Computational Commutative Algebra and Geometry

Supervised Research Exposition

Rathour Param Jitendrakumar
190070049
Department of Electrical Engineering
Indian Institue of Technology Bombay
Guide: Prof. Debasattam Pal

Abstract

This report is divided into parts: An Introduction to Algebra and Geometry followed by An Introduction to Gröbner Bases then Applications of Gröbner Bases. We start with an introduction to algebraic concepts, focussing over polynomials, ideals and their algorithms. Then we study geometric concepts such as varieties and their relationship with ideals which is probed with interesting problem. One such problem of "Ideal Membership" is broken down into simpler cases and the development of Gröbner Bases Theory and Computation is motivated using it. Then, we focus on select applications of Gröbner Bases from countless many available in literature and also discuss SageMath implementations for some of them. I have tried to make this report interesting and also covered fundamentals. Still, this is just a *glimpse* of an extensive topic like Gröbner Bases. Finally, I encourage you to look at all the SageMath programs and their diverse and exciting applications here.

Acknowledgements

This report was developed as a part of the course *EE451: Supervised Research Exposition* to compile together my learnings and experiences. I thank my parents for always motivating me. I would also like to express gratitude to my guide: Prof. Debasattam for introducing me to this fascinating topic. Most of the content here is inspired by [9], many statements are directly taken from here and my explanations are based on my understanding from the book. And, lastly thanks to you, reader, I have worked hard in making this report, in the hope that this work helps you in some way.

Contents

Part I

Algebra and Geometry: Introduction

1 Polynomials: Introduction

Let us start by defining notions of arithmetic. Loosely speaking, these notions are used to define some kind of operations over numbers. The benefit of such analysis is that results which do not assume properties other than above can be generalized to any other arithmetic of the same kind (i.e. a *field* or a *commutative ring*).

Definition 1.1 (Field). A set, with binary operations $(+, \cdot)$ (defined over all its elements) which satisfies the below properties is called a Field, usually denoted by $\mathbb{F}$.

- $x + y \in \mathbb{F}, \forall x, y \in \mathbb{F}$ (closure under addition)
- $x + y = y + x, \forall x, y \in \mathbb{F}$ (commutativity under addition)
- $x + (y + z) = (x + y) + z, \forall x, y, z \in \mathbb{F}$ (associativity under addition)
- $\exists! 0 \in \mathbb{F} : x + 0 = x, \forall x \in \mathbb{F}$ (existence of unique additive identity)
- $\forall x \in \mathbb{F}, \exists! y \in \mathbb{F} : x + y = 0$ (existence of unique additive inverse)
- $x \cdot y \in \mathbb{F}, \forall x, y \in \mathbb{F}$ (closure under multiplication)
- $x \cdot y = y \cdot x, \forall x, y \in \mathbb{F}$ (commutativity under multiplication)
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z, \forall x, y, z \in \mathbb{F}$ (associativity under multiplication)
- $\exists! 1 \in \mathbb{F} : x \cdot 1 = x, \forall x \in \mathbb{F}$ (existence of unique multiplicative identity)
- $\forall x \in \mathbb{F} \setminus \{0\}, \exists! y \in \mathbb{F} : x \cdot y = 1$ (existence of unique multiplicative inverse)
- $x \cdot (y + z) = x \cdot y + x \cdot z, \forall x, y, z \in \mathbb{F}$ (distributivity of multiplication over addition)

Note. *We also assume that the additive identity is different from multiplicative identity (i.e.* $0 \neq 1$*) so as to exclude fields with one element.*

Definition 1.2 (Commutative Ring). A set, with binary operations $(+, \cdot)$ (as above) which satisfies all the properties of fields except *existence of multiplicative inverse* is called a commutative ring.

Note, the operations are as necessary as the set while mentioning the field (or a commutative ring), but we may skip operations if they are understood without ambiguity. In such cases (like below), we may abuse the notation and refer to the set of the field as field itself.

The set of a field can have finite or infinite elements. = An example of a set which is not a field is $\mathbb{Z}$, as a multiplicative inverse does not exist for all its elements. But, it is a commutative ring. Another example of commutative ring, that the reader might be familiar with is "polynomials", which will be the focus of this report.

Definition 1.3 (Monomial). A monomial, denoted by x^α is defined as follows

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n} \qquad (\alpha_i \in \mathbb{Z}^+ \text{ and } \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)) \tag{1.1}$$

Note, when $\alpha = (0, 0, \ldots, 0)$ we take $x^\alpha = 1$.

The collection of all such α over $(x_1, x_2, \ldots, x_n)$ is denoted by $\mathbb{Z}^n_{\geq 0}$.

Definition 1.4 (Total degree of a monomial). The total degree, denoted by $|\alpha|$ is defined as

$$|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n \tag{1.2}$$

Definition 1.5 (Polynomial). A polynomial f in $(x_1, x_2, \ldots, x_n)$ is a *finite sum* denoted by

$$f(x_1, x_2, \ldots, x_n) = f(x) = f = \sum_{\alpha} a_\alpha x^\alpha \qquad (\text{where } a_\alpha \in \mathbb{F} \text{ and } \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)) \tag{1.3}$$

Here, a_α is the *coefficient* of x^α and $a_\alpha x^\alpha$ is called a *term* of f provided $a_\alpha \neq 0$.

An example of a polynomial is given below with its representation using monomials and its coefficients

$$\begin{aligned} f &= 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{Q}[x, y, z] \\ f &= \text{sum}\{(4, (1, 2, 1)), (4, (0, 0, 2)), (-5, (3, 0, 0)), (7, (2, 0, 2))\} \end{aligned} \tag{1.4}$$

Definition 1.6 (Total degree of a polynomial). The total degree of a polynomial, denoted by $\deg(f)$ is the maximum total degree of a monomial of f which has non-zero coefficient, i.e.

$$\deg(f) = \max_{\alpha \neq 0} |\alpha| \tag{1.5}$$

The collection of all polynomials in $(x_1, x_2, \ldots, x_n)$ with coefficients in $\mathbb{F}$ forms a commutative ring (more specifically a *polynomial ring*) which is denoted by $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

Note, if $n = 1$ then we get $\mathbb{F}[x]$ which are polynomials in one variable (x) (*univariate polynomials*). In this report, we will see how our understanding of $\mathbb{F}[x]$ can be used to get generalised notions of polynomials over multiple variables (*multivariate polynomials*).

Definition 1.7 (Algebraically Closed Field). If for every polynomial $f \in \mathbb{F}[x]$ of positive degree there exists a $x \in \mathbb{F}$ such that $f(x) = 0$ (x is a root) then $\mathbb{F}$ is an algebraically closed field.

The Fundamental Theorem of Algebra states that $\mathbb{C}$ is an algebraically closed field.

1.1 Monomial Order

From 1.4, one might ask about relative ordering between the elements. An ordering might be crucial in representing polynomials and their arithmetic.

Definition 1.8 (Monomial Ordering). A monomial ordering is a relation $>$ on monomials $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$ which satisfies the below properties.

