a, a') \leq t$ koşulunu sağladığı gösterilebilir. Bu nedenle alıcı, gönderilen kod sözcüğünün a olduğunu kesin olarak belirleyebilir. Bir kodun $k(C)$ boyutu önemlidir çünkü kodun ne kadar bilgi taşıyabileceğinin bir ölçüsüdür; bu durumda kod sözcüklerinin sayısı q^k dir. Kodun uzunluğu olan n büyüdükçe, her bir kod sözcüğünü iletmek için o kadar enerji harcanması gerekmektedir. İlgili parametreler $k(C)/n$ ve $d(C)/n$, bir kodun performans analizinde ortaya çıkan ve farklı kodlarla karşılaştırılmak istenildiğinde önemli bir rol oynayan temel değişmezlerdir. İdeal bir kod büyük bir boyuta, büyük bir minimum mesafeye sahip olurdu ancak bu gereksinimler aynı anda karşılanamaz. Aslında bu parametreler arasındaki temel bir ilişki,

$$k(C) + d(C) \leq n + 1$$

olduğunu belirten "Singleton eşitsizliği" olarak adlandırılan ilişkidir [3].

2.34 Tanım Bir $C \subseteq \mathbb{F}_q^n$ lineer kodunun *dual kodu* aşağıdaki biçimde tanımlanır:

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

Burada $C^\perp$, C 'ye dik olan tüm vektörlerden oluşan altuzayı temsil eder ve $\langle x, c \rangle$ ifadesi standart iç çarpımı belirtmektedir.

2.35 Tanım Bir C lineer kodunun

(i) *üreteç matrisi* G , satırları C 'nin bir bazını oluşturan matristir.

(ii) *eşlik-denetim matrisi* H , dual kod $C^\perp$ 'nin üreteç matrisi olarak tanımlanır.

$C, \mathbb{F}_q$ üzerinde bir $[n, k]$ -doğrusal kodu ve G, C 'nin bir üreteç matrisi olsun. Buna göre $\mathbf{v} \in \mathbb{F}_q^n$ elemanı $C^\perp$ içindedir ancak ve ancak $\mathbf{v}, G$ 'nin her satırına diktir. Özel olarak, $(n - k) \times n$ boyutlu bir H matrisi verildiğinde, H, C 'nin bir eşlik-denetim matrisidir ancak ve ancak H 'nin satırları doğrusal bağımsızdır ve $HG^T = 0$ koşulunu sağlar (bkz. [1]).

C bir doğrusal kod ve H, C 'nin bir eşlik-denetim matrisi olsun. Buna göre aşağıdakiler denktir:

(i) $d(C) = d$

(ii) H 'nin herhangi $d - 1$ adet sütunu doğrusal bağımsızdır ve H 'nin d adet doğrusal bağımlı sütunu vardır. (bkz. [1]).

3. Gröbner Tabanlar

Bu bölümde çok değişkenli polinom halkalarında ideallerin yapısını anlamak için kullanılan Gröbner tabanları ayrıntılı olarak ele alınmaktadır. Gröbner tabanları, polinomların bölünebilirlik özelliklerini düzenli bir biçimde ortaya koyarak cebirsel problemlerin çözümünde sistematik bir yöntem sunar. Tek terimliler üzerinde tanımlanan farklı sıralama yöntemleri sayesinde ideallerin yapısı daha açık bir şekilde incelenebilmekte, bu sıralamalar aracılığıyla polinomların karşılaştırılması ve düzenlenmesi mümkün hale gelmektedir.

Buchberger algoritması yardımıyla herhangi bir ideal için Gröbner tabanı elde edilebilmekte, böylece ideallerin yapısı üzerinde daha derinlemesine analiz yapılabilmektedir. Ayrıca Hilbert Baz Teoremi ve Nullstellensatz gibi temel sonuçlar sunulmaktadır. Özellikle, bir sonraki bölümlerde önemli bir role sahip olan ayak izi (footprint) kavramı ile ideallerin yapısı arasındaki ilişki ele alınmaktadır. Bu bağlamda, Gröbner tabanları hem teorik hem de uygulamalı açıdan cebirsel problemlerin çözümünde güçlü bir yöntem olarak ortaya çıkmaktadır. Bu bölümdeki temel bilgiler genel olarak [3] kaynağı kullanılarak derlenmektedir.

Aksi belirtilmedikçe tez boyunca F ile herhangi bir cisim gösterilecektir.

3.1 Tanım $(R, +, \cdot)$ bir değişmeli halka $\{0\} \neq I \subseteq R$ olsun. Eğer,

(i) her $a, b \in I$ için $a - b \in I$,

(ii) her $a \in I$ ve $r \in R$ için $r \cdot a \in I$

ise I 'ya R 'nin bir *ideali* denir.

3.2 Örnek Herhangi bir $p(x) \in F[x]$ polinomu için $I = \langle p(x) \rangle = \{r(x) \cdot p(x) \mid r(x) \in F(x)\}$ bir idealdir.

3.3 Tanım R bir halka ve I , R 'nin bir ideali olsun. Bu durumda I ideali kullanılarak tanımlanan denklik sınıflarının oluşturduğu küme *bölüm halkası* olarak tanımlanır ve R/I ile gösterilir, yani

$$R/I := \{a + I \mid a \in R\}$$

şeklinde ifade edilir. Buradaki her $a + I$ elemanı bir *koset* (*coset*) ifade eder. Bölüm halkası üzerinde cebirsel işlemler temsilciler üzerinden doğal biçimde tanımlanır:

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = ab + I.$$

I bir ideal olduğu için bu işlemler temsilci seçiminden bağımsızdır ve R/I kümesi bu işlemler altında bir halka yapısı oluşturur.

3.4 Örnek $f(x) = x^2 + 1 \in \mathbb{R}[x]$ indirgenemez bir polinom olsun ve $I = \langle f(x) \rangle$ idealini ele alalım. Bu durumda bölüm halkası $\mathbb{R}[x]/I$ bir cisimdir. Bölüm halkasında $\alpha = x + I$ elemanını alalım:

$$\alpha^2 + 1 = (x + I)^2 + 1 = (x^2 + I) + 1 = (x^2 + 1) + I = 0_{\mathbb{R}[x]/I}$$

elde edilir. Dolayısıyla $\alpha^2 = -1$ olur.

Bu özellik, kompleks sayılardaki i elemanının ($i^2 = -1$) özelliği ile aynıdır. Dolayısıyla her $a + bx \in \mathbb{R}[x]$ için bölümdeki karşılık $a + b\alpha$ olup, $\mathbb{C}$ 'nin bir elemanına

$$a + b\alpha \xrightarrow{\gamma} a + bi \in \mathbb{C}$$

şeklinde eşlenebilir. Bu eşleme, toplama ve çarpma işlemlerini koruyan, birebir ve örten bir homomorfizmdir. Sonuç olarak

$$\mathbb{R}[x]/\langle I \rangle \cong \mathbb{C}$$

izomorfizması elde edilir.

Tez boyunca $\mathbb{N}_0$ negatif olmayan tam sayılar kümesi ve $F^* = F \setminus \{0\}$ olarak kullanılacaktır. Ayrıca $F[x_1, \dots, x_n]$ çok değişkenli (n değişkenli) polinom halkası ele alınacaktır.

3.5 Tanım $a \in F^*$ ve $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{N}_0$ olmak üzere

$$a \cdot x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \cdots x_n^{\alpha_n}$$

çarpımına bir *terim* denir.

$$x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \cdots x_n^{\alpha_n}$$

çarpımına ise bir *tek terimli* denir.

Kısaca, $x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \cdots x_n^{\alpha_n} = X^\alpha$, $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}_0^n$ ile de gösterilebilir. Böylelikle $F[\mathbf{X}] = F[x_1, \dots, x_n]$ olarak alınabilir.

3.6 Örnek $F[x, y, z]$ halkasında $x^2 y z^2$ ve $x^3 y z$ birer tek terimlidir.

3.7 Örnek $F[x, y]$ halkasında $5xy^2$ ve $2xy$ birer terimdir.

3.8 Tanım Elemanları n değişkenli tüm tek terimliler olan kümeyi $\mathcal{M}$ ile göstereceğiz:

$$\mathcal{M} := \{X^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \cdots x_n^{\alpha_n} \mid \alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}_0^n\} \subseteq F[\mathbf{X}].$$

Herhangi bir $f \in F[\mathbf{X}]$ polinomunun, $i = 1, 2, \dots, k$ için $a_i \in F$ ve $M_i \in \mathcal{M}$ olmak üzere

$$f = a_1 M_1 + a_2 M_2 + \cdots + a_k M_k$$

şeklinde yazılabildiği açıktır.

3.9 Örnek $f = 2xy^3 + 5xyz^2 + 3z^7 \in F[x, y, z]$ alalım. Burada $a_1 = 2$, $a_2 = 5$, $a_3 = 3$ ve $M_1 = xy^3$, $M_2 = xyz^2$, $M_3 = z^7$ dir.

3.10 Tanım $\mathcal{M}$ üzerinde $\leq$ sıralaması, eğer

(i) her $\alpha, \beta, \gamma \in \mathbb{N}_0^n$ için $X^\alpha \leq X^\beta$ ise $X^{\alpha+\gamma} \leq X^{\beta+\gamma}$ ve

(ii) Herhangi bir $\{0\} \neq \mathcal{A} \subset \mathcal{M}$ kümesinin bir en küçük elemanı vardır

koşullarını sağlıyor ise bu sıralamaya bir *tek terimli sıralaması* denir.

3.11 Tanım $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}_0^n$, $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}_0^n$ olmak üzere

$X^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \dots x_n^{\alpha_n}$ ve $X^\beta = x_1^{\beta_1} x_2^{\beta_2} x_3^{\beta_3} \dots x_n^{\beta_n}$ tek terimlilerini alalım. Eğer $\alpha = \beta$ veya $\beta - \alpha$ farkında, soldan sıfır olmayan ilk eleman pozitif ise $X^\alpha \leq X^\beta$ şeklinde tanımlanan $\leq$ tekterimli sıralamasına *lex sıralaması* denir.

3.12 Örnek $F[\mathbf{X}]$ 'de $X^\alpha = x_1$ ve $X^\beta = x_2^{1000}$ elemanlarını alalım. Lex sıralamasına göre karşılaştırma yaparsak

$X^\alpha = x_1 = x_1^1 x_2^0 \dots x_n^0$ dir. Burada $\alpha = (1, 0, \dots, 0)$ dir.

$X^\beta = x_2^{1000} = x_1^0 x_2^{1000} \dots x_n^0$ dir. Burada $\beta = (0, 1000, 0, \dots, 0)$ dir.

$\alpha - \beta = (1, 0, \dots, 0) - (0, 1000, \dots, 0) = (1 - 0, 0 - 1000, \dots, 0 - 0) = (1, -1000, \dots, 0)$ elde edilir. Soldan sıfır olmayan ilk eleman 1 ve pozitif olduğundan $x_1 \geq_{lex} x_2^{1000}$ elde edilir.

3.13 Tanım $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}_0^n$, $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}_0^n$ olmak üzere

$X^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \dots x_n^{\alpha_n}$ ve $X^\beta = x_1^{\beta_1} x_2^{\beta_2} x_3^{\beta_3} \dots x_n^{\beta_n}$ tek terimlilerini alalım.

$|\alpha| = \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i = |\beta|$ veya $|\alpha| = \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i = |\beta|$ iken $X^\alpha \leq_{lex} X^\beta$ oluyor ise $\leq$ sıralamasına *grlex* sıralaması denir ve $X^\alpha \leq_{grlex} X^\beta$ ile gösterilir.

3.14 Örnek $F[\mathbf{X}] = F[x_1, x_2, x_3]$ olmak üzere $X^\alpha = x_1 x_2^3 x_3$ ve $X^\beta = x_1^2 x_2 x_3^2$ olsun.

Grlex sıralamasına göre bu iki elemanın karşılaştırmasını yapalım. Burada,

$\alpha = (1, 3, 1)$, $|\alpha| = 1 + 3 + 1 = 5$ ve $\beta = (2, 1, 2)$, $|\beta| = 2 + 1 + 2 = 5$ dir.

$\beta - \alpha = (2, 1, 2) - (1, 3, 1) = (2 - 1, 1 - 3, 2 - 1) = (1, -2, 1)$ elde edilir. Soldan sıfır olmayan ilk eleman 1 ve pozitif olduğundan $X^\alpha \leq_{grlex} X^\beta$ olur.

3.15 Tanım $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}_0^n, \beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}_0^n$ olmak üzere

$X^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \dots x_n^{\alpha_n}$ ve $X^\beta = x_1^{\beta_1} x_2^{\beta_2} x_3^{\beta_3} \dots x_n^{\beta_n}$ tek terimlilerini alalım.

Eğer, $|\alpha| = \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i = |\beta|$ veya $|\alpha| = \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i = |\beta|$ iken $\beta - \alpha$ farkında sağdan sıfır olmayan ilk eleman negatif ise $\leq$ sıralamasına *grevlex sıralaması* denir ve $X^\alpha \leq_{grevlex} X^\beta$ ile gösterilir.

3.16 Örnek $F[X] = F[x_1, x_2, x_3]$ olmak üzere $X^\alpha = x_1^2 x_2 x_3^2$ ve $X^\beta = x_1 x_2^3 x_3$ olsun.

Grevlex sıralamasına göre karşılaştırma yapalım.

