



**GRÖBNER TABANLARI VE BAZI UYGULAMALARINA GENEL BİR
BAKIŞ**

Sevde ÖZEN

Yüksek Lisans Tezi

Matematik Ana Bilim Dalı

Dr. Öğr. Üyesi Abdullah ÇAĞMAN

AĞRI-2019

(Her hakkı saklıdır.)

T.C.
AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

Sevde ÖZEN

**GRÖBNER TABANLARI VE BAZI UYGULAMALARINA GENEL BİR
BAKIŞ
YÜKSEK LİSANS TEZİ**

TEZ YÖNETİCİSİ
Dr. Öğr. Üyesi Abdullah ÇAĞMAN

AĞRI-2019

TEZ KABUL VE ONAY TUTANAĞI
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

.....danışmanlığında, tarafından
hazırlanan bu çalışma/...../..... tarihinde aşağıdaki jüri tarafından.
..... Anabilim Dalı'ndatezi
olarak kabul edilmiştir.

Başkan :

İmza:

Jüri Üyesi :

İmza:

Jüri Üyesi :

İmza:

Jüri Üyesi :

İmza:

Jüri Üyesi :

İmza:

Yukarıdaki imzalar adı geçen öğretim üyelerine ait olup;

Enstitü Yönetim Kurulunun/.../201.. tarih ve / nolu kararı ile
onaylanmıştır.

.... / /

Doç. Dr. İbrahim HAN

Enstitü Müdürü

ÖZET
YÜKSEK LİSANS TEZİ
GRÖBNER TABANLARI VE BAZI UYGULAMALARINA GENEL BİR
BAKIŞ

Sevde ÖZEN
Ağrı İbrahim Çeçen Üniversitesi
Matematik Anabilim Dalı
Cebir ve Sayılar Teorisi Bilim Dalı
Tez Danışmanı: Dr. Öğr. Üyesi Abdullah ÇAĞMAN
2019, 42 sayfa

Bu tezde, Gröbner tabanı incelenerek bazı uygulamalarına yer verilmiştir. Tezin ilk bölümünde Gröbner tabanının tarihçesinden söz edilmiş, ikinci bölümünde Gröbner tabanını anlamak için polinom halkaları ve gerekli teoremlerden bahsedilmiş, üçüncü bölümünde Gröbner tabanı teorem ve örneklerine yer verilmiştir. Son olarak dördüncü bölümünde ise Gröbner tabanı uygulamalarından bahsedilmiş ve örneklerine yer verilmiştir.

Bu tezin amacı, Gröbner tabanını incelemek ve bazı uygulamaları hakkında çalışmalar yapmaktır.

42 sayfa

Anahtar sözcükler: Polinom Halkaları, Gröbner Tabanı, Burchberger Algoritması, Gröbner Tabanı Uygulamaları.

ABSTRACT
MASTER'S THESIS
A GENERAL OVERVIEW TO GROBNER BASES AND ITS
APPLICATIONS

Sevde ÖZEN

Ağrı İbrahim Çeçen University

Department of Mathematics

Discipline of Algebra and Number Theory

Advisor: Assist. Prof. Dr. Abdullah ÇAĞMAN

2019, Page: 42

In this thesis, Gröbner base is examined and some applications are given. In the first part of the thesis, the history of the Gröbner base is mentioned, in the second part the polynomial rings and necessary theorems for understanding the Gröbner base are mentioned and in the third part the Gröbner base theorems and examples are given. Finally, in the fourth part, applications of Gröbner base are mentioned and examples are given.

The aim of this thesis is to examine the Gröbner base and to study some of its applications.

42 pages

Keywords: Polynomial Rings, Gröbner Basis, Buchberger Algorithm, Gröbner Basis Applications.

ÖN SÖZ ve/veya TEŞEKKÜR

Yüksek Lisans/Doktora eğitimim boyunca, benden bilgi ve deneyimlerini esirgemeyen, çalışmalarımın tamamlanabilmesi için her türlü şartı sağlayan ve bana her zaman her türlü desteği sunan çok değerli danışman hocam Sayın Dr. Öğr. Üyesi Abdullah ÇAĞMAN’a teşekkürlerimi sunarım.

Eğitimim tüm süreçlerinde her türlü destekleriyle beni hiç yalnız bırakmayan aileme özellikle hayattaki en büyük şansım olan sevgili anneme teşekkürü borç bilirim. Hayatımın her alanında olduğu gibi, tez çalışmamı hazırlarken de her aşamasında bana yardımcı olan sevgili eşime sonsuz teşekkür ederim.

20/08/2019

Sevde ÖZEN

İÇİNDEKİLER

ÖZET.....	ii
ABSTRACT	iii
ÖN SÖZ ve/veya TEŞEKKÜR	iv
SİMGELER ve KISALTMALAR DİZİNİ	vi
1. GİRİŞ	1
2. KURAMSAL TEMELLER	3
3.MATERYAL ve YÖNTEM	10
3.1 Tek Değişkenli Polinomlar için İndirgeme.....	10
3.2 Terim Sıralaması ve İndirgemeler	11
3.3 Polinomların İndirgemesi ve Bölme Algoritması.....	12
3.4 Gröbner Tabanı ile İlgili Tanımlar ve Teoremler	15
3.5 Eleminasyon	19
4. ARAŞTIRMA BULGULARI	21
4.1 Temel Gröbner Tabanı Uygulamaları.....	21
4.2 Üç Renk Problemi.....	27
4.3 Tamsayı Programlama	31
4.4 Sudoku Oyununda Gröbner Tabanı	36
4.4.1.Sudoku'yu Tanımlama ve Modelleme.....	36
KAYNAKLAR	41
ÖZGEÇMİŞ	42

SİMGELER VE KISALTMALAR DİZİNİ

$<$	Küçüktür
$>$	Büyüktür
$\leq$	Küçük veya Eşittir
$\geq$	Büyük veya Eşittir
$\subset$	Alt Küme
$\subseteq$	Alt Kümesi veya Eşit
$\supseteq$	Kapsar veya Eşit
$\cup$	Birleşim
$\cap$	Kesişim
$\in$	Elemanıdır
$\notin$	Elemanı Değildir
$\mathbb{N}$	Doğal Sayılar Kümesi
$\mathbb{R}$	Reel Sayılar Kümesi
$\mathbb{R}^n$	n –boyutlu Euclidean Uzay
$\deg(f)$	f polinomunun derecesi
$lt(f)$	f polinomunun baş terimi
$lc(f)$	f polinomunun baş katsayısı
$lp(f)$	f polinomunun en büyük kuvvet çarpımı
$lex(<_{lex})$	lexicographical terim sıralaması
$\deglex(<_{deglex})$	degree lexicographical terim sıralaması
$\degrevlex(<_{degrevlex})$	degree reverse lexicographical terim sıralaması

1.GİRİŞ

Gröbner tabanları polinom halkaları teorisinde kullanılan çok önemli bir araçtır. Gröbner tabanları teorik olarak 1964 yılında Hironaka, daha önce de 1899 yılında Gordan tarafından kullanılmıştı. 1965 yılında Buchberger Gröbner tabanlarının hesaplanmasını sağlayan bir algoritma buldu. Buchberger algoritmasının polinom sistemleri açısından önemi lineer cebirdeki Gauss yok etme yöntemiyle karşılaştırılabilir. Bu algoritmanın polinom denklemlerinin köklerinin bulunması, bir polinomun verilen başka polinomlar cinsinden ifade edilmesi gibi pek çok uygulaması vardır. Gröbner tabanları, yaygın olarak hesaplama zorluğu olarak kabul edilen problemleri çözmek için kullanılabilir. Gröbner tabanı kullanılarak, örneğin karmaşık sayılara göre bir polinom denklemleri kümesinin çözülebilirliğine karar vermek mümkündür ki aslında dikkat çekici olan, tamsayılar üzerinde bir polinom denklemleri kümesinin çözülebilirliğine karar vermek için bir algoritmanın olamayacağını 1970 de gösterilmiş olmasıdır (Hilbertin 10. Problemi). Gröbner tabanının kurulmasındaki zorluk için bir başka gösterge, bu sorunun en az 65 yıl açık kalmasıdır. Gordan'ın 1899 tarihli çalışmasında, Gröbner tabanlarının ilk kez örtülü olarak tanıtıldığı, ancak bunların hesaplanması için herhangi bir algoritma verilmediğine dikkat çekildi.

Gröbner taban hesaplaması, polinom denklem sistemlerinin çözümlenmesi ve yansıma veya rasyonel dönüşümler altında cebirsel çeşitlerin görüntüsel hesaplanması için kullanılan temel pratik araçlardan biridir. Bir Gröbner tabanı, matematik, doğal ve teknik bilimlerdeki birçok temel problem için basit algoritmik çözümlere izin veren belirli özelliklere sahip çok değişkenli doğrusal olmayan polinomlar kümesidir. Bu tür problemlerin örnekleri şunlardır: cebirsel denklem sistemlerinin çözümü, polinomların diğer polinomlar açısından temsili, doğrusal olmayan kriptosistemlerin analizi ve yapımı, kapalı form toplama ve özel fonksiyonlar içeren ifadelerin entegrasyonu, lineer kapalı form çözümü sınır değer problemleri (diferansiyel denklemler). Örneğin cebirsel teoremlerin otomatik kanıtı ve keşfi, grafik renklendirmelerinin oluşturulması ve Sudoku oyunlarının çözümü gibi çok uzak bir şekilde ortaya çıkan problemler, Gröbner taban hesaplamalarına indirgenebilir. Son zamanlarda Gröbner taban metodolojisi ile çözülen doğal ve

teknik bilimlerdeki problemlerin bazı örnekleri; petrol platformlarının akıllı kontrolü, yazılımın tersine mühendisliği, türler arasında genetik ilişki bulunması ve ters robot kinematiğinin çözülmesi şeklindedir. Bu tezin amacı, Gröbner tabanı konusunu incelemek ve bazı uygulamaları hakkında çalışmalar yapmaktır.



2. KURAMSAL TEMELLER

Bu kısımda cebirde önemli bir yer tutan polinomlar kavramı incelenecektir. Aksi söylenmedikçe “ R ” bir değişmeli halka olarak düşünülecektir.

Tanım 2.1: x bir bilinmeyen ve $a_0, a_1, a_2, \dots, a_n \in R$ olmak üzere,

$$p(x) = a_0 + a_1x + \dots + a_nx^n$$

şeklindeki bir ifadeye R üzerinde bir polinom denir. R üzerindeki tüm polinomların kümesi $R[x]$ ile gösterilir.

$p(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ olsun. Burada $i = 0, 1, \dots, n$ için a_i lere polinomun katsayıları ve a_0 ’a da polinomun sabit terimi denir. Eğer $a_n \neq 0$ ise a_n ’ye baş katsayı, n ye de $p(x)$ polinomunun derecesi denir ve der $p(x)$ veya $d^0p(x)$ ile gösterilir. Eğer R birimli bir halka ve $a_n = 1$ ise $p(x)$ polinomuna monik polinom denir. R nin herhangi bir elemanı da polinom olarak düşünülebilir. Bu polinomlara sabit polinomlar denir. $R[x]$ de sabit polinomun derecesi sıfırdır. Bütün katsayıları sıfır olan polinoma sıfır polinom denir. Sıfır polinomun derecesi $-\infty$ olarak kabul edilir.

Örnek 2.2: $p(x) = 2 + 3x^2 - 4x^5 \in \mathbb{Z}[x]$ polinomunun baş katsayısı 4 ve der $p(x) = 5$ dir. Ayrıca, $q(x) = \bar{1} + \bar{2}x + \bar{2}x^3 \in \mathbb{Z}_3[x]$ polinomunun baş katsayısı $\bar{2}$ ve der $q(x) = 3$ tür.

Tanım 2.3: $p(x) = a_0 + a_1x + \dots + a_nx^n$ ve $q(x) = b_0 + b_1x + \dots + b_mx^m \in R[x]$ de iki polinom olsunlar. $i > n$ için $a_i = 0$ ve $i > m$ için $b_i = 0$ olmak üzere;
 $p(x) = q(x) \Leftrightarrow \forall i$ için $a_i = b_i$ olmasıdır.