- $>$ is a total order, i.e., for $\beta \in \mathbb{Z}^n_{\geq 0}$ exactly one of the following happens

$$x^\alpha > x^\beta \text{ or } x^\alpha < x^\beta (\equiv x^\beta > x^\alpha) \text{ or } x^\alpha = x^\beta (\equiv x^\alpha \not> x^\beta, x^\beta \not> x^\alpha) \tag{1.6}$$

- $\alpha > \beta, \gamma \in \mathbb{Z}^n_{\geq 0} \Rightarrow \alpha + \gamma > \beta + \gamma$
- $>$ is a well-ordering, i.e.,

$$\text{for non-empty } A \subseteq \mathbb{Z}^n_{\geq 0} \Rightarrow \exists! \alpha \text{ such that } \beta \geq \alpha \text{ for } \beta \in \mathbb{Z}^n_{\geq 0} \tag{1.7}$$

  or equivalently, every strictly decreasing sequence $\{\alpha(i)\}$ eventually terminates.

Definition 1.9 (Lexicographic Order). For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{\text{lex}} \beta$ if leftmost non-zero entry of $\alpha - \beta$ is positive.
f of 1.4 with respect to lex order is as follows,

$$\begin{aligned} f &= -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2 \in \mathbb{Q}[x, y, z] \\ f &= \text{sum}\{(-5, (3, 0, 0)), (7, (2, 0, 2), (4, (1, 2, 1)), (4, (0, 0, 2)))\} \end{aligned} \tag{1.8}$$

Definition 1.10 (Graded Lex Order). For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{\text{grlex}} \beta$ if $|\alpha| > |\beta|$ or ($|\alpha| = |\beta|$ and $\alpha >_{\text{lex}} \beta$)
f of 1.4 with respect to grlex order is as follows,

$$\begin{aligned} f &= 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2 \in \mathbb{Q}[x, y, z] \\ f &= \text{sum}\{(7, (2, 0, 2), (4, (1, 2, 1)), (-5, (3, 0, 0)), (4, (0, 0, 2)))\} \end{aligned} \tag{1.9}$$

Definition 1.11 (Graded Reverse Lex Order). For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{\text{grevlex}} \beta$ if $|\alpha| > |\beta|$ or ($|\alpha| = |\beta|$ and rightmost non-zero entry of $\alpha - \beta$ is negative)
f of 1.4 with respect to grlex order is as follows,

$$\begin{aligned} f &= 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2 \in \mathbb{Q}[x, y, z] \\ f &= \text{sum}\{(4, (1, 2, 1)), (7, (2, 0, 2), (-5, (3, 0, 0)), (4, (0, 0, 2)))\} \end{aligned} \tag{1.10}$$

Note. *In Graded Lex Order, the intuition is higher total degree first and then leftmost non-zero entry $\alpha - \beta$ is positive. So, higher preference to* ***higher powers*** *of a x_i.*
In Graded Reverse Lex Order, the intuition is higher total degree first and then rightmost non-zero entry $\alpha - \beta$ is negative. So, lower preference to lower powers of a x_i, which equivalently means higher preference to ***higher sum of powers*** *of $x_j, j < i$*

Proposition 1.12. The lex, grlex and grevlex ordering on $\mathbb{Z}^n_{\geq 0}$ are monomial orderings.

Proof. We verify the properties of a monomial ordering for lex ordering.

- Total order is trivial.
- $\alpha >_{\text{lex}} \beta \Rightarrow$ leftmost non-zero entry in $\alpha - \beta$ is positive. $\alpha - \beta = (\alpha + \gamma) - (\beta + \gamma) \Rightarrow$ leftmost non-zero entry in $(\alpha + \gamma) - (\beta + \gamma)$ is positive. This implies $\alpha + \gamma >_{\text{lex}} \beta + \gamma$.
- To show that $>_{\text{lex}}$ is a well-ordering, the idea is that the sequence $\alpha(i)$ is strictly decreasing. Say $\alpha_i = (\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n})$. The leftmost element α_{i_1} will keep decreasing with i but it can't decreasing forever since it is non-negative, so eventually it stabilizes. As α_{i_1} are equal now, to continue the sequence, an element to the right of α_{i_1} will be compared and same reasoning applies here. In this way, eventually the sequence will terminate.

The grlex and grevlex orderings can be shown to be monomial order using similar arguments. ■

Definition 1.13 (Monomial Ordering-Specific Terminology). For a non-zero $f = \sum_\alpha a_\alpha x^\alpha$, and a monomial order $>$

multidegree of f

$$\text{multideg}(f) = \max_{\text{w.r.t. } >} (\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0) \tag{1.11}$$

leading coefficient of f

$$\text{LC}(f) = a_{\text{multideg}(f)} \in \mathbb{F} \tag{1.12}$$

leading monomial of f

$$\mathrm{LM}(f) = x^{\mathrm{multideg}(f)} \tag{1.13}$$

leading term of f

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f) \tag{1.14}$$

For f of 1.4 with respect to grlex order,

$$\mathrm{multideg}(f) = (2,0,2), \quad \mathrm{LC}(f) = 7, \quad \mathrm{LM}(f) = x^2z^2, \quad \mathrm{LT}(f) = 7x^2z^2 \tag{1.15}$$

2 Affine Varieties

Definition 2.1 (Affine Space). An $n-$dimensional affine space over $\mathbb{F}$ is a set denoted by $\mathbb{F}^n$ and defined as follows

$$\mathbb{F}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{F}\} \tag{2.1}$$

Now, a polynomial f can be defined as a function $f : \mathbb{F}^n \to \mathbb{F}$, where each x_i gets replaced by a_i. Since a function usually has a geometric interpretation, this is the beginning of the link between *algebra and geometry*.

Definition 2.2 (Affine Varieties). An affine variety V (over polynomials $f_1, f_2, \ldots, f_s$) is defined as follows

$$V = \mathbf{V}(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in \mathbb{F}^n \mid f_i(a_1, a_2, \ldots, a_n) = f_i(a) = 0 \ \forall i\} \tag{2.2}$$

Intuitively, this is a set of solutions of polynomial equations $f_1(x) = f_2(x) = \cdots = f_s(x) = 0$. A geometric interpretation is that the solution set is an *intersection of curves* represented by these functions. It turns out many important problems turns into finding such solution set (see **??**). Hence, it will be great to be able to solve such a system *algebraically* where a computer is proficient.

We know for univariate polynomials its coefficients are zero iff it evaluates to zero at all points. This is due to a fact that a polynomial $\in \mathbb{F}[x]$ of degree n can have at most n roots which can be proved via induction arguments.
It turns out the same does not hold for multivariate polynomials in general. Consider, a polynomial over GF(2), $f(x) = x^2 + x$. It has non-zero coefficients but $f(0) = f(1) = 0$.

Lemma 2.3 (Zero Polynomial on infinite fields). The following is true if $\mathbb{F}$ is an infinite field.

$$f(a_1, a_2, \ldots, a_n) = 0, \forall a \in \mathbb{F}^n \Leftrightarrow a_\alpha = 0, \forall a_\alpha \in \{\text{coefficients of } f\} \in \mathbb{F}^n \tag{2.3}$$

This implies, having all coefficients zero (zero polynomial) is equivalent to evaluating zero at all points (zero function).