$\alpha = (2, 1, 2), |\alpha| = 2 + 1 + 2 = 5$ ve $\beta = (1, 3, 1), |\beta| = 1 + 3 + 1 = 5$ dir.

$\beta - \alpha = (1, 3, 1) - (2, 1, 2) = (1 - 2, 3 - 1, 1 - 2) = (-1, 2, -1)$ elde edilir. Sağdan sıfır olmayan ilk eleman -1 ve negatif olduğundan $X^\beta \geq_{grevlex} X^\alpha$ olur.

3.17 Tanım Her $i = 1, 2, \dots, m$ için $0 \neq a_i \in F, M_i \in \mathcal{M}$ olmak üzere

$0 \neq f = \sum_{i=1}^m a_i M_i \in F[X]$ polinomu ve " $\leq$ ", $\mathcal{M}$ üzerinde bir tek terimli sıralaması olsun. f polinomunun " $\leq$ " sıralamasına göre *baş tek terimlisi*,

$M_l = \max\{M_i \mid i = 1, 2, \dots, m\}$, *baş tek terimlisinin katsayısı* a_l ve *baş terimi* $a_l M_l$ dir.

Kısaca,

$$lm(f) := M_l, lc(f) := a_l, lt(f) := a_l M_l$$

ile gösterilir.

3.18 Örnek $f(x_1, x_2, x_3) = 4x_1^3 x_2^4 + 5x_1 x_3^8 + 2$ ise lex sıralamasına göre $lt(f), lc(f)$ ve $lm(f)$ bulalım. Öncelikle M_1 ve M_2 'yi karşılaştıralım.

$M_1 = x_1^3 x_2^4, \alpha = (3, 4, 0)$ ve $M_2 = x_1 x_3^8, \beta = (1, 0, 8)$ dir. $\alpha - \beta = (3, 4, 0) - (1, 0, 8) = (2, 4, -8)$ farkında soldan sıfır olmayan ilk eleman 2 ve pozitiftir. Dolayısıyla $M_1 \geq_{lex} M_2$ olur.

Şimdi de M_2 ile M_3 'ü karşılaştıralım.

$M_3 = x^0, \gamma = (0, 0, 0)$ olduğundan $\beta - \gamma = (1, 0, 8)$ farkında soldan sıfır olmayan ilk eleman 1 ve pozitiftir. Dolayısıyla $M_1 \geq_{lex} M_2 \geq_{lex} M_3$ elde edilir. Buradan $lc(f) = 4$, $lm(f) = x_1^3 x_2^4$ ve $lt(f) = 4x_1^3 x_2^4$ olarak bulunur.

Burada not edelim ki Gröbner baz teorisindeki en önemli prosedürlerden biri bir polinomun sıfırdan farklı polinomlar ile bölünebilmesidir.

3.19 Tanım [3, Definition 2.4] Herhangi bir " $\leq$ " tek terimli sıralamasına göre bir $f \in F[\mathbf{X}]$ polinomunun $\{g_1, \dots, g_t\} \subseteq F[\mathbf{X}] \setminus \{0\}$ kümesine göre bölünebilmesi demek $F[\mathbf{X}]$ 'te $q_1, \dots, q_t$ bölüm polinomları ile r kalanının bulunmasıdır öyle ki

$$f = q_1 \cdot g_1 + q_2 \cdot g_2 + \dots + q_t \cdot g_t + r$$

eşitliği geçerlidir ve $r = 0$ veya r 'de her $i = \{1, \dots, t\}$ için $lm(g_i)$ ' nin bir katı olan tek terimli bulunamaz.

3.20 Örnek $f = x^2y + xy^2 + y^2 \in \mathbb{R}[x, y]$ polinomunu ve $\{xy - 1, y^2 - 1\} \subset \mathbb{R}[x, y]$ listesini ele alalım. " $\leq$ " sıralaması lex olsun. $lm(f)$ bulalım. $M_1 = x^2y$, $M_2 = xy^2$ ve $M_3 = y^2$ dir. Öncelikle M_1 ve M_2 'yi karşılaştıralım.

$\alpha = (2, 1)$ ve $\beta = (1, 2)$ dir. $\alpha - \beta = (1, -1)$ soldan sıfır olmayan ilk eleman 1 pozitif olduğundan $M_1 \geq_{lex} M_2$ olur. Bu işlemleri M_1 ve M_3 'e uyguladığımızda $M_1 \geq_{lex} M_3$ elde edilir. Buradan $lm(f) = x^2y$ bulunur. Şimdi aldığımız listede $g_1 = xy - 1$ ve $g_2 = y^2 - 1$ olsun. $lm(g_1)$ ve $lm(g_2)$ bulalım. Bunun için de aynı işlemleri uygulayarak açıkça $lm(g_1) = xy$ ve $lm(g_2) = y^2$ bulunabilir. Şimdi bölme algoritmasını uygulayalım:

$$\begin{array}{r|l} x^2y + xy^2 + y^2 & xy - 1 \\ - (x^2y - x) & x + y \\ \hline xy^2 + y^2 + x & \\ - (xy^2 - y) & \\ \hline y^2 + y + x & \end{array}$$

Dolayısıyla, $f = (x + y) \cdot g_1 + (x + y + y^2)$ şeklinde yazılabilir. Kalan polinom $y^2 + y + x$, g_2 'ye bölünürse $f = (x + y) \cdot g_1 + (y^2 + y) + x$ olur.

$$\begin{array}{r|l} y^2 + y + x & y^2 - 1 \\ - (y^2 - 1) & 1 \\ \hline y + x + 1 & \end{array}$$

Kalan polinomun baş terimi olan y , hem xy hem de y^2 'nin katı şeklinde yazılamaz. Buradan $f = (x + y) \cdot g_1 + 1 \cdot g_2 + (x + y + 1)$ olup $q_1 = x + y$, $q_2 = 1$ ve $r = x + y + 1$ elde edilir.

3.21 Teorem [4, Theorem 4] (*Hilbert Baz Teoremi*) $I, F[\mathbf{X}]$ polinom halkasında bir ideal olsun. Bu durumda öyle $f_1, f_2, \dots, f_k \in I$ vardır ki

$$I = \langle f_1, f_2, \dots, f_k \rangle$$

Başka bir deyişle, I ideali sonlu eleman tarafından üretilir. (Yani $F[x_1, \dots, x_n]$ bir Noether halkasıdır.)

3.22 Örnek $I = \langle x \rangle \subset F[x, y]$ alalım.

$$F[x, y]/I = F[x, y]/\langle x \rangle \cong F[y]$$

elde edilir. $F[y]$ 'nin bir bazı $\{1, y, y^2, y^3, \dots\}$ sonsuz elemanlı bir kümedir.

3.23 Tanım $0 \neq I \subset F[\mathbf{X}]$ bir ideal, $\mathcal{M}$, tek terimliler kümesi ve " $\leq$ " tek terimli sıralaması olsun. Eğer, her $0 \neq f \in I$ için $lm(f)$, bir $i = 1, \dots, s$ için $lm(g_i)$ 'nin bir katı oluyorsa, $\{g_1, g_2, \dots, g_s\} \subset I$ kümesi " $\leq$ " sıralamasına göre I ideali için bir *Gröbner bazıdır*, denir.

3.24 Örnek $I = \langle xy - 1, y^2 - 1 \rangle \subset \mathbb{R}[x, y]$ olsun ve " $\leq$ " lex sıralaması alalım.

$$y(xy - 1) - x(y^2 - 1) = -y + x = f \in I$$

$lm(f) = x$ ve $g_1 = xy - 1$, $g_2 = y^2 - 1$ olmak üzere x 'i, $lm(g_1)$ ve $lm(g_2)$ 'nin bir katı şeklinde yazılamadığından $\{xy - 1, y^2 - 1\}$ kümesi I için bir Gröbner baz olamaz.

I ideali için bir Gröbner baz, aynı zamanda ideal için bir bazdır. Şimdi bunu kanıtlayalım.

3.25 Yardımcı Önerme [3, Lemma 2.7] $\{g_1, \dots, g_s\} \subset I$, I için bir Gröbner baz olsun. Bu durumda, $f \in I$ ancak ve ancak f 'nin $\{g_1, \dots, g_s\}$ ile bölümünden kalan sıfırdır. Sonuç olarak, $I = \langle g_1, g_2, \dots, g_s \rangle$ tarafından üretilir.

İspat: Öncelikle, f 'nin $\{g_1, \dots, g_s\}$ ile bölümünden kalan $r = 0$ olduğunu varsayalım. O halde $f = q_1 \cdot g_1 + q_2 \cdot g_2 + \dots + q_s \cdot g_s \in \langle g_1, g_2, \dots, g_s \rangle \subseteq I$ olur.

Şimdi de $f \in I$ olduğunu varsayalım. f 'nin $\{g_1, \dots, g_s\}$ ile bölme algoritmasını uygularsak $f = q_1 \cdot g_1 + q_2 \cdot g_2 + \dots + q_s \cdot g_s + r = \sum_{i=1}^s q_i \cdot g_i + r$ eşitliğinden $r = f - \sum_{i=1}^s q_i \cdot g_i \in I$ elde edilir. Dolayısıyla $r = 0$ olmalıdır, aksi durumda, yani $r \neq 0$ ise, bölme algoritmasından $lm(r)$, her $i = 1, \dots, s$ için $lm(g_i)$ 'lerin bir katı olmayan bir polinom olur. Fakat $\{g_1, \dots, g_s\}$, I için bir Gröbner baz olduğundan bu bir çelişkidir.

$\langle g_1, g_2, \dots, g_s \rangle \subseteq I$ olduğunu biliyoruz. Sonuç olarak $I \subseteq \langle g_1, g_2, \dots, g_s \rangle$ olduğundan $I = \langle g_1, g_2, \dots, g_s \rangle$ elde edilir.

□

3.26 Önerme [3, Proposition 2.8] $\{g_1, \dots, g_s\}$, I için bir Gröbner baz olsun. $f \in F[\mathbf{X}]$ polinomunun $\{g_1, \dots, g_s\}$ ile bölümünden kalan, sıralamaya bakılmaksızın aynıdır.

İspat: Diyelim ki $f = q_1 \cdot g_1 + q_2 \cdot g_2 + \dots + q_s \cdot g_s + r$ ve $f = \tilde{q}_1 \cdot g_1 + \tilde{q}_2 \cdot g_2 + \dots + \tilde{q}_s \cdot g_s + \tilde{r}$ öyle ki $q_i, \tilde{q}_i \in F[\mathbf{X}]$ her $i = 1, \dots, s$ için $r, \tilde{r} \in F[\mathbf{X}]$ olmak üzere r 'de ve $\tilde{r}$ 'de her $i = 1, \dots, s$ için $lm(g_i)$ 'lerin katı olan tek terimli yoktur. O halde

$r - \tilde{r} = (\tilde{q}_1 - q_1) \cdot g_1 + \dots + (\tilde{q}_s - q_s) \cdot g_s \in \langle g_1, \dots, g_s \rangle = I$. Yardımcı Önerme 3.25'ten $r - \tilde{r} = 0$ yani $r = \tilde{r}$ elde edilir.

□

Buchberger, I ideali için herhangi bir sonlu üretilmiş bazdan başlayarak, bir dizi adımla, genişletilmiş baz Gröbner baz olana kadar devam eden bir algoritma verir. Şimdi de bu algoritmadan bahsedelim [?].

3.27 Tanım $f, g \in F[\mathbf{X}] \setminus \{0\}$ olsun. $lt(f) = a \cdot X^\alpha$, $\alpha = (\alpha_1, \dots, \alpha_n)$ ve $lt(g) = b \cdot X^\beta$, $\beta = (\beta_1, \dots, \beta_n)$ olmak üzere $\gamma_i = \max\{\alpha_i, \beta_i\}$, her $i = 1, \dots, n$ $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{N}_0^n$ alalım. f ve g polinomlarının S -polinomu,

$$S(f, g) = \left(\frac{X^\gamma}{lt(f)} \right) \cdot f - \left(\frac{X^\gamma}{lt(g)} \right) \cdot g$$

ile bulunur.

Buchberger, $\{g_1, \dots, g_s\}$ kümesinin bir Gröbner bazını oluşturmasının ancak ve ancak her i, j için $S(g_i, g_j)$ polinomunun $\{g_1, \dots, g_s\}$ kümesiyle yapılan bölme işleminden kalanının sıfır olması durumunda geçerli olduğunu göstermiştir.

$I = \langle g_1, \dots, g_s \rangle$ ve $i \neq j$, $i, j \in \{1, \dots, s\}$ için $S(g_i, g_j)$ -polinomunun, $\{g_1, \dots, g_s\}$ ile bölümünden kalan $R_{ij} \neq 0$ olursa, $g_{s+1} = R_{ij} \in I$ olduğundan $I = \langle g_1, \dots, g_{s+1} \rangle$ olur. Her $i \neq j$, $i, j \in \{1, \dots, s, s+1\}$ için $S(g_i, g_j)$ 'lerin $\{g_1, \dots, g_{s+1}\}$ ile bölümünden kalan sıfır ise $\{g_1, \dots, g_{s+1}\}$, I için bir Gröbner bazdır denir. Aksi durumda $g_{s+2} = R_{ij}$ olarak tanımlanır ve $\{g_1, \dots, g_s, g_{s+1}, g_{s+2}\}$ göz önüne alınır. Buchberger, sonlu adım sonunda bu prosedürün ürettiği $\{g_1, \dots, g_t\}$ kümesinin I için bir Gröbner baz olduğunu kanıtlamıştır.