Tanım 2.4: $p(x) = a_0 + a_1x + \dots + a_nx^n$ ve $q(x) = b_0 + b_1x + \dots + b_mx^m \in R[x]$ olsun. $\forall i$ için $c_i = a_i + b_i$ olmak üzere; $p(x) + q(x) = c_0 + c_1x + \dots + c_tx^t$ olarak tanımlanır. Bu iki polinomun çarpımı da;

$$d_k = a_kb_0 + a_{k-1}b_1 + \dots + a_0b_k$$

olmak üzere;

$$p(x)q(x) = d_0 + d_1x + \cdots + d_kx^k + \cdots + d_5x^5$$

olarak tanımlanır.

Örnek 2.5: $p(x) = 2 - x^2 + x^3$ ve $q(x) = x^2 - 4x^3 \in \mathbb{Z}[x]$ polinomları için $p(x) + q(x)$ toplamını ve $p(x) \cdot q(x)$ çarpımını bulunuz.

$$c_0 = a_0 + b_0 = 2 + 0 = 2$$

$$c_1 = a_1 + b_1 = 0 + 0 = 0$$

$$c_2 = a_2 + b_2 = (-1) + 1 = 0$$

$$c_3 = a_3 + b_3 = 1 + (-4) = -3$$

olup,

$$p(x) + q(x) = 2 - 3x^3$$

olarak bulunur.

Şimdi de $p(x) \cdot q(x)$ çarpımı bulunmaya çalışalım:

$$d_0 = a_0b_0 = 2 \cdot 0 = 0$$

$$d_1 = a_1b_0 + a_0b_1 = 0 \cdot 0 + 2 \cdot 0 = 0$$

$$d_2 = a_2b_0 + a_1b_1 = (-1) \cdot 0 + 0 \cdot 0 + 2 \cdot 1 = 2$$

$$d_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = 1 \cdot 0 + (-1) \cdot 0 + 0 \cdot 1 + 2 \cdot (-4) = -8$$

$$d_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 0 \cdot 0 + 1 \cdot 0 + (-1) \cdot 1 + 0 \cdot (-4) + 2 \cdot 0 = -1$$

$$\begin{aligned} d_5 &= a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 \\ &= 0 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 + (-1) \cdot 4 + 0 \cdot 0 + 2 \cdot 0 = 5 \end{aligned}$$

$$\begin{aligned} d_6 &= a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4 + a_1b_5 + a_0b_6 \\ &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 + 1 \cdot (-4) + (-1) \cdot 0 + 0 \cdot 0 + 2 \cdot 0 = -4 \end{aligned}$$

ve

$$d_7 = d_8 = \cdots = 0$$

olup,

$$\begin{aligned} p(x)q(x) &= d_0 + d_1x + \cdots + d_6x^6 \\ &= 0 + 0x + 2x^2 + (-8)x^3 + (-1)x^4 + 5x^5 + (-4)x^6 \\ &= 2x^2 - 8x^3 - x^4 + 5x^5 - 4x^6 \text{ dir.} \end{aligned}$$

Teorem 2.6: R bir halka ise $R[x]$ de bir halkadır (Yeşilot ve Özavşar 2012).

İspat: Tanım 2.4 de tanımlanan toplama ve çarpma işlemlerine göre $R[x]$ in bir halka yapısına sahip olduğu kolaylıkla gösterilebilir. Burada $R[x]$ toplama işlemine göre etkisiz elemanı 0_R polinomudur. Toplama işlemine göre bir polinomun tersi katsayıların R halkasındaki toplama işlemine göre tersleri alınarak elde edilen polinomdur. Diğer halka aksiyomları R nin bir halka oluşu ve $R[x]$ de tanımlanan toplama çarpma işlemleri kullanılarak gösterilebilir.

Teorem 2.7:

- (i) R değişmeli bir halka ise $R[x]$ de değişmeli bir halkadır.
- (ii) R birimli bir halka ise $R[x]$ de birimli bir halkadır.
- (iii) R bir tamlık bölgesi ise $R[x]$ de bir tamlık bölgesidir

(Yeşilot ve Özavşar 2012).

İspat:

(i) R değişmeli bir halka olsun. Teorem 2.6' dan $R[x]$ de bir halkadır.

$p(x) = a_0 + a_1x + \dots + a_nx^n$ ve $q(x) = b_0 + b_1x + \dots + b_mx^m$ $R[x]$ den alınan iki

polinom olsun. Ayrıca, $p(x)q(x) = c_0 + c_1x + \dots + c_kx^k$ ve

$q(x)p(x) = d_0 + d_1x + \dots + d_tx^t$ olsun. Burada her $i = 0, 1, 2, \dots$ için,

$$c_i = a_0b_i + a_1b_{i-1} + \dots + a_ib_0 = b_ia_0 + b_{i-1}a_1 + \dots + b_0a_i = d_i$$

elde edilir. Böylece $p(x)q(x) = q(x)p(x)$ olacaktır. Bu durumda, $R[x]$ değişmeli bir halkadır.

(ii) R birimli bir halka olsun. Teorem 2.6 dan $R[x]$ de bir halkadır. R nin birimi 1_R , aynı zamanda $R[x]$ de bir sabit polinomdur. Ayrıca her $p(x) \in R[x]$ için $1_R \cdot p(x) = p(x) \cdot 1_R = p(x)$ olur. Böylece $R[x]$ birimli halkadır.

(iii) R bir tamlık bölgesi olsun. Teorem 2.6 dan ve yukarıdaki (i) ve (ii) den $R[x]$ değişmeli ve birimli bir halkadır. Şimdi $R[x]$ in sıfır bölen içermediği gösterilecektir.

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$

$$q(x) = b_0 + b_1x + \cdots + b_mx^m$$

$R[x]$ de sıfırdan farklı iki polinom olsun. Şu halde $a_i \neq 0, b_j \neq 0, k \geq 1$ için $a_{i+k} = 0$ ve $b_{j+k} = 0$ olmak üzere a_i ve b_j katsayıları vardır. $p(x)q(x) = c_0 + c_1x + \cdots + c_tx^t$ polinomu için $c_{i+j} = a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_ib_j + \cdots + a_{i+j}b_0$ olur. $a_i \neq 0, b_j \neq 0$ ve R bir tamlık bölgesi olduğundan $c_{i+j} = a_ib_j \neq 0$ olur. Şu halde $R[x]$ sıfır bölensiz olup bir tamlık bölgesidir.

Teorem 2.8: $p(x), q(x) \in R[x]$ olsun.

- (i) $\text{der}[p(x) + q(x)] \leq \max\{\text{der } p(x), \text{der}(q(x))\}$
- (ii) $\text{der}[p(x)q(x)] \leq \text{der } p(x) + \text{der } q(x)$
- (iii) R sıfır bölensiz ise $\text{der}[p(x)q(x)] = \text{der } p(x) + \text{der } q(x)$
- (iv) $p(x)$ veya $q(x)$ polinomlarından birinin baş katsayısı R nin sıfır böleni değilse $\text{der}[p(x)q(x)] = \text{der } p(x) + \text{der } q(x)$ dir

(Yeşilot ve Özavşar 2012).

Tanım 2.9: $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ ve $r \in R$ olsun.

$f(r) = a_0 + a_1r + \cdots + a_nr^n \in R$ ye f polinomunun R deki değeri denir. Eğer $r \in R$ için, $f(r) = 0$ ise r ye f polinomunun kökü veya sıfırı denir.

Teorem 2.10: R bir değişmeli halka ve $f, g \in R[x]$ olsun. $g \neq 0$ ve $g(x)$ polinomunun baş katsayısı terslenebilsin. Bu takdirde; $f(x) = q(x)g(x) + r(x)$ ve $\text{der } r(x) < \text{der } g(x)$ olacak şekilde tek türlü olarak belirli $\exists q, r \in R[x]$ polinomları bulunabilir (Yeşilot ve Özavşar 2012).

Sonuç 2.11: F bir cisim ise $\forall f, g \in F[x], g \neq 0$ polinomuna bölme algoritması uygulanabilir (Çallıalp 2009).

Sonuç 2.12: $f \in R[x]$ ve $a \in R$ olsun. $f(x) = (x - a)q(x) + f(a)$ olacak şekilde bir ve yalnız bir $q(x) \in R[x]$ vardır (Çallıalp 2009).

İspat: $f(x)$ ve $(x - a)$ polinomlarına bölme algoritması uygulansın.

$f(x) = (x - a)q(x) + r(x)$ olacak şekilde $\exists q, r \in R[x]$ bulunabilir ve

$\deg r < \deg(x - a) = 1$, yani $r(x) = r \in R$ sabittir. Yukarıdaki eşitlikte $x = a$ alınırsa; $f(a) = r(a) = r$ bulunur ve $q(x)$ teklikle belirlidir.

Önerme 2.13: F bir cisim ve $f \in F[x], \deg f \geq 1$ olsun. (f) esas ideali için $F[x]/(f)$ bölüm halkasının tam temsilciler sistemi olarak, $\deg r < \deg f$ olan $r \in F[x]$ polinomları alınabilir (Çallıalp 2009).

İspat: $\forall g \in F[x]$ polinomu için f ile kalanlı bölerek;

$$g(x) = f(x)q(x) + r(x), \deg r < \deg f$$

olacak şekilde, $\exists q, r \in F[x]$ bulunabilir. Şu halde $g \equiv r \pmod{f}$ dir. Yani her $\pmod{f}$ denklik sınıfında $\deg r < \deg f$, olmak üzere $\exists r \in F[x]$ vardır. Ayrıca, $r_1 \neq r_2, \deg r_1 < \deg f, \deg r_2 < \deg f$ ise $r_1, r_2 \in F[x]$ polinomları aynı denklik sınıfında olmazlar. Gerçekten,

$$r_1 \equiv r_2 \pmod{f} \Leftrightarrow r_1 - r_2 \in (f)$$

$$\Leftrightarrow r_1 - r_2 = fg, \exists g \in F[x]$$

demektir. $\deg(r_1 - r_2) \leq \max(\deg r_1, \deg r_2) < \deg f$ olduğundan, yukarıdaki denklik sağlanır. Sonuç olarak; $F[x]/(f)$ bölüm halkası için,

$$\{r \in F[x] : \deg r < \deg f\}$$

kümesi her sınıftan bir ve yalnız bir eleman alınarak elde edilmiştir, yani bir tam temsilciler sistemidir.

Tanım 2.14: R bir halka $x_1, x_2, \dots, x_n$ ler birer bilinmeyen olmak üzere; $R[x_1, x_2, \dots, x_n] = R[x_1, x_2, \dots, x_{n-1}][x_n]$ şeklinde tanımlanır. Tümevarım ile $R[x_1, x_2, \dots, x_n]$ in bir halka yapısına sahip olduğu gösterilebilir. $R[x_1, x_2, \dots, x_n]$ halkasına n değişkenli bir polinomlar halkası denir.

Tanım 2.15: $f \in k[x_1, x_2, \dots, x_n]$ için $f = 0$ denkleminin çözümlerinin kümesi $V(f) = \{(a_1, a_2, \dots, a_n) \in k^n \mid f(a_1, a_2, \dots, a_n) = 0\} \subseteq k^n$ şeklindedir. $V(f)$ kümesine f tarafından tanımlanan varyete denir.

Tanım 2.16: $f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$ polinomları verilsin.

$f_1 = 0, f_2 = 0, \dots, f_s = 0$ sisteminin tüm çözümleri $V(f_1, f_2, \dots, f_s)$ varyete kümesi olarak tanımlanır ve

$$V(f_1, f_2, \dots, f_s) = \{a_1, a_2, \dots, a_n\} \in k^n \mid f_i(a_1, a_2, \dots, a_n) = 0, i = 1, 2, \dots, s\}$$

şeklindedir. Burada;

$$V(f_1, f_2, \dots, f_s) = \bigcap_{i=1}^s V(f_i) \text{ şeklindedir.}$$

Örneğin; $V(x^2 + y^2 - 4, x - 4y^2) \subseteq \mathbb{R}^2$ varyete kümesi $x^2 + y^2 = 4$ çemberi ile $x = 4y^2$ parabolünün $x - y$ koordinat düzlemindeki kesişimidir.