Proof. Clearly, RHS $\Rightarrow$ LHS.
We can show LHS $\Rightarrow$ RHS using induction over total degree, they key idea in the inductive step is to rewrite the polynomial as a single variable and coefficients as multivariate polynomials. Then use the equivalence for univariate polynomials over infinite fields to get that the coefficients which are multivariate polynomials of lesser total degree. So they must be zero by inductive hypothesis. ■

Lemma 2.4. $V_1, V_2 \subseteq \mathbb{F}^n$ are affine varieties $\Rightarrow V_1 \cap V_2$ and $V_1 \cup V_2$ are also affine varieties. Moreover,

$$\begin{aligned} V_1 &= \mathbf{V}(f_1, f_2, \ldots, f_{s_1}) \\ V_2 &= \mathbf{V}(g_1, g_2, \ldots, g_{s_2}) \end{aligned} \quad \Rightarrow \quad \begin{aligned} V_1 \cap V_2 &= \mathbf{V}(f_1, f_2, \ldots, f_{s_1}, g_1, g_2, \ldots, g_{s_2}) \\ V_1 \cup V_2 &= \mathbf{V}(f_i \cdot g_j \mid \forall i, j) \end{aligned} \tag{2.4}$$

Proof. We show both one-by-one

- $a = (a_1, a_2, \ldots, a_n) \in V_1$ and $a \in V_2$ is equivalent to $a \in V_1 \cap V_2$, as varieties are set so their intersection is also a set. Also, both the statement means $f_i(a) = 0 = g_j(a), \forall i, j$. Hence, the result.
- $a = (a_1, a_2, \ldots, a_n) \in V_1$ or $a \in V_2$ is equivalent to $a \in V_1 \cup V_2$, as varieties are set so their union is also a set. $a \in V_1$ implies $f_i(a) = 0, \forall i$ which implies $f_i(a) \cdot g_j(a) = 0, \forall i$ implies $a \in V_1 \cup V_2$. Similarly, $a \in V_2 \Rightarrow a \in V_1 \cup V_2$. Hence $V_1 \cup V_2 \subseteq \mathbf{V}(f_i \cdot g_j \mid \forall i, j)$.

  Now, to prove $\mathbf{V}(f_i \cdot g_j \mid \forall i, j) \subseteq V_1 \cup V_2$, we need to show $a \in \mathbf{V}(f_i \cdot g_j \mid \forall i, j) \Rightarrow a \in V_1 \cup V_2$. We will prove its contrapositive, i.e., $a \notin V_1, a \notin V_2 \Rightarrow a \notin \mathbf{V}(f_i \cdot g_j \mid \forall i, j)$.
  $a \notin V_1, a \notin V_2$ implies $\exists f_i, g_j$ such that $f_i(a) \neq 0 \neq g_j(a)$ which implies $a \notin \mathbf{V}(f_i \cdot g_j \mid \forall i, j)$.

■

Let us take an example, to gain more familiarity with varieties. Consider, multivariate polynomials with total degree = 1 (*i.e., linear polynomials*). Say, $f_i(x) = \alpha_{i_0} + \sum_{j=1}^{n} \alpha_{i_j} \cdot x_j$ where, $\alpha_{i_j} \in \mathbb{F}$.
Now, this can be converted to a linear algebra problem of solving system of linear equations $Ax = b$ where, $(i, j)^{\text{th}}$ entry of A is given by $[A_{i,j}] = \alpha_{i_j}$ and $(i)^{\text{th}}$ entry of b is given by $[b_i] = -\alpha_{i_0}$ with appropriately selected indices i and j.

After this, we can convert the augmented matrix ($[A : b]$) into row-reduced echelon form (rref) by Gaussian elimination. Once we get rref, determining the existence of solutions, their cardinality and "dimension" is a simple task. The question we ask now is if given any affine variety can we determine something similar about it. More precisely, the questions of interests concerning an affine variety $V = \mathbf{V}(f_1, f_2, \ldots, f_s)$ are

Consistency Is there a way to determine if V is non-empty. Then, we will know if the system $f_i(x) = 0$ is *consistent*.

Finiteness Is there a way to determine if V is finite. Then, the next problem is about whether we can find all such solutions.

Dimension Is there a way to determine the "dimension" of V.

Surprisingly, if we choose the underlying field carefully we can get the answer to every question stated above provided we define the notions appropriately. In fact the process, is quite similar to converting a system to rref by *elimination* as we will see in 1 and 1.

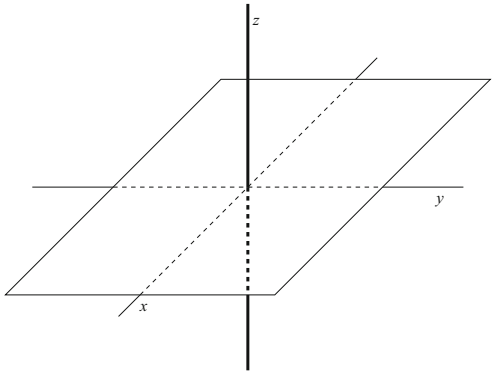

Figure 2.1: $\mathbf{V}(xz, yz)$ - a union of a line and a plane. From [9]

Note. *The "dimension" of a variety is not exactly as the dimension of vector space. See 2.1,* $\boldsymbol{V}(xz, yz) = \boldsymbol{V}(z) \cup \boldsymbol{V}(xy)$ *as* $xz = yz = 0$ *implies* $z = 0$ *(*$x - y$ *plane) or* $x = y = 0$ *(*$z-$*axis). The variety is a union of line and a plane, two different dimensional objects from linear algebra. Hence, the term needs to be defined appropriately first for an affine variety.*

3 Ideals

Definition 3.1 (Ideal). A subset $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ which satisfies the below properties is called an Ideal.

- $0 \in I$
- $f(x), g(x) \in I \Rightarrow f(x) + g(x) \in I, \forall x \in \mathbb{F}^n$
- $f(x) \in I \Rightarrow h(x)f(x) \in I, \forall h(x) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\forall x \in \mathbb{F}^n$

As I is subset, its operations are same as defined over $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

Lemma 3.2. For $f_1, f_2, \ldots, f_s \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $\langle f_1, f_2, \ldots, f_s \rangle$ is the *ideal generated* by $f_1, f_2, \ldots, f_s$. Also, $f_1, f_2, \ldots, f_s$ is a *generating set* of $\langle f_1, f_2, \ldots, f_s \rangle$.

$$I = \langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i \cdot f_i | h_i \in \mathbb{F}[x_1, x_2, \ldots, x_n] \right\} \tag{3.1}$$

It is trivial to show that $\langle f_1, f_2, \ldots, f_s \rangle$ is indeed an ideal, use the representation 3.1 and verify the three properties.

Notice, how the definition of an ideal seems similar to a vector space, and 3.1 looks similar to a linear combination. While multiplying, all polynomials are considered as "scalars" of the system.