3.28 Örnek $\{xy - 1, y^2 - 1\} \subset \mathbb{R}[x, y]$ listesinin $I = \langle xy - 1, y^2 - 1 \rangle$ ideali için bir Gröbner baz olmadığını biliyoruz. " $\leq$ " lex sıralaması alalım ve $x \geq_{lex} y$ olsun. İlk olarak $S(g_1, g_2)$ yi bulalım. $g_1 = xy - 1$ ise $lt(g_1) = xy$ ve $\alpha = (1, 1)$, $g_2 = y^2 - 1$ ise $lt(g_2) = y^2$ ve $\beta = (0, 2)$ olur. $X^\gamma = xy^2$ ve $\gamma = (1, 2)$ olup

$$\begin{aligned} S(g_1, g_2) &= \frac{xy^2}{x} \cdot (xy - 1) - \frac{xy^2}{y^2} \cdot (y^2 - 1) = y \cdot (xy - 1) - x \cdot (y^2 - 1) \\ &= xy^2 - y - xy^2 + x = x - y \end{aligned}$$

bulunur ve $lm(x - y) = x$ dir. Burada x , hem xy ye hem de y^2 ye bölünemediğinden dolayı $S(g_1, g_2) = 0 \cdot g_1 + 0 \cdot g_2 + (x - y)$ olur. Burada kalan 0 olmadığı için kalanı yeni listeye ekleyerek devam edeceğiz. Yeni listemiz $\{g_1, g_2, g_3\} = \{xy - 1, y^2 - 1, x - y\}$ şeklindedir. Şimdi ise $S(g_1, g_3)$ ü bulalım. $g_3 = x - y$ ise $lt(g_3) = x$ ve $\delta = (1, 0)$ olur. $X^\gamma = xy$ ve $\gamma = (1, 1)$ olup

$$S(g_1, g_3) = \frac{xy}{xy} \cdot (xy - 1) - \frac{xy}{x} \cdot (x - y) = xy - 1 - xy + y^2 = y^2 - 1 = g_2$$

bulunur. Bu listenin genişletilmiş listeye göre bölümünden kalan 0 olduğundan yeni bir eleman ekleyemiyoruz. Şimdi de $S(g_2, g_3)$ ü bulalım. $X^\gamma = xy^2$ ve $\gamma(1, 2)$ olup

$$S(g_2, g_3) = \frac{xy^2}{y^2} \cdot (y^2 - 1) - \frac{xy^2}{x} \cdot (x - y) = xy^2 - x - xy^2 + y^3 = -x + y^3$$

bulunur. $lm(-x + y^3) = -x$ dir. Bu $lm(g_3) = x$ e bölünürse kalan $y^3 - y$ olur ve $lm(y^3 - y) = y^3$ olup $lm(g_2)$ ye bölersek kalan 0 bulunur. Buradan $\{xy - 1, y^2 - 1, x - y\}$ listesinin $I = \langle xy - 1, y^2 - 1 \rangle$ ideali için bir Gröbner baz olduğu bulunur.

Şimdi de bu tezde önemli bir rol oynayan Buchberger'in tanımladığı ayak izi (footprint) kavramını ele alalım.

3.29 Tanım $I \subset F[X]$ bir ideal olsun. $\mathcal{M}$ 'deki bir tek terimli sıralamasına göre, I idealinin ayak izi (footprint)

$$\Delta(I) := \{M \in \mathcal{M} \mid M, I\text{'daki herhangi bir polinomun baş tekterimi değildir.}\}$$

olarak tanımlanır.

Bir I idealinin ayak izi, I idealinin Gröbner bazı ile yakından ilişkilidir. (I ve $\Delta(I)$, $\mathcal{M}$ 'de aynı tek terimli sıralamasına göre tanımlı olmalıdır.)

3.30 Önerme [3, Proposition 2.12] $I \subseteq F[X]$ ve $\{g_1, \dots, g_s\}$, I için bir Gröbner baz ve $M \in \mathcal{M}$ olsun. $M \in \Delta(I)$ ancak ve ancak M , her $i = 1, \dots, s$ için $lm(g_i)$ 'lerin bir katı değildir.

İspat: Öncelikle $M \in \Delta(I)$ olduğunu varsayalım. Tanım 3.29'den M , I 'daki hiçbir polinomun baş tekterimlisi olamaz. $\{g_1, \dots, g_s\} \subseteq I$ olduğundan M , $\{g_1, \dots, g_s\}$ 'lerin baş tekterimlisi olamaz.

Şimdi de M , her $i = 1, \dots, s$ için $lm(g_i)$ 'lerin bir katı olmadığını varsayalım. Tanım 3.23'den M , I 'daki hiçbir polinomun baş tekterimlisi olamaz.

□

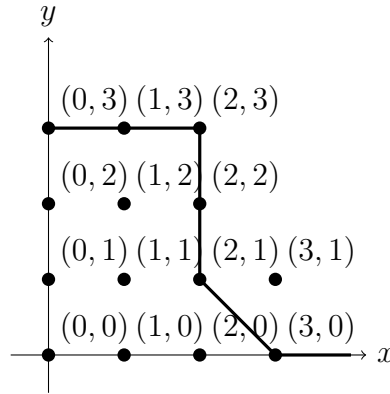
Aşağıdaki örnek ile ayak izinin grafiksel gösteriminin nasıl elde edileceğini gösterelim.

3.31 Örnek $I = \langle x^3 - x, y^3 - y, x^2y - y \rangle \subset \mathbb{R}[x, y]$ olsun. $\mathcal{M}$ üzerinde $\leq_{lex}$ sıralamasını düşünelim. $\{x^3 - x, y^3 - y, x^2y - y\}$ kümesi açıkça I için bir Gröbner bazdır.

$lm(x^3 - x) = x^3, \alpha = (3, 0), lm(y^3 - y) = y^3, \beta = (0, 3)$ ve $lm(x^2y - y) = x^2y, \gamma = (2, 1)$ şeklindedir. Dolayısıyla

$$\Delta(I) = \{x^0y^0, x^1y^0, x^2y^0, x^0y^1, x^1y^1, x^0y^2, x^1y^2\} = \{1, x, x^2, y, xy, y^2, xy^2\}.$$

Bu durumda $\Delta(I)$ 'nin grafiği aşağıdaki gibidir:



Şekil 3.1: $\Delta(I)$ 'nin (ayak izinin) şekli

Çizginin altında kalan noktalar: $\Delta(I)$ 'nin tek terimlileri (I 'daki hiçbir polinomun baş tekterimlisi olamaz.)

Çizginin geçtiği ve üstünde kalan noktalar: I idealinin Gröbner bazının baş tekterimlileri

Aşağıda daha sonra da kullanılacak olan Buchberger'in tezinde elde ettiği önemli bir sonuç verilmektedir.

3.32 Teorem [3, Theorem 2.14] $I \subseteq F[\mathbf{X}]$ olsun. $\mathcal{B} = \{M + I \mid M \in \Delta(I)\}$ kümesi $F[\mathbf{X}]/I$ için bir tabandır.

İspat: $\mathcal{G}$ kümesinin $\Delta(I)$ 'yı belirlemek için kullanılan aynı tek terimli sıralamasına göre, I ideali için bir Gröbner baz olduğunu varsayalım. $f \in F[\mathbf{X}]$ olsun. f 'yi $\mathcal{G}$ 'ye böldüğümüzde r kalanı,

$$r = \sum_{i=1}^t a_i M_i, \quad a_i \in F[\mathbf{X}], \quad M_i \in \Delta(I), \quad i = 1, \dots, t$$

şeklinde elde edilir. Şimdi de $f + I = r + I$ olduğundan $\mathcal{B}$ 'nin $F[\mathbf{X}]/I$ 'yı ürettiğini yani

$\langle (\mathcal{B}) \rangle = F[\mathbf{X}]/I$ olduğunu gösterelim. Öncelikle $\langle (\mathcal{B}) \rangle \subseteq F[\mathbf{X}]/I$ olduğu açıktır. Şimdi de $\langle (\mathcal{B}) \rangle \supseteq F[\mathbf{X}]/I$ olduğunu gösterelim. $f + I \in F[\mathbf{X}]/I$ alalım. $f - r \in I$ olduğundan,

$$f + I = r + I = \sum_{i=1}^t a_i M_i + I = (a_1 M_1 + I) + (a_2 M_2 + I) + \dots + (a_t M_t + I) \in \langle (\mathcal{B}) \rangle.$$

Dolayısıyla $\langle (\mathcal{B}) \rangle = F[\mathbf{X}]/I$ dir.

Şimdi de $\mathcal{B}'$ nin lineer bağımsız olduğunu gösterelim:

$$b_1(M + I) + b_2(M_2 + I) + \dots + b_l M_{l+I} = 0 + I, \quad b_i \in F, \quad M_i \in \Delta(I) \quad i = 1, \dots, l$$

olduğunu varsayalım. O halde

$(b_1 M_1 + b_2 M_2 + \dots + b_l M_l) + I = 0 + I = I$ olduğundan $b_1 M_1 + \dots + b_l M_l = \sum_{i=1}^l b_i M_i \in I$ olur. Fakat her $i = 1, \dots, l$ için $M_i \in \Delta(I)$ olduğundan $b_i = 0$ olmalıdır, aksi durumda $\sum_{i=1}^l b_i M_i \in I$ sıfırdan farklı ve baş tekterimlisi I 'daki herhangi bir polinomun baş tekterimlisi olamaz.

Sonuç olarak $\mathcal{B}, F[\mathbf{X}]/I$ için bir tabandır.

□

3.33 Örnek Örnek 3.31'yle devam edelim. $\{x^3 - x, y^3 - y, x^2 y - y\}$ kümesinin bir Gröbner baz ve $\Delta(I) = \{1, x, x^2, y, xy, y^2, xy^2\}$ olduğunu biliyoruz. Teorem 3.32'den $\mathcal{B} = \{1 + I, x + I, x^2 + I, y + I, xy + I, y^2 + I, xy^2 + I\}$ bir baz olduğundan $\mathbb{R}[x, y]/I$ 'nin boyutu $|\langle (\mathcal{B}) \rangle| = 7$ olur.

3.34 Uyarı $I \subseteq F[\mathbf{X}]$ bir ideal ve $\{f_1, \dots, f_t\}$, I için bir baz olmak üzere

$$\Delta(\text{lm}(f_1), \dots, \text{lm}(f_t)) := \{M \in \mathcal{M} \mid M, \text{ her } i = 1, \dots, t \text{ için } f_i\text{'nin bir katı değildir}\}.$$

3.35 Uyarı Şunu gözlemleyelim ki $\Delta(I) \subseteq \Delta(\text{lm}(f_1), \dots, \text{lm}(f_t))$.

Aslında, Önerme 3.30'dan şu sonuç elde edilir: $\{f_1, \dots, f_t\}$, I ideali için bir Gröbner bazdır ancak ve ancak

$$\Delta(I) = \Delta(\text{lm}(f_1), \dots, \text{lm}(f_t)).$$

4. Afin Varyeteler ve Afin Varyete Kodları

Matematikte afin varyete, cebirsel geometri ve deęişmeli cebirde ele alınan en temel kavramlardan biridir. Polinom denklemlerinden oluşan bir sistemin koordinat uzayındaki ortak sıfırlarının (köklerinin) oluşturduğu geometrik kümeleri ifade eder. Bu bölümde öncelikle afin varyeteler ile ilgili temel tanım ve sonuçlar sunulmaktadır. Daha sonra afin varyeteler kullanılarak afin varyete kodlarının nasıl tanımlandığı açıklanmaktadır. Ayrıca, Gröbner tabanları ile ilişkili ayak izi kavramına dayanan ve afin varyete kodlarının temel parametrelerinin belirlenmesini sağlayan yöntem incelenmektedir. Bu bölümde genel olarak [2], [3] ve [4] kaynaklarından yararlanılmaktadır.

4.1 Afin Varyeteler

Bu kısımda, varyetelerin tanımı ve örnekleri verilerek ideal-varyete dönüşümleri açıklanmakta; Hilbert Nullstellensatz gibi temel sonuçlar üzerinde durulmaktadır.

4.1 Tanım Bir $I \subseteq F[X]$ idealinin *afin varyetesi*,

$$V(I) := \{(a_1, \dots, a_n) \in F^n \mid f(a_1, \dots, a_n) = 0, \text{ her } f \in I \text{ için} \}$$

olarak tanımlanır.

$I \subseteq F[X]$ olmak üzere Teorem 3.21'den öyle bir $t \geq 1$ vardır ki $g_1, \dots, g_t \in I$ olmak üzere $I = \langle g_1, \dots, g_t \rangle$ olduğunu hatırlayalım. $V(I)$ 'yı bulalım. $f \in I$ olsun.

