PM 6 - Understanding Geometric Objects With Computer Algebra System

Adrina Esfandiari, Bowen Dai, Jessica Ni, Xena Jiang
Mentor: Erica Liu

WiM Directed Reading Program

2025

Overview

In this presentation, we will go over the following:

Overview

In this presentation, we will go over the following:

- Introduction to definitions/terminology

Overview

In this presentation, we will go over the following:

- Introduction to definitions/terminology
- Important theorems and results

Overview

In this presentation, we will go over the following:

- Introduction to definitions/terminology
- Important theorems and results
- Application of Gröbner bases to Sudoku puzzles

Overview

In this presentation, we will go over the following:

- Introduction to definitions/terminology
- Important theorems and results
- Application of Gröbner bases to Sudoku puzzles
- Working algorithm to solve given Sudoku puzzles + live demo

Full Document

Scan here for the full document containing more detailed definitions and proofs:

Multi-variable Monomial and Polynomial

Monomial:

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

for a monomial of n variables, $x_1, x_2, ..., x_n$

- Commonly written as x^α
- x^3y^2 is a multivariable monomial

Polynomial:

$$f = \sum_\alpha a_\alpha x^\alpha$$

- $k[x_1, x_2, \ldots, x_s]$ is the set of all polynomials with variable $x_1, x_2, \ldots, x_s$
- $f = 2x^3y^2z - 3xyz + \frac{3}{2}y^3z^3 + y^2$ is a polynomial in $\mathbf{Q}[x, y, z]$

Affine Variety

We commonly write it as:

$$\mathbf{V}(f_1, \ldots, f_s)$$

Affine variety is the set of solutions in k^n to a system of equations $f_1, f_2, f_3, \ldots, f_s$.

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n | f_i(a_1, \ldots, a_n) = 0, \forall 1 \leq i \leq s\}.$$

Examples

- $\mathbf{V}(x^2 + y^2 - 1)$ contains all the values in $\mathbf{R}$ that makes $x^2 + y^2 - 1 = 0$ true, which is all the points in the circle
- $\mathbf{V}(y - x, y + x)$ contains all the values in $\mathbf{R}$ that makes $y - x = 0, y + x = 0$ true; visualized graphically, it is the intersection of two functions, which is $(0, 0)$

Ideals

Ideal: I the set of polynomials
$I \subseteq k[x_1, x_2, ..., x_n]$

- $0 \in I$
- $f, g \in I$ then $f + g \in I$
- If $f \in I$ and $h \in k[x_1, x_2, ..., x_n]$, then $hf \in I$

Ideals commonly comes in the form of $\langle f_1, f_2, f_3, \ldots, f_s \rangle$ where

$$\langle f_1, f_2, f_3, \ldots, f_s \rangle = \{\sum_{i=1}^{s} h_i f_i | h_1, \ldots h_s \in k[x_1, x_2, ..., x_n]\}$$

Ideal Examples

Ideal belonging problem: Does $x^2 - 2x + 2 - y$ belong in $\langle x - 1 - t, y - 1 - t^2 \rangle$?

Ideal Examples

Ideal belonging problem: Does $x^2 - 2x + 2 - y$ belong in $\langle x - 1 - t, y - 1 - t^2 \rangle$?

Yes! $x^2 - 2x + 2 - y = (x - 1 + t)(x - 1 - t) + (-1)(y - 1 - t^2)$ this is in the form of

$$\sum_{i=1}^{s} h_i f_i$$

Relationship between Affine Variety and Ideals

When we are trying to find $V(f_1, f_2, \ldots, f_n)$ and $\langle f_1, f_2, \ldots, f_s \rangle = \langle g_1, g_2, \ldots, g_s \rangle$

then...

- $V(g_1, g_2, \ldots, g_s) = V(f_1, f_2, \ldots, f_n)$

Monomial Ideal

Monomial ideal is a special special polynomial ideal where it can be written in the form of

$$I = \langle x^{a_1}, x^{a_2}, x^{a_3} \ldots \rangle$$

Ideal generated by leading terms of an ideal

$$\langle LT(I) \rangle$$

Leading term is a term of a polynomial

- Determine a monomial ordering, order the terms of the polynomial
- Leading term is the first term of the ordered polynomials.