Definition 3.3 (Finitely Generated Ideal). An ideal I is finitely generated if

$$\exists f_1, f_2, \ldots, f_s \in \mathbb{F}[x_1, x_2, \ldots, x_n] \text{ such that } I = \langle f_1, f_2, \ldots, f_s \rangle \tag{3.2}$$

Definition 3.4 (Principle Ideal). An ideal I generated by single element is a principle ideal.

Definition 3.5 (Principle Ideal Domain (PID)). If every ideal in a domain is a principle ideal then the domain is called principle ideal domain.

Definition 3.6 (Ideal of an affine variety). The set $\mathbf{I}(V)$ is the ideal of an affine variety.

$$\mathbf{I}(V) = \{ f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \mid f(a_1, a_2, \ldots, a_n) = 0, \forall a \in V \} \tag{3.3}$$

It is trivial to show that $\mathbf{I}(V)$ is indeed an ideal, as for any $a \in V$:

- $0 \in \mathbf{I}(V)$ as $0(a) = 0, \forall a \in V$
- $f, g \in \mathbf{I}(V) \Rightarrow f(a) = g(a) = 0 \Rightarrow f(a) + g(a) = 0 \Rightarrow f + g \in \mathbf{I}(V)$
- $f \in \mathbf{I}(V) \Rightarrow f(a) = 0 \Rightarrow h(a)f(a) = 0 \Rightarrow hf \in \mathbf{I}(V)$

Lemma 3.7. For $f_1, f_2, \ldots, f_s \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $\langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbf{I}(V(f_1, f_2, \ldots, f_s))$

Proof. Take $f \in \langle f_1, f_2, \ldots, f_s \rangle \Rightarrow \exists h_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that $f = \sum_{i=1}^{s} h_i \cdot f_i$
Now, consider $a \in \mathbf{V}(f_1, f_2, \ldots, f_s) \Rightarrow f_i(a) = 0 \Rightarrow f(a) = 0 \Rightarrow \mathbf{I}(V)$. ■

Note. *The above containment need can be strict.*
Consider $f = x^2$, $I = \langle f \rangle = h \cdot f$, $\forall h \in \mathbb{F}[x] \Rightarrow I$ *contains polynomials of total degree* ≥ 2.
But $V(f) = V(x^2) \Rightarrow V = \{0\} \Rightarrow g = x \in \boldsymbol{I}(V) \Rightarrow \boldsymbol{I}(V)$ *contains polynomials of total degree 1.*

Similar to affine varieties, we can ask some interesting questions about ideals

Ideal Description Does every ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ has a finite generating set.

Ideal Membership If $I = \langle f_1, f_2, \ldots, f_s \rangle$, is there a way to determine if $f \in I$.

Nullstellensatz Is there an exact relation between $\langle f_1, f_2, \ldots, f_s \rangle$ and $\mathbf{I}(V(f_1, f_2, \ldots, f_s))$

Again, surprisingly, we can answer all these questions. See 2.

4 Polynomials: Algorithms

Proposition 4.1 (Divison Algorithm (Univariate Polynomials)). For every $f \in \mathbb{F}[x]$ and non-zero $g \in \mathbb{F}[x]$, $\exists! q, r \in \mathbb{F}[x]$ such that $f = qg + r$, where either $r = 0$ or $\deg(r) < \deg(g)$.
Proof. Proof by construction, we "divide" f by g to get q, r.
One thing to note is that, for non-zero f, g

$$\text{LT}(f) \text{ divides } \text{LT}(g) \Leftrightarrow \deg(f) \leq \deg(g) \tag{4.1}$$

Algorithm 1 Polynomial Division (Single Variable)

Input: f, g where $f, g \in \mathbb{F}[x], g! = 0$
Output: q, r
  $q \leftarrow 0$
  $r \leftarrow f$
  while $r \neq 0$ and $\text{LT}(g) | \text{LT}(r)$ ($a|b$ is a divides b) **do**
    $q \leftarrow q + \dfrac{\text{LT}(r)}{\text{LT}(g)}$
    $r \leftarrow r - \dfrac{\text{LT}(r)}{\text{LT}(g)} g$
  end while
  return q, r

Note that, $f = qg + r$ always holds. It holds iniatilly and then,

$$f = qg + r \Leftrightarrow f = \left(q + \frac{\text{LT}(r)}{\text{LT}(g)}\right) g + \left(r - \frac{\text{LT}(r)}{\text{LT}(g)} g\right) \tag{4.2}$$

The algorithm terminates because, $\deg(r)$ drops at each iteration or r becomes 0.
Uniqueness follows from contradiction argument. ■

Note. *If* $r = 0$ *we say that* g ***divides*** f

Theorem 4.2 (Divison Algorithm (Multivariate Polynomials)). For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $F = (f_1, f_2, \ldots, f_s)$ where $f_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ on a monomial order,
$\exists q_i, r \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ where either $r = 0$ or $r = \sum_{\alpha} a_\alpha \cdot x^\alpha, \text{LT } f_i \nmid x^\alpha, \forall i, \alpha$.
Moreover, $q_i \cdot f_i \neq 0 \Rightarrow \text{multideg}(f) \geq \text{multideg}(q_i \cdot f_i)$

Proof. Proof by construction, we divide f by f_i to get q_i, until we can't divide further (Division Step), then the leading terms move to remainder until one of them divides f_{i+1} (Remainder Step). Now, divide by f_{i+1} and repeat the steps till the end.

Algorithm 2 Polynomial Division (Multiple Variable)

Input: $F = (f_1, f_2, \ldots, f_s)$ and f where $f, f_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$
Output: $q_1, q_2, \ldots, q_s, r$

```
q_i ← 0, ∀i
r ← 0
p ← f
while p ≠ 0 do
    i ← 1
    division ← false
    while i ≤ s and division = false do
        if LT(f_i) | LT(p) then
            q_i ← q_i + LT(p)/LT(f_i)
            p ← p − (LT(p)/LT(f_i)) f_i
            division ← true
        else
            i ← i + 1
        end if
    end while
    if division = false then
        r ← r − LT(p)
        p ← p − LT(p)
    end if
end while
return q_1, q_2, ..., q_s, r
```

Proof is similar to 4 but lengthier. Here, $f = \sum_i q_i \cdot f_i + p + r$ always holds. It holds initially and then during division step,

$$q_i \cdot f_i + p \Leftrightarrow \left(q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i + \left(p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right) \tag{4.3}$$

and during the remainder step,

$$p + r \Leftrightarrow (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p)) \tag{4.4}$$

■

Note. *In 2, the remainder and quotients are not uniquely determined, they may change with permutation of F. Applying the division algorithm on $f = xy^2 - x$ over $F = (f_1, f_2) = (y^2 - 1, xy^2 - x)$ gives $(q_1, q_2, r) = (x, 0, 0) \Rightarrow f \in \langle f_1, f_2 \rangle$ whereas, over $F = (f_2, f_1)$ gives $(q_1, q_2, r) = (y, 0, -x + y)$.*

Part II

Gröbner Bases: Introduction

1 Motivation: The Ideal Membership Problem

Recall the Ideal Membership Problem. If $I = \langle f_1, f_2, \ldots, f_s \rangle$, is there a way to determine if $f \in I$? We first look at the univariate case,

Proposition 1.1. For every ideal $I \subseteq \mathbb{F}[x]$, $\exists! f \in \mathbb{F}[x]$ such that $I = \langle f \rangle$. Also, this f either is zero polynomial (iff $I = \{0\}$) or it is *monic* (*i.e.*, $\mathrm{LC}(f) = 1$).
This means that every ideal in $\mathbb{F}[x]$ is a principle ideal and $\mathbb{F}[x]$ is a principle ideal domain.