$f = h_1g_1 + h_2g_2 + \dots + h_tg_t$, $h_1, \dots, h_t \in F[X]$ olarak yazılabilir. Bu yüzden

$$\begin{aligned} f(a_1, \dots, a_n) &= (h_1g_1, \dots, +h_tg_t)(a_1, \dots, a_n) \\ &= h_1(a_1, \dots, a_n)g_1(a_1, \dots, a_n) + \dots + h_t(a_1, \dots, a_n)g_t(a_1, \dots, a_n). \end{aligned}$$

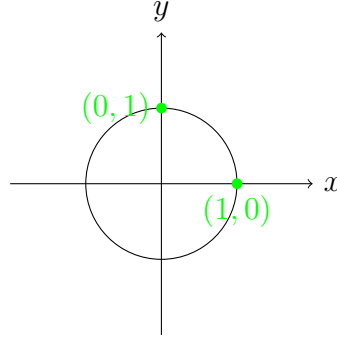
Dolayısıyla her $i = 1, \dots, t$ için $g_i(a_1, \dots, a_n) = 0$ ancak ve ancak $(a_1, \dots, a_n) \in V(I)$ olduğu açıktır. Böylece, $V(I) = V(g_1, \dots, g_n)$ olur.

4.2 Örnek $f(x, y) = x^2 + y^2 - 1 \in F[x, y]$ ve $I = \langle f \rangle$ olsun. O halde

$$V(I) = \{(a_1, a_2) \in F^2 \mid f(a_1, a_2) = 0\}.$$

$f(a_1, a_2) = a_1^2 + a_2^2 - 1 = 0$ ise $a_1^2 + a_2^2 = 1$ dir. Dolayısıyla,

$V(I) = \{(a_1, a_2) \in F^2 \mid a_1^2 + a_2^2 = 1\}$ varyetesi geometrik olarak aşağıdaki şekilde gösterilebilir:

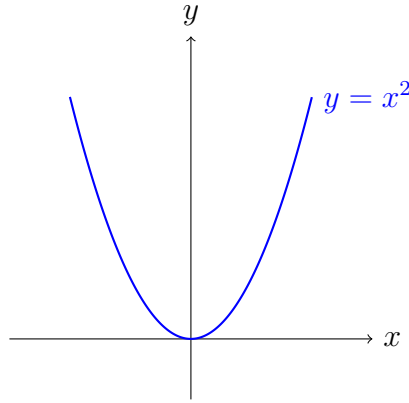


Şekil 4.1: $V(I)$ nın grafiği

4.3 Örnek $f_1(x, y) = x^2 - 1 \in F[x, y]$, $f_2(x, y) = y^2 - 1 \in F[x, y]$ ve $I = \langle f_1, f_2 \rangle$ olsun. O halde $V(I) = \{(x, y) \in \mathbb{R}^2 \mid f_1(x, y) = f_2(x, y) = 0\}$.

Buradan $f_1(x, y) = x^2 - 1 = 0$ ise $x^2 = 1$ olup $x = \pm 1$ ve $f_2(x, y) = y^2 - 1 = 0$ ise $y^2 = 1$ olup $y = \pm 1$ bulunur. Sonuç olarak, $V(I) = \{(1, 1), (-1, -1), (1, -1), (-1, 1)\}$ elde edilir.

4.4 Uyarı Bir I ideali için $V(I)$ varyetesi sonsuz tane noktaya sahip olabilir. Örneğin, $I = \langle y - x^2 \rangle \subset \mathbb{R}[x, y]$ ve $f(x, y) = y - x^2$ olsun. $y - x^2 = 0$ ise $y = x^2$ dir. Buradan $V(I) = \{(x, x^2) \in \mathbb{R}^2 \mid y = x^2\}$ bulunur. $V(I)$ nın geometrik şekli aşağıdaki gibidir.



Şekil 4.2: $V(I)$ nın grafiği

Tanım 4.1'den $V = V(I)$ verildiğinde, V üzerinde sıfır olan tüm polinomların kümesi aşağıdaki şekilde tanımlanmaktadır.

4.5 Tanım Bir $I \subseteq F[\mathbf{X}]$ ideali için $V = V(I)$ varyetesinin ideali

$$I(V) = \{f \in F[\mathbf{X}] \mid f(a_1, \dots, a_n) = 0, \text{ her } (a_1, \dots, a_n) \in V \text{ için } \}$$

şeklinde tanımlanır.

4.6 Uyarı $I(V)$ kümesinin $F[\mathbf{X}]$ halkasının bir ideali olduğu kolaylıkla gösterilebilir: $(a_1, \dots, a_n) \in V$ alalım.

(i) Sıfır polinomu $0 \in F[\mathbf{X}]$ olmak üzere $0(a_1, \dots, a_n) = 0$ olup $0 \in I(V)$ 'dir.

(ii) Her $f, g \in I(V)$ için $f + g \in I(V)$ olduğunu gösterelim. $f, g \in I(V)$ ise her $(a_1, \dots, a_n) \in V$ için $f(a_1, \dots, a_n) = g(a_1, \dots, a_n) = 0$ dır. Buradan

$(f + g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) + g(a_1, \dots, a_n) = 0 + 0 = 0$ olur. Böylece Tanım 4.5'den $f + g \in I(V)$ elde edilir.

(iii) Her $f \in I(V)$ ve $h \in F[\mathbf{X}]$ için $h \cdot f \in I(V)$ olduğunu gösterelim. $f \in I(V)$ ise her $(a_1, \dots, a_n) \in V$ için $f(a_1, \dots, a_n) = 0$ dır. Buradan

$(h \cdot f)(a_1, \dots, a_n) = h(a_1, \dots, a_n) \cdot f(a_1, \dots, a_n) = h(a_1, \dots, a_n) \cdot 0 = 0$ dır. Böylece, $h \cdot f \in I(V)$ elde edilir.

Sonuç olarak (i), (ii) ve (iii) den dolayı $I(V)$, $F[\mathbf{X}]$ halkasının bir idealidir.

Aynı zamanda $I \subseteq I(V(I))$ 'dir, çünkü herhangi bir $f \in I$ ve $(a_1, \dots, a_n) \in V(I)$ için Tanım 4.1'den $f(a_1, \dots, a_n) = 0$ olur. Buradan $f \in I(V(I))$ elde edilir.

4.7 Örnek $V = \{(0, 0)\} \subset F^2$ varyetesini alalım. $I(V)$ 'yi bulalım.

İddia: $I(V) = \{f \in F[x, y] \mid f(a_1, a_2) = 0, \text{ her } (a_1, a_2) \in V \text{ için} \} = \langle x, y \rangle$ dir. Bunu gösterelim. Öncelikle $\langle x, y \rangle \subseteq I(V)$ olduğunu gösterelim. $f \in \langle x, y \rangle$ alalım.

$$f(x, y) = A(x, y) \cdot x + B(x, y) \cdot y, \quad A, B \in F[x, y] \quad (4.1)$$

şeklinde yazılabilir. (4.1)'den $f(0, 0) = A(0, 0) \cdot 0 + B(0, 0) \cdot 0 = 0 + 0 = 0$. Dolayısıyla, $f \in I(V)$ olur.

Şimdi de $I(V) \subseteq \langle x, y \rangle$ olduğunu gösterelim. $g \in I(V)$ alalım.

$g(x, y) = \sum_{i,j} a_{ij} x^i y^j$, $a_{ij} \in F$ ve $g(0, 0) = 0$ olduğundan $0 = a_{00} + 0$, yani $a_{00} = 0$ olur.

O halde $g(x, y) = \sum_{(i,j) \neq (0,0)} a_{ij} x^i y^j = \sum_{i>0} a_{ij} x^{i-1} y^j \cdot x + \sum_{\substack{j>0 \\ i=0}} a_{0j} y^{j-1} \cdot y$ olduğundan

$g \in \langle x, y \rangle$ olur. Sonuç olarak $I(V) = \langle x, y \rangle$ elde edilir.

Burada not edelim ki herhangi bir $V \subseteq F^n$ afin varyetesi için

$$I(V) = \{f \in F[\mathbf{X}] \mid f(p) = 0, \text{ her } p \in V \text{ için} \}$$

olmak üzere $V \xrightarrow{I} I(V)$ dönüşümü vardır. Benzer şekilde herhangi bir $I \subseteq F[\mathbf{X}]$ ideali için Teorem 3.21'den öyle $f_1, \dots, f_s \in I$ vardır ki $I = \langle f_1, \dots, f_s \rangle$ dir.

$$V(I) = V(\langle f_1, \dots, f_s \rangle) = \{(a_1, \dots, a_n) \in F^n \mid f_i(a_1, \dots, a_n) = 0, \text{ her } i = 1, \dots, s \text{ için} \}$$

olmak üzere $I \xrightarrow{V} V(I)$ dönüşümü de vardır.

4.8 Yardımcı Önerme [4, Lemma 1] Herhangi bir V varyetesi ve $m \geq 1$ tam sayısı için $f^m \in I(V)$ ise $f \in I(V)$ dir.

İspat: Eğer $f^m \in I(V)$ ise her $p \in V$ için $f^m(p) = 0$ dir. Buradan $(f(p))^m = 0$ olup $f(p)f(p)\dots f(p) = 0$ şeklindedir. Dolayısıyla $f(p) = 0$ olur yani $f \in I(V)$ elde edilir.

□

4.9 Tanım $I \subseteq F[\mathbf{X}]$ bir ideal ve I 'nın *radikali*

$$\sqrt{I} := \{f \in F[\mathbf{X}] \mid f^m \in I \text{ bir } m \geq 1 \text{ tam sayısı için} \}$$

şeklinde tanımlanır. Eğer $I = \sqrt{I}$ ise I idealine *radikal ideal* denir.

4.10 Uyarı $I(V)$ bir radikal idealdir.

4.11 Uyarı $I \subseteq F[\mathbf{X}]$ bir ideal olsun.

(i) $f \in I$ olsun. Eğer $f^1 \in I$ ise $f \in \sqrt{I}$ dir. Dolayısıyla $I \subseteq \sqrt{I}$ olur.

(ii) $\sqrt{I}$ nın $F[\mathbf{X}]$ 'de bir ideal olduğunu göstermek için öncelikle her $f, g \in \sqrt{I}$ için $f + g \in \sqrt{I}$ olduğunu gösterelim. Öncelikle $f, g \in \sqrt{I}$ olduğundan öyle m, n pozitif tam sayıları vardır ki $f^m, g^n \in I$ dir. O halde

$$(f+g)^{m+n-1} = f^{m+n-1} + f^{m+n-2} \cdot g^1 + \dots + f^m \cdot g^{n-1} + f^{m-1} \cdot g^n + \dots + f \cdot g^{m+n-2} + g^{m+n-1} \in I$$

olduğundan $f + g \in \sqrt{I}$ elde edilir.

Şimdi de $f \in \sqrt{I}$ ve $h \in F[\mathbf{X}]$ iken $h \cdot f \in \sqrt{I}$ olduğunu gösterelim. Herhangi bir $m \geq 1$ için $(h \cdot f)^m = h^m \cdot f^m \in I$ ise $h \cdot f \in \sqrt{I}$ olduğu açıktır. Sonuç olarak $\sqrt{I}, F[\mathbf{X}]$ 'de bir idealdir.

(iii) $\sqrt{I}$ bir radikal idealdir. $f^n \in \sqrt{I}$ iken $f \in \sqrt{I}$ olduğunu gösterelim. Eğer $f^n \in \sqrt{I}$ ise bir $m \geq 1$ tam sayısı için $(f^n)^m \in I$. Buradan $f^{n \cdot m} \in I, n \cdot m \geq 1$ olur ve $f \in \sqrt{I}$ elde edilir.

4.12 Örnek $J = \langle x^2, y^3 \rangle \subset F[x, y]$ idealini ele alalım. $x + y \in \sqrt{J}$ olduğunu gösterelim. $x^2 \in J$ ise $x \in \sqrt{J}$ ve $y^3 \in J$ ise $y \in \sqrt{J}$ olur.

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \in J \text{ şeklinde olup } x + y \in \sqrt{J} \text{ elde edilir.}$$

4.13 Teorem [4, Theorem 6] (*Hilbert Nullstellensatz*) F cebirsel kapalı bir cisim olmak üzere $I \subseteq F[\mathbf{X}]$ ideali için $I(V(I)) = \sqrt{I}$ dir.

Herhangi bir I ideali için $\Delta(I)$ sonlu olduğunda, I 'nin varyetesi ve I 'nin ayak izi $\Delta(I)$ arasındaki ilişkiyi kanıtlamak için aşağıdaki yardımcı önermeye ihtiyaç duyulmaktadır.

4.14 Yardımcı Önerme [3, Lemma 3.2] $I \subseteq F[\mathbf{X}]$ bir ideal ve $p_1, \dots, p_r, V(I)$ 'nin farklı noktaları olsun. Bu durumda her $i, j \in \{1, \dots, r\}$ için

$$f_i(p_j) = \delta_{i,j} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

olacak şekilde $f_1, \dots, f_r \in F[\mathbf{X}]$ vardır.

İspat: $P_i = (a_{i1}, \dots, a_{in}) \in F^n, i = 1, \dots, r$ noktalarını ele alalım. Bu yardımcı önermede f_1 polinomunu nasıl elde ettiğimizi gösterelim. Tüm P_i noktaları birbirinden farklı olduğundan, her $i \in 2, \dots, r$ için bazı $j_i \in 1, \dots, n$ vardır ki $a_{1j_i} \neq a_{ij_i}$ olur. Bu durumda

$$h_i := \frac{x_{j_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}}$$

şeklinde tanımlayalım. Paydanın sıfırdan farklı olduğu açıktır. Böylece aşağıdaki durum elde edilir:

$$h_i(P_1) = \frac{a_{1j_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}} = 1 \text{ ve her } i = 2, \dots, r \text{ için } h_i(P_i) = \frac{a_{ij_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}} = 0$$

$f_1 = \prod_{i=2}^r h_i = h_2 h_3 \dots h_r$ alırsak $f_1(P_1) = 1$ ve $f_1(P_i) = 0$ olur. Benzer şekilde $f_2, \dots, f_r$ polinomları elde edilir.

