Win 2025 DRP-Reading

Gröbner Basis and Computational Algebraic Geometry

1 Definitions

1.1 Field

- A field a set, well-defined under binary operations (addition and multiplication), such that
  - addition and multiplication is commutative, associative
  - additive and multiplication identity exist
  - distribution law exist
- Some properties are:
  - it is a integral domain
- Some examples are:
  - **R** is a field
  - **Z** is not a field

1.2 Monomial

- It is in the form
$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$
for a monomial of n variables, $x_1, x_2, ..., x_n$
- This is commonly written as x^α for simplicity, where x is a tuple of $(x_1, x_2, ..., x_n)$ and α is a tuple of $(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$
- Its degree is $|\alpha_1 + \alpha_2 + \alpha_3 + \cdots = \alpha_n|$
- for example: x^3y^2 with variables x, y, with degree 5

1.3 Polynomial

- It is a sum of monomials with variable $x_1, x_2, ..., x_n$ in the form
$$f = \sum_\alpha a_\alpha x^\alpha,$$
where a_α is an element of the field.
- a_α is the **coefficient** of the monomial that belongs to field K

- $\sum_\alpha a_\alpha x^\alpha$ is a **term** of f
- **Total degree** is the sum of α (order well-defined in a field)
- Again, α is a tuple of $(\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_n)$
- This is commonly expressed by $k[x_1, x_2, ..., x_n]$ where k is the field where the coefficients belongs to, and $x_1, x_2, ..., x_n$ are the variables
- Example: $f = 2x^3y^2z - 3xyz + \frac{3}{2}y^3z^3 + y^2$ is a polynomial in $\mathbf{Q}[x, y, z]$
  - $2x^3y^2z, \frac{3}{2}y^3z^3, 3xyz, y^2$ are terms
  - the total degree is 6
  - $2, \frac{3}{2}, 3, 1$ are coefficient

1.4 Affine Variety

- Let k be a field, $f_1, f_2, f_3, \ldots, f_s$ are polynomials in $k[x_1, x_2, ..., x_n]$, then the affine variety, or $\mathbf{V}(f_1, \ldots, f_s)$, is equal to the set of solutions to all the functions $f_1, f_2, f_3, \ldots, f_s$.

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

- For example:
  - $\mathbf{V}(x^2 + y^2 - 1)$ 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 $(0, 0)$

1.5 Ideals

- A subset $I \subseteq k[x_1, x_2, ..., x_n]$ is an idea if it satisfies
  - $0 \in I$
  - $f, g \in I$ then $f + g \in I$
  - If $f \in I$ and $h \in k[x_1, x_2, ..., x_n]$, then $hf \in I$
- Ideal commonly comes in the form of $\langle f_1, f_2, f_3, \ldots, f_s \rangle$ where

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

  - $f_1, f_2, f_3, \ldots, f_s$ are the generator of this ideal
  - belonging problem: $x^2 - 2x + 2 - y \in \langle x - 1 - t, y - 1 - t^2 \rangle$ because $x^2 - 2x + 2 - y = (x - 1 + t)(x - 1 - t) + (-1)(y - 1 - t^2)$

1.6 Monomial Ideal

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

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

- when written in this form $I = \langle x^{a_1}, x^{a_2}, x^{a_3} \dots \rangle$, the generators $x^{a_1}, x^{a_2}, x^{a_3} \dots$ is called the minimal basis
- the minimal basis is unique
- suggest $f \in I$, I is a monomial ideal, then every term of f must lies in $\langle x^{a_i} \rangle$ for some $i, 1 \leq i \leq s$.
- the minimal basis is finitely generated (see Dickson's lemma)

1.7 Leading term

- The leading term for multivariable polynomials may be different depending on choice of monomial ordering
- It is the first term of the polynomial after ordering the terms.

1.8 Ideal generated by Leading terms of an ideal

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

The generators of this ideal is the leading term of every polynomial in ideal I let $f_1, f_2, \dots$ be the generator of ideal I, that is $I = \langle f_1, f_2, \dots \rangle$, then $\langle LT(f_1), \dots LT(f_s) \rangle \subseteq \langle LT(I) \rangle$ It is a very special instance when $\langle LT(f_1), \dots LT(f_s) \rangle = \langle LT(I) \rangle$ (see Hilbert Basis's Theorem)

1.9 Greatest common divisor

- the **greatest common divisor** of polynomials $f_1, f_2, \dots, f_s \in k[x]$ is a polynomial s.t.
- h divides $f_1, \dots, f_s$
- if p is another polynomial which divides $f_1, \dots, f_s$, then p divides h

1.10 Gröbner Basis

- Fix an I, then we produce a basis $g_1, \dots, g_s \in I$ s.t. $\langle LT(g_1), \dots, \langle LT(g_t) \rangle = \langle LT(I) \rangle$, then $g_1, g_2, \dots g_s$ is called the Gröbner basis of I

2 Theories

Monomial Ideals and Dickson's Lemma:

Recall that an ideal $I \subset k[x_1, x_2, \ldots, x_n]$ is a **monomial ideal** if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ such that I consists of all polynomials which are finite sums of the form

$$\sum_{\alpha \in A} h_\alpha x^\alpha, \quad h_\alpha \in k[x_1, \ldots, x_n].$$

Lemma:
Let $I = \langle x^\alpha \mid \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I *if and only if* x^β is divisible by x^α for some $\alpha \in A$.