Proof. We consider the cases,

- $I = \{0\} \Rightarrow I = \langle 0 \rangle \Rightarrow f = 0$ and $\langle f \rangle = \langle 0 \rangle = \{0\}$.
- $I \supset \{0\}$, we claim the monic polynomial of minimum degree in the ideal is such an f.
  - $f \in I \Rightarrow \langle f \rangle \subseteq I$, since I is an ideal.
  - For any $g \in I$, we can divide it by f using 4 to get $g = qf + r$. As $g, f \in I \Rightarrow r \in I$. Now, r is either 0 or $\deg(r) < \deg(f)$. Since the latter is not possible, $r = 0$ which implies $g \in \langle f \rangle$. Hence $I \subseteq \langle f \rangle$.

For uniqueness, $\langle f \rangle = \langle \tilde{f} \rangle \Rightarrow f = c\tilde{f}$, where $c \in \mathbb{F} \setminus \{0\} \Rightarrow c = 1$ (as both $f, \tilde{f}$ are monic). ■

This essentially solves the Ideal Membership Problem for ideals $\in \mathbb{F}[x]$.
A way to compute that f is by calculating the *GCD* of its generating set.

Definition 1.2 (Greatest Common Divisor (GCD)). $g \in \mathbb{F}[x]$ is a greatest common divisor of $f_1, f_2, \ldots, f_s \in \mathbb{F}[x]$ if it satisfies the below properties,

- g divides $f_1, f_2, \ldots, f_s$.
- p divides $f_1, f_2, \ldots, f_s \Rightarrow p$ divides g

g if exists is unique up to a multiplication by $c \in \mathbb{F} \setminus \{0\}$. As any gcd $g, \tilde{g}$ divides each other. We denote this gcd by $\gcd(f_1, f_2, \ldots, f_s)$.

Proposition 1.3.

$$I = \langle \gcd(f_1, f_2, \ldots, f_s) \rangle = \langle f_1, f_2, \ldots, f_s \rangle \tag{1.1}$$

Proof. By 1.1, $\exists f \in \langle f_1, f_2, \ldots, f_s \rangle$ such that $\langle f \rangle = \langle f_1, f_2, \ldots, f_s \rangle$. Now, $f = \gcd(f_1, f_2, \ldots, f_s)$.

- Any f divides f_i as $f_i \in \langle f \rangle \Rightarrow f_i = h_i \cdot f$.
- Any p divides $f_i \Rightarrow f_i = A_i \cdot p \Rightarrow f = \sum_i B_i \cdot f_i = \left(\sum_i A_i \cdot B_i \cdot \right) p \Rightarrow f$ divides p.

■

This GCD can be computed by applying Euclid's Algorithm successively to pairs of $f_1, f_2, \ldots, f_s$.

Proposition 1.4 (Euclid's Algorithm). Euclid's Algorithm is used to compute $\gcd(f_1, f_2)$ where $f_1, f_2 \in \mathbb{F}[x], f_2 \neq 0$.

Algorithm 3 Euclid's Algorithm

Input: f_1, f_2 where $f_1, f_2 \in \mathbb{F}[x], f_2 \neq 0$
Output: $g = \gcd(f, g)$
  $g \leftarrow f_1$
  $h \leftarrow f_2$
  while $h \neq 0$ **do**
    $g, h \leftarrow h, r$ where r is the remainder of g when divided by h $(g = qh + r)$
  end while
  return g

The algorithm terminates because, $\deg(r)$ drops at each iteration or r becomes 0.

Theorem 1.5 (Ideal Membership Problem (Univariate Polynomial Ideals)). For an ideal $I = \langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbb{F}[x]$, and $f, f_i \in \mathbb{F}[x]$,

$$f \in I \Leftrightarrow \gcd(f_1, f_2, \ldots, f_s) \text{ divides } f. \tag{1.2}$$

Proof. Trivial from 1.3. ■

Now, we move to ideals in domain of multivariate polynomials.

As seen at the end of 2, for a arbitrary generating set. The remainder when f is divided by $F = (f_1, f_2, \ldots, f_s)$ need not be zero for all orderings of F. In worst case, we may need to check all permutations of F until we get zero remainder. This can be shown to be *worse than exponential complexity*. Hence, for a generating set, it is desirable that the remainder is 0 when divided by all possible orderings of F iff F divides f. In fact, such a generating set does exist for each ideal in $\mathbb{F}[x_1, x_2, \ldots, x_n]$. This set is the **Gröbner Basis** of the ideal.

Before we jump onto it, let us understand Monomial Ideals.

1.1 Monomial Ideals

Definition 1.6 (Monomial Ideals). An ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$ such that

$$I = \langle x^\alpha | \alpha \in A \rangle \tag{1.3}$$

Intuitively, the ideal is generated by a set of monomials (possibly infinite).

Lemma 1.7. Given a monomial ideal I and a $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $f \in I$ iff every term of f lies in I.

Proof. The if direction is trivial since any f is a linear combination of monomials.
For the only if direction, consider the contrapositive, i.e., $\exists a_{\tilde{\alpha}} \cdot x^{\tilde{\alpha}} \notin I \Rightarrow f \notin I$.
$a_{\tilde{\alpha}} \cdot x^{\tilde{\alpha}} \notin I \Rightarrow \forall \alpha \in A, x^\alpha$ doesn't divide $x^{\tilde{\alpha}}$. Hence, when we divide f by the monomials of I, the remainder will always contain $x^{\tilde{\alpha}}$ or its multiple $\Rightarrow f \notin I$. ■

Theorem 1.8 (Dickson's Lemma). Every monomial ideal $I = \langle x^\alpha | \alpha \in A \rangle$ has a finite basis[1], i.e., $\exists \alpha(1), \alpha(2), \ldots, \alpha(s) \in A$ such that $I = \langle x^{\alpha(1)}, x^{\alpha(2)}, \ldots, x^{\alpha(s)} \rangle$.

[1] we also call a generating set a basis. This is unlike the definitions from vector spaces.