□

4.15 Önerme [3, Proposition 3.3] $I \subseteq F[\mathbf{X}]$ bir ideal ve $\Delta(I)$ kümesi sonlu olsun. Bu durumda, $V(I)$ sonlu bir kümedir ve $|V(I)| \leq |\Delta(I)|$ eşitsizliği sağlanır.

İspat: $P_1, P_2, \dots, P_r, V(I)$ 'nin birbirinden farklı elemanları olsun. Teorem 3.32'den $\mathcal{B} = \{M + I \mid M \in \Delta(I)\}$ 'nin $F[\mathbf{X}]/I$ 'nin bir bazı olduğu bilinmektedir. Buradan $\Delta(I)$ nin eleman sayısı $|\Delta(I)|$, $F[\mathbf{X}]/I$ nin boyutuna eşittir. Yardımcı Önerme 4.14'den her $i, j \in 1, \dots, r$ için $f_i(P_j) = \delta_{ij}$ olacak şekilde $f_1, \dots, f_r \in F[\mathbf{X}]$ polinomların olduğunu

biliyoruz. $\{f_1 + I, \dots, f_r + I\}$ 'nin, $F[\mathbf{X}]/I$ 'da lineer bağımsız olduğunu gösterelim. Bunun için $a_1, \dots, a_r \in F$ olmak üzere $a_1(f_1 + I) + \dots + a_r(f_r + I) = 0 + I$ olduğunu varsayalım. O halde $(a_1f_1 + I) + \dots + (a_rf_r + I) = (a_1f_1 + \dots + a_rf_r) + I = 0 + I$ dır. Dolayısıyla $\sum_{i=1}^r a_i f_i \in I$ olur. $P_1, \dots, P_r \in V(I)$ olduğundan $\sum_{i=1}^r a_i f_i(P_j) = 0$, her $j = 1, \dots, r$ için $a_j = 0$ dır. Sonuç olarak, $\{f_1 + I, \dots, f_r + I\}$ lineer bağımsız ve r elemanlıdır.

□

4.16 Teorem [3, Theorem 3.4] $I \subseteq F[\mathbf{X}]$ te bir ideal öyle ki $\Delta(I)$ sonlu bir küme ve L, F cisminin kapalı bir cebirsel genişlemesi olsun.

$$V_L(I) = \{(a_1, \dots, a_n) \in L^n \mid f(a_1, \dots, a_n) = 0, \text{ her } f \in I \text{ için} \}$$

sonlu bir kümedir ve $|V_L(I)| \leq |\Delta(I)|$ dır. Üstelik F , bir mükemmel cisim ve I radikal ideal ise $|V_L(I)| = |\Delta(I)|$ olur.

4.2 Afin Varyete Kodları

Afin varyete kodları çok değişkenli polinomların sonlu cisimler üzerindeki bir afin varyetenin noktalarında değerlendirilmesiyle elde edilen lineer kodlardır.

$\mathbb{F}_q$, q elemanlı bir sonlu cisim olmak üzere $S \subseteq \mathbb{F}_q[x_1, \dots, x_s]$ olsun. S 'nin bir ortak çözümü (sıfırı), $(a_1, \dots, a_s) \in \overline{\mathbb{F}}_q^s = \overline{\mathbb{F}}_q \times \dots \times \overline{\mathbb{F}}_q$ (s çarpan) şeklindedir, burada $\overline{\mathbb{F}}_q, \mathbb{F}_q$ 'nun cebirsel kapalı bir genişlemesidir ve $f(a_1, \dots, a_s) = 0$ eşitliği S 'deki her f için geçerlidir.

4.17 Tanım [2] $\mathbb{F}_q[x_1, \dots, x_s]$, $\mathbb{F}_q$ cismi üzerinde s -değişkenli polinom halkası ve $S \subseteq \mathbb{F}_q[x_1, \dots, x_s]$ olsun. S kümesinin *ortak çözümleri kümesi*

$$V(S) := \{(a_1, \dots, a_s) \in \overline{\mathbb{F}}_q^s \mid f(a_1, \dots, a_s) = 0 \text{ her } f \in S \text{ için} \} \quad (4.2)$$

ile gösterilip, $\overline{\mathbb{F}}_q^s$ kümesinde bir *afin varyetedir*, denir. $(a_1, \dots, a_s) \in V(S)$ elemanları $V(S)$ *varyetesinin noktaları* olarak bilinir. $V(S)$ 'nin tüm koordinatlarının $\mathbb{F}_q$ cisminde olan noktalarına $V(S)$ 'nin $\mathbb{F}_q$ -rasyonel noktaları denir.

Aksi belirtilmedikçe, buradan itibaren

$V(I) = \{(a_1, \dots, a_s) \in \overline{\mathbb{F}}_q^s \mid f(a_1, \dots, a_s) = 0 \text{ her } f \in S \text{ için} \}$ olarak alınacaktır.

Eğer $I = \langle S \rangle$ yani I ideali S ile üretiliyor ise $V(I) = V(S)$ olur. Bu terminolojide, bir varyete, afin uzayın bir indirgenemez alt kümesi olmak zorunda değildir.

Tersine, $Y \subseteq \overline{\mathbb{F}}_q^s$ için Y kümesinin ideali

$$I(Y) := \{f \in \mathbb{F}_q[x_1, \dots, x_s] \mid f(a_1, \dots, a_s) = 0, \text{ her } (a_1, \dots, a_s) \in Y \text{ için} \}$$

ile tanımlanır. Teorem 4.13'ten $I(V(I)) = \sqrt{I}$.

4.18 Tanım $I \subseteq \mathbb{F}_q[x_1, \dots, x_s]$ bir ideal olsun.

$$I_q := I + \langle x_1^q - x_1, \dots, x_s^q - x_s \rangle \quad (4.3)$$

olarak tanımlanır.

4.19 Not Bu bölümde $V(I)$, $\overline{\mathbb{F}}_q$ 'daki varyete olacaktır.

4.20 Önerme [2, Proposition 1.1.2] $I, \mathbb{F}_q[x_1, \dots, x_s]$ in bir ideali olsun. Bu durumda $V(I_q)$ nun noktaları, $V(I)$ nin $\mathbb{F}_q$ -rasyonel noktalarıdır.

İspat: Öncelikle $V(I_q) \subseteq V(I)$ olduğunu gösterelim. $I \subseteq I_q$ olduğundan $V(I_q) \subseteq V(I)$ olduğu açıktır. $P = (a_1, \dots, a_s) \in V(I_q)$ olsun. (4.2)'den her $f \in I_q$ için $f(P) = 0$ dır. Özellikle (4.3)'ten $f_i = x_i^q - x_i \in I_q$ olduğundan $f_i(a_1, \dots, a_s) = 0$ ve dolayısıyla her $i = 1, \dots, s$ için $a_i^q - a_i = 0$ olur. Sonlu cisim teorisinin iyi bilinen bir özelliği Yardımcı Önerme 2.20'ye göre bu eşitlik ancak $a_i \in \mathbb{F}_q$, $1 \leq i \leq s$ olduğunda sağlanır. Ayrıca $I \subseteq I_q$ olduğundan her $f \in I$ için $f(a_1, \dots, a_s) = 0$ dır. Buradan $P = (a_1, \dots, a_s) \in V(I)$ ve $(a_1, \dots, a_s) \in \mathbb{F}_q^s$ bulunur, yani $(a_1, \dots, a_s)$, $V(I)$ 'nin $\mathbb{F}_q$ -rasyonel bir noktasıdır.

Tersine $(a_1, \dots, a_s) \in V(I)$ 'nin $\mathbb{F}_q$ -rasyonel noktası olsun. Teorem 2.20'den $a_i^q - a_i = 0$ 'dır. Dolayısıyla $f_i(a_1, \dots, a_s) = 0$ olur. Ayrıca (4.2)'ten dolayı her $g \in I$ için $g(a_1, \dots, a_s) = 0$ dır. $I_q = I + \langle x_1^q - x_1, \dots, x_s^q - x_s \rangle$ olduğundan her $G(x_1, \dots, x_s) \in I_q$ için $G(x_1, \dots, x_s) = g(x_1, \dots, x_s) + \sum_{i=1}^s h_i(x_1, \dots, x_s) \cdot (x_i^q - x_i)$ $g(x_1, \dots, x_s) \in I$ ve $h_i(x_1, \dots, x_s) \in \mathbb{F}_q[x_1, \dots, x_s]$, $i = 1, \dots, s$ formunda yazılabilir.

$g(a_1, \dots, a_s) = 0$ ve $f_i(a_1, \dots, a_s) = 0$ olduğundan

$$G(a_1, \dots, a_s) = g(a_1, \dots, a_s) + \sum_{i=1}^s h_i(a_1, \dots, a_s) \cdot (a_i^q - a_i) = 0 + \sum_{i=1}^s h_i(a_1, \dots, a_s) \cdot 0 = 0$$

bulunur. Böylece $(a_1, \dots, a_s) \in V(I_q)$ olur ve $V(I) \subseteq V(I_q)$ bulunur.

Sonuç olarak $V(I) = V(I_q)$ elde edilir.

□

Dikkat edilmelidir ki herhangi bir $P = (a_1, \dots, a_s) \in \mathbb{F}_q^s$ ve herhangi bir $f \in \mathbb{F}_q[x_1, \dots, x_s]$ için $f(P) = f(a_1, \dots, a_s)$ hesaplandığında elde edilen değer, $\mathbb{F}_q$ 'nın bir elemanıdır, çünkü tüm noktaların koordinatları a_i ve f polinomunun katsayıları $\mathbb{F}_q$ 'ya aittir.

4.21 Uyarı $\mathbb{F}_q$ 'nın eleman sayısı q olduğundan, $V(I)$ en fazla q^s tane $\mathbb{F}_q$ -rasyonel nokta içerir. Böylece $V(I_q)$ 'nın eleman sayısı sonludur.

4.22 Tanım $I \subseteq \mathbb{F}_q[x_1, \dots, x_s]$ bir ideal olsun. $V(I)$ 'nin noktalarının sayısı sonlu ise, I idealine *sıfır-boyutlu* bir ideal denir.

Uyarı 4.21'ten I_q sonlu boyutlu bir idealdir.

4.23 Yardımcı Önerme [2, Lemma 1.1.4] (*Seidenberg's Lemma 92*) $J, \mathbb{F}_q[x_1, \dots, x_s]$ halkasının sıfır-boyutlu bir ideali ve $1 \leq i \leq s$ için, J 'nin $obeb(f_i, f'_i) = 1$ olacak şekilde bir $f_i \in \mathbb{F}_q[x_i]$ polinomunu içerdiğini varsayalım, burada f'_i, f_i 'nin türevidir. Bu durumda J , sonlu tane maksimal idealin kesişimidir. Üstelik J bir radikal idealdir.

4.24 Sonuç [2, Corollary 1.1.5] $I \subseteq \mathbb{F}_q[x_1, \dots, x_s]$ bir ideal olsun. Bu durumda I_q bir radikal idealdir.

İspat: I_q 'nın sıfır-boyutlu ideal bir olduğunu biliyoruz. $1 \leq i \leq s$, $f_i = x_i^q - x_i$ için $obeb(f_i, f'_i) = 1$ olduğunu göstermek yeterlidir. $f_i = x_i^q - x_i$ ise $f'_i = qx_i^{q-1} - 1 = -1$, çünkü $q = p^n, n \in \mathbb{N}$ iken $\mathbb{F}_q$ 'nın karakteristiği p 'dir. Buradan $obeb(f_i, f'_i) = obeb(x_i^q - x_i, -1) = 1$ dir. Yardımcı Önerme 4.23'dan I_q bir radikal idealdir.

□

$R = \mathbb{F}_q[x_1, \dots, x_s]/I_q$ olsun. R halkasına $V(I_q)$ varyetesinin *koordinat halkası* ve R 'nin elemanlarına da $V(I_q)$ üzerindeki *düzenli (regular) fonksiyonlar* denir. R 'nin elemanları, $f \in \mathbb{F}_q[x_1, \dots, x_s]$ için $f + I_q$ denklik sınıfını gösteren $\bar{f}$ ile ifade edilir. Ayrıca R bir $\mathbb{F}_q$ -vektör uzayıdır.

4.25 Yardımcı Önerme [2, Lemma 1.1.6] R 'nin $\mathbb{F}_q$ -vektör uzayı olarak boyutu, $V(I_q)$ 'daki noktaların sayısı olan n 'dir.

Bundan böyle, $n, V(I_q)$ 'daki noktaların sayısı olmak üzere $\mathbb{F}_q^n, \mathbb{F}_q$ üzerinde bir n -uzay olarak alalım. $V(I_q)$ 'daki P_i noktaları için $P_1, \dots, P_n$ sıralamasını sabitleyelim.