Bununla beraber genel olarak;

$$S = \{f \mid f \in k[x_1, x_2, \dots, x_n]\} \subseteq k[x_1, x_2, \dots, x_n] \text{ ise}$$

$$V(S) = \{(a_1, a_2, \dots, a_n) \in k^n \mid \forall f \in S \text{ için } f(a_1, a_2, \dots, a_n) = 0\}$$

kümesi tanımlanır.

Teorem 2.16 (Hilbert Taban Teoremi):

k bir cisim ve $k[x_1, x_2, \dots, x_n]$ k cismi üzerine n deęiřkenli bir polinom halkası olsun.

- i) I , $k[x_1, x_2, \dots, x_n]$ halkasının herhangi bir ideali ise $I = \langle f_1, f_2, \dots, f_s \rangle$ olacak řekilde $f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$ polinomları vardır.
- ii) Eęer $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$ $k[x_1, x_2, \dots, x_n]$ halkasının ideallerin artan bir zinciri ise $I_N = I_{N+1} = I_{N+2} = \dots$ olacak řekilde bir $N \in \mathbb{N}$ vardır

(Adams and Lousaunau 1994).

Tanım: R bir halka I , R halkasının herhangi bir ideali olsun. R 'nin $I = \langle a_1, a_2, \dots, a_s \rangle$ olacak řekilde $a_1, a_2, \dots, a_s$ elemanları varsa I idealine **sonlu üretilmiř ideal** denir.

3. MATERYAL VE METOD

3.1 Tek Değişkenli Polinomlar İçin İndirgeme

Tanım 3.1.1: $0 \neq f \in k[x]$ için f polinomundaki x değişkeninin en büyük kuvvetine f polinomunun derecesi denir ve $\deg(f)$ ile gösterilir.

Tanım 3.1.2: $0 \neq f \in k[x]$ için f polinomundaki en büyük dereceli terime f polinomunun baş terimi denir ve $lt(f)$ ile gösterilir.

Tanım 3.1.3: $0 \neq f \in k[x]$ için f polinomundaki baş terimin kat sayısına f polinomunun baş katsayısı denir ve $lc(f)$ ile gösterilir.

$a_0, a_1, \dots, a_n \in k$ ve $a_n \neq 0$ olmak üzere

$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ise

$\deg(f) = n, lt(f) = a_n x^n, lc(f) = a_n$ olur.

Tanım 3.1.4: $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ve

$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0,$

$n = \deg(f) \geq m = \deg(g)$ olmak üzere iki polinom ise f nin g ile bölünmesinde ilk adım $\frac{a_n}{b_m} x^{n-m} \cdot g$ çarpımını f polinomundan çıkarmaktır.

Verilen gösterim kullanılarak bu çarpımda g polinomunun çarpanının $\frac{lt(f)}{lt(g)}$ olduğu görülebilir.

Böylece $h = f - \frac{lt(f)}{lt(g)} \cdot g$ nin ilk kalan olduğu görülür.

Bu işleme f polinomunun g polinomu tarafından h polinomuna indirgenmesi denir ve $f \xrightarrow{g} h$ ile gösterilir.

Teorem 3.1.5: k değişmeli bir cisim ve $0 \neq g, f \in k[x]$ olsun.

$f = q \cdot g + r$ ve $r = 0$ ya da $\deg(r) < \deg(g)$ olacak şekilde tek türlü belirli $q, r \in k[x]$ vardır (Adams and Lousaunau 1994).

Algoritma 3.1.6: Tek Değişkenli Polinomlar İçin Bölme Algoritması

Giriş: $g \neq 0$ olmak üzere $f, g \in k[x]$ alınsın.

Çıkış: $\exists q, r \in k[x] f = q \cdot g + r, r = 0$ veya $\deg(r) < \deg(g)$

Başlangıç: $q := 0; r := f$

Döngü: $r \neq 0$ ve $\deg(g) \leq \deg(r)$ olduğu sürece aşağıdaki işlemler yapılır.

$$q := q + \frac{lt(r)}{lt(g)}, \quad r := r - \frac{lt(r)}{lt(g)} \cdot g,$$

Algoritma r polinomu $r = 0$ veya g polinomunun derecesinden kesinlikle daha küçük bir dereceye sahip oluncaya kadar döngüdeki adımlar tekrarlanır.

3.2 Terim Sıralamaları Ve İndirgemeler

Tanım 3.2.1: T^n üzerinde aşağıdaki iki koşulu sağlayan “ $<$ ” tam sıralamasına terim sıralaması denir.

- (i) $X^\beta \neq 1$ olan her $X^\beta \in T^n$ için $1 < X^\beta$ dir.
- (ii) $X^\alpha < X^\beta$ ise her $X^\gamma \in T^n$ için $X^\alpha \cdot X^\gamma < X^\beta \cdot X^\gamma$ dir.

Tanım 3.2.2: $x_1 > x_2 > x_3 > \dots > x_n$ olmak üzere T^n üzerinde

$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n), \beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ için;

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \alpha \text{ ve } \beta \text{ içinde soldan itibaren farklı ilk} \\ \alpha_i \text{ ve } \beta_i \text{ koordinatlarının } \alpha_i < \beta_i \text{ sağlamasıdır.} \end{cases}$$

biçiminde tanımlanan terim sıralamasına lexicographical sıralama olarak adlandırılır ve $lex(<_{lex})$ ile gösterilir.

Tanım 3.2.3: $x_1 > x_2 > x_3 > \dots > x_n$ olmak üzere T^n üzerinde,

$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n), \beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ için;

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \text{ ya da} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ ise olmak üzere} \\ \text{lex sıralamasına göre } X^\alpha < X^\beta \text{ olmalıdır.} \end{cases}$$

biçiminde tanımlanan terim sıralaması degree lexicographical sıralama olarak adlandırılır ve $deglex(<_{deglex})$ ile gösterilir.

Tanım 3.2.4: $x_1 > x_2 > x_3 > \dots > x_n$ olmak üzere T^n üzerinde

$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n), \beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ için;

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \text{ ya da} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ ise } \alpha \text{ ve } \beta \text{ içinde sağdan itibaren} \\ \text{farklı ilk } \alpha_i \text{ ve } \beta_i \text{ kordinatları için } \alpha_i > \beta_i \text{ sağlanmalıdır.} \end{cases}$$

biçiminde tanımlanan terim sıralaması degree reverse lexicographical sıralama olarak adlandırılır ve $degrevlex(<_{degrevlex})$ ile gösterilir.

3.3 Polinomların İndirgenmesi ve Bölme Algoritması

k bir cisim ve $k[x_1, x_2, \dots, x_n]$ k cismi üzerine n değişkenli bir polinom halkası olsun.

$k[x_1, x_2, \dots, x_n]$ üzerinde bir terim sıralaması seçilsin.

$0 \neq a_i \in k, X^{a_i} \in T^n$ ($i = 1, 2, \dots, r$), $X^{a_1} > X^{a_2} > \dots > X^{a_r}$ ve $f \neq 0$ olmak üzere;

$f \in k[x_1, x_2, \dots, x_n]$ polinomu,

$f = a_1 X^{a_1} + a_2 X^{a_2} + \dots + a_r X^{a_r}$ olarak yazılır.

Tanım 3.3.1: Yukarıdaki f polinomu ifadesinde;

f polinomunun en büyük kuvvet çarpımı, $lp(f) = X^{a_1}$

f polinomunun baş katsayısı, $lc(f) = a_1$

f polinomunun baş terimi, $lt(f) = a_1 X^{a_1}$ olarak tanımlanır.

Not: $f, g \in k[x_1, x_2, \dots, x_n]$ için;

$$lp(0) = lc(0) = lt(0) = 0$$

$$lp(f \cdot g) = lp(f) \cdot lp(g)$$

$$lc(f \cdot g) = lc(f) \cdot lc(g)$$

$$lt(f \cdot g) = lt(f) \cdot lt(g)$$

şeklindedir. Aynı zamanda terim sıralaması değiştirilirse, $lp(f), lc(f), lt(f)$ değişebilir.

Örnek 3.3.2: $x > y > z$ olmak üzere $f = 2x^2yz + 3xy^3 - 2x^3$ olsun.

Lex sıralamasına göre $lp(f) = x^3, lc(f) = -2, lt(f) = -2x^3$ dür.

Deglex sıralamasına göre $lp(f) = x^2yz, lc(f) = 2, lt(f) = 2x^2yz$ dir.

Degrevlex sıralamasına göre $lp(f) = xy^3, lc(f) = 3, lt(f) = 3xy^3$ dür.

Tanım 3.3.3: $g \neq 0$ olmak üzere; verilen $f, g, h \in k[x_1, x_2, \dots, x_n]$ için $lp(g), f$ polinomunun sıfırdan farklı bir X terimini bölüyorsa ve $h = f - \frac{X}{lt(g)} \cdot g$ ise f polinomu modülo g ye göre bir adımda h polinomuna indirgenir denir ve $f \xrightarrow{g} h$ ile gösterilir.

Tanım 3.3.4: $f, h \in k[x_1, x_2, \dots, x_n]$ ve $1 \leq i \leq s$ için $f_i \neq 0$ olmak üzere;
 $k[x_1, x_2, \dots, x_n]$ halkasındaki polinomların bir kümesi $F = \{f_1, f_2, \dots, f_s\}$ olsun.
 Eğer;

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \dots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$$

olacak şekilde, $h_1, h_2, \dots, h_{t-1} \in k[x_1, x_2, \dots, x_n]$ polinomların bir dizisi ve $i_1, i_2, \dots, i_t \in \{1, 2, \dots, s\}$ indislerin bir dizisi varsa f polinomu modülo F ye göre h polinomuna indirgenir denir ve $f \xrightarrow{F}_+ h$ ile gösterilir.

Tanım 3.3.5: $F = \{f_1, f_2, \dots, f_s\}$, $k[x_1, x_2, \dots, x_n]$ deki sıfırdan farklı polinomların bir kümesi ve $r \in k[x_1, x_2, \dots, x_n]$ bir polinom olsun.

$r = 0$ veya r polinomunda ortaya çıkan hiçbir terim $i = 1, 2, \dots, s$ olmak üzere $lp(f_i)$ ' lerin herhangi biri tarafından bölünmüyorsa r polinomuna F kümesine göre indirgenmiştir denir. Diğer bir deyişle r modülo F ye göre indirgenemezdir denir.

Tanım 3.3.6: $f \xrightarrow{F}_+ r$ (f modülo F ye göre indirgenmiş) ise ve r polinomu da F kümesine göre indirgenmişse r polinomuna F kümesine göre f polinomu için kalan denir.

Algoritma 3.3.7: Çok Değişkenli Polinomlar İçin Bölme Algoritması

Giriş: $1 \leq i \leq s$ için $f_i \neq 0$ olmak üzere $f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$ alınsın.

Çıkış: $f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s + r$ ve

$\max(lp(u_1).lp(f_1), \dots, lp(u_s).lp(f_s), lp(r)) = lp(f)$ olacak şekilde $\{f_1, f_2, \dots, f_s\}$ kümesine göre indirgenmiş bir r polinomu ve $u_1, u_2, \dots, u_s$ polinomları istenmektedir.

Başlangıç: $u_1 := 0, u_2 := 0, \dots, u_s := 0, r := 0, h := f$

Döngü: $h \neq 0$ olduğu sürece:

$lp(f_i) | lp(h)$ olacak şekilde i varsa o zaman $lp(f_i) | lp(h)$ olacak şekildeki en küçük i indisi seçilir ve

$$u_i := u_i + \frac{lt(h)}{lt(f_i)}, \quad h := h - \frac{lt(h)}{lt(f_i)} \cdot f_i \text{ işlemleri yapılır.}$$

$lp(f_i) | lp(h)$ olacak şekilde i yoksa aşağıdaki işlemler yapılır.

$$r := r + lt(h), \quad h := h - lt(h)$$

Teorem 3.3.8: $F = \{f_1, f_2, \dots, f_s\} \subseteq k[x_1, x_2, \dots, x_n]$ sıfırdan farklı polinomların bir kümesi ve $f \in k[x_1, x_2, \dots, x_n]$ verilsin. Algoritma 3.3.7 den dolayı r polinomu F kümesine göre indirgenmiş olacak şekilde $\exists u_1, u_2, \dots, u_s, r \in k[x_1, x_2, \dots, x_n]$ vardır

ve $f = u_1f_1 + u_2f_2 + \dots + u_sf_s + r$ dir. Bu durumda;

$$lp(f) = \max\left(\max(lp(u_i) \cdot lp(f_i)), lp(r)\right) \text{ olur}$$

(Adams and Laustunau 1994).