Examples

$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$

Ideal generated by leading terms of an ideal

$$\langle LT(I) \rangle$$

Leading term is a term of a polynomial

- Determine a monomial ordering, order the terms of the polynomial
- Leading term is the first term of the ordered polynomials.

Examples

$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$
$f = 2x^3y^2z - 3xyz + \frac{3}{2}y^3z^3 + y^2$

Ideal generated by leading terms of an ideal

$$\langle LT(I) \rangle$$

Leading term is a term of a polynomial

- Determine a monomial ordering, order the terms of the polynomial
- Leading term is the first term of the ordered polynomials.

Examples

$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$
$f = 2x^3y^2z - 3xyz + \frac{3}{2}y^3z^3 + y^2$
$f = 2x^3y^2z - 3xyz + \frac{3}{2}y^3z^3 + y^2$

Ideal generated by leading terms of an ideal

$$\langle LT(I) \rangle$$

- $LT(I)$ is the leading term of every polynomial in ideal I
- $\langle LT(I) \rangle$ is the ideal generated by those leading term

Important Theorems and Results:

Dickson's Lemma:
Let $I = \langle x^\alpha \mid \alpha \in A \rangle \subset k[x_1, \dots, x_n]$ be a monomial ideal. Then I can be written in the form

$$I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle,$$

where $\alpha(1), \dots, \alpha(s) \in A$. In particular, I has a finite basis.

Important Theorems and Results:

Dickson's Lemma:
Let $I = \langle x^\alpha \mid \alpha \in A \rangle \subset k[x_1, \ldots, x_n]$ be a monomial ideal. Then I can be written in the form

$$I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle,$$

where $\alpha(1), \ldots, \alpha(s) \in A$. In particular, I has a finite basis.

Results:

- Necessary for the proof of Hilbert Basis theorem.
- Ensures finite Gröbner basis exists.

Important Theorems and Results:

Hilbert Basis Theorem:
Every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a finite generating set. In other words, $I = \langle g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in I$.
Example:
$I = \left\langle x^2 + y^3 - z^5,\ xyz + 1,\ x^3y^2z^4 - 7xy + z^2,\ x^2z - y^4,\ \ldots \right\rangle$
will have a finite generating set.

Results:

- Any affine variety can be defined by a finite number of equations, no infinite constraints are needed.

Important Theorems and Results:

Gröbner Bases: Let I be an ideal from $k[x_1, \cdots x_n]$. Fix a monomial ordering. A finite subset $G = \{g_1, \ldots, g_r\} \subseteq I$ is called a *Gröbner basis* for I if:

$$1. \quad I = \langle g_1, \cdots, g_r \rangle$$

$$2. \quad \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle = \langle \mathrm{LT}(f) \mid f \in I \rangle$$

Property of G:
If $G = \{g_1, \ldots, g_r\}$ is a Gröbner basis for an ideal, then every polynomial $f \in k[x_1, \ldots, x_n]$ can be divided by G, and the remainder satisfies:

- The remainder is **unique**.
- The remainder is **zero** if and only if $f \in I$.

Important Theorems and Results:

Results:

This helps us to solve the ideal membership problem!!

Example:

Let our polynomial ring be $\mathbb{Q}[x, y]$. Let
$I = \langle f_1, f_2 \rangle = \langle x^2 + y,\ xy - 1 \rangle$.

Question: Does $f = x^3y + x \in I$?

We compute a Gröbner basis using lexicographic order with $x > y$. Then $G = \{y^2 + x,\ xy - 1,\ x^2 + y\}$. By performing multivariate polynomial division of f with respect to G, the remainder is 0 hence, $f \in I$.