$\varphi : R \longrightarrow \mathbb{F}_q^n$ dönüşümü şu şekilde tanımlanmaktadır:

$$\varphi(\bar{f}) := (f(P_1), \dots, f(P_n)),$$

burada $\bar{f} = f + I_q$ dir. Daha önceden $f \in \mathbb{F}_q[x_1, \dots, x_s]$ ve $P_i \in V(I_q)$ için $f(P_i) \in \mathbb{F}_q$ olduğu biliniyor. Böylece $\varphi(\bar{f}) \in \mathbb{F}_q^n$. Şimdi φ 'nin iyi tanımlı olduğunu gösterelim.

Varsayalım ki $\bar{f}_1 = \bar{f}_2$ olsun. $\bar{f}_1 = f_1 + I_q$ ve $\bar{f}_2 = f_2 + I_q$ olmak üzere $f_1 + I_q = f_2 + I_q$ dır. Buradan $f_1 - f_2 = g \in I_q$ olup $f_1 = f_2 + g$, $g \in I_q$ dır. Her $i = 1, \dots, n$ için $P_i \in V(I_q)$ ise $f_1(P_i) = (f_2 + g)(P_i) = f_2(P_i) + g(P_i) = f_2(P_i) + 0 = f_2(P_i)$ yani $f_2(P_i) = f_1(P_i)$ olur. Bu yüzden $\varphi(\bar{f}_2) = \varphi(\bar{f}_1)$ ve dolayısıyla φ iyi tanımlıdır.

4.26 Yardımcı Önerme [2, Lemma 1.1.7] φ dönüşümü bir izomorfizmadır.

İspat: Polinomların toplama ve skaler çarpma tanımlarını kullanarak φ 'nin lineer olduğunu gösterelim. Her $i = 1, \dots, n$ için $P_i \in V(I_q)$ noktaları ele alalım. Herhangi bir $\bar{f}_1, \bar{f}_2 \in R$ için ilk olarak $\varphi(\bar{f}_1 + \bar{f}_2) = \varphi(\bar{f}_1) + \varphi(\bar{f}_2)$ olduğunu gösterelim:

$$\begin{aligned}\varphi(\bar{f}_1 + \bar{f}_2) &= \varphi((f_1 + I_q) + (f_2 + I_q)) = \varphi((f_1 + f_2) + I_q) \\ &= ((f_1 + f_2)(P_1), \dots, (f_1 + f_2)(P_n)) \\ &= (f_1(P_1) + f_2(P_1), \dots, f_1(P_n) + f_2(P_n)) \\ &= (f_1(P_1), \dots, f_1(P_n)) + (f_2(P_1), \dots, f_2(P_n)) = \varphi(\bar{f}_1) + \varphi(\bar{f}_2)\end{aligned}$$

elde edilir. Şimdi ise her $c \in \mathbb{F}_q$ ve $\bar{f} = f + I_q \in R$ için $\varphi(c \cdot \bar{f}) = c \cdot \varphi(\bar{f})$ olduğunu gösterelim:

$$\begin{aligned}\varphi(c \cdot \bar{f}) &= \varphi(c \cdot (f + I_q)) = \varphi(c \cdot f + I_q) \\ &= (c \cdot f(P_1), \dots, c \cdot f(P_n)) = c \cdot (f(P_1), \dots, f(P_n)) = c \cdot \varphi(\bar{f}).\end{aligned}$$

Dolayısıyla, φ lineerdir. Şimdi de φ 'nin birebir olduğunu gösterelim. $\varphi(\bar{f}_1) = \varphi(\bar{f}_2)$ olduğunu varsayalım.

$\varphi(\bar{f}_1) - \varphi(\bar{f}_2) = 0_{A^n}$ dır ve lineer olduğundan $\varphi(\bar{f}_1 - \bar{f}_2) = 0_{A^n}$ olur. Buradan $\varphi((f_1 + I_q) - (f_2 + I_q)) = \varphi(f_1 - f_2 + I_q) = ((f_1 - f_2)(P_1), \dots, (f_1 - f_2)(P_n)) = (0, \dots, 0)$ dır. Her $i = 1, \dots, n$ için $(f_1 - f_2)(P_i) = 0$ dır.

Bu yüzden, Teorem 4.13'ten $f_1 - f_2 \in I(V(I_q)) = \sqrt{I_q}$ dır. Sonuç 4.24'den $\sqrt{I_q} = I_q$ olup $f_1 - f_2 \in I_q$ dır. Buradan $\bar{f}_1 - \bar{f}_2 = \bar{0}$ yani $\bar{f}_1 = \bar{f}_2$ elde edilir. Yardımcı Önerme 4.25'e göre R ve A^n nin boyutu n dir. φ birebir olduğundan, görüntüsünün boyutu da n 'dir. Dolayısıyla φ örten olur ve bu nedenle bir izomorfizmadır.

□

Hatırlayalım ki $\mathbb{F}_q$ üzerinde uzunluğu n olan bir lineer kod, $\mathbb{F}_q^n$ 'nin bir alt vektör uzayıdır.

Şimdi $I \subset \mathbb{F}_q[x_1, \dots, x_s]$ bir ideal, L ise $\mathbb{F}_q[x_1, \dots, x_s]/I_q$ 'nun bir $\mathbb{F}_q$ alt vektör uzayı ve $P_1, \dots, P_n, V(I_q)$ nun tüm noktaları olsun.

4.27 Tanım Afin varyete kodları $C(I, L)$ ve $C^\perp(I, L)$ 'yi aşağıdaki gibi tanımlanmaktadır:

$$C(I, L) := \varphi(L),$$

$$C^\perp(I, L) := \varphi(L)^\perp.$$

Burada $\varphi(L)$, L altuzayının φ dönüşümü altındaki görüntüsüdür ve $\varphi(L)^\perp, \mathbb{F}_q^n$ 'de $\varphi(L)$ 'nin olağan iç çarpımına göre ortogonal tümleyenidir, yani $C^\perp(I, L)$, $C(I, L)$ kodunun dual kodudur.

4.28 Tanım $\mathbb{F}_q$ üzerinde iki adet (n, M) -kodundan biri diğerinden aşağıdaki işlemlerin bir dizisi uygulanarak elde edilebiliyorsa bu iki kod *denktir* denir:

- (i) Kod sözcüklerinin koordinatlarının permütasyonu,
- (ii) Sabit bir konumdaki koordinatın sıfırdan farklı bir skaler ile çarpımı.

4.29 Örnek $\mathbb{F}_3$ üzerinde

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

kodunun sözcüklerinin 3. koordinatlarını 2 ile çarpıp, koordinatları $(2, 3, 1)$ sırasına göre yazarsak C' ye denk olan

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

kodunu elde ederiz.

4.30 Uyarı Genel olarak, varyetenin $V(I_q)$ üzerindeki noktaların $P_1, \dots, P_n$ farklı bir sıralaması, farklı fakat eşdeğer bir lineer kod verir.

4.31 Tanım [9, Definition 2.1] $\{f_1, \dots, f_r\}$, L 'nin $\mathbb{F}_q$ üzerindeki lineer bir tabanı ise

$$\begin{pmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_r(P_1) & f_r(P_2) & \cdots & f_r(P_n) \end{pmatrix}$$

matrisi $C(I, L)$ için bir *üreteç matrisi* ve $C^\perp(I, L)$ için bir *eşlik-denetim matrisi* olur.

4.32 Teorem [2, Theorem 1.2.8] Her lineer kod bir afin varyete kodudur.

4.33 Tanım $n \leq q$ ve her $1 \leq i \leq n$ için α_i 'ler $\mathbb{F}_q$ 'nin birbirinden farklı elemanları olmak üzere $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ ve $v_i \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ olmak üzere $v = (v_1, \dots, v_n)$ olsun. $k \leq n$ için Genelleştirilmiş Reed–Solomon kodu $C = \text{GRS}_k(a, v)$ şu şekilde tanımlanmaktadır:

$$C := \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) ; f(x) \in \mathbb{F}_q[x], \text{ ve } \deg(f(x)) < k\},$$

burada k , kodun boyutudur.

4.34 Teorem [2, Theorem 1.1.6] $\mathbb{F}_q$ üzerinde tanımlı uzunluğu n olan Genelleştirilmiş Reed–Solomon kodu $C = \text{GRS}_k(a, v)$ 'nin dual kodu $C^\perp$ öyle bir $v' \in (\mathbb{F}_q^*)^n$ için bir $\text{GRS}_{n-k}(a, v')$ kodudur.

4.35 Örnek Tanım 4.27'de $s = 1$, $I = \langle 0 \rangle$ alalım. O halde,

$$I_q = \langle x^q - x \rangle \quad \text{ve} \quad V(I_q) = \{p \in \mathbb{F}_q \mid p^q - p = 0\} = \mathbb{F}_q.$$

Buradan $n = q$ olur. $\alpha, \mathbb{F}_q$ 'nin bir ilkel elemanı yani $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$ olsun. $V(I_q)$ 'nin noktalarını şu şekilde sıralayalım:

$$P_1 = \alpha^1 = \alpha, P_2 = \alpha^2, \dots, P_{q-1} = \alpha^{q-1} = 1, P_q = 0.$$

$C = \{(f(P_1), \dots, f(P_q)) \mid f(x) \in \mathbb{F}_q[x] \text{ ve } \deg f(x) < k\} \subseteq \mathbb{F}_q^q$ bir uzatılmış Reed–Solomon kodudur, burada k , kodun boyutudur. Dikkat edilirse $v = (1, \dots, 1)$ ve $a = (\alpha, \alpha^2, \dots, \alpha^{q-1}, 0)$ alınırsa C kodu bir $\text{GRS}_k(a, v)$ 'dir.

Derecesi k 'dan küçük olan bu $f(x)$ polinomlarının oluşturduğu kümenin, $\mathbb{F}_q[x]/I_q$ da bir tabanı olarak $\{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{k-1}\}$ alalım, dolayısıyla

$$L = \{a_1 + a_2\bar{x} + \dots + a_k\bar{x}^{k-1} \mid a_1, \dots, a_k \in \mathbb{F}_q\} \subseteq \mathbb{F}_q[x]/I_q$$

bir alt uzaydır. Buradan

$$\varphi(L) = \{\varphi(\bar{f}) \mid \bar{f} \in L\} = \{(f(P_1), \dots, f(P_q)) \mid f(x) \in \mathbb{F}_q[x], \deg f(x) < k\} = C$$

olur.

4.36 Örnek (Reed–Solomon Kodu) $I = \langle x^{q-1} - 1 \rangle \subseteq \mathbb{F}_q[x]$ olsun. O halde

$I_q = I + \langle x^q - x \rangle = I$, çünkü $x^q - x = x \cdot (x^{q-1} - 1)$. Dolayısıyla

$$V(I_q) = \{p \in \mathbb{F}_q \mid p^{q-1} - 1 = 0\} = \mathbb{F}_q \setminus \{0\} = \mathbb{F}_q^* \text{ ve } n = |\mathbb{F}_q^*| = q - 1 \text{ olur.}$$

$L = \{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{k-1}\}$, $R = \mathbb{F}_q[x]/I_q$ nun bir alt uzayı olduğundan $C(I, L)$ boyutu k olan bir klasik Reed–Solomon kodudur. $\alpha, \mathbb{F}_q$ 'nin bir ilkel elemanı olmak üzere $V(I_q)$ 'nin noktaları:

$$P_1 = \alpha^1 = \alpha, P_2 = \alpha^2, \dots, P_{q-1} = \alpha^{q-1} = 1.$$

Dikkat edilirse $v = (1, \dots, 1)$ ve $a = (\alpha, \alpha^2, \dots, \alpha^{q-2}, 1)$ alınırsa C kodu bir $\text{GRS}_k(a, v)$ 'dir.

4.37 Örnek (*Genelleştirilmiş Reed–Muller Kodu*) $I = \langle 0 \rangle \subseteq \mathbb{F}_q[x_1, x_2, \dots, x_s]$, $s \geq 1$ ve $0 \leq v \leq s \cdot (q - 1)$ olsun. Böylece $I_q = I + \langle x_1^q - x_1, \dots, x_s^q - x_s \rangle = \langle x_1^q - x_1, \dots, x_s^q - x_s \rangle$ olur ve

$$V(I_q) = \{p = (x_1, \dots, x_s) \mid x_1^q = x_1, x_2^q = x_2, \dots, x_s^q = x_s\} = \mathbb{F}_q^s, \quad n = q^s.$$

L , total derecesi en fazla v olan polinomların oluşturduğu $\mathbb{F}_q[x_1, x_2, \dots, x_s]/I_q$ nun bir alt uzayı olsun. Bu durumda $C(I, L)$, $\mathbb{F}_q$ -üzerinde tanımlı bir v -mertebeli genelleştirilmiş Reed–Muller kodudur $R(v, s)$ 'dir. Dikkat edilirse bu kodlar da Örnek 4.36'te verilen uzatılmış Reed Solomon kodlara benzerdir.

Şimdi ayak izi kavramına dayanan, bir afin varyete kodunun temel parametrelerinin belirlenmesinde kullanılan yöntemi ele alalım. Aşağıdaki sonuç, daha genel ayak izi (footprint) sınırının özel bir durumudur [10].

4.38 Sonuç [11, Corollary 1] $I \subseteq \mathbb{F}_q[x_1, \dots, x_s]$ bir ideal ve $I_q = I + \langle x_1^q - x_1, \dots, x_s^q - x_s \rangle$ olsun. Herhangi bir $\leq$ tek terimli sıralaması için, I_q idealinin varyetesinin eleman sayısı, $\Delta(I_q)$ ayak izinin eleman sayısına eşittir.

