Computational Commutative Algebra and Geometry

EE451 Supervised Research Exposition

Rathour Param Jitendrakumar
190070049

Department of Electrical Engineering
Indian Institute of Technology Bombay

Autumn 2022-23

Guide: Prof. Debasattam Pal

Outline

Polynomials I

Introduction

Definition (Monomial)

A monomial in $(x_1, x_2, \ldots, x_n)$, denoted by x^α is defined as follows

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n} \qquad (\alpha_i \in \mathbb{Z}^+ \text{ and } \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)) \tag{1}$$

Note, when $\alpha = (0, 0, \ldots, 0)$ we take $x^\alpha = 1$. The collection of all such α is denoted by $\mathbb{Z}^n_{\geq 0}$.

Definition (Total degree of a monomial)

The total degree of a monomial, denoted by $|\alpha|$ is defined as

$$|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n \tag{2}$$

Polynomials II

Introduction

Definition (Polynomial)

A polynomial f in $(x_1, x_2, \ldots, x_n)$ is a finite sum denoted by

$$f(x_1, x_2, \ldots, x_n) = f(x) = f = \sum_{\alpha} a_\alpha x^\alpha \qquad (\textit{where } a_\alpha \in \mathbb{F} \textit{ and } \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)) \tag{3}$$

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

Definition (Total degree of a polynomial)

The maximum total degree of a monomial of f which has non-zero coefficient, i.e.

$$\deg(f) = \max_{\alpha \neq 0} |\alpha| \tag{4}$$

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 $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

Polynomials III

Introduction

Example

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

What about order?

Monomial Orderings

Motivation

Definition (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*

$$x^\alpha > x^\beta \text{ or } x^\alpha < x^\beta (\equiv x^\beta > x^\alpha) \text{ or } x^\alpha = x^\beta (\equiv x^\alpha \not> x^\beta, x^\beta \not> x^\alpha) \tag{6}$$

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

$$\text{for non-empty } A \subseteq \mathbb{Z}^n_{\geq 0} \Rightarrow \exists! \alpha \text{ such that } \beta \geq \alpha \text{ for } \beta \in \mathbb{Z}^n_{\geq 0} \tag{7}$$

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

Monomial Orderings

Examples

Definition (Lexicographic Order)

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{lex} \beta$ *if leftmost non-zero entry of* $\alpha - \beta$ *is positive.*

Definition (Graded Lex Order)

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{grlex} \beta$ *if* $|\alpha| > |\beta|$ *or* ($|\alpha| = |\beta|$ *and* $\alpha >_{lex} \beta$)

Definition (Graded Reverse Lex Order)

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{grevlex} \beta$ *if* $|\alpha| > |\beta|$ *or* ($|\alpha| = |\beta|$ *and rightmost non-zero entry of* $\alpha - \beta$ *is negative*)

Examples

f of 5 with respect to grlex order is as follows,

Example (Lexicographic Order)

$$\begin{aligned} f &= -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2 \\ f &= \text{sum}\{(-5,(3,0,0)),(7,(2,0,2),(4,(1,2,1)),(4,(0,0,2)))\} \end{aligned} \tag{8}$$

Example (Graded Lex Order)

$$\begin{aligned} f &= 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2 \\ f &= \text{sum}\{(7,(2,0,2),(4,(1,2,1)),(-5,(3,0,0)),(4,(0,0,2)))\} \end{aligned} \tag{9}$$

Example (Graded Reverse Lex Order)

$$\begin{aligned} f &= 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2 \\ f &= \text{sum}\{(4,(1,2,1)),(7,(2,0,2),(-5,(3,0,0)),(4,(0,0,2)))\} \end{aligned} \tag{10}$$

Monomial Ordering-Specific Terminology

For a non-zero $f = \sum_\alpha a_\alpha x^\alpha$, and a monomial order $>$

Definition (multidegree of f)

$$\mathrm{multideg}(f) = \max_{w.r.t.\ >} (\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0) \tag{11}$$

Definition (leading coefficient of f)

$$\mathrm{LC}(f) = a_{\mathrm{multideg}(f)} \in \mathbb{F} \tag{12}$$

Definition (leading monomial of f)

$$\mathrm{LM}(f) = x^{\mathrm{multideg}(f)} \tag{13}$$

Definition (leading term of f)

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f) \tag{14}$$

Division Algorithm I

Theorem (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, $q_i \cdot f_i \neq 0 \Rightarrow \mathrm{multideg}(f) \geq \mathrm{multideg}(q_i \cdot f_i)$

Note, 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 $(q_1, q_2, r) = (y, 0, -x + y)$.