Sudoku Application: Rules

To begin, we will consider a 4x4 sudoku grid with the following rules:

			3
	4		
1			4
		3	

Sudoku Application: Rules

To begin, we will consider a 4x4 sudoku grid with the following rules:

			3
	4		
1			4
		3	

1. All values
   must be integers between 1 and 4

Sudoku Application: Rules

To begin, we will consider a 4x4 sudoku grid with the following rules:

			3
	4		
1			4
		3	

1. All values
   must be integers between 1 and 4
2. The sum of every row,
   column, and 2x2 block must be 10

Sudoku Application: Rules

To begin, we will consider a 4x4 sudoku grid with the following rules:

			3
	4		
1			4
		3	

1. All values must be integers between 1 and 4
2. The sum of every row, column, and 2x2 block must be 10
3. No two blocks in the same row, column, or 2x2 block can be equal

Sudoku Application Overview

Now, using what we have learned, we can find a solution to any proper 4x4 sudoku with the following steps:

Sudoku Application Overview

Now, using what we have learned, we can find a solution to any proper 4x4 sudoku with the following steps:

- Assign the variables $x_0, x_1, ..., x_{14}, x_{15}$ to each grid

Sudoku Application Overview

Now, using what we have learned, we can find a solution to any proper 4x4 sudoku with the following steps:

- Assign the variables $x_0, x_1, \ldots, x_{14}, x_{15}$ to each grid
- Create polynomials representing each rule from before

Sudoku Application Overview

Now, using what we have learned, we can find a solution to any proper 4x4 sudoku with the following steps:

- Assign the variables $x_0, x_1, \ldots, x_{14}, x_{15}$ to each grid
- Create polynomials representing each rule from before
- Generate an ideal using these polynomials

Sudoku Application Overview

Now, using what we have learned, we can find a solution to any proper 4x4 sudoku with the following steps:

- Assign the variables $x_0, x_1, ..., x_{14}, x_{15}$ to each grid
- Create polynomials representing each rule from before
- Generate an ideal using these polynomials
- Use an algorithm (Buchberger's algorithm) to generate Gröbner basis

Sudoku Application Overview

Now, using what we have learned, we can find a solution to any proper 4x4 sudoku with the following steps:

- Assign the variables $x_0, x_1, ..., x_{14}, x_{15}$ to each grid
- Create polynomials representing each rule from before
- Generate an ideal using these polynomials
- Use an algorithm (Buchberger's algorithm) to generate Gröbner basis
- Find the variety (solutions) of the ideal using generated basis

Polynomials Needed

For $0 \leq i, j \leq 15$, consider the following polynomials used to generate our ideal:

Polynomials Needed

For $0 \leq i, j \leq 15$, consider the following polynomials used to generate our ideal:

- $F(x_i) = (x_i - 1)(x_i - 2)(x_i - 3)(x_i - 4)$

Polynomials Needed

For $0 \leq i, j \leq 15$, consider the following polynomials used to generate our ideal:

- $F(x_i) = (x_i - 1)(x_i - 2)(x_i - 3)(x_i - 4)$
- $G(x_i, x_j) = \frac{F(x_i) - F(x_j)}{x_i - x_j}$

Polynomials Needed

For $0 \leq i, j \leq 15$, consider the following polynomials used to generate our ideal:

- $F(x_i) = (x_i - 1)(x_i - 2)(x_i - 3)(x_i - 4)$
- $G(x_i, x_j) = \frac{F(x_i) - F(x_j)}{x_i - x_j}$
- $x_i - a$ for $1 \leq a \leq 4$ (the pre-existing squares)

Ideal and Gröbner Basis Generated

Now, we can create an ideal I using these polynomials and use Buchberger's algorithm to generate the unique Gröbner basis G with the following properties:

Ideal and Gröbner Basis Generated

Now, we can create an ideal I using these polynomials and use Buchberger's algorithm to generate the unique Gröbner basis G with the following properties:

- If the sudoku is proper, each element of this basis is of the form $x_i - a_i$ for $1 \leq a_i \leq 4$

Ideal and Gröbner Basis Generated

Now, we can create an ideal I using these polynomials and use Buchberger's algorithm to generate the unique Gröbner basis G with the following properties:

- If the sudoku is proper, each element of this basis is of the form $x_i - a_i$ for $1 \leq a_i \leq 4$
- The solutions to the variety of I is simply the solution to setting each element of G to zero

Ideal and Gröbner Basis Generated

Now, we can create an ideal I using these polynomials and use Buchberger's algorithm to generate the unique Gröbner basis G with the following properties:

