Gröbner Bases Tutorial

Part I: Gröbner Bases and the Geometry of Elimination

David A. Cox

Department of Mathematics and Computer Science
Amherst College
`dac@cs.amherst.edu`

ISSAC 2007 Tutorial

Outline

Begin Gröbner Basics

- k – field (often algebraically closed)
- $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ – monomial in $x_1, \ldots, x_n$
- $c\,\mathbf{x}^\alpha$, $c \in k$ – term in $x_1, \ldots, x_n$
- $k[\mathbf{x}] = k[x_1, \ldots, x_n]$ – polynomial ring in n variables
- $\mathbb{A}^n = \mathbb{A}^n(k)$ – n-dimensional affine space over k
- $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s) \subseteq \mathbb{A}^n$ – variety of $I = \langle f_1, \ldots, f_s \rangle$
- $\mathbf{I}(V) \subseteq k[\mathbf{x}]$ – ideal of the variety $V \subseteq \mathbb{A}^n$
- $\sqrt{I} = \{f \in k[\mathbf{x}] \mid \exists m\ f^m \in I\}$ – the radical of I

Recall that I is a radical ideal if $I = \sqrt{I}$.

Monomial Orders

Definition

A monomial order is a total order $>$ on the set of monomials $\mathbf{x}^\alpha$ satisfying:

- $\mathbf{x}^\alpha > \mathbf{x}^\beta$ implies $\mathbf{x}^\alpha\mathbf{x}^\gamma > \mathbf{x}^\beta\mathbf{x}^\gamma$ for all $\mathbf{x}^\gamma$
- $\mathbf{x}^\alpha > 1$ for all $\mathbf{x}^\alpha \neq 1$

We often think of a monomial order as a total order on the set of exponent vectors $\alpha \in \mathbb{N}^n$.

Lemma

A monomial order is a well-ordering on the set of all monomials.

Examples of Monomial Orders

Examples

- Lex order with $x_1 > \cdots > x_n$: $\mathbf{x}^\alpha >_{lex} \mathbf{x}^\beta$ iff

$$\alpha_1 > \beta_1, \text{ or } \alpha_1 = \beta_1 \text{ and } \alpha_2 > \beta_2, \text{ or } \ldots$$

- Weighted order using $w \in \mathbb{R}^n_+$ and lex to break ties: $\mathbf{x}^\alpha >_{w,lex} \mathbf{x}^\beta$ iff

$$w\cdot\alpha > w\cdot\beta, \text{ or } w\cdot\alpha = w\cdot\beta \text{ and } \mathbf{x}^\alpha >_{lex} \mathbf{x}^\beta$$

- Graded lex order with $x_1 > \cdots > x_n$: This is $>_{w,lex}$ for $w = (1,\ldots,1)$

Weighted orders will appear in Part II when we discuss the Gröbner walk.

Leading Terms

Definition

Fix a monomial order $>$ and let $f \in k[\mathbf{x}]$ be nonzero. Write

$$f = c\,\mathbf{x}^{\alpha} + \text{terms with exponent vectors } \beta \neq \alpha$$

such that $c \neq 0$ and $\mathbf{x}^{\alpha} > \mathbf{x}^{\beta}$ wherever $\beta \neq \alpha$ and $\mathbf{x}^{\beta}$ appears in a nonzero term of f. Then:

- $\mathrm{LT}(f) = c\,\mathbf{x}^{\alpha}$ is the leading term of f
- $\mathrm{LM}(f) = \mathbf{x}^{\alpha}$ is the leading monomial of f
- $\mathrm{LC}(f) = c$ is the leading coefficient of f

The leading term $\mathrm{LT}(f)$ is sometimes called the initial term, denoted $\mathrm{in}(f)$.

The Division Algorithm

Division Algorithm

Given nonzero polynomials $f, f_1, \ldots, f_s \in k[\mathbf{x}]$ and a monomial order $>$, there exist $r, q_1, \ldots, q_s \in k[\mathbf{x}]$ with the following properties:

- $f = q_1 f_1 + \cdots + q_s f_s + r$.
- No term of r is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.
- $\mathrm{LT}(f) = \max_{>}\{\mathrm{LT}(q_i)\mathrm{LT}(f_i) \mid q_i \neq 0\}$.

Definition

Any representation

$$f = q_1 f_1 + \cdots + q_s f_s$$

satisfying the third bullet is a standard representation of f.

The Ideal of Leading Terms

Definition

Given an ideal $I \subseteq k[\mathbf{x}]$ and a monomial order $>$, the ideal of leading terms is the monomial ideal

$$\langle \mathrm{LT}(I) \rangle := \langle \mathrm{LT}(f) \mid f \in I \rangle.$$

If $I = \langle f_1, \ldots, f_s \rangle$, then

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \subseteq \langle \mathrm{LT}(I) \rangle,$$

though equality need not occur.