3.4 Gröbner Tabanı İle İlgili Tanımlar ve Teoremler

Tanım 3.4.1: $I, k[x_1, x_2, \dots, x_n]$ halkasının bir ideali ve $G = \{g_1, g_2, \dots, g_t\}$ sıfırdan farklı polinomlarının bir kümesi olmak üzere $G \subseteq I$ olsun. $f \neq 0$ sağlayan her $f \in I$ için $lp(g_i), lp(f)$ yi bölecek şekilde $i \in \{1, 2, \dots, t\}$ varsa G kümesine I ideali için bir Gröbner Tabanı denir.

Diğer bir deyişle G, I ideali için bir Gröbner tabanı ise I idealinde G kümesine göre indirgenmiş sıfırdan farklı polinom yoktur.

Tanım 3.4.2: Herhangi bir $S \subseteq k[x_1, x_2, \dots, x_n]$ için $Lt(S) = \langle \{lt(s) | s \in S\} \rangle$ ideali tanımlanır. Bu ideale S kümesinin baş terim ideali denir.

Teorem 3.4.3: $I, k[x_1, x_2, \dots, x_n]$ halkasının sıfırdan farklı bir ideali olsun. Sıfırdan farklı polinomların bir kümesi olan $G = \{g_1, g_2, \dots, g_t\} \subseteq I$ için aşağıdaki durumlar denktir.

(i) G, I ideali için bir Gröbner tabanıdır.

(ii) $f \in I$ olması için gerekli ve yeterli koşul $f \xrightarrow{G} 0$ olmasıdır.

(iii) $f \in I$ olması için gerekli ve yeterli koşul

$$lp(f) = \max_{1 \leq i \leq t} (lp(h_i) \cdot lp(g_i)) \text{ olmak üzere } f = \sum_{i=1}^t h_i \cdot g_i \text{ olmasıdır.}$$

(iv) $Lt(G) = Lt(I)$ (Adams and Loustaunau 1994).

İspat: (i) $\Rightarrow$ (ii):

G, I ideali için bir Gröbner tabanı ve $f \in k[x_1, x_2, \dots, x_n]$ olsun.

Teorem 3.3.8 den $f \xrightarrow{G}_+ r$ olacak şekilde G kümesine göre indirgenmiş bir

$r \in k[x_1, x_2, \dots, x_n]$ elemanı vardır.

Böylece $f - r \in I$ olur. Dolayısıyla $f \in I$ ve $r \neq 0$ ise $r \in I$ olur.

(i) den $lp(g_i) | lp(r)$ olacak şekilde $i \in \{1, 2, \dots, n\}$ vardır. Bu r polinomunun G kümesine göre indirgenmiş olması ile çelişir. Böylece $r = 0$ olmalıdır.

Yani $f \xrightarrow{G}_+ 0$ dır.

(ii) $\Rightarrow$ (iii):

$f \in I \Leftrightarrow f \xrightarrow{G}_+ 0$ olsun.

$$f \in I \Leftrightarrow f \xrightarrow{G}_+ 0 \xLeftrightarrow_{\text{Teorem 3.3.8}} f = \sum_{i=1}^t h_i \cdot g_i, lp(f) = \max_{1 \leq i \leq t} (lp(h_i) \cdot lp(g_i))$$

(iii) $\Rightarrow$ (iv):

$$x \in Lt(G) \Rightarrow \forall g_i \in G \text{ ve } \exists a_i \in k \text{ için } x = \sum_{i=1}^t a_i \cdot lt(g_i)$$

$$\xRightarrow{G \subseteq I} \exists g_i \in I \text{ ve } \exists a_i \in k \text{ için } x = \sum_{i=1}^t a_i \cdot lt(g_i) \Rightarrow x \in Lt(I)$$

$Lt(G) \subseteq Lt(I)$ olur.

Diğer taraftan $f \in I$ için $lp(f)$ ve $Lt(I)$ nin üreteçleri olduğundan her $f \in I$ için $lt(f) \in Lt(G)$ olduğunu göstermek yeterlidir.

Varsayımımızdaki gibi $f = \sum_{i=1}^t h_i \cdot g_i$ olarak yazılan her f polinomu için $lt(f) = \sum_{i=1}^t lt(h_i) \cdot lt(g_i)$ dir. Buradan $lt(f) \in Lt(G)$ olur. Böylece $Lt(I) \subseteq Lt(G)$ dir. $Lt(G) = Lt(I)$ bulunur.

(iv) $\Rightarrow$ (i):

$f \in I$ için $lt(f) \in Lt(G)$ dir. Buradan $lt(f) = \sum_{i=1}^t h_i \cdot lt(g_i)$, $h_i \in k[x_1, x_2, \dots, x_n]$ olur. Toplam ifadesi açılırsa toplamdaki her bir terimin en az bir $lp(g_i)$ tarafından

bölündüğü görülür. Böylece eşitliğin sol tarafındaki tek terim olan $lt(f)$ en az bir $lp(g_i)$ tarafından bölünür. Buradan Gröbner tabanı tanımına gelinmiş olur.

Sonuç olarak G kümesi I idealinin bir Gröbner tabanı olur.

Sonuç 3.4.4: $G = \{g_1, g_2, \dots, g_t\}$ kümesi I ideali için bir Gröbner tabanı ise $I = \langle g_1, g_2, \dots, g_t \rangle$ dir (Adams and Lousaunau 1994).

İspat: $G \subseteq I$ olduğu açıktır. Her bir $i = \{1, 2, \dots, t\}$ için $g_i \in I$ olduğundan $\langle g_1, g_2, \dots, g_t \rangle \subseteq I$ 'dır.

$f \in I$ olsun. Teorem 3.4.3 den $f \xrightarrow{G}_+ 0$ dir. Buradan $f \in \langle g_1, g_2, \dots, g_t \rangle$ olur. Böylece $I \subseteq \langle g_1, g_2, \dots, g_t \rangle$ ' dir.

Dolayısıyla $I = \langle g_1, g_2, \dots, g_t \rangle$ bulunur.

Lemma 3.4.5: $f \in k[x_1, x_2, \dots, x_n]$ ve I ideali sıfırdan farklı terimlerin bir S kümesi tarafından üretilmiş olsun. $f \in I$ olması için gerekli ve yeterli koşul f polinomunda ortaya çıkan her X terimi için $Y \mid X$ olacak şekilde bir $Y \in S$ var olmasıdır. Ayrıca $I = \langle S_0 \rangle$ olacak şekilde S kümesinin sonlu bir S_0 alt kümesi vardır (Adams and Lousaunau 1994).

İspat: $\Rightarrow$: $I = \langle S \rangle$ olsun.

$f \in I \Rightarrow f = \sum_{i=1}^t h_i X_i$, $i = 1, 2, \dots, t$ için $h_i \in k[x_1, x_2, \dots, x_n]$, $X_i \in S$ dir.

Toplam ifadesi açılırsa toplam ifadesindeki her terimin S kümesindeki en az bir X_i terimi tarafından bölünebildiği görülür. Bu durumda aynı zamanda eşitliğin sol tarafındaki polinomun her terimi en az bir $X_i \in S$ tarafından bölünmek zorunda kalır.

$\Leftarrow$: f polinomunda ortaya çıkan her bir X terimi için $Y \mid X$ olacak şekilde bir $Y \in S$ terimi var olsun.

$Y \mid X \Rightarrow \exists Z \in k[x_1, x_2, \dots, x_n], X = Y \cdot Z \xRightarrow{Y \in S} X \in I = \langle S \rangle$ olur. Buradan $f \in I$ bulunur.

Son durumu kanıtlamak için, Hilbert Taban Teoremi'nden I sonlu bir üreteç kümesine sahiptir. Lemma'nın birinci kısmından üreteç kümesinin elemanı olan her

bir terim S kümesinin bir elemanı tarafından bölünür. Bölenlerin sonlu kümesi S_0 olmak üzere $I = \langle S_0 \rangle$ olur.

Sonuç 3.4.6: $k[x_1, x_2, \dots, x_n]$ halkasının sıfırdan farklı her ideali bir Gröbner tabanına sahiptir (Adams and Loustaunau 1994).

İspat: Lemma 3.4.5 den baş terim ideali $Lt(I)$ sonlu bir üreteç kümesine sahiptir. $g_1, g_2, \dots, g_t \in I$ olmak üzere bu kümenin $\{lt(g_1), lt(g_2), \dots, lt(g_t)\}$ olduğunu varsayalım. $G = \{g_1, g_2, \dots, g_t\}$ ise $Lt(G) = Lt(I)$ dir. Teorem 3.4.3 den G kümesi I ideali için bir Gröbner tabanıdır.

Önerme 3.4.7: $G = \{g_1, g_2, \dots, g_t\} \subseteq k[x_1, x_2, \dots, x_n]$ kümesinin bir Gröbner tabanı olması için gerek ve yeter koşul $\langle G \rangle$ ideali için bir Gröbner tabanı olmasıdır (Adams and Loustaunau 1994).

Teorem 3.4.8: $G = \{g_1, g_2, \dots, g_t\}, k[x_1, x_2, \dots, x_n]$ halkasındaki sıfırdan farklı polinomların bir kümesi olsun.

G 'nin bir Gröbner tabanı olması için gerekli ve yeterli koşul $\forall f \in k[x_1, x_2, \dots, x_n]$ için f polinomunun G kümesine bölümünden kalanın tek olmasıdır (Adams and Loustaunau 1994).

Tanım 3.4.9: $0 \neq f, g \in k[x_1, x_2, \dots, x_n]$ ve $L = lcm(lp(f_1), lp(f_2))$ olsun.

$S(f, g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$ polinomuna f ve g nin S-Polinomu denir.

Teorem 3.4.10 (Buchberger): $G = \{g_1, g_2, \dots, g_t\}, k[x_1, x_2, \dots, x_n]$ halkasındaki sıfırdan farklı polinomların bir kümesi ve $I = \langle g_1, g_2, \dots, g_t \rangle, k[x_1, x_2, \dots, x_n]$ 'nin sıfırdan farklı bir ideali olsun.

G kümesi I ideali için bir Gröbner tabanıdır. $\Leftrightarrow \forall i \neq j$ için $S(g_i, g_j) \xrightarrow{G} 0$ dir (Adams and Loustaunau 1994).

Algoritma 3.4.11: Gröbner Tabanları İçin Buchberger Algoritması

Giriş: $F = \{f_1, f_2, \dots, f_s\} \subseteq k[x_1, x_2, \dots, x_n]$, $f_i = 0$ ($1 \leq i \leq s$) alınsın.

Çıkış: $G = \{g_1, g_2, \dots, g_t\}, \langle f_1, f_2, \dots, f_s \rangle$ için bir Gröbner tabanı istenmektedir.

Başlangıç: $G := F, K = \{\{f_i, f_j\} \mid f_i \neq f_j, f_i, f_j \in G\}$

Döngü: $K \neq \emptyset$ olduğu sürece aşağıdaki işlemler yapılır.

Herhangi bir $\{f, g\} \in K$ seçilir.

$K := K - \{\{f, g\}\}$

$S(f, g) \xrightarrow{G}_+ h$ burada h polinomu G ye göre indirgenmiştir.

$h \neq 0$ ise aşağıdaki işlemler yapılır.

$K := K \cup \{\{u, h\}\} \mid \forall u \in G$ için

$G := G \cup \{h\}$

(Adams and Lousaunau 1994).

Teorem 3.4.12: $\forall i = 1, 2, \dots, s$ için $f_i \neq 0$ için olmak üzere $F = \{f_1, f_2, \dots, f_s\}$ verilsin. Buchberger Algoritması $I = \langle f_1, f_2, \dots, f_s \rangle$, ideali için bir Gröbner tabanı verir (Adams and Lousaunau 1994).