- If the sudoku is proper, each element of this basis is of the form $x_i - a_i$ for $1 \leq a_i \leq 4$
- The solutions to the variety of I is simply the solution to setting each element of G to zero
- Thus, each a_i describes the value present in grid x_i (or the solution to the sudoku) since each $x_i = a_i$

Implementation

```
import itertools

#initialize varibles x_0,...,x_15
var_names = ['x_{}'.format(i) for i in range(0,16)]

#initialize polynomial ring with x_0,...,x_15
R = PolynomialRing(QQ, var_names, order='lex')
R.inject_variables()

#generate the polynomial (x_i-1)(x_i-2)(x_i-3)(x_i-4)
#These polynomials restrict that x_i must equals to
#1, 2, 3, or 4
poly_List = []
for x in R.gens():
    poly_List.appen(prod([(x-i) for i in [1..4]]))
```

Implementation

```
    row_List = [] #generate a list of polynomial for each row
    for i in range(4):
        temp =[]
        for j in range(4):
            temp.append(poly_List[i*4+j])
        row_List.append(temp)

    col_List = [] #generate a list of polynomial for each column
    for i in range(4):
        temp = []
        for j in range(4):
            temp.append(poly_List[i+4*j])
        col_List.append(temp)

    block_List =[] #generate a list of polynomial for each block
    for i in range(4):
        start = (i//2)*8 +(i%2)*2
        temp = []
        for j in range(4):
            temp.append(poly_List[start + j%2 + (j//2)*4])
        block_List.append(temp)
```

Implementation

```
    # combine all lists
    adjacent_List = row_List + col_List + block_List
    diff_List = []
    for l in adjacent_List:
        comb = list(itertools.combinations(l,2))
        # take all possible combinations and eliminate the
        # factor (x_i-x_j), so x_i =\= x_j if they are in
        # the same row, column or block
        for c in comb:
            diff = c[0] - c[1]
            vars = diff.variables()
            diff_List.append(diff/(vars[0]-vars[1]))

    #clues from sudoku
    initial_clues = [x_3-3,x_5-4,x_8-1,x_11-4,x_14-3]

    #generate the ideal using the clues, non-repetitive
    #restrictions and number restriction of each variables
    I = R.ideal(initial_clues + diff_List + poly_List)
    G = I.groebner_basis()
    show(G)
```

Result

```
# the groebner basis of the ideal I is the solution of
# the sukodu
[x_0 - 2, x_1 - 1, x_2 - 4, x_3 - 3,
 x_4 - 3, x_5 - 4, x_6 - 1, x_7 - 2,
 x_8 - 1, x_9 - 3, x_10 - 2, x_11 - 4,
 x_12 - 4, x_13 - 2, x_14 - 3, x_15 - 1]
```

Conclusion and Further Applications

Today, we went over:

Conclusion and Further Applications

Today, we went over:

- Varieties, ideals, and Gröbner bases

Conclusion and Further Applications

Today, we went over:

- Varieties, ideals, and Gröbner bases
- Dickson's Lemma and Hilbert Basis Theorem w

Conclusion and Further Applications

Today, we went over:

- Varieties, ideals, and Gröbner bases
- Dickson's Lemma and Hilbert Basis Theorem w
- Application to solving sudoku puzzles in computer algebra systems

Conclusion and Further Applications

Today, we went over:

- Varieties, ideals, and Gröbner bases
- Dickson's Lemma and Hilbert Basis Theorem w
- Application to solving sudoku puzzles in computer algebra systems

Further applications:

Conclusion and Further Applications

Today, we went over:

- Varieties, ideals, and Gröbner bases
- Dickson's Lemma and Hilbert Basis Theorem w
- Application to solving sudoku puzzles in computer algebra systems

Further applications:

- Similar usage of Gröbner bases to solve other games (eg. minesweeper) or more complex sudoku puzzles (eg. 9x9)

Conclusion and Further Applications

Today, we went over:

- Varieties, ideals, and Gröbner bases
- Dickson's Lemma and Hilbert Basis Theorem w
- Application to solving sudoku puzzles in computer algebra systems

Further applications:

- Similar usage of Gröbner bases to solve other games (eg. minesweeper) or more complex sudoku puzzles (eg. 9x9)
- Algebraic Geometry appears in other areas of pure math such as topology, complex analysis, number theory and more.