Proof. The idea is to use induction on the number of variables. Base case ($n = 1$) follows from 1.1. In inductive case, consider monomials in $\mathbb{F}[x_1, x_2, \ldots, x_{n-1}, y]$. They can be written as $x^\alpha y^m, \alpha \in \mathbb{Z}_{\geq 0}^{n-1}$. Now, take J as the ideal in $\mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$ generated by x^α where $x^\alpha y^m \in I$. Use the inductive hypothesis to represent this J with a finite generating set such that $J = \langle x^{\alpha(1)}, x^{\alpha(2)}, \ldots, x^{\alpha(s)} \rangle$. Now create, m ideals $J_l \in \mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$ where $0 \leq l \leq m-1$ such that it is generated by monomials $x^\beta y^l \in I$. Again, by inductive hypothesis, J_l has finite generating set. Now, $J \cup \bigcup_{l=0}^{m-1} J_l$ is a finite generating set of given monomial ideal. ■

Definition 1.9 (Minimal Basis). A monomial ideal $I = \langle x^{\alpha(1)}, x^{\alpha(2)}, \ldots, x^{\alpha(s)} \rangle$ has a minimal basis if $\forall i, j$ $(i \neq j)$, $x^{\alpha(i)}$ doesn't divide $x^{\alpha(j)}$. Also, this basis is unique.

Proof. Repeatedly remove the monomials which have divisors until it not possible. Uniqueness follows from contradiction arguments as monomials from two minimal basis will divide each other. ■

Theorem 1.10 (Ideal Membership Problem (Monomial Ideals)). For a monomial ideal $I = \langle x^{\alpha(1)}, x^{\alpha(2)}, \ldots, x^{\alpha(s)} \rangle$ and a $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that $f = \sum_\alpha a_\alpha \cdot x^\alpha$,

$$f \in I \Leftrightarrow \forall \alpha \exists i \text{ such that } x^{\alpha(i)} \text{ divides } x^\alpha. \tag{1.4}$$

Proof. Application of 1.7 and 1.8. ■

2 Gröbner Bases

Definition 2.1. For a non-zero ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n] \backslash$ and a monomial ordering on $\mathbb{F}[x_1, x_2, \ldots, x_n]$, we denote the set of leading terms of non-zero elements of I as

$$\mathrm{LT}(I) = \{a_\alpha x^\alpha | \exists f \in I \setminus \{0\} \text{ such that } \mathrm{LT}(f) = a_\alpha x^\alpha\} \tag{2.1}$$

The motivation for this definition is then, $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal. So by 1.8, it has a finite basis.

Theorem 2.2 (Hilbert Basis Theorem). Every ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ has a finite basis.

Note, the Hilbert Basis Theorem solves the **Ideal Description** problem.

Proof. For $I = \{0\}$, we have $I = \langle 0 \rangle$. For other I, by 1.8 $\exists g_1, g_2, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle$. Now, we can show that $I = \langle g_1, g_2, \ldots, g_t \rangle$, by dividing $f \in$ with $G = (g_1, g_2, \ldots, g_t)$ and proving that the remainder is zero. ■

Theorem 2.3 (Ascending Chain Condition). $I_i \in \mathbb{F}[x_1, x_2, \ldots, x_n], \forall i \in \mathbb{Z}^+$ such that $I_i \subseteq I_{i+1} \Rightarrow \exists N \in \mathbb{Z}^+$ such that $I_N = I_{N+1}$. Intuitively, it states that the sequence of ideals where previous ideals are contained within current ideal stabilizes.

Proof. Consider $I = \bigcup_{i=1}^{\infty} I_i$, clearly, I is an ideal. Now, by 2.2, it has a finite generating set where each of its generator f_i is contained in some I_{j_i}. This implies due to ascending chain, all generators are contained in I_N where $N = \max_i j_i \Rightarrow$ generators of I_k where $k \geq N$ are same. So, $I_N = I_{N+1}$ ■

Definition 2.4 (Affine Variety of an Ideal). For an ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that $I = \langle f_1, f_2, \ldots, f_s \rangle$, the affine variety of an Ideal is defined as below,

$$\mathbf{V}(I) = \mathbf{V}(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, a_2, \ldots, a_n) = f(a) = 0 \ \forall f \in I\} \tag{2.2}$$

Definition 2.5 (Gröbner Basis). For a fixed monomial ordering on $\mathbb{F}[x_1, x_2, \ldots, x_n]$ and $G = \{g_1, g_2, \ldots, g_t\}$, G is called a Gröbner basis of a non-zero ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ if

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle \tag{2.3}$$

The Gröbner basis of $I = \{0\}$ is defined as $\varnothing$.

Proposition 2.6 (Property of Gröbner Bases). For a Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ for an ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ and a given $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $\exists! r \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that no term of r is divisible by $\mathrm{LT}(g_i)$ for any i.

The uniqueness of remainder is the reason the ordered tuple we divide with is a set.

Note. *Only remainder is guarenteed to be unique, the quotients need not be unique.*

Theorem 2.7 (Ideal Membership Problem (Multivariate Polynomial Ideals)). For a Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ for an ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$,

$$f \in I \Leftrightarrow \text{ remainder on division of } f \text{ by } G \text{ is zero.} \tag{2.4}$$

2.1 Computation of Gröbner Basis

Definition 2.8. Here are some additional notations that will be helpful.

- $\overline{f}^F$ is the remainder on division of f by $F = (f_1, f_2, \ldots, f_s)$.
- $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$, i.e., it is the least common multiple of $\mathrm{LM}(f), \mathrm{LM}(g)$ with $\gamma_i = \max(\alpha_i, \beta_i)$ where $\mathrm{multideg}(f) = \alpha, \mathrm{multideg}(g) = \beta$.
- $S(f, g) = \left(\dfrac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \dfrac{x^\gamma}{\mathrm{LT}(g)} \cdot g \right)$ is the S-polynomial of f, g.

Theorem 2.9 (Buchberger's Criterion). A basis $G = \{g_1, g_2, \ldots, g_t\}$ is a Gröbner basis of $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ iff $\overline{S(g_i, g_j)}^G = 0, \forall i, j \ (i \neq j)$

Theorem 2.10 (Buchberger's Algorithm). For a non-zero ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$, Gröbner basis for I is constructed as follows:
Given a basis, we can extend the basis to a Gröbner basis by repeatedly adding the non-zero remainders of S-polynomials between pairs of basis to the basis until 2.9 is satisfied.

Algorithm 4 Buchberger's Algorithm

Input: $F = (f_1, f_2, \ldots, f_s)$ where f_i's are non-zero
Output: $G = (g_1, g_2, \ldots, g_t)$ where G is a Gröbner Basis for I

```
G ← F
repeat
    G' ← G
    for all pairs {p, q} where p, q ∈ G', p ≠ q do
        r ← S(p, q)^{G'}
        if r ≠ 0 then
            G ← G ∪ {r}
        end if
    end for
until G = G'
return G
```

Proof. In the beginning, $G \in I$, let each iterate of G be called $G^{(i)}$. Now, if $G^{(i)} \in I$then whenever a remainder $r = \overline{S(g_i, g_j)}^{G^i}$ is added to $G^{(i)}$ then $G^{(i+1)} \in I$ as $r \in I$. As $F \subseteq Gand \langle F \rangle = I \Rightarrow \langle G \rangle = I$. So, the algorithm if terminates gives a Gröbner basis.
Now, due to addition of r, $\langle \mathrm{LT}(G^{(i)}) \rangle \subseteq \langle \mathrm{LT}(G^{(i+1)}) \rangle$, so this sequence forms an ascending chain and thus, by 2.3 it converges. Hence, the algorithm terminates. ■

Definition 2.11 (Reduced Gröbner Basis). A reduced Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ of an ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ is such that $\forall i, \mathrm{LC}(g_i) = 1$ and no monomial of g_i belongs to $\langle \mathrm{LT}(G \setminus \{g_i\}) \rangle$. Also, a reduced Gröbner basis is unique for an ideal subject to monomial ordering.