Proof. If x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$ by the definition of ideal. Conversely, if $x^\beta \in I$, then

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)},$$

where $h_i \in k[x_1, \ldots, x_n]$ and $\alpha(i) \in A$. Expanding each h_i gives

$$x^\beta = \sum_{i=1}^{s} \left(\sum_j c_{i,j} x^{\beta(i,j)} \right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}.$$

Since each term on the right is divisible by some $x^{\alpha(i)}$, it follows that x^β must also be divisible. $\square$

Theorem (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.

Proof.
We proceed by induction on n, the number of variables.

Base case: When $n = 1$, the ideal $I \subseteq k[x]$ is generated by monomials x^α for $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Let $\beta = \min A$. Then for all $\alpha \in A$, we have $\beta \leq \alpha$, so x^β divides every x^α. Thus, $I = \langle x^\beta \rangle$ is finitely generated.

Inductive hypothesis: Assume the result holds for $n - 1$ variables. Let $n > 1$, and write

$$k[x_1, \ldots, x_n] = k[x_1, \ldots, x_{n-1}, y] \quad \text{with } y = x_n$$

Each monomial in $k[x_1, \ldots, x_n]$ can be written as $x^\gamma y^m$, where $x^\gamma \in k[x_1, \ldots, x_{n-1}]$ and $m \in \mathbb{Z}_{\geq 0}$.

Inductive step:
Suppose the result holds for $n - 1$ variables. Let $I \subseteq k[x_1, \ldots, x_{n-1}, y]$ be a monomial ideal. Each monomial in I has the form $x^\gamma y^m$, where $\gamma \in \mathbb{Z}^{n-1}_{\geq 0}$ and $m \geq 0$.

We define a projection map:

$$\pi : \mathbb{Z}^n_{\geq 0} \to \mathbb{Z}^{n-1}_{\geq 0}, \quad \pi(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = (\alpha_1, \ldots, \alpha_{n-1}).$$

Let $J \subseteq k[x_1, \ldots, x_{n-1}]$ be the monomial ideal defined as

$$J = \langle x^\gamma \mid x^\gamma y^m \in I \text{ for some } m \rangle.$$

By the inductive hypothesis, J is finitely generated: $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$.

For each i, there exists $m_i \in \mathbb{Z}_{\geq 0}$ such that $x^{\alpha(i)} y^{m_i} \in I$. Let $m = \max\{m_1, \ldots, m_s\}$.

Define, for $0 \leq \ell < m$, the *slice ideals*

$$J_\ell = \langle x^\beta \mid x^\beta y^\ell \in I \rangle \subseteq k[x_1, \ldots, x_{n-1}].$$

Each J_ℓ is finitely generated by the inductive hypothesis:

$$J_\ell = \langle x^{\alpha_\ell(1)}, \ldots, x^{\alpha_\ell(s_\ell)} \rangle.$$

Claim: The ideal I is generated by the finite set

$$I = \left\langle \underbrace{x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m}_{\text{from } J}, \underbrace{x^{\alpha_0(1)} y^0, \ldots, x^{\alpha_0(s_0)} y^0}_{\text{from } J_0}, \cdots, \underbrace{x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1}}_{\text{from } J_{m-1}} \right\rangle$$

To see this, let $x^\gamma y^p \in I$ be an arbitrary monomial.

- If $p \geq m$, then $x^\gamma \in J$, so x^γ is divisible by some $x^{\alpha(i)}$, hence $x^\gamma y^p$ is divisible by $x^{\alpha(i)} y^m$.
- If $p < m$, then $x^\gamma \in J_p$, so $x^\gamma y^p$ is divisible by one of the generators $x^{\alpha_p(j)} y^p$.

So all monomials in I are divisible by one of these finitely many generators. Therefore, I is finitely generated.

□

Proposition. Let $I \subseteq k[x_1, \ldots, x_n]$ be a nonzero ideal. Then:

(i) $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal.