Yukarıdaki sonuçtan ve afin varyete kodu $C(I, L)$ 'nin tanımından kodun uzunluğu açıkça

$$n = |V(I_q)| = |V_{\mathbb{F}_q}(I)| = |\Delta(I_q)|$$

şeklindedir. φ bir izomorfizma olduğundan, $C(I, L)$ 'nin boyutu $\text{boy}(L)$ iken $C(I, L)^\perp$ 'in boyutu $n - \text{boy}(L)$ 'ye eşit olur.

Genel afin varyete kodu $C(I, L)$ 'nin minimum uzaklığının elde edilmesinde ayak izi sınırından yararlanılır. F , n değişkenli bir polinom ve $F + I_q \in L$ olmak üzere $J_F := I_q + \langle F \rangle$ idealini ele alalım. Kod sözcüğü $\varphi(F + I_q)$ ve G , I_q idealinin bir Gröbner bazı olsun. Bu durumda

$$\text{wt}(\varphi(F + I_q)) = n - |V(J_F)|.$$

Ayrıca Önerme 4.15 ve Uyarı 3.35'ten

$$|V(J_F)| \leq |\Delta(J_F)| \leq |\Delta(\{lm(f) \mid f \in G\} \cup \{lm(F)\})|.$$

eşitsizlikleri sağlanır. Uyarı 3.35'ten yukarıdaki ikinci eşitsizlikte eşitliğin sağlanabilmesi için $G \cup \{F\}$ kümesinin J_F idealinin bir Gröbner bazı olması gerekir. Böylece,

$$\text{wt}(\varphi(F + I_q)) \geq n - |\Delta(\{lm(f) \mid f \in G\} \cup \{lm(F)\})|$$

elde edilir.

5. Afin Kartezyen Kodlar

Bu bölümde afin varyete kodların özel bir hali olan afin kartezyen kodları ele alınmaktadır. Bu kodlar H. Lopez, C. Renteria-Marquez ve R. Villareal tarafından [5] çalışmasında tanıtılmakta ve bağımsız olarak O. Geil ile C. Thomsen tarafından daha genel bir biçimde [6] çalışmasında ele alınmaktadır. Burada öncelikle afin kartezyen kodların tanımı ayrıntılı olarak verilmektedir. Daha sonra bu kodların minimum mesafesi ve boyutu hesaplanmasında [3] ve [5] çalışmalarında verilen ve bu tezde de sunulan teoriyi içeren teknikler açıklanmaktadır. Bu parametrelerle ilgili sonuçlar detaylı olarak sunulmaktadır.

Her $\mathbb{F}_q$ -lineer kodun uygun şekilde seçilmiş bazı $n \geq 1$ tam sayısı, I ideali ve L alt uzayı için bir $C(I, L)$ afin varyete koduna eşit olduğu Teorem 4.32 da verilmektedir.

Şimdi $A_1, \dots, A_n, \mathbb{F}_q$ 'nin boş olmayan altkümeleri olsun ve $A := A_1 \times \dots \times A_n$ olarak tanımlansın. Her $i \in \{1, \dots, n\}$ için $f_i := \prod_{c \in A_i} (x_i - c)$ ve $I := (f_1, \dots, f_n)$ olsun. O halde

$$\begin{aligned} V(I) &= \{p \in \mathbb{F}_q^n \mid \text{her } i = 1, \dots, n \text{ için } f_i(p) = 0\} \\ &= \{p = (p_1, \dots, p_n) \in \mathbb{F}_q^n \mid \text{her } i = 1, \dots, n \text{ için } \prod_{c \in A_i} (p_i - c) = 0\} \\ &= \{p = (p_1, \dots, p_n) \in \mathbb{F}_q^n \mid \text{her } i = 1, \dots, n \text{ için } p_i = a_i, a_i \in A_i\} \\ &= A_1 \times \dots \times A_n = A. \end{aligned}$$

Yani $V(I) = A$ dır. Denklem (4.3)'teki gibi

$$I_q = I + \langle x_1^q - x_1, \dots, x_n^q - x_n \rangle = \langle f_1, \dots, f_n, x_1^q - x_1, \dots, x_n^q - x_n \rangle = I$$

olur çünkü Yardımcı Önerme 2.20'den tüm $i = 1, \dots, n$ için $A_i \subseteq \mathbb{F}_q$ olduğundan her $f_i, x_i^q - x_i$ 'nin bir çarpanıdır. Her $d \geq 0$ tam sayısı için,

$$L_d := \{p + I \mid p = 0 \text{ veya } \deg(p) \leq d\}$$

şeklinde tanımlanan $\mathbb{F}_q[X]/I$ 'nin $\mathbb{F}_q$ -alt uzaylarını ele alalım. Burada $\deg(p), p \in \mathbb{F}_q[X]$ polinomun toplam derecesidir.

5.1 Tanım [3, Definition 3.9] Her $d \geq 0$ tam sayısı için afin kartezyen kod $C(d), \varphi(L_d)$ 'nin görüntüsü olarak tanımlanır.

5.2 Örnek $n = q = 2$ alalım. $A_1 = A_2 = \mathbb{F}_2$ seçersek $f_1(x, y) = (x - 0) \cdot (x - 1) = x^2 - x$ ve $f_2(x, y) = (y - 0) \cdot (y - 1) = y^2 - y$ olur. O halde $I = \langle f_1, f_2 \rangle = I_q$ dir.

$V(I) = A = A_1 \times A_2 = \mathbb{F}_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$ dir. $d = 1$ seçersek, $L_1 = \{p + I \mid p = 0 \text{ veya } \deg(p) \leq 1\}$ olur. Yani polinomlar, $p(x, y) = a + bx + cy$, $a, b, c \in \mathbb{F}_2$ şeklindedir. O halde tüm polinomlar $0, 1, x, y, x + y, x + 1, y + 1, x + y + 1$ olarak elde edilir. $P_1, P_2, P_3, P_4 \in \mathbb{F}_2^2$ olmak üzere afin kartezyen kod

$$\begin{aligned} C(1) &= \varphi(L_1) = \{\varphi(\bar{p}) \mid \bar{p} \in L_1\} \\ &= \{(p(P_1), p(P_2), p(P_3), p(P_4)) \mid p(x, y) \in \mathbb{F}_2[x, y], p = 0 \text{ veya } \deg(p) \leq 1\}. \end{aligned}$$

Şimdi bu kümenin tüm elemanlarını açıkça bulalım. Sırasıyla

Tablo 5.1: Polinomlar ve kod sözcükleri

$p(x, y)$	$(p(P_1), \dots, p(P_4))$
0	(0, 0, 0, 0)
1	(1, 1, 1, 1)
x	(0, 0, 1, 1)
y	(0, 1, 0, 1)
$x + y$	(0, 1, 1, 0)
$x + 1$	(1, 1, 0, 0)
$y + 1$	(1, 0, 1, 0)
$x + y + 1$	(1, 0, 0, 1)

Sonuç olarak

$\{(0, 0, 0, 0), (1, 1, 1, 1), (0, 0, 1, 1), (0, 1, 0, 1), (0, 1, 1, 0), (1, 1, 0, 0), (1, 0, 1, 0), (1, 0, 0, 1)\}$ elde edilir.

5.3 Yardımcı Önerme [3, Lemma 3.10] $\{f_1, \dots, f_n\}$, I için bir Gröbner bazdır.

İspat: $f_i = \prod_{c \in A_i} (x_i - c_i)$ ve $|A_i| = d_i$ olduğundan her $i = 1, \dots, n$ için açıkça $lm(f_i) = x_i^{d_i}$ dir. Buradan

$$\Delta(I) \subseteq \{x_1^{\alpha_1} \dots x_n^{\alpha_n} \mid 0 \leq \alpha_i < d_i, \text{ her } i = 1, \dots, n\}$$

ve Önerme 4.15 kullanılarak

$$|V(I)| = d_1 \dots d_n \leq |\Delta(I)| \leq d_1 \dots d_n$$

elde edilir. Böylelikle, $|\Delta(I)| = d_1 \dots d_n$ elde edilir. Bu durum, $\mathbb{B} := \{f_1, \dots, f_n\}$ kümesinin I için bir Gröbner tabanı olduğunu gösterir. Aksi takdirde, Buchberger algoritmasına göre

$\mathbb{B}$ 'ye baş terimi her $i = 1, \dots, n$ için $x_i^{d_i}$ 'nin katı olmayan bir polinom eklemek gerekir. Bu ise $|\Delta(I)| < d_1 \dots d_n$ sonucunu doğurur ki bu da bir çelişkidir.

□

5.4 Yardımcı Önerme [3, Lemma 3.15] $0 < d_1 \leq \dots \leq d_n$ ve $s < \sum_{i=1}^n (d_i - 1)$ tam sayılar olsun.

$$m(\alpha_1, \dots, \alpha_n) := \prod_{i=1}^n (d_i - \alpha_i)$$

olsun, öyle ki her $i = 1, \dots, n$ için $0 \leq \alpha_i < d_i$ bir tam sayıdır. O halde,

$$\min\{m(\alpha_1, \dots, \alpha_n) \mid \alpha_1 + \dots + \alpha_n \leq s\} = (d_{k+1} - l) \prod_{i=k+2}^n d_i$$

olur, öyle ki k ve l

$$s = \sum_{i=1}^k (d_i - 1) + l, \quad 0 \leq l < d_{k+1} - 1$$

eşitliğiyle tek türlü olarak tanımlanmaktadır. Burada, eğer $k+1 = n$ ise $\prod_{i=k+2}^n d_i = 1$ olduğu anlaşılır ve eğer $s < d_1 - 1$ ise o zaman $k = 0$ ve $l = s$ olarak belirlenmektedir.

İspat: Bir $\alpha = (\alpha_1, \dots, \alpha_n)$ 'de $m(\alpha)$ 'nın minimum olduğunu varsayalım. Bu yardımcı önerme, öyle bir $k \geq 1$ vardır ki

$$\alpha = (d_1 - 1, \dots, d_k - 1, l, 0, \dots, 0), \quad (0 \leq l < d_{k+1} - 1)$$

olduğunu iddia ediyor. Diyelim ki $s = \sum_{i=1}^n \alpha_i$ ve bazı $i_1 \in \{1, \dots, k\}$ için $\alpha_{i_1} < d_{i_1} - 1$ olduğunu varsayalım. Aşağıda verilen (i) ve (ii) durumları oluşur:

(i) $\alpha_{i_2} > 0$ ve $\alpha_{i_1} + \alpha_{i_2} \leq d_{i_1} - 1$ olacak şekilde bir $i_2 \in \{k+1, \dots, n\}$ olduğunu varsayalım.

Bu durumda, α_i yerine $\alpha_{i_1} + \alpha_{i_2}$ ve α_{i_2} yerine 0 yazılırsa,

$$\alpha' = (\alpha_1, \dots, \alpha_{i_1} + \alpha_{i_2}, \dots, \alpha_k, \dots, \alpha_{i_2-1}, 0, \alpha_{i_2+1})$$

olur. Böylece,

$$\begin{aligned} m(\alpha) - m(\alpha') &= \prod_{i=1}^n (d_i - \alpha_i) - m(\alpha') \\ &= (d_{i_1} - \alpha_{i_1}) \cdot (d_{i_2} - \alpha_{i_2}) \prod_{\substack{i=1 \\ i \neq i_1 \\ i \neq i_2}}^n (d_i - \alpha_i) - (d_{i_1} - (\alpha_{i_1} + \alpha_{i_2})) \cdot (d_{i_2} - 0) \cdot \prod_{\substack{i=1 \\ i \neq i_1 \\ i \neq i_2}}^n (d_i - \alpha_i) \end{aligned}$$

Kolaylık olması için

$$A_i := \prod_{\substack{i=1 \\ i \neq i_1 \\ i \neq i_2}}^n (d_i - \alpha_i)$$

olsun.

$$\begin{aligned} m(\alpha) - m(\alpha') &= [(d_{i_1} \cdot d_{i_2} - d_{i_1} \cdot \alpha_{i_2} - \alpha_{i_1} \cdot d_{i_2} + \alpha_{i_1} \cdot \alpha_{i_2}) - ((d_{i_1} \cdot d_{i_2} - \alpha_{i_1} \cdot d_{i_2} - \alpha_{i_2} \cdot d_{i_2}))] \cdot A \\ &= (\alpha_{i_1} \cdot \alpha_{i_2} - d_{i_1} \cdot \alpha_{i_2} + \alpha_{i_2} \cdot d_{i_2}) \cdot A \\ &= (\alpha_{i_1} \cdot \alpha_{i_2} + \alpha_{i_2} \cdot (d_{i_2} - d_{i_1})) \cdot A \geq 0. \end{aligned}$$

Yani, $m(\alpha) \geq m(\alpha')$ elde edilir. Ancak $m(\alpha)$ 'yı minimum kabul ettiğimiz için

$m(\alpha) = m(\alpha')$ olur, böylelikle α yerine α' alınabilir.

(ii) $\alpha_{i_2} > 0$ ve $\alpha_{i_1} + \alpha_{i_2} > d_{i_1} - 1$ olacak şekilde bir $i_2 \in \{k+1, \dots, n\}$ olduğunu varsayalım.