Such, a Gröbner basis can be constructed by repeatedly removing g_i where $\mathrm{LT}(g_i) \in \langle \mathrm{LT}(G \setminus \{g_i\}) \rangle$. These new sets are also a Gröbner basis.

Note, the process of computing Gröbner basis is very expensive but once computed, we can solve plethora of applications as we will see in next parts.

Part III

Algebra and Geometry: Interconnection

1 Nullstellensatz

The following results are taken from [9].

Theorem 1.1 (The Weak Nullstellensatz). For an algebraically closed field $\mathbb{F}$ and if $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ is an ideal satisfying $\mathbf{V}(I) = \varnothing$ then $I = \mathbb{F}[x_1, x_2, \ldots, x_n]$ Intuitively, this means that every system of polynomials than generates an ideal strictly smaller than $\mathbb{F}[x_1, x_2, \ldots, x_n]$ has a zero in $\mathbb{C}^n$.

This theorem allows us to solve the **consistency** problem,

Corollary 1.2 (Consistency Problem). $V = \mathbf{V}(f_1, f_2, \ldots, f_s) = \varnothing \Leftrightarrow$ the reduced Gröbner basis of $I = \langle f_1, f_2, \ldots, f_s \rangle$ is $\{1\}$

Theorem 1.3 (Hilbert's Nullstellensatz). For an algebraically closed field $\mathbb{F}$ and if $f, f_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ then

$$f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s)) \Leftrightarrow \exists m \geq 1 \text{ such that } f^m \in \langle f_1, f_2, \ldots, f_s \rangle \tag{1.1}$$

Definition 1.4 (Radical Ideal). For a radical ideal I, $f^m \in I$ for some $m \geq 1 \Rightarrow f \in I$.

Definition 1.5 (Radical of Ideal). The radical of an ideal $I \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is denoted by $\sqrt{I}$ which is defined as

$$I \subseteq \sqrt{I} = \{f | f^m \in I \text{ for some } m \geq 1\} \tag{1.2}$$

Also, $\sqrt{I}$ is a radical ideal.

Theorem 1.6 (The Strong Nullstellensatz). For an algebraically closed field $\mathbb{F}$ and if $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ is an ideal then

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I} \tag{1.3}$$

Theorem 1.7 (The Ideal–Variety Correspondence). For an arbitrary field, $\mathbf{I}, \mathbf{V}$ are inclusion reversing, i.e.,

$$\begin{aligned} I_1 \subseteq I_2 &\Rightarrow \mathbf{V}(I_1) \supseteq \mathbf{V}(I_2) \\ V_1 \subseteq V_2 &\Rightarrow \mathbf{I}(V_1) \supseteq \mathbf{I}(V_2) \end{aligned} \tag{1.4}$$

Part IV

Gröbner Bases: Applications

1 Elimination Theory

Recall that the Gröbner basis generalizes the idea of gcd as seen from the Ideal Membership problem for polynomial ideals in one variable. Now, we will see that it Gröbner basis also generalizes the notion of rref and the process of "elimination" of variables is crucial one. This was hinted back then during our solving of polynomial equations with total degree one which were systems of linear equations from linear algebra.

Now, the key to eliminating variables from systems of polynomial equations lies in two step

Elimination Step With which we can eliminate certain variables from the equation to get "simpler" equations to work with and find solutions.

Extension Step Once we have solutions for "simpler" equations we can extend these to get solutions of original equations.

Definition 1.1 (Elimination Ideal). For an ideal $I = \langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$, the $l-^{\text{th}}$ elimination ideal I_l is the ideal in $\mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n]$ defined by

$$I_l = I \cap \mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n] \tag{1.1}$$

Intuitively, I_l consists of functions in I which eliminate the variables $x_1, x_2, \ldots, x_l$. Hence, the *elimination step* is to determine elements of I_l.

Theorem 1.2 (The Elimination Theorem). For an ideal $I = \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ and its Gröbner basis G with respect to lex order $(x_1 > x_2 > \cdots > x_n)$,

$$G_l = G \cap \mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n] \tag{1.2}$$

where G_l is the Gröbner basis of the $l-^{\text{th}}$ elimination ideal.

Proof. $G_l \subseteq I_l$ by definition. Now, for $f \in I_l \Rightarrow f \in I \Rightarrow \exists g \in G$ such that $\text{LT}(g)$ divides $\text{LT}(f) \Rightarrow \text{LT}(g) \in \mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n] \Rightarrow g \in \mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n]$ due to lex order $(x_1 > x_2 > \cdots > x_n) \Rightarrow g \in G_l \Rightarrow I_l \subseteq \langle G_l \rangle$. ■

Theorem 1.3 (The Extension Theorem). For an ideal $I = \langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$ if its first elimanation ideal is I_1. Then,

$$f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ terms in } x_1 \text{ with degree} < N_i \ (N_i \geq 0, c_i \in \mathbb{C}[x_2, \ldots, x_n] \setminus \{0\}) \tag{1.3}$$

If there exists a partial solution $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$
then $(a_2, \ldots, a_n) \notin \mathbf{V}(c_1, c_2, \ldots, c_s) \Rightarrow \exists a_1 \in \mathbb{C}$ such that $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Notice, how the working field is now $\mathbb{C}$, an algebraically closed field.

2 Implicitization Problem

The problem is to find implicit polynomial equations that represent a variety $V \in \mathbb{F}^n$ using parametrised variables.

$$x_i = f_i(t_1, t_2, \ldots, t_m) \text{ (for all } i) \tag{2.1}$$

Theorem 2.1 (Polynomial Implicitization). For an infinite field $\mathbb{F}$, $F : \mathbb{F}^m : \mathbb{F}^n$ denotes the parametrization and an ideal

$$I = \langle x_1 - f_1, x_2 - f_2, \ldots, x_n - f_n \rangle \subseteq \mathbb{F}[t_1, t_2, \ldots, t_m, x_1, x_2, \ldots, x_n] \tag{2.2}$$

and I_m be its m^{th}elimination ideal. Then $\mathbf{V}(I_m)$ is the smallest variety in $\mathbb{F}^n$ containing $F(\mathbb{F}^m)$.

Hence, we can compute Gröbner basis with respect to lex order such that every t_i is higher than x_i.

Theorem 2.2 (Rational Implicitization). For an infinite field $\mathbb{F}$, $F : \mathbb{F}^m \setminus W : \mathbb{F}^n$ denotes the parametrization and an ideal

$$x_i = \frac{f_i(t_1, t_2, \ldots, t_m)}{g_i(t_1, t_2, \ldots, t_m)} \text{ (for all } i) \quad \text{and} \quad g = g_1 g_2 \cdots g_n, W = \mathbf{V}(g) \tag{2.3}$$

$$I = \langle g_1 x_1 - f_1, g_2 x_2 - f_2, \ldots, g_n x_n - f_n, 1 - gy \rangle \subseteq \mathbb{F}[y, t_1, t_2, \ldots, t_m, x_1, x_2, \ldots, x_n] \tag{2.4}$$

I_{m+1} be its $(m+1)^{\text{th}}$elimination ideal. Then $\mathbf{V}(I_{1+m})$ is the smallest variety in $\mathbb{F}^n$ containing $F(\mathbb{F}^m \setminus W)$.