This is where Gröbner bases enter the picture!

Gröbner Bases

Fix a monomial order $>$ on $k[\mathbf{x}]$.

Definition

Given an ideal $I \subseteq k[\mathbf{x}]$ a finite set $G \subseteq I \setminus \{0\}$ is a Gröbner basis for I under $>$ if

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

Definition

A Gröbner basis G is reduced if for every $g \in G$,

- $\mathrm{LT}(g)$ divides no term of any element of $G \setminus \{g\}$.
- $\mathrm{LC}(g) = 1$.

Theorem

Every ideal has a unique reduced Gröbner basis under $>$.

Criteria to be a Gröbner Basis

Given $>$ and $g,h \in k[\mathbf{x}] \setminus \{0\}$, we get the S-polynomial

$$S(g,h) := \frac{\mathbf{x}^\gamma}{\mathrm{LT}(g)}\, g - \frac{\mathbf{x}^\gamma}{\mathrm{LT}(h)}\, h, \quad \mathbf{x}^\gamma = \mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h)).$$

Three Criteria

- (SR) *$G \subseteq I$ is a Gröbner basis of $I \iff$ every $f \in I$ has a standard representation using G.*
- (Buchberger) *G is a Gröbner basis of $\langle G \rangle \iff$ for every $g,h \in G$, $S(g,h)$ has a standard representation using G.*
- (LCM) *G is a Gröbner basis of $\langle G \rangle \iff$ for every $g,h \in G$, $S(g,h) = \sum_{\ell \in G} A_\ell\, \ell$, where $A_\ell \neq 0$ implies $\mathrm{LT}(A_\ell\, \ell) < \mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h))$ (a lcm representation).*

The Consistency Theorem

Fix an ideal $I \subseteq k[\mathbf{x}]$, where k is algebraically closed.

Nullstellensatz

- (Strong) $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.
- (Weak) $\mathbf{V}(I) = \emptyset \iff 1 \in I \iff I = k[\mathbf{x}]$.

The Consistency Theorem

The following are equivalent:

- $I \neq k[\mathbf{x}]$.
- $1 \notin I$.
- $\mathbf{V}(I) \neq \emptyset$.
- *I has a Gröbner basis consisting of nonconstant polynomials.*
- *I has a reduced Gröbner basis $\neq \{1\}$.*

The Finiteness Theorem

Fix an ideal $I \subseteq k[\mathbf{x}]$, where k is algebraically closed. Also fix a monomial order $>$.

The Finiteness Theorem

The following are equivalent:

- $\mathbf{V}(I) \subseteq \mathbb{A}^n$ *is finite.*
- $k[\mathbf{x}]/I$ *is a finite-dimensional vector space over* k*.*
- I *has a Gröbner basis* G *where* $\forall i$, G *has a element whose leading monomial is a power of* x_i*.*
- *Only finitely many monomials are not in* $\langle \textsc{lt}(I) \rangle$*.*

When these conditions are satisfied:

- $\#$ solutions $\leq \dim_k k[\mathbf{x}]/I$.
- Equality holds $\iff$ I is radical.
- $\dim_k k[\mathbf{x}]/I = \#$ solutions counted with multiplicity.

Begin Elimination Theory

Given

$$k[\mathbf{x},\mathbf{y}] = k[x_1,\dots,x_s,y_{s+1},\dots,y_n],$$

we write monomials as $\mathbf{x}^\alpha\mathbf{y}^\beta$.

Definition

A monomial order $>$ on $k[\mathbf{x},\mathbf{y}]$ eliminates $\mathbf{x}$ whenever

$$\mathbf{x}^\alpha > \mathbf{x}^\beta \Rightarrow \mathbf{x}^\alpha\mathbf{y}^\gamma > \mathbf{x}^\beta\mathbf{y}^\delta$$

for all $\mathbf{y}^\gamma, \mathbf{y}^\delta$.

Example

Lex with $x_1 > \cdots > x_n$ eliminates $\mathbf{x} = \{x_1,\dots,x_s\}$ $\forall s$.

The Elimination Theorem

Fix an ideal $I \subseteq k[\mathbf{x},\mathbf{y}]$.

Definition

$I \cap k[\mathbf{y}]$ is the elimination ideal of I that eliminates $\mathbf{x}$.

Theorem

Let G be a Gröbner basis of I for a monomial order $>$ that eliminates $\mathbf{x}$. Then $G \cap k[\mathbf{y}]$ is a Gröbner basis of the elimination ideal $I \cap k[\mathbf{y}]$ for the monomial order on $k[\mathbf{y}]$ induced by $>$.