3.5 Eleminasyon

Önceki bölümde Gröbner tabanının sözlüksel terim sıralamasına göre hesaplanmasının avantajını gördük. Bu bölümde bu fikrin geniş kapsamlı bir genellemesini sunuyoruz.

Değişkenleri $\{x_1, \dots, x_n\}$ ve $\{y_1, \dots, y_m\}$ olan iki küme düşünelim.

x değişkenlerinin kuvvet çarpımlarının ve y değişkenlerinin kuvvet çarpımlarının ayrı ayrı $<_x, <_y$ terim sıralamasına göre sıralandığını varsayalım. x ve y değişkenlerindeki kuvvet çarpımı üzerinde $<$ işaretine göre aşağıdaki gibi terim sıralaması tanımlarız.

Tanım 3.5.1: x deęişkenindeki kuvvet arpımı X_1, X_2 iin ve y deęişkenindeki kuvvet arpımı Y_1, Y_2 iin;

$$X_1 Y_1 < X_2 Y_2 \Leftrightarrow \begin{cases} X_1 <_x X_2 \\ ya\ da \\ X_1 = X_2\ ve\ Y_1 <_y Y_2 \end{cases}$$

tanımlanır. Bu terim sıralaması y deęişkenlerinden büyük x deęişkenleri ile eliminasyon sıralama olarak adlandırılır.



4. ARAŞTIRMA BULGULARI

4.1 Temel Gröbner Tabanı Uygulamaları

$I = \langle f_1, \dots, f_s \rangle$, $k[x_1, \dots, x_n]$ nin bir ideali olsun. Bu bölümde aşağıdaki görevlerin nasıl etkili bir şekilde yerine getirileceği gösterilecektir. Burada etkili bir getiriden kasıt bilgisayarda programlanabilen bir algoritmanın verilmesidir.

- (i) $f \in k[x_1, \dots, x_n]$ verilsin. f nin I da olup olmadığının belirlenmesi (ideal aitlik problemi) ve eğer öyleyse $f = v_1 f_1 + \dots + v_s f_s$ olacak şekilde $v_1, \dots, v_s \in k[x_1, \dots, x_n]$ lerin bulunması.
- (ii) $k[x_1, \dots, x_n]$ de I ve J gibi iki idealin eşit olup olmadığının belirlenmesi.
- (iii) $k[x_1, \dots, x_n]/I$ 'nin her bir elemanı için yanküme temsilcisinin bulunması.
- (iv) $k[x_1, \dots, x_n]/I$ k-vektör uzayının tabanının bulunması.
- (v) $k[x_1, \dots, x_n]/I$ da ki işlemlerin belirlenmesi.
- (vi) $k[x_1, \dots, x_n]/I$ da eğer var ise terslerin bulunması.

Şimdi bu problemlerden bazılarının nasıl çözülebileceği hakkında bilgiler verilecektir. (i) problemi ile başlanılsın. $F = \langle f_1, \dots, f_s \rangle$ ve $G = \langle g_1, \dots, g_t \rangle$ sabit bir terim sıralamasına göre

$I = \langle f_1, \dots, f_s \rangle$ idealinin birer Gröbner tabanı olsunlar. Daha önce verilen Teorem 3.4.3 ten,

$$f \in I \Leftrightarrow f \xrightarrow{G} 0$$

olduğu biliniyor. Böylece ideal aitlik problemi cevaplanmış olur. Diğer taraftan, $f \in I$ ya bölme algoritması uygulanırsa,

$$f = u_1 g_1 + \dots + u_t g_t \quad (4.1.1)$$

olacak şekilde $u_1, \dots, u_t$ elde edilir. Ayrıca Buchberger algoritması, f_i lerin g_j leri ortaya çıkaran lineer kombinasyonlarını elde edebilmek için uygulanabilir. Bu şekilde görülebilir:

Gröbner tabanı hesaplaması için Buchberger algoritması (Algoritma 3.4.11) sırasında eğer bir S-polinomunun mevcut taban $\{h_1, \dots, h_l\}$ ile bölümünden kalan sıfır olmayan g polinomu ise bu g polinomu tabana eklenir. Yani, bazı $v, \mu \in \{1, 2, \dots, l\}$ ve Bölme Algoritmasında hesaplanan bazı w_i polinomları için,

$$g = S(h_v, h_\mu) - \sum_{i=1}^l w_i h_i$$

dir. Bu yöntem aşağıdaki örnekte gösterilmiştir. Böylece Buchberger Algoritmasının çıktısı olarak sadece $\{g_1, \dots, g_t\}$ Gröbner tabanını değil aynı zamanda,

$$\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_t \end{bmatrix} = M \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_s \end{bmatrix} \quad (4.1.2)$$

olacak şekilde polinom girdili bir $t \times s$ tipinde M matrisi elde edilir. Dolayısıyla, (4.1.1) denklemi f yi, orijinal polinomlar $f_1, \dots, f_s$ nin bir lineer kombinasyonu olarak verecek şekilde dönüştürebilir:

$$f = v_1 f_1 + \dots + v_s f_s.$$

Örnek 4.1.1 Bu örnekte $k = \mathbb{Q}$ olarak alınsın. $f_1 = x^2y - y + x$, $f_2 = xy^2 - x$ ve $I = \langle f_1, f_2 \rangle$ olsun. $x < y$ olmak üzere deglex terim sıralaması kullanılsın. Buchberger algoritması takip edilecek fakat üreteç kümesinde yeni polinomlara yol açan lineer kombinasyonlar elde tutulacaktır.

BAŞLANGIÇ: $G := \{f_1, f_2\}, G := \{\{f_1, f_2\}\}$.

1. While Döngüsü:

$$G := \emptyset$$

$$S(f_1, f_2) = yf_1 - xf_2 = -y^2 + xy + x^2$$

(G'ye göre indirgenmiş)

$$f_3 := -y^2 + xy + x^2$$

$$f_3 = y \cdot (x^2y - y + x) - x(xy^2 - x)$$

$$f_3 = yf_1 - xf_2$$

$$G := \{\{f_1, f_3\}, \{f_2, f_3\}\}$$

$$G := \{f_1, f_2, f_3\}$$

2. While Döngüsü:

$$G := \{\{f_2, f_3\}\}$$

$$S(f_1, f_3) = yf_1 - x^2f_3 = x^3y + x^4 - y^2 + xy$$

$$\xrightarrow{f_1} x^4 - y^2 + 2xy - x^2$$

$$\xrightarrow{f_3} x^4 + xy - 2x^2$$

(G'ye göre indirgenmiş)

$$f_4 := x^4 + xy - 2x^2$$

$$f_4 = (yf_1 + x^2f_3) - xf_1 - f_3$$

$$= (x^2y - x)f_1 + (-x^3 + x)f_2$$

$$G := \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$$

$$G := \{f_1, f_2, f_3, f_4\}$$

3. While Döngüsü:

$$G := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$$

$$S(f_2, f_3) = f_2 - xf_3 = x^2y + x^3 - x \xrightarrow{f_1} x^3 + y - 2x$$

(G'ye göre indirgenmiş)

$$f_5 := x^3 + y - 2x$$

$$f_5 = (f_2 - xf_3) - f_1 = (xy - 1)f_1 + (-x^2 + 1)f_2$$

$$G := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$$

$$G := \{f_1, f_2, f_3, f_4, f_5\}$$

Kalan S-polinomlarının tamamı sıfıra indirgenir ve dolayısıyla $G := \{f_1, f_2, f_3, f_4, f_5\}$, I için bir Gröbner tabanıdır. $lt(f_2)$ polinomu $lt(f_3)$ ile bölünebildiğinden ve $lt(f_4)$ polinomu $lt(f_5)$ ile bölünebildiğinden $\{f_1, f_3, f_5\}$ de I için bir Gröbner tabanıdır. Aslında $\{f_1, f_3, f_5\}$, $x < y$ olmak üzere deglex terim sıralamasına göre I için bir indirgenmiş Gröbner tabanıdır. Dahası, yukarıdaki hesaplamada f_3 ve f_5 e yol açan f_1 ve f_2 nin lineer kombinasyonları elde tutulmuş ve bu da aşağıdaki sonucu vermiştir:

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ y & -x \\ xy - 1 & -x^2 + 1 \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} \quad (4.1.3)$$

Şimdi,

$$f = x^4y - 2x^5 + 2x^2y^2 - 2x^3y - 2x^4 - 2y^3 + 4xy^2 - 3x^2y + 2x^3 - y + 2x.$$

polinomu ele alınsın. $f \in I$ olduğu gösterilecektir:

$$f \xrightarrow{x^2, f_1} -2x^5 + 2x^2y^2 - 2x^3y - 2x^4 - 2y^3 + 4xy^2 - 2x^2y + x^3 - y + 2x$$

$$\xrightarrow{-2x^2, f_5} 2x^2y^2 - 2x^3y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 - y + 2x$$

$$\xrightarrow{2y, f_1} -2x^3y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 + 2y^2 - 2xy - y + 2x$$

$$\xrightarrow{-2y, f_5} -2x^4 - 2y^3 + 4xy^2 - 3x^3 + 4y^2 - 6xy - y + 2x$$

$$\xrightarrow{-2x, f_5} -2y^3 + 4xy^2 - 3x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$

$$\xrightarrow{2y, f_3} 2xy^2 - 2x^2y - 3x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$

$$\xrightarrow{-2x, f_3} -x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$

$$\xrightarrow{-1, f_5} 4y^2 - 4xy - 4x^2$$

$$\xrightarrow{-4, f_3} 0.$$

Dolayısıyla,

$$\begin{aligned} f &= x^2f_1 - 2x^2f_5 + 2yf_1 - 2yf_5 - 2xf_5 + 2yf_3 - 2xf_3 - f_5 - 4f_3 \\ &= (x^2 + 2y)f_1 + (2y - 2x - 4)f_3 + (-2x^2 - 2y - 2x - 1)f_5. \end{aligned}$$

olduğu görülür. Denklem (4.1.3) kullanılırsa,

$$\begin{aligned} f &= (x^2 + 2y)f_1 + (2y - 2x - 4)(yf_1 - xf_2) \\ &\quad + (-2x^2 - 2y - 2x - 1)((xy - 1)f_1 + (-x^2 + 1)f_2) \\ f &= (-2x^3y - 2xy^2 - 2x^2y + 2y^2 - 3xy + 3x^2 + 2x + 1)f_1 \\ &\quad + (2x^4 + 2x^2y + 2x^3 - 2xy + x^2 - 2y + 2x - 1)f_2 \end{aligned}$$

Şimdi (iii) deki problem ele alınsın.

Tanım 4.1.2: Daha önce verilen Teorem 3.4.3 ve 3.4.8 e göre; $G = \{g_1, g_2, \dots, g_t\}$ kümesi I ideali için bir Gröbner taban olsun. Dolayısıyla, $\forall f \in k[x_1, x_2, \dots, x_n]$ için f polinomunun G kümesine bölümünden kalan tek olup bu eleman r olarak ele alınsın. $f \xrightarrow{G} r$ ile gösterilebilir. Bu r elemanı f nin G ye göre normal formu olarak adlandırılır ve $N_G(f)$ ile gösterilir.

Önerme 4.1.3: $f, g \in k[x_1, x_2, \dots, x_n]$ olsun. Bu durumda, $f \equiv g \pmod{I}$ ancak ve ancak $N_G(f) = N_G(g)$ dir. Dolayısıyla $\{N_G(f) \mid f \in k[x_1, \dots, x_n]\}$ kümesi $k[x_1, \dots, x_n]/I$ için yanküme temsilcilerinin bir kümesidir. Dahası $N_G: k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_n]$ dönüşümü k -lineerdir (Adams and Laustanau 1994).

İspat: Bölme algoritmasından, $f = q + N_G(f)$ olacak şekilde $q \in I$ vardır. Böylece $f - N_G(f) \in I$ dir. Bu nedenle $f + I = N_G(f) + I$ $k[x_1, \dots, x_n]/I$ nın bir elemanıdır. Ayrıca herhangi bir $c_1, c_2 \in k$ ve herhangi bir $f_1, f_2 \in k[x_1, \dots, x_n]$ için, $c_1 f_1 + c_2 f_2 - (c_1 N_G(f_1) + c_2 N_G(f_2)) \in I$ ve $c_1 N_G(f_1) + c_2 N_G(f_2)$ G ye göre indirgenmiştir. Bu nedenle $N_G(c_1 f_1 + c_2 f_2) = c_1 N_G(f_1) + c_2 N_G(f_2)$ dir ve bu yüzden $N_G: k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_n]$ dönüşümü k -lineerdir.