α' 'da α_i yerine $d_{i_1} - 1$ ve α_{i_2} yerine $\alpha_{i_2} - (d_{i_1} - 1 - \alpha_{i_1})$ yazılırsa,

$$\alpha'' = (\alpha_1, \dots, d_{i_1} - 1, \dots, \alpha_k, \dots, \alpha_{i_2} - (d_{i_1} - 1 - \alpha_{i_1}), \dots, \alpha_n)$$

olur. Bu durumda,

$$\begin{aligned} m(\alpha) - m(\alpha'') &= [(d_{i_1} - \alpha_{i_1}) \cdot (d_{i_2} - \alpha_{i_2}) - (d_{i_1} - (d_{i_1} - 1)) \cdot (d_{i_2} - (\alpha_{i_2} - (d_{i_1} - 1 - \alpha_{i_1})))] \cdot A \\ &= [d_{i_1} \cdot d_{i_2} - d_{i_1} \cdot \alpha_{i_2} - \alpha_{i_1} \cdot d_{i_2} + \alpha_{i_1} \cdot \alpha_{i_2} - d_{i_2} + \alpha_{i_2} - d_{i_1} + 1 + \alpha_{i_1}] \cdot A \\ &= (d_{i_1} - 1 - \alpha_{i_1}) \cdot (d_{i_2} - 1 - \alpha_{i_2}) \cdot A \geq 0 \end{aligned}$$

Yani $m(\alpha) \geq m(\alpha'')$ olur. Dolayısıyla $\alpha = \alpha''$ alınabilir.

Sonuç olarak (i) ve (ii)'den $m(\alpha)$ minimum ise $\alpha = (\alpha_1, \dots, \alpha_n)$ 'de $\alpha_i = d_i - 1$ her $i \in \{1, \dots, k\}$ olarak alınabilir. Benzer şekilde, $\alpha_{k+1} = l$ varsayılabilir de gösterilebilir.

□

5.5 Teorem [3, Lemma 3.16] $0 \leq d < \sum_{i=1}^n (d_i - 1)$ olsun. Bu durumda $C(d)$ 'nin minimum mesafesi $(d_{k+1} - l) \prod_{i=k+2}^n d_i$ şeklindedir. Burada k ve l ,

$$d = \sum_{i=1}^k (d_i - 1) + l \quad \text{ile} \quad 0 \leq l < d_{k+1} - 1$$

eşitliğiyle tek türlü olarak tanımlanmaktadır. Eğer $k+1 = n$ ise $\prod_{i=k+2}^n d_i = 1$ olduğu anlaşılır ve $d < d_1 - 1$ ise $k = 0$ ve $l = d$ olarak belirlenmektedir.

İspat: F , n değişkenli bir polinom ve $F + I \in L_d$ olsun ve $J_F := (F, f_1, \dots, f_n)$ tanımlansın.

Tanım gereği,

$\varphi(F + I) \in C(d) = \{(F(P_1), \dots, F(P_m)) \mid P_i \in V(I), i = 1, \dots, m \text{ için}\}$ kod sözcüğünün sıfır olan koordinatlarının sayısı $|V(J_F)|$ 'dir çünkü, herhangi bir i için $P_i \in V(J_F)$ ise $F(P_i) = 0$ 'dır. Dolayısıyla

$$|V(J_F)| \leq (\varphi(F + I)\text{'nin sıfırlarının sayısı}) \text{ olur.}$$

Benzer şekilde herhangi bir i için $F(P_i) = 0$ olsun. Her $i = 1, \dots, n$ için $P_i \in V(I)$ ise $f_i(P_i) = 0$ olur ve $P_i \in V(J_F)$ ise $\varphi(F + I)$ 'nin sıfırlarının sayısı $\leq |V(J_F)|$ olur. Şimdi de $\varphi(F + I)$ 'nin ağırlığını (yani sıfır olmayan yerlerin sayısını) bulalım.

$$wt(\varphi(F + I)) = |V(I)| - |V(J_F)| = \prod_{i=1}^n d_i - |V(J_F)|.$$

Önerme 4.15'dan $|V(J_F)| \leq \Delta(J_F)$ 'dir. F 'nin baş terimi $M := x_1^{\alpha_1} \dots x_n^{\alpha_n}$ olmak üzere Uyarı 3.35'dan

$$\Delta(J_F) \subseteq \Delta(lm(F), lm(f_1), \dots, lm(f_n)).$$

Tanım 3.29'dan

$$\begin{aligned} \Delta(J_F) &\subseteq \Delta(M, x_1^{d_1}, \dots, x_n^{d_n}) \\ &\subseteq \{\tilde{M} \in \mathcal{M} \mid \tilde{M} < M, x_1^{d_1}, \dots, x_n^{d_n} > \text{deki herhangi bir polinomun baş terimi değil}\} \\ &= \{\tilde{M} \in \mathcal{M} \mid \tilde{M}, M \text{ ile } x_i^{d_i} \text{ lere bölünmüyor demek}\}. \end{aligned}$$

Dolayısıyla $|\Delta(J_F)| \leq \prod_{i=1}^n d_i - \prod_{i=1}^n (d_i - \alpha_i)$ olur. Yardımcı Önerme 5.4 kullanılarak

$$\begin{aligned} wt(\varphi(F + I)) = \prod_{i=1}^n d_i - |V(J_F)| &\geq \prod_{i=1}^n d_i - (\prod_{i=1}^n d_i - \prod_{i=1}^n (d_i - \alpha_i)) \\ &= \prod_{i=1}^n (d_i - \alpha_i) \geq (d_{k+1} - l) \prod_{i=k+2}^n d_i \end{aligned}$$

elde edilir. Şimdi de aslında bu alt sınırın, $C(d)$ kodunun en küçük ağırlığı olduğunu gösterelim. Öncelikle $\mathbb{B}_i := \{b_{i_1}, \dots, b_{i_{d_i}}\}, i = 1, \dots, n$ ve

$$G(x_1, \dots, x_n) := \left(\prod_{i=1}^k \prod_{j=1}^{d_i-1} (x_i - b_{ij}) \right) \cdot \prod_{j=1}^l (x_{k+1} - b_{k+1j})$$

olsun. O halde, $der(G) = \prod_{i=1}^k (d_i - 1) + l = d$ olur. Dolayısıyla, $G + I \in L_d$ dir ve $\varphi(G + I) \in C(d) = \varphi(L_d)$ olur. Şimdi de $\varphi(G + I) = (G(P_1), \dots, G(P_m))$ olmak üzere

$wt(G + I)$ 'yı (yani $\varphi(G + I)$ 'nin sıfır olmayan koordinatlarının sayısını) bulalım.

$P = (a_1, \dots, a_k, a_{k+1}, \dots, a_n) \in V(I) = A_1 \times \dots \times A_k \times A_{k+1} \times \dots \times A_n$, öyle ki $G(P) \neq 0$ olsun. O halde

$$G(P) = \prod_{i=1}^k \prod_{j=1}^{d_i-1} (a_i - b_{ij}) \prod_{j=1}^l (a_{k+1} - b_{k+1j}).$$

Bu durumda $a_{k+1} \in A_{k+1}$, $a_{k+1} \neq b_{k+1j}$, $j = 1, \dots, l$ ise $\prod_{j=1}^l (a_{k+1} - b_{k+1j}) \neq 0$ olur.

Bu şekildeki noktaların sayısı $|A_{k+1}| - l = d_{k+1} - l$ tanedir. Yani a_{k+1} 'i $d_{k+1} - l$ farklı şekilde seçilebilir. Şimdi de $\prod_{i=1}^k \prod_{j=1}^{d_i-1} (a_i - b_{ij})$ 'nin sıfır olmadığı noktaları bulalım, yani $i = 1, \dots, k$ ve $j = 1, \dots, d_i-1$ için $a_i \neq b_{ij}$ dir. Bu durumda $j = d_i, i = k+1, \dots, n$ için $a_i \neq b_{ij}$ olur. Yani $a_i = b_{idi} \in A_i, i = k+2, \dots, n$ yazılabilir. Bunlar, $\prod_{i=k+2}^n d_i$

tanedir. Dolayısıyla $(d_{k+1} - l) \cdot \prod_{i=k+2}^n d_i$ nokta için $\varphi(G + I)$ sıfırdan farklıdır. Yani,

$wt(\varphi(G + I)) = (d_{k+1} - l) \cdot \prod_{i=k+2}^n d_i$ dir. Sonuç olarak $C(d)$ 'nin minimum mesafesi Teorem

2.33'den $(d_{k+1} - l) \cdot \prod_{i=k+2}^n d_i$ olarak elde edilir.

□

Teorem 5.5'in ispatı ile [5, Theorem 3.8]'de sunulan orijinal ispatla karşılaştırdığımızda, ayak izi tekniğinin ispatta önemli bir basitleştirme sağladığı görülmektedir. Bu teknik daha önce [7]'de genelleştirilmiş Reed-Muller kodlarının ve [8]'de afin kartezyen kodların yüksek Hamming ağırlıklarını incelemek için kullanılmaktadır.

Şimdi de $A = A_1 \times \dots \times A_n$ olduğunu hatırlayalım. Afin kartezyen kod $C(d)$ nin boyutu $boy(C(d))$ ile ilgili sonuçları sunalım.

5.6 Yardımcı Önerme [3, Lemma 3.11] A 'nın ideali $I(A) = I$ 'dir.

Hatırlayalım ki φ bir izomorfizma olduğundan ve $C(d) = \varphi(L_d)$ eşitliğinden dolayı

$$boy(C(d)) = boy(L_d)$$

elde edilir. Öncelikle

$$\Delta(I)_{\leq d} := \{ M \in \Delta(I) \mid der(M) \leq d \}$$

olsun.

5.7 Önerme [3, Proposition 3.12] $\{M + I \mid M \in \Delta(I)_{\leq d}\}$ kümesi, L_d için bir tabandır.

5.8 Yardımcı Önerme [3, Lemma 3.13] $C(d)$ 'nin boyutu $\text{boy}(C(d)) = |\Delta(I)_{\leq d}|$ 'dir.

Özellikle, tüm $d \geq \sum_{i=1}^n (d_i - 1)$ için $\text{boy}(C(d)) = d_1 \cdots d_n$ ve $d(C(d)) = 1$ dir.

İspat: Yardımcı Önerme 5.3 ve Önerme 5.7 kullanılarak ispatlanabilir (bkz. [3]).

5.9 Teorem [3, Lemma 3.14] $0 \leq d < \sum_{i=1}^n (d_i - 1)$ için $C(d)$ 'nin boyutu aşağıdaki şekildedir:

$$\begin{aligned} \text{boy}(C(d)) &= \binom{n+d}{d} - \sum_{i=1}^n \binom{n+d-d_i}{d-d_i} + \dots + \\ &(-1)^j \sum_{1 \leq i_1 < \dots < i_j \leq n} \binom{n+d-d_{i_1}-\dots-d_{i_j}}{d-d_{i_1}-\dots-d_{i_j}} + \dots + (-1)^n \binom{n+d-d_1-\dots-d_n}{d-d_1-\dots-d_n} \end{aligned}$$

burada $b < 0$ ise $\binom{a}{b} = 0$ kabul edilir.

İspat: [3]

6. KAYNAKLAR

- [1] **Ling, S., and Xing, C.** (2004). *Coding Theory: A First Course*. Cambridge University Press, İngiltere, 222.
- [2] **Fitzgerald, J.** (1996). Applications of Gröbner Bases to Linear Codes. Doctoral dissertation, Louisiana State University and Agricultural & Mechanical College, Baton Rouge, 88.
- [3] **Carvalho, C.** (2024). Applications of results from commutative algebra to the study of certain evaluation codes. Article, Lecture Notes of CIMPA Research School on Algebraic Methods in Coding Theory, Sao Paulo, Brazil, 23 .
- [4] **Cox, D., Little, J. and O’Shea, D.** (2007). *Ideals, Varieties, and Algorithms*. Springer, New York, 3rd.
- [5] **López, H. H., Rentería-Márquez, C. and Villarreal, R. H.** (2014). Affine cartesian codes. *Designs, Codes and Cryptography*, vol. 71, pp. 5-19.
- [6] **Geil, O. and Thomsen, C.** (2013). Weighted Reed-Muller codes revisited. *Designs, Codes and Cryptography*, vol. 66, pp. 195-220.
- [7] **Geil, O.** (2008). On the second weight of generalized Reed-Muller codes. *Designs, Codes and Cryptography*, vol. 48, pp. 323-330.
- [8] **Carvalho, C.** (2013). On the second Hamming weight of some Reed-Muller type codes. *Finite Fields and Their Applications*, vol. 24, pp. 88-94.
- [9] **Marcolla, C., Orsini, E. and Sala, M.** (2012). Improved decoding of affine-variety codes. *Journal of Pure and Applied Algebra*, vol. 216 (7), pp. 1533-1565.
- [10] **Høholdt, T.** (1998). On (or in) Dick Blahut’s footprint. *Codes, Curves and Signals: Common Threads in Communications*, pp. 3-7.
- [11] **Geil, O. and Özbudak, F.** (2019). On affine variety codes from the Klein quartic. *Cryptography and Communications*, vol. 11 (2), pp. 237-257.
- [12] **Buchberger, B.** (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Doctoral dissertation, Universität Innsbruck, Innsbruck, Austria, 252.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Cemile CÜR

Doğum tarihi ve yeri :

e-posta :

Öğrenim Bilgileri

Derece	Okul / Program	Yıl
Lisans	Balıkesir Üniversitesi / Matematik Bölümü	2022
Lise	15 Temmuz Şehitler Anadolu Lisesi	2018