Proof

$f \in I \cap k[\mathbf{y}]$ has standard representation $f = \sum_{g \in G} A_g\, g$. If $A_g \neq 0$, then $\mathrm{LT}(g) \leq \mathrm{LT}(A_g\, g) \leq \mathrm{LT}(f) \in k[\mathbf{y}]$, so $g \in G \cap k[\mathbf{y}]$.
SR Criterion $\Rightarrow G \cap k[\mathbf{y}]$ is a Gröbner basis of $I \cap k[\mathbf{y}]$. □

Partial Solutions

Given $I \subseteq k[\mathbf{x},\mathbf{y}] = k[x_1,\ldots,x_s,y_{s+1},\ldots,y_n]$, the elimination ideal $I \cap k[\mathbf{y}]$ will be denoted

$$I_s := I \cap k[\mathbf{y}] \subseteq k[\mathbf{y}].$$

Definition

The variety of partial solutions is

$$\mathbf{V}(I_s) \subseteq \mathbb{A}^{n-s}.$$

Question

How do the partial solutions $\mathbf{V}(I_s) \subseteq \mathbb{A}^{n-s}$ relate to the original variety $V := \mathbf{V}(I) \subseteq \mathbb{A}^n$?

Partial Solutions

Given coordinates $x_1, \ldots, x_s, y_{s+1}, \ldots, y_n$, let

$$\pi_s : \mathbb{A}^n \longrightarrow \mathbb{A}^{n-s}$$

denote projection onto the last $n - s$ coordinates.

An ideal $I \subseteq k[\mathbf{x}, \mathbf{y}]$ gives:

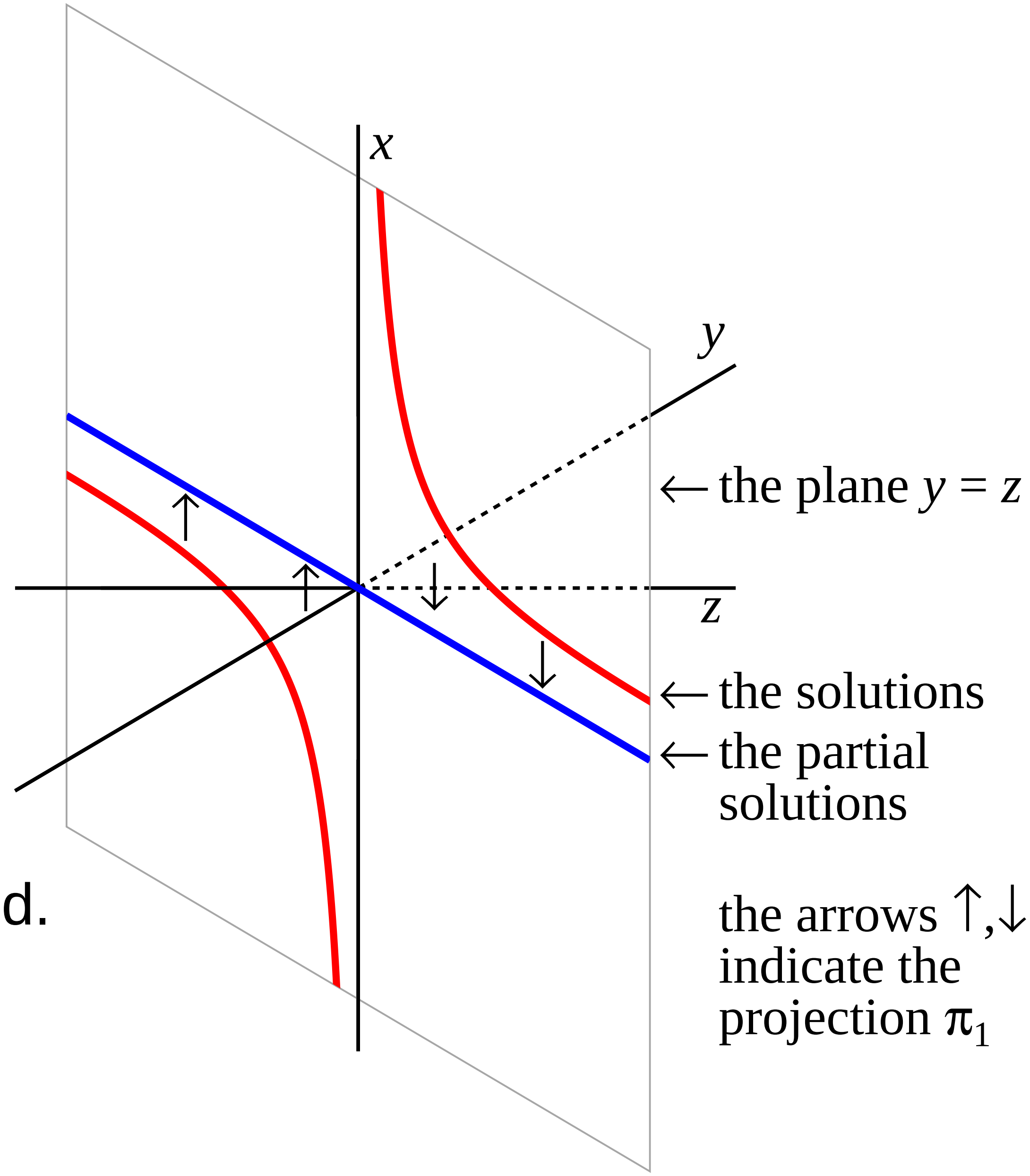
- $V = \mathbf{V}(I) \subseteq \mathbb{A}^n$ and $\pi_s(V) \subseteq \mathbb{A}^{n-s}$.
- $I_s = I \cap k[\mathbf{y}] \subseteq k[\mathbf{y}]$ and $\mathbf{V}(I_s) \subseteq \mathbb{A}^{n-s}$.

