Researching about Computational Commutative Algebra and Geometry

Sudoku Solver

Utkarsh Gupta

Deptt. of CS&E, IIT Delhi

Contents

Part I

Algebra and Geometry: Introduction

1 Polynomials: Introduction

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)

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.

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, is "polynomials", which will be the focus of this document.

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

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

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). Denoted by $|\alpha|$:

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

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

Note, if $n = 1$ then we get $\mathbb{F}[x]$ which are polynomials in one variable (x) (*univariate polynomials*).

1.1 Monomial Order

Definition 1.7 (Monomial Ordering-Specific Terminology). For a non-zero $f = \sum_\alpha a_\alpha x^\alpha$, and a monomial order $>$

multidegree of f

$$\text{multideg}(f) = \max_{\text{w.r.t. } >} (\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0) \tag{1.6}$$

leading coefficient of f

$$\text{LC}(f) = a_{\text{multideg}(f)} \in \mathbb{F} \tag{1.7}$$

leading monomial of f

$$\text{LM}(f) = x^{\text{multideg}(f)} \tag{1.8}$$

leading term of f

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f) \tag{1.9}$$

For f of 1.4 with respect to grlex order,

$$\text{multideg}(f) = (2, 0, 2), \quad \text{LC}(f) = 7, \quad \text{LM}(f) = x^2z^2, \quad \text{LT}(f) = 7x^2z^2 \tag{1.10}$$

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

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

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 $f_1, f_2, \dots, f_s$) is defined as follows

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

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 .

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. ■

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.

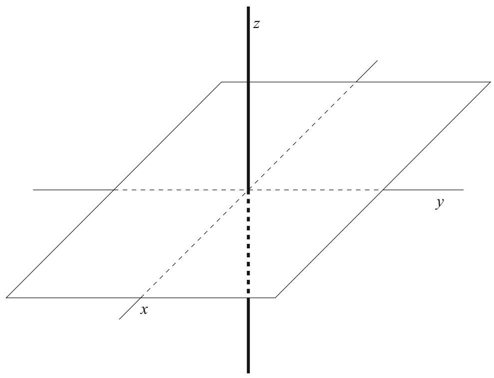

Figure 2.1: $\mathbf{V}(xz, yz)$ - a union of a line and a plane. From [3]

Note. *The "dimension" of a variety is not exactly the same 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 (Principle Ideal). An ideal I generated by single element is a principle ideal.

Definition 3.4 (Principle Ideal Domain (PID)). If every ideal in a domain is a principle ideal then the domain is called principle ideal domain.

Definition 3.5 (Ideal of an affine variety). The set $\mathbf{I}(V)$ is the ideal of an affine variety.

$$\mathbf{I}(V) = \{f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \mid f(a_1, a_2, \ldots, a_n) = 0, \forall a \in V\} \tag{3.2}$$

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 3.6. 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 $a \in \mathbf{V}(f_1, f_2, \ldots, f_s) \Rightarrow f_i(a) = 0 \Rightarrow f(a) = 0 \Rightarrow f \in \mathbf{I}(V)$. ∎

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

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

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 $\mathrm{LT}(g) | \mathrm{LT}(r)$ ($a|b$ is a divides b) **do**
$\quad q \leftarrow q + \dfrac{\mathrm{LT}(r)}{\mathrm{LT}(g)}$
$\quad r \leftarrow r - \dfrac{\mathrm{LT}(r)}{\mathrm{LT}(g)} g$
end while
return q, r

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

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

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 $r = \sum_\alpha a_\alpha \cdot x^\alpha, \mathrm{LT}\, f_i \nmid x^\alpha, \forall i, \alpha$.

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 $\gcd(\mathrm{f}_1, \mathrm{f}_2)$ 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 ← f_1
h ← f_2
while h ≠ 0 do
    g, h ← 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 $I = \langle x^{\alpha(1)}, x^{\alpha(2)}, \ldots, x^{\alpha(s)} \rangle$.