Şimdi $f \equiv g \pmod{I}$ ancak ve ancak $f = q + g$ olacak şekilde $q \in I$ vardır. Böylece $N_G(f) = N_G(q) + N_G(g)$ dir. Ama $q \in I$ olduğundan $N_G(q) = 0$ dir, bu yüzden $N_G(f) = N_G(g)$ dir. Tersine, eğer $N_G(f) = N_G(g)$ ise $f - g = (f - N_G(f)) - (g - N_G(g)) \in I$ ve dolayısıyla $f \equiv g \pmod{I}$ dir.

Örnek 4.1.4: Örnek 4.1.1 e yeniden ele alınsın.

$$x^3 \xrightarrow{f_5} -y + 2x$$

olarak bulunmuştu. $-y + 2x$ indirgenmiş olduğundan, $N_G(x^3) = -y + 2x$ elde edilir. Ayrıca,

$$x^2 y + y \xrightarrow{f_1} 2y - x \text{ dir.}$$

$2y - x$ indirgenmiş olduğundan, $N_G(x^2 y + y) = 2y - x$ olur. Dahası, $N_G(x^3) \neq N_G(x^2 y + y)$ olduğundan, $x^3 \neq x^2 y + y \pmod{I}$ dir.

Aşağıdaki önerme (iv) deki problemin yani $k[x_1, \dots, x_n]/I$ vektör uzayının tabanının bulunması için gerekli bilgiyi vermektedir.

Önerme 4.1.5: $k[x_1, \dots, x_n]/I$ k -vektör uzayı için bir taban, her $i = 1, 2, \dots, t$ için $lp(g_i)$ nin X i bölmediği bütün $X \in T^n$ kuvvet çarpımlarının yan kümelerinden oluşur (Adams and Lousaunau 1994).

İspat: $k[x_1, \dots, x_n]/I$ da herhangi bir $f \in k[x_1, \dots, x_n]$ için $f + I = N_G(f) + I$ olduğu görüldü. $N_G(f)$, G ye göre indirgenmiş olduğundan, indirgemenin tanımından, her $i = 1, 2, \dots, t$ için $lp(g_i)$ nin X i bölmediği $X \in T^n$ nin bütün kuvvet çarpımlarının bir k -lineer kombinasyonudur. Son olarak bu kuvvet çarpımlarının yan kümeleri normal formun tekliğinden lineer bağımsızdır.

4.2 Üç Renk Problemi

Bu kısımda graf teorisinde iyi bilinen bir problemi çözmek için Gröbner taban tekniğinin nasıl kullanılacağı gösterilecektir: Verilen bir grafın 3-renk boyanıp boyanamayacağı belirlenecektir (Aynı teknik herhangi bir renklendirme için de çalışır).

İlk önce problem tam olarak belirlensin. Herhangi iki köşe arasında en fazla bir kenar olan n köşeli $\mathcal{G}$ grafı verilsin. Köşeler sadece 3 renk kullanılarak renklendirilecek ve bir kenarla bağlı iki köşe aynı renkle renklendirilmeyecek. Eğer $\mathcal{G}$ bu şekilde renklendirilebilir ise $\mathcal{G}$ 3-renklendirilebilir olarak adlandırılır. Bu problem dönüşümler için 3-renk problemi ile aynı düşünülebilir: köşeler renklendirilecek bölgeleri temsil eder ve iki köşe, eğer karşılık gelen iki bölge bitişik ise bir kenar ile bağlantılıdır.

İlk olarak, $\xi = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ birimin küp kökü olsun (ör: $\xi^3 = 1$). 3 renk birimin 3 farklı küp kökü olan $1, \xi, \xi^2$ ile temsil edilsin. Şimdi, $x_1, \dots, x_n$ ler $\mathcal{G}$ grafının farklı köşelerini temsil eden değişkenler olsun. Her bir köşe 3 renk olan $1, \xi, \xi^2$ den birine atanacaktır. Bu aşağıdaki n denklemlerle temsil edilebilir.

$$x_i^3 - 1 = 0, 1 \leq i \leq n. \quad (4.2.1)$$

Ayrıca x_i ve x_j köşe noktaları bir kenar ile birbirine bağlıysa farklı renk olmaları gerekir. $x_i^3 = x_j^3$ olduğundan $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$ elde edilir. Bu nedenle, x_i ve x_j nin farklı renk olması için gerek ve yeter şart

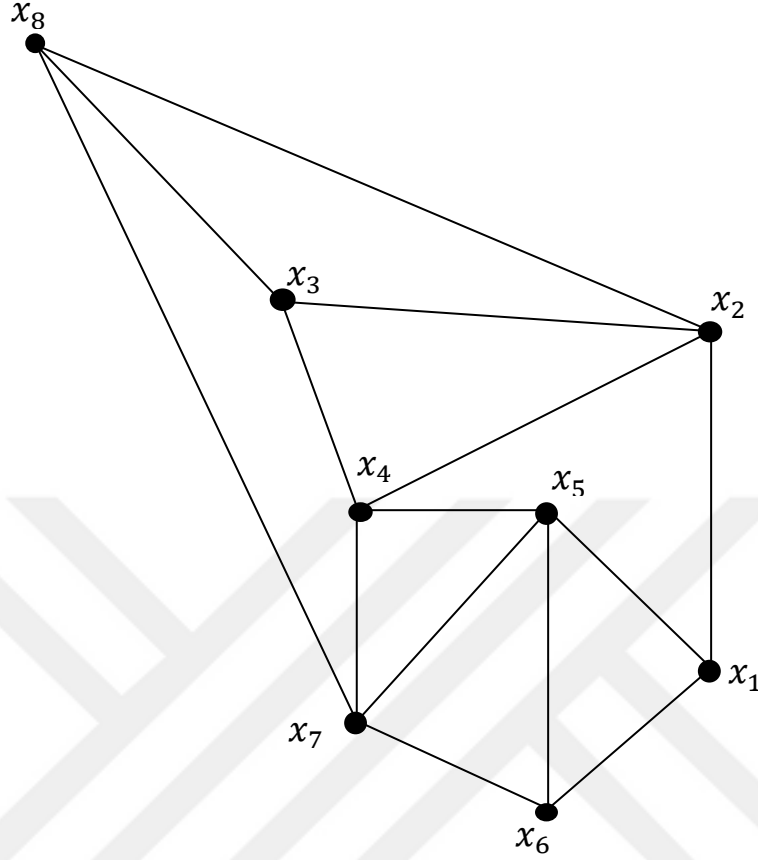
$$x_i^2 + x_i x_j + x_j^2 = 0 \quad (4.2.2)$$

olmasıdır. I , (4.2.1) denklemindeki polinomlar tarafından üretilen ve denklem (4.2.2) deki polinomlar tarafından bir kenarla bağlanan her bir x_i, x_j köşe çifti için $\mathbb{C}[x_1, \dots, x_n]$ nin bir ideali olsun. $\mathbb{C}^n$ nin kapsadığı $V(I)$ varyete kümesi göz önünde bulundurulacaktır. Aşağıdaki teorem bu kısımda ele alınan problemin çözümünü vermektedir.

Teorem 4.2.1: G grafının 3 renklendirilebilir olabilmesi için gerek ve yeter şart $V(I)$ nin boş kümeden farklı olmasıdır (Adams and Lousaunau 1994).

$V(I)$ varyete kümesinin boştan farklı olup olmadığının tespiti için Gröbner tabanı kullanılabilir. İlk olarak I için bir G indirgenmiş Gröbner tabanı hesaplanır. Eğer $1 \in G$ ise $V(I) = \emptyset$ aksi halde $V(I) \neq \emptyset$ dir.

Örnek 4.2.2: Şekil 4.2.3 deki $\mathcal{G}$ grafi ele alınsın.



Şekil 4.2.3. Renklendirilecek Graf

$\mathcal{G}$ ye karşılık gelen polinomlar;

$i = 1, \dots, 8$ için $x_i^3 - 1$ ve

$(i, j) \in \{(1,2), (1,5), (1,6), (2,3), (2,4), (2,8), (3,4), (3,8), (4,5), (4,7), (5,6), (5,7), (6,7), (7,8)\}$ çiftleri için de $x_i^2 + x_i x_j + x_j^2$ dir.

Yukarıdaki polinomlara karşılık gelen I ideali için G gröbner tabanı hesaplanacaktır..

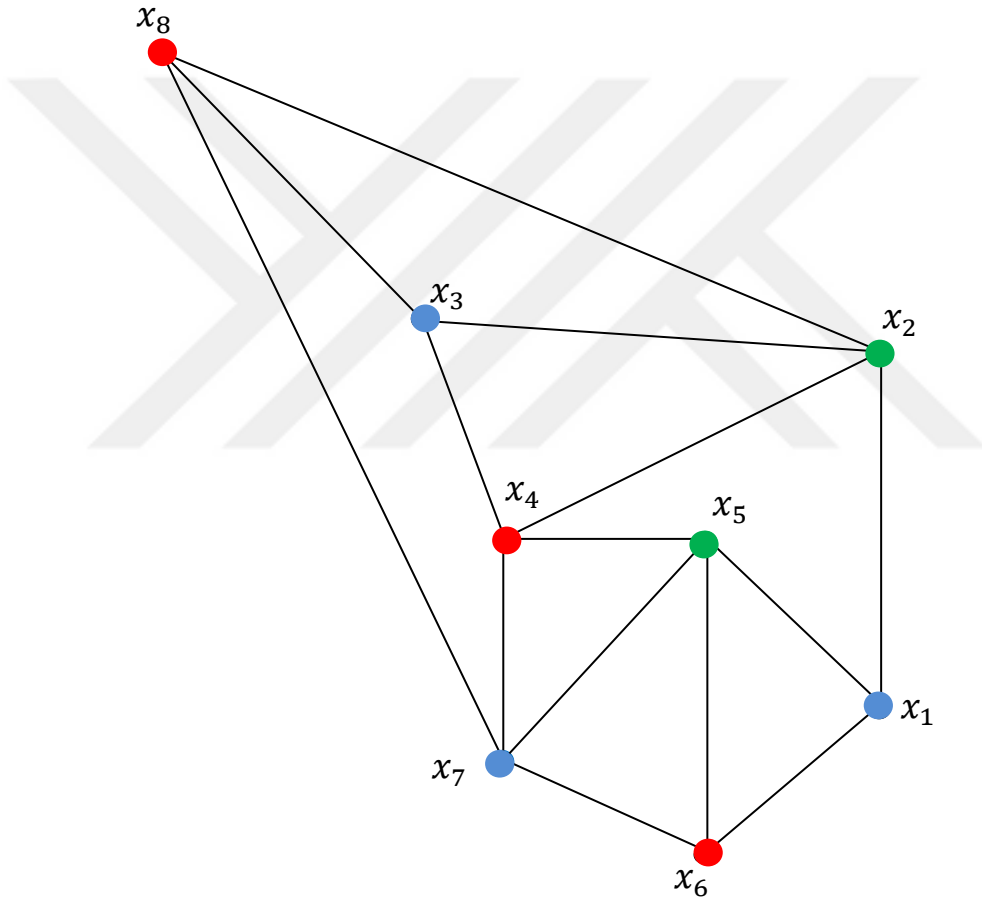
$x_1 > x_2 > \dots > x_8$ olmak üzere lex terim sıralaması kullanılsın. Bu durumda,

$$G = \{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_5 + x_7 + x_8, x_6 - x_8, x_7^2 + x_7 x_8 + x_8^2, x_8^3 - 1\}$$

elde edilir.