The Division Algorithm I

Algorithm 1 Polynomial Division (Single Variable)[1]

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**
    $q \leftarrow q + \dfrac{\mathrm{LT}(r)}{\mathrm{LT}(g)}$
    $r \leftarrow r - \dfrac{\mathrm{LT}(r)}{\mathrm{LT}(g)} g$
  end while
  return q, r

---

[1] Donal O'Shea David A. Cox, John Little. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.

Frame Title

Algorithm 2 Polynomial Division (Multiple Variable)[2]

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
```

[2] Donal O'Shea David A. Cox, John Little. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.

Affine Varieties

Definition (Affine Space)

An $n-$dimensional affine space over $\mathbb{F}$ is a set denoted by $\mathbb{F}^n$ and defined as follows

$$\mathbb{F}^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in \mathbb{F}\} \tag{15}$$

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.

Definition (Affine Varieties)

An affine variety V (over polynomials $f_1, f_2, \dots, f_s$) is defined as follows

$$V = \mathbf{V}(f_1, f_2, \dots, f_s) = \{(a_1, a_2, \dots, a_n) \in \mathbb{F}^n \mid f_i(a_1, a_2, \dots, a_n) = f_i(a) = 0 \ \forall i\} \tag{16}$$

Varieties I

Examples

Example

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 $[b_i] = -\alpha_{i_0}$.

Varieties II

Examples

Example

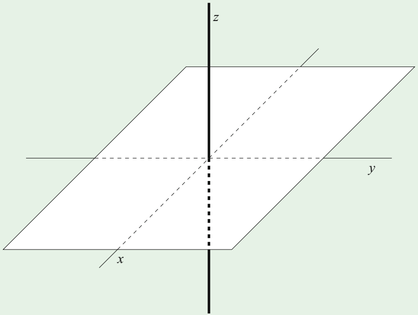

Figure: $\mathbf{V}(xz, yz)$ - a union of a line and a plane[a]

[a] Donal O'Shea David A. Cox, John Little. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.

Varieties

Motivation

The questions of interests concerning an affine variety $V = \mathbf{V}(f_1, f_2, \dots, f_s)$ 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.

Ideals I

Definition (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* $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

Ideals II

Definition (Ideal of an affine variety)

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

$$\mathbf{I}(V) = \{f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \mid f(a_1, a_2, \ldots, a_n) = 0, \forall a \in V\} \tag{17}$$

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

Ideals III

Lemma

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 $\langle f_1, f_2, \ldots, f_s \rangle$.

$$I = \langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i \cdot f_i | h_i \in \mathbb{F}[x_1, x_2, \ldots, x_n] \right\} \tag{18}$$

It is trivial to show that $\langle f_1, f_2, \ldots, f_s \rangle$ is indeed an ideal, use the representation 18 and verify the three properties.

Definition (Finitely Generated Ideal)

An ideal I is finitely generated if

$$\exists f_1, f_2, \ldots, f_s \in \mathbb{F}[x_1, x_2, \ldots, x_n] \text{ such that } I = \langle f_1, f_2, \ldots, f_s \rangle \tag{19}$$

Ideals

Motivation

The questions of interests concerning an ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ are

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 $\mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$ where the set $\mathbf{I}(V)$ is the ideal of an affine variety given by,

$$\mathbf{I}(V) = \{f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \mid f(a_1, a_2, \ldots, a_n) = 0, \forall a \in V\} \tag{20}$$

Gröbner Bases I

Theorem (Hilbert Basis Theorem (Ideal Description Problem))

Every ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ *has a finite basis.*

Definition (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*

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle \tag{21}$$

where,

$$\mathrm{LT}(I) = \{a_\alpha x^\alpha | \exists f \in I \setminus \{0\} \text{ such that } \mathrm{LT}(f) = a_\alpha x^\alpha\} \tag{22}$$

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

Gröbner Bases II

Proposition (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.

Theorem (Ideal Membership Problem)

For a Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ *for an ideal* $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$,

$$f \in I \Leftrightarrow \text{ remainder on division of } f \text{ by } G \text{ is zero.} \tag{23}$$

Computation of Gröbner Basis I

Definition