Lemma

$$\pi_s(V) \subseteq \mathbf{V}(I_s).$$

Partial Solutions Don't Always Extend

In $\mathbb{A}^3$, consider $V = \mathbf{V}(xy-1, y-z)$. Using lex order with $x > y > z$, $I = \langle xy-1, y-z\rangle$ has Gröbner basis $xy-1, y-z$. Thus $I_1 = \langle y-z\rangle$, so the partial solutions are the line $y = z$. The The partial solution $(0,0)$ does **not** extend.



The Extension Theorem

Let $I \subseteq k[x,y_2,\ldots,y_n] = k[x,\mathbf{y}]$ with variety $V = \mathbf{V}(I) \subseteq \mathbb{A}^n$, and let $I_1 := I \cap k[\mathbf{y}]$ be the first elimination ideal. We assume that k is algebraically closed.

Theorem

Let $\mathbf{b} = (a_2,\ldots,a_n) \in \mathbf{V}(I_1)$ be a partial solution. If the ideal I contains a polynomial f such that

$$f = c(\mathbf{y})x^N + \textit{terms of degree } < N \textit{ in } x$$

with $c(\mathbf{b}) \neq 0$, then there is $a \in k$ such that $(a,\mathbf{b}) = (a,a_2,\ldots,a_n)$ is a solution, i.e.,

$$(a,a_2,\ldots,a_n) \in V.$$

Zariski Closure

Definition

Given a subset $S \subseteq \mathbb{A}^n$, the Zariski closure of S is the smallest variety $\overline{S} \subseteq \mathbb{A}^n$ containing S.

Lemma

The Zariski closure of $S \subseteq \mathbb{A}^n$ is $\overline{S} = \mathbf{V}(\mathbf{I}(S))$.

Example

Over $\mathbb{C}$, the set $\mathbb{Z}^n \subseteq \mathbb{C}^n$ has Zariski closure $\overline{\mathbb{Z}^n} = \mathbb{C}^n$.

The Closure Theorem

Let $V = \mathbf{V}(I) \subseteq \mathbb{A}^n$ and let k be algebraically closed.

Theorem

$$\mathbf{V}(I_s) = \overline{\pi_s(V)}.$$

Thus $\mathbf{V}(I_s)$ is the smallest variety in $\mathbb{A}^{n-s}$ containing $\pi_s(V)$. Furthermore, there is an affine variety

$$W \subseteq \mathbf{V}(I_s) \subseteq \mathbb{A}^{n-s}$$

with the following properties:

- $\overline{\mathbf{V}(I_s) \setminus W} = \mathbf{V}(I_s)$.
- $\mathbf{V}(I_s) \setminus W \subseteq \pi_s(V)$.

Thus "most" partial solutions in $\mathbf{V}(I_s)$ come from actual solutions, i.e, the projection of V fills up "most" of $\mathbf{V}(I_s)$.

Prove Extension and Closure Theorems

Traditional proofs of the Extension and Closure Theorems use resultants or more abstract methods from algebraic geometry.

Recently, Peter Schauenberg wrote

"A Gröbner-based treatment of elimination theory for affine varieties"

(Journal of Symbolic Computation, to appear). This paper uses Gröbner bases to give new proofs of the Extension and Closure Theorems.

Part I of the tutorial will conclude with these proofs. We begin with the Extension Theorem.

Prove the Extension Theorem

Fix a partial solution $\mathbf{b} = (a_2, \ldots, a_n) \in \mathbf{V}(I_1) \subset \mathbb{A}^{n-1}$.

Notation for the Proof

Let $f \in k[x, y_2, \ldots, y_n] = k[x, \mathbf{y}]$.