$1 \notin G$ olduğu için $V(I) \neq \emptyset$ dir. Dolayısıyla, Teorem 4.2.1 e göre $\mathcal{G}$ grafi 3-renklendirilebilir. G ile temsil edilen denklem sisteminin çözülmesi kolay olduğu için G Gröbner tabanı belirgin bir renklendirme için kullanılabilir. Kullanılacak 3 rengin mavi, kırmızı ve yeşil olduğu kabul edilsin. İlk olarak, x_8 için bir renk

seçilmelidir. Bu renk kırmızı olsun. Çünkü G deki tek değişkenli tek polinom $x_8^3 - 1$ dir. $x_7^2 + x_7x_8 + x_8^2$ polinomu G nin elemanı olduğundan x_7 için farklı bir renk seçilmelidir. Bu renk mavi olsun. Bu durumda, $x_1 - x_7, x_3 - x_7 \in G$ polinomlarından dolayı x_1 ve x_3 mavi ayrıca $x_4 - x_8, x_6 - x_8 \in G$ polinomlarından dolayı da x_4 ve x_6 kırmızı olmalıdır. Son olarak, x_2 ve x_5, x_7 ve x_8 e atanan renklerden farklı bir renk olmak üzere aynı renge sahiptir. $x_2 + x_7 + x_8$ ve $x_5 + x_7 + x_8$ polinomları G nin elemanı olduğundan x_2 ve x_5 yeşildir.



Şekil 4.2.4 Renklendirilmiş Graf

4.3 Tamsayı Programlama

Tamsayı programlama problemi şu şekilde tanımlanabilir: $a_{ij} \in \mathbb{Z}, b_i \in \mathbb{Z}$ ve $c_j \in \mathbb{R}, i = 1, \dots, n, j = 1, \dots, m$ olsun.

$$c(\sigma_1, \sigma_2, \dots, \sigma_m) = \sum_{j=1}^m c_j \sigma_j \quad (4.3.1)$$

maliyet fonksiyonunu minimize eden

$$\begin{cases} \alpha_{11}\sigma_1 + \alpha_{12}\sigma_2 + \dots + \alpha_{1m}\sigma_m = b_1 \\ \alpha_{21}\sigma_1 + \alpha_{22}\sigma_2 + \dots + \alpha_{2m}\sigma_m = b_2 \\ \vdots \\ \alpha_{n1}\sigma_1 + \alpha_{n2}\sigma_2 + \dots + \alpha_{nm}\sigma_m = b_n, \end{cases} \quad (4.3.2)$$

sisteminin $\mathbb{N}^m$ de bir $(\sigma_1, \sigma_2, \dots, \sigma_m)$ çözümü bulunmak istenilmektedir.

Bu problem sıklıkla fen ve mühendislik uygulamalarında ortaya çıkmaktadır. Bu problemin çözümünde izlenilecek strateji şu şekildedir:

- (i) Tamsayı programlama probleminin polinomlarla ilgili problemlere dönüştürülmesi;
- (ii) Polinom problemini çözmek için şimdiye kadar geliştirilen Gröbner tabanı tekniklerinin kullanılması;
- (iii) Polinom probleminin çözümünün tamsayı programlama probleminin çözümüne çevrilmesi.

Bu kısımda a_{ij} lerin ve b_i lerin negatif tamsayı olmadığı özel durum ele alınacaktır. Ayrıca ilk olarak maliyet fonksiyonu şartını dikkate almadan (denklem 4.3.1) (4.3.2) sisteminin çözümüne odaklanılacaktır.

(4.3.2) sistemindeki her lineer denklem için $x_1, x_2, \dots, x_n$ değişkenleri ve her bir bilinmeyen σ_j için $y_1, y_2, \dots, y_m$ değişkenleri tanımlansın. Bu durumda (4.3.2) deki denklemler $i = 1, \dots, n$ için,

$$x_i^{\alpha_{i1}\sigma_1+\dots+\alpha_{im}\sigma_m} = x_i^{b_i}$$

şeklinde temsil edilebilir. Bu durumda (4.3.2) sistemi kuvvet çarpımlarının tek bir denklemi olarak,

$$x_1^{\alpha_{11}\sigma_1+\dots+\alpha_{1m}\sigma_m} \dots x_n^{\alpha_{n1}\sigma_1+\dots+\alpha_{nm}\sigma_m} = x_1^{b_1} x_2^{b_2} \dots x_n^{b_n},$$

şeklinde ya da denk olarak,

$$(x_1^{\alpha_{11}} x_2^{\alpha_{21}} \dots x_n^{\alpha_{n1}})^{\sigma_1} \dots (x_1^{\alpha_{1m}} x_2^{\alpha_{2m}} \dots x_n^{\alpha_{nm}})^{\sigma_m} = x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \quad (4.3.3)$$

şeklinde yazılabilir. Denklem (4.3.3) ün sol tarafındaki kuvvet çarpımı

$$\begin{array}{ccc} k[y_1, \dots, y_m] & \xrightarrow{\Phi} & k[x_1, \dots, x_n] \\ y_j & \longrightarrow & x_1^{\alpha_{1j}} x_2^{\alpha_{2j}} \dots x_n^{\alpha_{nj}} \end{array}$$

polinom dönüşümü altında $y_1^{\sigma_1} y_2^{\sigma_2} \dots y_m^{\sigma_m}$ kuvvet çarpımının görüntüsü olarak düşünülebilir. Bu durumda aşağıdaki lemma yazılabilir.

Lemma 4.3.1: Yukarıda tanımlanan notasyon sabit olmak şartıyla bütün α_{ij} lerin ve b_i lerin negatif olmadığı kabul edilsin. Bu durumda, (4.3.2) denklem sisteminin bir $(\sigma_1, \sigma_2, \dots, \sigma_m) \in \mathbb{N}^m$ çözümünün olabilmesi için gerek ve yeter şart $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ in Φ altında $k[y_1, \dots, y_m]$ de bir kuvvet çarpımının görüntüsü olmasıdır. Dahası, eğer $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} = \Phi(y_1^{\sigma_1} y_2^{\sigma_2} \dots y_m^{\sigma_m})$ ise $(\sigma_1, \sigma_2, \dots, \sigma_m) \in \mathbb{N}^m$, (4.3.2) denklem sisteminin bir çözümüdür (Adams and Lousaunau 1994).

Şimdi polinom dönüşümler hakkında bazı bilgiler verilerek tekrar bu sistemin çözümüne geri dönecektir. $k[y_1, \dots, y_m]$ ve $k[x_1, \dots, x_n]$ birer polinom halkası olmak üzere,

$$\phi: k[y_1, \dots, y_m] \rightarrow k[x_1, \dots, x_n]$$

dönüşümü bir halka homomorfizmidir. Bu dönüşüm $1 \leq i \leq m$ ve $f_i \in k[x_1, \dots, x_n]$ olmak üzere

$$\phi: y_i \rightarrow f_i \quad (4.3.4)$$

ile tek türlü belirlidir. Yani, eğer, $h \in k[y_1, \dots, y_m]$ polinomu $c_v \in k$, $v = (v_1, \dots, v_m) \in \mathbb{N}^m$ olmak üzere $h = \sum_v c_v y_1^{v_1} \dots y_m^{v_m}$ olarak alınır ve sadece sonlu sayıda c_v ler sıfırdan farklı ise,

$$\phi(h) = \sum_v c_v f_1^{v_1} \dots f_m^{v_m} = h(f_1, \dots, f_m) \in k[x_1, \dots, x_n] \quad (4.3.5)$$

elde edilir.

Teorem 4.3.2: $K = \langle y_1 - f_1, \dots, y_m - f_m \rangle \subseteq k[y_1, \dots, y_m, x_1, \dots, x_n]$ bir ideal ve G de x değişkeni y değişkeninden büyük olmak üzere bir eliminasyon sıralamasına göre K için bir indirgenmiş Gröbner taban olsun. Bu durumda, $f \in k[x_1, \dots, x_n]$ polinomunun ϕ nin görüntü kümesinde olması için gerek ve yeter şart $f \xrightarrow{G} h$ olacak şekilde $h \in k[y_1, \dots, y_m]$ olmasıdır. Bu durumda, $f = \phi(h) = h(f_1, \dots, f_m)$ dir (Adams and Lousstau 1994).

Teorem 4.3.2 bir polinomun ϕ nin görüntü kümesinde olup olmadığının belirlenmesi için algoritmik bir metod sunmaktadır. Ancak Lemma 4.3.1 de $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ kuvvet çarpımının polinomdan ziyade başka bir kuvvet çarpımın görüntüsü olması istenmektedir. Fakat, ϕ dönüşümü y_j değişkenlerini $k[x_1, \dots, x_n]$ de kuvvet çarpımlarına götürdüğünden aşağıdaki lemma elde edilir.

Lemma 4.3.3: Yukarıda tanımlanan notasyon sabit olmak şartıyla bütün α_{ij} lerin ve b_i lerin negatif olmadığı kabul edilsin. Eğer $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \in \phi$ nin görüntü kümesinde

ise bu kuvvet çarpımı bir $y_1^{\sigma_1} y_2^{\sigma_2} \dots y_m^{\sigma_m} \in k[y_1, \dots, y_m]$ kuvvet çarpımının görüntüsüdür (Adams and Lousstaunau 1994).

İspat: $K = \langle y_j - x_1^{a_{1j}} x_2^{a_{2j}} \dots x_n^{a_{nj}} \mid j = 1, \dots, m \rangle$ olsun. G, x değişkenleri y değişkenlerinden daha büyük olmak üzere bir eliminasyon sıralamasına göre K için bir Gröbner tabanı olsun. Bu durumda Teorem 4.3.2 ye göre;

$$x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \in \text{im}(\phi) \Leftrightarrow x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \xrightarrow{G}_+ h, h \in k[y_1, \dots, y_m]$$

dır. Dahası, eğer $h \in k[y_1, \dots, y_m]$ iken

$$x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \xrightarrow{G}_+ h \text{ ise } x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} = \phi(h) \text{ dır.}$$

İlk olarak, K yı üreten polinomların tamamı iki kuvvet çarpımının farkı şeklindedir. Bu nedenle, G yi hesaplayan Buchberger Algoritması boyunca sadece iki kuvvet çarpımının farkı olan polinomlar üretilecektir. Aslında, her ikisi de iki kuvvet çarpımının farkı olan iki polinomun S -polinomu da yine iki kuvvet çarpımının farkı şeklindedir ve iki kuvvet çarpımının farkı şeklinde olan bir polinomun aynı formdaki başka bir polinomla tek adım indirgemesi yine iki kuvvet çarpımının farkı şeklinde olan bir polinom üretir. Dolayısıyla, G deki polinomların tamamı iki kuvvet çarpımının farkı şeklindedir. Şimdi, eğer $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \in \phi$ nin görüntü kümesinde ise, bu kuvvet çarpımı bir $h \in k[y_1, \dots, y_m]$ polinomuna indirgenir. Ancak, bir kuvvet çarpımının, iki kuvvet çarpımının farkı olan bir polinomla tek adım indirgemesi yine bir kuvvet çarpımı üretir. Bu nedenle h bir kuvvet çarpımıdır ve istenen elde edilmiş olur.

Lemma 4.3.3 ün ispatı, (4.3.2) Sisteminin bir çözümünün olup olmadığının belirlenmesi ve çözümün bulunması için bir yöntem sunmaktadır:

- (i) x değişkeninin y değişkeninden daha büyük olduğu bir eliminasyon sıralamasına göre, $K = \langle y_j - x_1^{a_{1j}} x_2^{a_{2j}} \dots x_n^{a_{nj}} \mid j = 1, \dots, m \rangle$ için bir G Gröbner tabanı hesaplanır.
- (ii) $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ kuvvet çarpımının G ile bölümünden kalan h bulunur.

- (iii) Eğer $h \notin k[y_1, \dots, y_m]$ ise (4.3.2) Sistemi negatif olmayan tamsayı çözümüne sahip değildir. Eğer $h = y_1^{\sigma_1} y_2^{\sigma_2} \dots y_m^{\sigma_m}$ ise $(\sigma_1, \sigma_2, \dots, \sigma_m)$ (4.3.2) Sisteminin bir çözümüdür.