- $\overline{f}^F$ *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.,* $\gamma_i = \max(\alpha_i, \beta_i)$ *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 (Buchberger's Criterion)

A basis $G = \{g_1, \ldots, g_t\}$ *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 (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 until Buchberger's Criterion is satsified.

Computation of Gröbner Basis II

Algorithm 3 Buchberger's Algorithm[3]

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

$G \leftarrow F$
repeat
  $G' \leftarrow G$
  for all pairs $\{p, q\}$ where $p, q \in G', p \neq q$ **do**
    $r \leftarrow \overline{S(p,q)}^{G'}$
    if $r \neq 0$ **then**
      $G \leftarrow G \cup \{r\}$
    end if
  end for
until $G = G'$
return G

[3] Donal O'Shea David A. Cox, John Little. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.

Reduced Gröbner Basis

Definition (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 $\mathrm{LT}(g_i) \in \langle \mathrm{LT}(G \setminus \{g_i\})$.
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.

Elimination Theory I

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 (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 $l-^{th}$ elimination ideal I_l is the ideal in $\mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n]$ defined by

$$I_l = I \cap \mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n] \tag{24}$$

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.

Elimination Theory II

Theorem (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* $(x_1 > x_2 > \cdots > x_n)$,

$$G_l = G \cap \mathbb{F}[x_{l+1}, x_{l+2}, \ldots, x_n] \tag{25}$$

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

Theorem (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,*

$$f_i = c_i(x_2, \ldots, x_n) x_1^{N_i} + \text{ terms in } x_1 \text{ with degree} < N_i \; (N_i \geq 0, c_i \in \mathbb{C}[x_2, \ldots, x_n] \setminus \{0\}) \tag{26}$$

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* $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Sudoku

Example

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

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

Figure: Sudoku Game and its solution[4]

[4] Elizabeth Arnold, Stephen Lucas, and Laura Taalman. Gröbner basis representations of sudoku

Sudoku I

Formulation and Modelling

- 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

Sudoku

Representation

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,

$$\begin{aligned} \forall i, \sum_{j=0}^{m-1} \prod_{k \neq j} x_{i,k} &= 0 \text{ (for each } i, \ x_{i,j} = 0 \text{ for atleast } m-1 \ j\text{'s)} \\ \forall i, \sum_{j=0}^{m-1} x_{i,j} &= 1 \text{ (for each } i, \text{ not all } x_{i,j} = 0) \end{aligned} \tag{27}$$

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

$$\sum_{j=0}^{m-1} x_{i_1,j} \cdot x_{i_2,j} = 0 \text{ (for all valid } (i_1, i_2) \text{ pairs)} \tag{28}$$

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

Sudoku

Solution

- 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.

Sudoku

SageMath Demo.

Conclusion

- **NP-hard** to compute and generated Gröbner Basis have polynomials of higher degrees and larger coefficients.
- Applications designed for Solving Polynomial Equations, Lagrange Optimizations. Check here
- More possible applications Vertex Coloring, Design of Computer Algebra Systems, Coding Theory are developed.
- Future Directions on Fast Computations of Gröbner Basis: Faugère's F4 and F5 algorithms and more application-specific development such as, PolyBoRi, a Gröbner basis framework for Boolean polynomials.

References I

Elizabeth Arnold, Stephen Lucas, and Laura Taalman.
Gröbner basis representations of sudoku.
The College Mathematics Journal, 41:101–112, 03 2010.
doi:10.4169/074683410X480203.

B. Buchberger.
Introduction to Gröbner Bases.
London Mathematical Society Lectures Notes Series 251. Cambridge University Press, 4 1998.

Donal O'Shea David A. Cox, John Little.
Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.
Undergraduate Texts in Mathematics. Springer International Publishing, 4th edition, 2015.

The Sage Development Team.
URL: https://doc.sagemath.org/.