- We write
$$f = \underbrace{c(\mathbf{y})}_{\mathrm{LC}_x(f)} x^M + \text{terms of degree} < M \text{ in } x$$
- We set
$$\bar{f} := f(x, \mathbf{b}) \in k[x].$$

By hypothesis, there is $f \in I$ with $\overline{\mathrm{LC}_x(f)} \neq 0$.

Lemma

Let G be a Gröbner basis of I using $>$ that eliminates x.

Lemma

There is $g \in G$ with $\overline{\mathrm{LC}_x(g)} \neq 0$.

Proof

Let $f = \sum_{g\in G} A_g\, g$ be a standard representation of $f \in I$ with $\overline{\mathrm{LC}_x(f)} \neq 0$. Thus

$$\mathrm{LT}(f) = \max\{\mathrm{LT}(A_g\, g) \mid A_g \neq 0\}.$$

Since $>$ eliminates x, it follows that

$$\begin{aligned} \deg_x(f) &= \max\{\deg_x(A_g\, g) \mid A_g \neq 0\} \\ \mathrm{LC}_x(f) &= \sum_{\deg_x(A_g\, g)=\deg_x(f)} \mathrm{LC}_x(A_g)\,\mathrm{LC}_x(g) \end{aligned}$$

□

Main Claim

By the lemma, we can pick $g \in G$ with $\overline{\mathrm{LC}_x(g)} \neq 0$ and $M := \deg_x(g)$ minimal. Note that $M = \deg_x(\bar{g}) > 0$.

Main Claim

$$\{\bar{f} \mid f \in I\} = \langle \bar{g} \rangle \subseteq k[x].$$

Consequence: If $\bar{g}(a) = 0$ for some $a \in k$, then

$$f(a, \mathbf{b}) = \bar{f}(a) = 0$$

for all $f \in I$, so $(a, \mathbf{b}) = (a, a_2, \ldots, a_n) \in V = \mathbf{V}(I)$.
This proves the Extension Theorem!

Strategy to prove Main Claim: Show $\bar{h} \in \langle \bar{g} \rangle$ for all $h \in G$.

Claim

Consider $h \in G$ with $\deg_x(h) < M = \deg_x(g)$. M minimal implies $\overline{\mathrm{LC}_x(h)} = 0$, so $\deg_x(\bar{h}) < \deg_x(h)$.

Claim

$\bar{h} = 0$.

Proof. Let $m := \deg_x(h) < M$ and set

$$S := \mathrm{LC}_x(g)x^{M-m}h - \mathrm{LC}_x(h)g \in I,$$

with standard representation $S = \sum_{\ell \in G} A_\ell\, \ell$. Observe:

- $\overline{\mathrm{LC}_x(g)}\, x^{M-m}\, \bar{h} = \overline{S} = \sum_{\ell \in G} \overline{A_\ell}\, \bar{\ell}$
- $\max\{\deg_x(A_\ell) + \deg_x(\ell) \mid A_\ell \neq 0\} = \deg_x(S) < M$

Prove the Claim

- $\overline{\text{LC}_x(g)}\, x^{M-m}\,\bar{h} = \bar{S} = \sum_{\ell \in G} \overline{A_\ell}\,\bar{\ell}$
- $\max\{\deg_x(A_\ell) + \deg_x(\ell)\} = \deg_x(S) < M$

First bullet implies: Since $\overline{\text{LC}_x(g)} \neq 0$ and $m = \deg_x(h)$,

$$M - \deg_x(h) + \deg_x(\bar{h}) \leq \max\{\deg_x(\overline{A_\ell}) + \deg_x(\bar{\ell})\}$$

so that

$$\deg_x(h) - \deg_x(\bar{h}) \geq \min\{M - (\deg_x(\overline{A_\ell}) + \deg_x(\bar{\ell}))\}.$$

Second bullet implies: All $\ell \in G$ in S have $\deg_x(\ell) < M$, so $\deg_x(\bar{\ell}) < \deg_x(\ell)$. Hence

$$\deg_x(\overline{A_\ell}) + \deg_x(\bar{\ell}) < \deg_x(A_\ell) + \deg_x(\ell) < M.$$

The two strict inequalities give $\deg_x(h) - \deg_x(\bar{h}) \geq 2$.

Finish the Claim

The inequality $\deg_x(h) - \deg_x(\bar{h}) \geq 2$ applies to all $h \in G$ with $\deg_x(h) < M$ and hence to all $\ell \in G$ in $S = \sum_\ell A_\ell \ell$.