(ii) There exist $g_1, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

Proof:

(i) The leading monomials $\mathrm{LM}(g)$ of elements $g \in I \setminus \{0\}$ generate the monomial ideal

$$\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle.$$

Since $\mathrm{LM}(g)$ and $\mathrm{LT}(g)$ differ by a nonzero constant, this ideal equals

$$\langle \mathrm{LT}(g) \mid g \in I \setminus \{0\} \rangle = \langle \mathrm{LT}(I) \rangle.$$

Thus, $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal.

(ii) Since $\langle \mathrm{LT}(I) \rangle$ is generated by the monomials $\mathrm{LM}(g)$ for $g \in I \setminus \{0\}$, Dickson's Lemma tells us that

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t) \rangle$$

for finitely many $g_1, \ldots, g_t \in I$. Since $\mathrm{LM}(g_i)$ differs from $\mathrm{LT}(g_i)$ by a nonzero constant, it follows that

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle.$$

This completes the proof. □

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 $g_1, \ldots, g_t \in I$.

Proof: If $I = \{0\}$, we take our generating set to be $\{0\}$, which is certainly finite. If I contains some nonzero polynomial, then a generating set $g_1, \ldots, g_t$ for I can be constructed as follows.

We first select one particular monomial order to use in the division algorithm and in computing leading terms. Then I has an ideal of leading terms $\langle \mathrm{LT}(I) \rangle$. We know there are $g_1, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. We claim that $I = \langle g_1, \ldots, g_t \rangle$.

It is clear that $\langle g_1, \ldots, g_t \rangle \subseteq I$ since each $g_i \in I$. Conversely, let $f \in I$ be any polynomial. If we apply the division algorithm f by $(g_1, \ldots, g_t)$, then we get an expression of the form

$$f = q_1 g_1 + \cdots + q_t g_t + r$$

where no term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. We claim that $r = 0$.

To see this, note that

$$r = f - q_1 g_1 - \cdots - q_t g_t \in I.$$

If $r \neq 0$, then $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Then we know a lemma that says let $I = \langle x^\alpha \mid \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I *if and only if* x^β is divisible by x^α for some $\alpha \in A$. So by applying that it follows that $\mathrm{LT}(r)$ must be divisible by some $\mathrm{LT}(g_i)$. This contradicts what it means to be a remainder, and, consequently, r must be zero. Thus,

$$f = q_1 g_1 + \cdots + q_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle,$$

which shows that $I \subseteq \langle g_1, \ldots, g_t \rangle$. This completes the proof.

3 Sudoku Application

To begin, the rules of a sudoku game, which we will take to be 4x4 in this example, are as follows:

1. Each grid on the board must be an integer value between 1 and 4
2. The sum of each column, row, or 2x2 block on the board must be equal to 10
3. No two grids in the same column, row, or 2x2 block can be equal

Now, to apply our knowledge of Gröbner bases onto this kind of puzzle, we should first denote each of the 81 grids on the 4x4 board as $x_0, x_1, .., x_{14}, x_{15}$ where each variable is restricted to the integers.

We will then find the solution to any given sudoku puzzle by using polynomials to represent the restrictions on our variables and generating an ideal using them. In particular, the variety of this ideal (or values for each variable such that every equation is equal to zero) would be equal to the solution space of the sudoku puzzle. As such, we wish to find the Gröbner basis of this ideal which will make it much easier to find the variety.

Now, to address the first restriction, consider the following polynomial for each x_j where $0 \leq j \leq 15$:

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

Combining this with the fact that each x_j must be an integer, we have successfully represented the restriction of each x_j being between 1 and 4.

Next, notice that the second restriction will always hold true so long as the first and third are satisfied. As such, we only need to satisfy the third restriction. For any two grids in the same column, row, or 2x2 block, which we will denote x_i and x_j for $0 \leq i < j \leq 15$, we will define the following polynomial:

$$G(x_i, x_j) = \frac{F(x_i) - F(x_j)}{x_i - x_j}$$

Now, notice that the denominator ensures that $x_i \neq x_j$ while the top will be zero so long as the first restriction is satisfied.

Lastly, we need to add in any pre-existing numbers on the grid. For any x_j that has a number already inside, we must add a new generator in the form $x_j - a$ (with $1 \leq a \leq 4$ in the integers) to represent that restriction.

With these three sets of polynomials, we have successfully created an ideal whose variety will have same solution set as the sudoku puzzle we inputted.

To determine this solution set, we would then algorithmically find the unique Gröbner basis for the generated ideal which will create a much simpler generating set. This is because, as mentioned before, the Gröbner basis of an ideal is simply a generating set that of the ideal that allows for algebraically convenient properties. In fact, for any proper sudoku with a single solution, the resulting Gröbner basis will end up being in the following form:

$$\{x_i - a_i : 0 \leq i \leq 15\}$$

This allows us to easily read off the solutions to the variety as they will be $x_i = a_i$ for all i. Thus, we have successfully computed the solutions to a given sudoku and can fill out the grids accordingly.