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 $x^{\alpha} y^m, \alpha \in \mathbb{Z}^{n-1}_{\geq 0}$. 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 $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n] \setminus$ 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. ■

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

Definition 2.3 (Affine Variety of an Ideal). For an ideal $I \subseteq \mathbb{F}[x_1, x_2, \dots, x_n]$ such that $I = \langle f_1, f_2, \dots, f_s \rangle$, the affine variety of an Ideal is defined as below,

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

Definition 2.4 (Gröbner Basis). For a fixed monomial ordering on $\mathbb{F}[x_1, x_2, \dots, x_n]$ and $G = \{g_1, g_2, \dots, g_t\}$, G is called a Gröbner basis of a non-zero ideal $I \subseteq \mathbb{F}[x_1, x_2, \dots, x_n]$ if

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

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

Proposition 2.5 (Property of Gröbner Bases). For a Gröbner basis $G = \{g_1, g_2, \dots, g_t\}$ for an ideal $I \subseteq \mathbb{F}[x_1, x_2, \dots, x_n]$ and a given $f \in \mathbb{F}[x_1, x_2, \dots, x_n]$, $\exists! r \in \mathbb{F}[x_1, x_2, \dots, x_n]$ 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 2.6 (Ideal Membership Problem (Multivariate Polynomial Ideals)). For a Gröbner basis $G = \{g_1, g_2, \dots, g_t\}$ for an ideal $I \subseteq \mathbb{F}[x_1, x_2, \dots, x_n]$,

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

2.1 Computation of Gröbner Basis

Definition 2.7. Here are some additional notations that will be helpful.

- $\overline{f}^F$ is the remainder on division of f by $F = (f_1, f_2, \dots, f_s)$.
- $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$, 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 2.8 (Buchberger's Criterion). A basis $G = \{g_1, g_2, \dots, g_t\}$ is a Gröbner basis of $I \subseteq \mathbb{F}[x_1, x_2, \dots, x_n]$ iff $\overline{S(g_i, g_j)}^G = 0, \forall i, j \; (i \neq j)$

Theorem 2.9 (Buchberger's Algorithm). For a non-zero ideal $I = \langle f_1, f_2, \dots, f_s \rangle$, 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 2.8 is satisfied.

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 **??** it converges. Hence, the algorithm terminates. ∎

Definition 2.10 (Reduced Gröbner Basis). A reduced Gröbner basis $G = \{g_1, g_2, \dots, g_t\}$ of an ideal $I \subseteq \mathbb{F}[x_1, x_2, \dots, x_n]$ 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.

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'}   (remainder of S(p,q) on division by G')
        if r ≠ 0 then
            G ← G ∪ {r}
        end if
    end for
until G = G'
return G
```

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

Gröbner Bases: Applications, Interconnection of Algebra & Geometry

1 System of Linear Equations

The problem of our interest is

$$Ax = b \quad (A \in \mathbb{F}^{n\times n}, \text{ and } b, x \in \mathbb{F}^{n\times 1}) \tag{1.1}$$

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

$$f_i(x_1, x_2, \ldots, x_n) = -b_i + a_{i,1}x^1 + a_{i,2}x^2 + \cdots + a_{i,n}x^n = -b_i + \sum_{j=1}^{n} a_{i,j}x^j = 0(1 \le i, j \le n) \tag{1.2}$$

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.

2 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.

3 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 $0 \le i \le m^2 - 1$ and $0 \le j \le m - 1$, 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,

$$\begin{aligned} \forall i, \sum_{j=0}^{m-1} \prod_{k \neq j} x_{i,k} &= 0 \text{ (for each } i, x_{i,j} = 0 \text{ for atleast } m-1\ j\text{'s)} \\ \forall i, \sum_{j=0}^{m-1} x_{i,j} &= 1 \text{ (for each } i, \text{ not all } x_{i,j} = 0) \end{aligned} \tag{3.1}$$

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

$$\sum_{j=0}^{m-1} x_{i_1,j} \cdot x_{i_2,j} = 0 \text{ (for all valid } (i_1, i_2) \text{ pairs)} \tag{3.2}$$

- 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. Note, even after having 1000+ equations the solution is calculated within 2 minutes if unique.

Note. *My 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] 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.

[3] 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.

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