Arguing as before gives

$$\deg_x(\overline{A_\ell}) + \deg_x(\bar{\ell}) < \deg_x(A_\ell) + \deg_x(\ell) < M,$$

$\uparrow$

drops by at least 2

and

$$\deg_x(h) - \deg_x(\bar{h}) \geq \min\{\underbrace{M - (\deg_x(\overline{A_\ell}) + \deg_x(\bar{\ell}))}_{\geq 3}\} \geq 3.$$

Continuing this way, we see that $\bar{h} = 0$ for all $h \in G$ with $\deg_x(h) < M$, as claimed. $\square$

Prove the Main Claim

Proof. For $h \in G$, we show $\bar{h} \in \langle \bar{g} \rangle$ by induction on $\deg_x(h)$.

Base Case: $\deg_x(h) < M$ implies $\bar{h} = 0 \in \langle \bar{g} \rangle$ by Claim.

Inductive Step: Assume $\bar{h} \in \langle \bar{g} \rangle$ for all $h \in G$ with $\deg_x(h) < m \geq M$. Take $h \in G$ with $\deg_x(h) = m$. Then

$$S := \mathrm{LC}_x(g)\,h - \mathrm{LC}_x(h)\,x^{m-M}\,g \in I$$

has standard representation $S = \sum_{\ell \in G} A_\ell\,\ell$, so

$$\deg_x(S) < m \Rightarrow \deg_x(\ell) < m \quad \forall \ell \text{ in } S.$$

By inductive hypothesis, $\bar{\ell} \in \langle \bar{g} \rangle$. Hence

$$\overline{\mathrm{LC}_x(g)}\,\bar{h} - \overline{\mathrm{LC}_x(h)}\,x^{m-M}\,\bar{g} = \bar{S} = \sum_{\ell \in G} \overline{A_\ell}\,\bar{\ell}.$$

Then $\overline{\mathrm{LC}_x(g)} \neq 0$ implies $\bar{h} \in \langle \bar{g} \rangle$. □

The Closure Theorem

We next give Schauenberg's proof of the Closure Theorem.

Fix a partial solution $\mathbf{b} = (a_{s+1}, \ldots, a_n) \in \mathbf{V}(I_s) \subset \mathbb{A}^{n-s}$ and a Gröbner basis G of I for $>$ that eliminates $\mathbf{x} = (x_1, \ldots, x_s)$.

Notation for the Proof

Let $f \in k[x_1, \ldots, x_s, y_{s+1}, \ldots, y_n] = k[\mathbf{x}, \mathbf{y}]$.

- We write
$$f = \underbrace{c(\mathbf{y})}_{\mathrm{LC}_s(f)} \mathbf{x}^{\alpha(f)} + \text{terms} < \mathbf{x}^{\alpha(f)}.$$
- We set
$$\bar{f} := f(\mathbf{x}, \mathbf{b}) \in k[\mathbf{x}].$$

A Special Case

Special Case

If $\mathbf{b} \in \mathbf{V}(I_s)$ satisfies

$$\overline{\mathrm{LC}_s(g)} \neq 0 \text{ for all } g \in G \setminus k[\mathbf{y}],$$

then $\mathbf{b} \in \pi_s(V)$.

Proof. If we can find $\mathbf{a} = (a_1, \dots, a_s)$ such that $\bar{g}(\mathbf{a}) = 0$ for all $g \in G$, then $g(\mathbf{a}, \mathbf{b}) = 0$ for all $g \in G$. This implies

$$(\mathbf{a}, \mathbf{b}) \in V,$$

and $\mathbf{b} \in \pi_s(V)$ follows.

Prove the Special Case

Let $\overline{G} = \{\bar{\ell} \mid \ell \in G \setminus k[\mathbf{y}]\}$. Take $g, h \in G \setminus k[\mathbf{y}]$ and set

$$S := \mathrm{LC}_S(g)\,\frac{\mathbf{x}^\gamma}{\mathbf{x}^{\alpha(h)}}\,h - \mathrm{LC}_S(h)\,\frac{\mathbf{x}^\gamma}{\mathbf{x}^{\alpha(g)}}\,g$$

where $\mathbf{x}^\gamma = \mathrm{lcm}(\mathbf{x}^{\alpha(g)}, \mathbf{x}^{\alpha(h)})$. A standard representation $S = \sum_{\ell \in G} A_\ell\, \ell$ gives

$$\overline{\mathrm{LC}_S(g)}\,\frac{\mathbf{x}^\gamma}{\mathbf{x}^{\alpha(h)}}\,\bar{h} - \overline{\mathrm{LC}_S(h)}\,\frac{\mathbf{x}^\gamma}{\mathbf{x}^{\alpha(g)}}\,\bar{g} = \overline{S} = \sum_{\bar{\ell} \in \overline{G}} \overline{A_\ell}\,\bar{\ell}.$$

Then $\overline{\mathrm{LC}_S(g)} \neq 0$ and $\overline{\mathrm{LC}_S(h)} \neq 0$ imply:

- $\overline{S} = \sum_{\bar{\ell} \in \overline{G}} \overline{A_\ell}\,\bar{\ell}$ is a lcm representation.
- $\overline{S}$ is the S-polynomial of $\bar{g}, \bar{h}$ up to a constant.