Hence, we can compute Gröbner basis with respect to lex order such that y and every t_i is higher than x_i.

Now, let us look at concrete applications which uses Elimination Theory to solve for polynomial equations. The entire code for these are available here. I will also add programs for even more applications.

3 System of Linear Equations

The problem of our interest is

$$Ax = b \quad (A \in \mathbb{F}^{n \times n}, \text{ and } b, x \in \mathbb{F}^{n \times 1}) \tag{3.1}$$

To convert the problem into polynomial equations, we rewrite it as

$$f_i(x_1, x_2, \ldots, x_n) = -b_i + a_{i,1}x^1 + a_{i,2}x^2 + \cdots + a_{i,n}x^n = -b_i + \sum_{j=1}^{n} a_{i,j}x^j = 0 (1 \leq i, j \leq n) \tag{3.2}$$

where $a_{i,j}$ is the entry in the i^{th}row and j^{th}column of A and b_i is the entry in the i^{th}row of B.

Then, we construct an ideal $I = \langle f_1, f_2, \ldots, f_n \rangle$ and find its Gröbner basis G.

If the system has no solution then $G = \{1\}$, else the polynomials of G give exactly the row reduced echelon form of the augmented matrix $[A : b]$. To solve such a system, we use Back-Substitution. This is akin to applying extension theorem to the ideals I_l.

The SageMath program to symbolically compute **all solutions** is attached at the end and can also be found here

4 System of Polynomial Equations

The problem is to solve, $f_i(x) = 0$ where $f_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ Similar to the first problem, we construct an ideal $I = \langle f_1, f_2, \ldots, f_n \rangle$ and find its Gröbner basis G.

If the system has no solution then $G = \{1\}$, else the polynomials of G are in eliminated form. To solve such a system, we use Back-Substitution. This is akin to applying extension theorem to the ideals I_l. In this case, we will have to solve polynomial equations in one variable, which may require numerical approximation techniques for higher degree.

The SageMath program to symbolically compute **some solutions** is attached at the end and can also be found here.

5 Sudoku

The objective is to fill a $m \times m$ grid ($m = n^2$) with integers from 1 to m such that no row or column or block has a same number appear twice. Any such board, can be represented in the block matrix form with its each entry being a *block* of dimension $n \times n$.
We model a sudoku using Boolean Polynomials by creating $m \cdot (m^2) = m^3$ variables. m boolean variables for every element of the grid. Let these variables be denoted by $x_{i,j}$ where $0 \leq i \leq m^2 - 1$ and $0 \leq j \leq m - 1$, where i represents the element number and j represents the value that element can take.
There are three kinds of polynomial equations to be created to denote the following conditions,

- for every i, exactly one of $x_{i,j}$ must be 1. This is achieved using following,

$$\begin{aligned} \forall i, \sum_{j=0}^{m-1} \prod_{k \neq j} x_{i,k} = 0 \text{ (for each } i,\ x_{i,j} = 0 \text{ for atleast } m-1 \ j\text{'s)} \\ \forall i, \sum_{j=0}^{m-1} x_{i,j} = 1 \text{ (for each } i, \text{ not all } x_{i,j} = 0) \end{aligned} \tag{5.1}$$

- for i_1, i_2 such that they are in same row or column or block, they should not have the same number.

$$\sum_{j=0}^{m-1} x_{i_1,j} \cdot x_{i_2,j} = 0 \text{ (for all valid } (i_1, i_2) \text{ pairs)} \tag{5.2}$$

- encode the given value, if x_i is k then $x_{i,j} = 1$ iff $j == k - 1$. (i.e., other $x_{i,j} = 0$)

Now, create an ideal and add all the equations to it as polynomials and find its Gröbner basis G.

- If the system has no solution then $G = \{1\}$, else the polynomials of G are in eliminated form.
- If G contains m^3 polynomials then there is a unique solution since each of the m^3 variable will have it's own linear equation (as $x^2 = x$ for binary numbers) which is $x = 0$ or $x + 1 = 0$.
- If G contains less than m^3 polynomials but more than one then x's can be both 0 or 1 and x is either eliminated from the equation or it is uniquely dependent on other variables which are eliminated at a later stage and the number of elements in G would be less than m^3.

Hence, solving if a unqiue solution exists is trivial but if more than one solutions are possible then to solve such a system, we use Back-Substitution. This is akin to applying extension theorem to the ideals I_l. The SageMath program to symbolically compute **all solutions** is attached at the end and can also be found here. Note, even after having 1000+ equations the solution is calculated within 2 minutes if unique.

Note. *Our approach was very similar to integer programming and in fact, it can be changed a bit (by changing the field) to apply for integer programs as well.*

References

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*. English. Amer Mathematical Society, July 1994.

[2] B. Buchberger. *Introduction to Gröbner Bases*. English. Ed. by F. Winkler B. Buchberger. London Mathematical Society Lectures Notes Series 251. Cambridge University Press, Apr. 1998, pp. 3–31.

[3] G. Greuel and G. Pfister. *A Singular Introduction to Commutative Algebra*. English. Springer, 2002. URL: http://www.springeronline.com/sgw/cda/frontpage/0,11855,1-10042-22-2133945-detailsPage%253Dppmmedia%257Ctoc%257Ctoc,00.html.

[4] Donal O'shea (auth.) David A. Cox John Little. *Using Algebraic Geometry*. 2nd ed. Graduate Texts in Mathematics 185. Springer-Verlag New York, 2005. ISBN: 9780387984872.

[5] Christoph Lossen Wolfram Decker. *Computing in algebraic geometry: A quick start using SINGULAR*. 1st ed. Algorithms and Computation in Mathematics. Springer, 2006. ISBN: 9788185931654.

[6] Michael Brickenstein and Alexander Dreyer. "PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials". In: *Journal of Symbolic Computation* 44.9 (2009). Effective Methods in Algebraic Geometry, pp. 1326–1345. ISSN: 0747-7171. DOI: https://doi.org/10.1016/j.jsc.2008.02.017.

[7] Elizabeth Arnold, Stephen Lucas, and Laura Taalman. "Gröbner Basis Representations of Sudoku". In: *The College Mathematics Journal* 41 (Mar. 2010), pp. 101–112. DOI: 10.4169/074683410X480203.

[8] Gerhard J. von zur Gathen J. *Modern computer algebra*. 3ed. Cambridge University Press, 2013. ISBN: 9781107039032.

[9] Donal O'Shea David A. Cox John Little. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 4th Edition. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. ISBN: 978-3-319-16720-6.

[10] The Sage Development Team. "Polynomials". In: (Sept. 2022). URL: https://doc.sagemath.org/pdf/en/reference/polynomial_rings/polynomial_rings.pdf.