Örnek 4.3.3: Aşağıda verilen denklem sistemi ele alınsın.

$$\begin{cases} 3\sigma_1 + 2\sigma_2 + \sigma_3 + \sigma_4 = 10 \\ 4\sigma_1 + \sigma_2 + \sigma_3 = 5 \end{cases} \quad (4.3.6)$$

Her bir denklem için bir tane olmak üzere x_1, x_2 olarak adlandırılan iki x değişkeni vardır. Ayrıca her bilinmeyen için bir tane olmak üzere y_1, y_2, y_3 ve y_4 olarak adlandırılan dört tane y değişkeni vardır. Buna karşılık gelen polinom dönüşümü,

$$\begin{aligned} \mathbb{Q}[y_1, y_2, y_3, y_4] &\xrightarrow{\phi} \mathbb{Q}[x_1, x_2] \\ y_1 &\mapsto x_1^3 x_2^4 \\ y_2 &\mapsto x_1^2 x_2 \\ y_3 &\mapsto x_1 x_2 \\ y_4 &\mapsto x_1 \end{aligned}$$

dir ve böylece,

$K = \langle y_1 - x_1^3 x_2^4, y_2 - x_1^2 x_2, y_3 - x_1 x_2, y_4 - x_1 \rangle \subseteq \mathbb{Q}[y_1, y_2, y_3, y_4, x_1, x_2]$ dir. K için Gröbner tabanı $x_1 > x_2 > y_1 > y_2 > y_3 > y_4$ olmak üzere lex sıralamasına göre

$f_1 = x_1 - y_4, f_2 = x_2 y_4 - y_3, f_3 = x_2 y_3^3 - y_1, f_4 = y_2 - y_3 y_4, f_5 = y_1 y_4 - y_3^4$ olan $G = \{f_1, f_2, f_3, f_4, f_5\}$ kümesidir. Bu durumda,

$$x_1^{10} x_2^5 \xrightarrow{\{f_1, f_2\}} y_3^5 y_4^5$$

ve $h = y_3^5 y_4^5$ kuvvet çarpımı G ye göre indirgenmiştir. h nin kuvvetleri olan $(0,0,5,5)$ (4.3.6) Sisteminin bir çözümüdür.

4.4. Sudoku Oyununda Gröbner Tabanı

Son yıllarda “sayı yerleştirme” olarak adlandırılan bazı oyunlar çok popüler hale geldi. Bu oyunlarda hedef, başka sayılar tarafından verilen bazı bilgilerden yola çıkarak tahtaya eksik verileri, sayıları veya parçaları koymaktır.

Bu kısımda bahsedilen bulmacaların bazıları analiz edilerek bunlar polinom denklemlerin eşdeğer cebirsel sistemlerine indirgenecektir.

4.4.1. Sudokuyu Tanımlama ve Modelleme

Japon dilinde, sayıların tek olması anlamındaki “suuji wa dokishin ni kagiru” sözcüklerinin kısaltması olan sudoku, geçmişte sadece Japonya ile sınırlıyken günümüzde tüm dünya ülkelerine ulaşmış, ilgi çekmiş bir zeka oyunudur.

Sudoku Japonya’da 1984 yılında bir bulmaca dergisinde yayınlanmıştır. Derginin ait olduğu şirketin kurucusu Maki Kaji’dir. Keşfedilmesindeki kaynak Latin karesidir. ‘Sayı Yerleştirme’ adının kökeni New York’tan gelmesine rağmen, Sudoku; 1986’da Japonya’da ve 2005’te de tüm dünyada popüler hale gelen bir bilmece olmuştur.

Sudoku’nun bildiğimiz şekline gelmesinde ise emekli mimar Howard Garn etkili olmuştur. Garn’ın bulmacaları 1979 yılında bir dergide yayınlanmıştır. 1997 yılında sudoku, bulmaca kitabından bilgisayar ortamına taşınmış ve sudoku hazırlanması için program geliştirilmiştir.

Bu bulmaca da; 3x3 boyutunda 9 bölgeye bölünmüş 9x9’luk bir panoyu 1 ile 9 arasındaki rakamlarla doldurmamız gerekir. Kartta verilen bazı numaralardan, herhangi bir satır, sütun veya 3x3 bölgesinde iki sayı tekrarlanmayacak şekilde yazılır. Uygun ve hatasız bir Sudoku’nun tek bir çözümü vardır.

Sudoku, graf renklendirme problemi olarak da ifade edilebilir:

- Graf, her bir hücre için bir tane olacak şekilde 81 köşeye sahiptir.
- Her bir sayı için bir tane olmak üzere 9 renge ihtiyaç vardır.
- Kenarlar Sudoku’nun bitişiklik ilişkileri ile tanımlanır: farklı sayılar istenilen yerde (satırlar, sütunlar ve bölgeler dikkate alınarak) farklı renklere ihtiyaç vardır.

	9				4			7
					7	9		
8								
4		5	8					
3								2
					9	7		6
								4
		3	5					
2			6				8	

Şekil 4.4.1.1: Tipik bir Sudoku

Elde edilen $\mathcal{G}$ grafi, 20. dereceden düzgün bir graftır. Dolayısıyla, $\mathcal{G}$ nin kenarlarının sayısı $\frac{81 \cdot 20}{2} = 810$ a eşittir.

Renklendirme problemi, üreteçleri $F(x_j)$, $j = 1, \dots, 81$ ve $G(x_i, x_j)$, $1 \leq i \leq j \leq 81$ olan $\mathbb{Q}[x_1, \dots, x_{81}]$ in (her bir köşeye bir değişken) I ideali tarafından tanımlanan bir polinom sistemiyle de çözülebilir.

- 1 den 9 a kadar olan renkler dikkate alınsın. Her bir x_j köşesi için

$F(x_j) = \prod_{i=1}^9 (x_j - i)$ polinomu ele alınsın.

- Eğer iki köşe bitişik ise $F(x_i) - F(x_j) = (x_i - x_j)G(x_i, x_j) = 0$ dır.

Dolayısıyla, farklı renklerle ilgili şart $G(x_i, x_j)$ polinomu eklenerek verilir.

Sudoku'daki hücreler Şekil 2 deki gibi numaralandırılsın.

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81

Şekil 4.4.1.2: Hücre numaralandırması.

Buna ek olarak, Sudoku'nun tüm başlangıç bilgileri içerilmek zorundadır. Örneğin, Şekil 1 deki Sudoku çözülmek isteniyorsa, I idealine aşağıdaki polinomlar eklenmek zorundadır:

$$x_2 - 9, x_6 - 4, x_9 - 7, x_{15} - 7, x_{16} - 9, x_{19} - 8,$$

$$x_{28} - 4, x_{30} - 5, x_{31} - 8, x_{37} - 3,$$

$$x_{45} - 2, x_{51} - 9, x_{52} - 7, x_{56} - 6, x_{63} - 4,$$

$$x_{66} - 3, x_{67} - 5, x_{73} - 2, x_{76} - 6, x_{80} - 8.$$

Verilen bir Sudoku'nun çözümleriyle ilgili tüm bilgiler I nın sıfırlarının kümesi olan $V(I)$ tarafından içerilmektedir.

$$V(I) = V_Q(I) = \{(s_1, \dots, s_{81}) \in \mathbb{Q}^{81} \mid \text{her } f \in I \text{ için } f(s_1, \dots, s_{81}) = 0\}.$$

Not 4.4.1.1: Başlangıç verilerine karşılık gelen polinomlar ekledikten sonra, $F(x_i)$ polinomlarının fazlalık olduğunu görmek kolaydır, böylece bunlar silinebilir.

Denklem sistemi, grafın her bir kenarı için bir tane olacak şekilde 810 tane denkleme sahiptir.

Aşağıdakiler temel sonuçlardır:

Önerme 4.4.1.2: Bir Sudokunun çözümünün olabilmesi için gerek ve yeter şart

$$I \neq \mathbb{Q}[x_1, \dots, x_{81}]$$

gerek ve yeter şart I nin herhangi bir terim sıralamasına göre herhangi bir indirgenmiş Gröbner tabanının $\{1\}$ olmamasıdır (Vargas et al. 2006).

Önerme 4.4.1.3: Eğer özel dizayn edilmiş bir Sudoku ile başlanılırsa, I nin herhangi bir terim sıralamasına göre herhangi bir indirgenmiş Gröbner tabanı, a_i ler 1'den 9'a kadar olan sayılar olmak üzere $G = \{x_i - a_i \mid i = 1, \dots, 81\}$ formundadır. Burada a_i sayıları çözümü tanımlar (Vargas et al. 2006).

Örnek 4.4.1.4: Şekil 4.4.1.3 teki problem ele alınsın.

9								8
5			2		8		6	
		3	7	1				9
				7	3		5	
2								4
	5		1	6				
8				2	7	3		
	4		3		9			1
7								2

Şekil 4.4.1.3: Hücre numaralandırması.

Yukarıda bahsedilen teorik bilgiler doğrultusunda Sudoku problemini çözmek için gerekli algoritmanın Syntaxı Singular paket program için aşağıdaki gibidir:

```
<"sudoku";
intmat A[9][9] =
    9,0,0,0,0,0,0,8, 5,0,0,2,0,8,0,6,0,
    0,0,3,7,1,0,0,0,9,
    0,0,0,0,7,3,0,5,0, 2,0,0,0,0,0,0,4,
    0,5,0,1,6,0,0,0,0,
    8,0,0,0,2,7,3,0,0, 0,4,0,3,0,9,0,0,1,
    7,0,0,0,0,0,0,0,2;
def G = sudoku(A); vdim(G);
//used time: 1.65 sec
//-> 1
```

Bu Sudoku tek bir çözüme sahiptir ve G indirgenmiş Gröbner tabanında kodlanmıştır.

9	2	6	5	3	4	7	1	8
5	7	1	2	9	8	4	6	3
4	8	3	7	1	6	5	2	9
1	9	8	4	7	3	2	5	6
2	6	7	9	8	5	1	3	4
3	5	4	1	6	2	9	8	7
8	1	9	6	2	7	3	4	5
6	4	2	3	5	9	8	7	1
7	3	5	8	4	1	6	9	2

Şekil 4.4.1.4: Şekil 4.4.1.3 için çözüm

KAYNAKLAR

- Adams, W. W. and Loustaunau P. 1994. An Introduction to Gröbner Bases. The American Mathematical Society, Providence, RI, USA.
- Arnold, E. and Lucas, S and Taalman, L. 2009. Gröbner Bases Representations of Sudoku. Department of Matematics and Statistics, James Medison University, Harrisonburg.
- Balkanay, E. and Ağargün, G. and Aygör, N. 2000. Soyut Cebir Cilt I. Yıldız Teknik Üniversitesi Vakfı Yayınları, İstanbul.
- Çallıhap, F. 2009. Örneklerle Soyut Cebir. Birsen Yayınevi, İstanbul.
- Falcon, R. M. and Morales J. M. 2007. Gröbner bases and the number of Latin squares related to autopisms of order ≤ 7 . Spain, <https://www.sciencedirect.com/science/article/pii/S0747717107001009> (15.04.2018).
- Özenir, Y. 2011. Gröbner Tabanları. Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.
- Vargas, J.G. and Hermoso I.H. 2006. Sudokus and Gröbner Bases: not only a Divertimento, 9th International Workshop, CASC 2006, September 11-15, Chişinău, Moldova.
- Yeşilot, G. and Özavşar M. 2012. Soyut Cebir Çözümlü Problemleri. Nobel Yayınları, Ankara.

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Sevde ÖZEN
Doğum Yeri ve Tarihi	Bakırköy /14.07.1992
Eğitim Durumu	
Lisans Öğrenimi	Yıldız Teknik Üniversitesi
Yüksek Lisans Öğrenimi	-
Bildiği Yabancı Diller	İngilizce
Bilimsel Faaliyetler	
İş Deneyimi	
Stajlar	Dede Korkut Anadolu Lisesi (Bahçelievler /İst)
Projeler	TÜBİTAK 4006 Bilim Şenliği
Çalıştığı Kurumlar	Milli Eğitim Bakanlığı'nda Matematik Öğretmeni Arif Nihat Asya Anadolu Lisesi (Van/Erciş) Şehit Abdülkadir Bahçe MTAL (Van/Erciş) Sevim Kürüm Anadolu Lisesi (Van/ Erciş)
İletişim	
E-posta Adresi	sevde_kaya_07@hotmail.com
Mezuniyet Tarihi	
Lisans-2014	