Finish the Special Case

- $\overline{S} = \sum_{\bar{\ell}\in\overline{G}} \overline{A_\ell}\,\bar{\ell}$ is a lcm representation.
- $\overline{S}$ is the S-polynomial of $\bar{g},\bar{h}$ up to a nonzero constant.

These tell us that for every

$$\bar{g},\bar{h} \in \overline{G} = \{\bar{\ell} \mid \ell \in G \setminus k[\mathbf{y}]\},$$

the S-polynomial of $\bar{g},\bar{h}$ has a lcm representation with respect to $\overline{G}$. LCM Criterion $\Rightarrow$ $\overline{G}$ is a Gröbner basis of $\langle \overline{G} \rangle$.

Since $\overline{\mathrm{LT}_{\mathbf{x}}(g)} \neq 0$ for $g \in G \setminus k[\mathbf{y}]$, $\bar{g}$ is nonconstant for every $\bar{g} \in \overline{G}$. Consistency Theorem $\Rightarrow$ $\mathbf{V}(\overline{G}) \neq \emptyset$.

Hence there exits $\mathbf{a}$ such that $\bar{g}(\mathbf{a}) = 0$ for all $g \in G$. □

Saturation

Fix ideals $I, J \subseteq k[\mathbf{x}]$.

Definition

The saturation of I with respect to J is

$$I : J^\infty := \{f \in k[\mathbf{x}] \mid J^M f \subseteq I \text{ for } M \gg 0\}.$$

To see what this means geometrically, let

$$V := \mathbf{V}(I)$$
$$W := \mathbf{V}(J).$$

Then:

Lemma

$$\overline{V \setminus W} = \mathbf{V}(I : J^\infty).$$

Proof of the Closure Theorem

Proof. The goal is to find a variety $W \subseteq \mathbf{V}(I_s)$ such that

$$\mathbf{V}(I_s) \setminus W \subseteq \pi_s(V) \quad \text{and} \quad \overline{\mathbf{V}(I_s) \setminus W} = \mathbf{V}(I_s).$$

Let G be a reduced Gröbner basis of I that eliminates $\mathbf{x}$. Set

$$J := I_s + \langle \textstyle\prod_{g \in G \setminus k[\mathbf{y}]} \mathrm{LC}_s(g) \rangle.$$

Then

$$\mathbf{V}(J) = \bigcup_{g \in G \setminus k[\mathbf{y}]} \mathbf{V}(I_s) \cap \mathbf{V}(\mathrm{LC}_s(g)).$$

Notice that

$$\mathbf{b} \in \mathbf{V}(I_s) \setminus \mathbf{V}(J) \Rightarrow \overline{\mathrm{LC}_s(g)} \neq 0 \ \forall g \in G \setminus k[\mathbf{y}].$$

By Special Case, $\mathbf{b} \in \pi_s(V)$. Hence

$$\mathbf{V}(I_s) \setminus \mathbf{V}(J) \subseteq \pi_s(V).$$

Two Cases

Case 1. $\overline{\mathbf{V}(I_s)\setminus\mathbf{V}(\mathrm{LC}_s(g))} = \mathbf{V}(I_s)$ for all $g \in G \setminus k[\mathbf{y}]$.

Intersecting finitely many open dense sets is dense, so

$$\overline{\mathbf{V}(I_s)\setminus\mathbf{V}(J)} = \overline{\bigcap_{g\in G\setminus k[\mathbf{y}]} \mathbf{V}(I_s)\setminus\mathbf{V}(\mathrm{LC}_s(g))} = \mathbf{V}(I_s).$$

Thus the theorem holds with $W = \mathbf{V}(J)$.

Case 2. $\overline{\mathbf{V}(I_s)\setminus\mathbf{V}(\mathrm{LC}_s(g))} \subsetneq \mathbf{V}(I_s)$ for some $g \in G \setminus k[\mathbf{y}]$.

The strategy will be to enlarge I. First suppose that $\mathbf{V}(I_s) \subseteq \mathbf{V}(\mathrm{LC}_s(g))$. Then:

- $\mathrm{LC}_s(g)$ vanishes on $\mathbf{V}(I_s)$ and hence on V. Hence Nullstellensatz $\Rightarrow \mathrm{LC}_s(g) \in \sqrt{I}$.
- G reduced $\Rightarrow \mathrm{LC}_s(g) \notin I$ (since $\mathrm{LT}(\mathrm{LC}_s(g))$ divides $\mathrm{LT}(g)$).

Finish the Proof

Together, these bullets imply that

$$I \subsetneq I + \langle \mathrm{LC}_S(g) \rangle \subset \sqrt{I},$$

so in particular, $\mathbf{V}(I) = \mathbf{V}(I + \langle \mathrm{LC}_S(g) \rangle)$. So it suffices to prove the theorem for $I + \langle \mathrm{LC}_S(g) \rangle$ when $\mathbf{V}(I_S) \subseteq \mathbf{V}(\mathrm{LC}_S(g))$.

On the other hand, when $\mathbf{V}(I_S) \not\subseteq \mathbf{V}(\mathrm{LC}_S(g))$, we have a union of proper subsets

$$\begin{aligned} \mathbf{V}(I_S) &= \overline{\mathbf{V}(I_S) \setminus \mathbf{V}(\mathrm{LC}_S(g))} \cup (\mathbf{V}(I_S) \cap \mathbf{V}(\langle \mathrm{LC}_S(g) \rangle)) \\ &= \mathbf{V}(I_S : \mathrm{LC}_S(g)^\infty) \quad \cup \quad \mathbf{V}(I_S + \langle \mathrm{LC}_S(g) \rangle) \end{aligned}$$

Hence it suffices to prove the theorem for

$$I \subsetneq I + \langle I_S : \mathrm{LC}_S(g)^\infty \rangle \quad \text{and} \quad I \subsetneq I + \langle \mathrm{LC}_S(g) \rangle.$$

ACC $\Rightarrow$ these enlargements occur only finitely often. $\square$

Example

Consider $\mathbb{A}^4$ with variables w, x, y, z. Let $\pi_1 : \mathbb{A}^4 \to \mathbb{A}^3$ be projection onto the last three coordinates. Set

$$f = x^5 + x^4 + 2 - yz$$

and $I = \langle (y-z)(fw-1), (yw-1)(fw-1)\rangle$. This defines

$$V := \mathbf{V}(I) = \mathbf{V}(y-z, yw-1) \cup \mathbf{V}((x^5+x^4+2-yz)w-1) \subseteq \mathbb{A}^4.$$

Then:

- $\{g_1, g_2\} = \{(y-z)(fw-1), (yw-1)(fw-1)\}$ is a Gröbner basis of I for lex with $w > x > y > z$.
- $I_1 = 0$.

Furthermore,

$$g_1 = ((y-z)(x^5+x^4+2-yz))w + \cdots$$
$$g_2 = (y(x^5+x^4+2-yz))w^2 + \cdots$$

Continue Example

As in the proof of the Closure Theorem, let

$$\begin{aligned} J &= I_1 + \big\langle \textstyle\prod_{g \in G \setminus k[x,y,z]} \mathrm{LC}_1(g) \big\rangle \\ &= \langle (y-z)(x^5+x^4+2-yz) \cdot y(x^5+x^4+2-yz) \rangle \\ &= \langle y(y-z)(x^5+x^4+2-yz)^2 \rangle. \end{aligned}$$

This satisfies Case 1 of the proof, so that

$$\mathbf{V}(I_1) \setminus \mathbf{V}(J) = \mathbb{A}^3 \setminus \mathbf{V}(J) \subseteq \pi_1(V).$$

However,

$$\begin{aligned} \pi_1(V) = \big(\mathbb{A}^3 &\setminus \mathbf{V}(x^5+x^4+2-yz)\big) \cup \\ &\big(\mathbf{V}(y-z, x^5+x^4+2-yz) \setminus \mathbf{V}(x^5+x^4+2, y, z)\big). \end{aligned}$$

Constructible Sets

Definition

A set $S \subseteq \mathbb{A}^n$ is constructible if there are affine varieties $W_i \subseteq V_i \subseteq \mathbb{A}^n$, $i = 1, \ldots, N$, such that

$$S = \bigcup_{i=1}^{N} (V_i \setminus W_i).$$

Theorem

Let k be algebraically closed and $\pi_s : \mathbb{A}^n \to \mathbb{A}^{n-s}$ be projection onto the last $n-s$ coordinates. If $V \subseteq \mathbb{A}^n$ is an affine variety, then $\pi_s(V) \subseteq \mathbb{A}^{n-s}$ is constructible.

The proof of the Closure Theorem can be adapted to give an algorithm for writing $\pi_s(V)$ as a constructible set.

References

- T. Becker, V. Weispfenning, *Gröbner Bases*, Graduate Texts in Mathematics **141**, Springer, New York, 1993.
- D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, Third Edition, Undergraduate Texts in Mathematics, Springer, New York, 2007.
- P. Schauenberg, *A Gröbner-based treatment of elimination theory for affine varieties*, Journal of Symbolic Computation, to appear.