

Computational Algebraic Geometry

Lecture II - Division & Hidden Equations

Juliette Bruce (Dartmouth)

Review: ① We are interested in solving systems of polynomial equations

$$\textcircled{2} \quad V_K(I) = \{ \bar{x} \in K^n \mid f(\bar{x}) = 0 \quad \forall f \in I \} \quad \text{"variety"}$$

$$I(X) = \{ f \in K[x_1, \dots, x_n] \mid f(\bar{x}) = 0 \quad \forall \bar{x} \in X \} \quad \text{"defining ideal"}$$

③ Thm: (Hilbert's Nullstellensatz): If $K = \bar{K}$ then V and I are mutual inverses, inclusion reversing bijections:

$$\left\{ \begin{array}{c} \text{varieties} \\ \text{in } K^n \end{array} \right\} \xrightleftharpoons[I]{I} \left\{ \begin{array}{c} \text{radical ideals in} \\ K[x_1, \dots, x_n] \end{array} \right\}$$

④ Friends:

$$\bullet \text{ Circle - Parabola : } \langle x^2 - y, x^2 + y^2 - 1 \rangle \subseteq K[x, y]$$

$$\bullet \text{ Affine Twisted Cubic : } K \longrightarrow K^3 \quad t \longmapsto (t, t^2, t^3)$$

$$\langle y - x^2, z - xy \rangle \subseteq K[x, y, z]$$

Cor: If $K = \bar{K}$ then $V(I) = \emptyset$ if and only if $1 \in \sqrt{I}$

if $1 \in I \subseteq \sqrt{I} \Rightarrow V(I) = \emptyset$

• Ideal Membership Problem: Given an ideal $I \subseteq K[x_1, \dots, x_n]$ and $f \in K[x_1, \dots, x_n]$ how can we determine if $f \in I$.

$f \in I \iff \exists \theta_1, \dots, \theta_t \in I$ such that

$f = \theta_1 h_1 + \dots + \theta_t h_t$ for some h_i

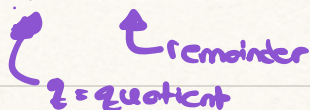
Solutions: ① If I is generated by linear poly. and f linear
(Gaussian Elimination)

② $K[x]$ Division Algorithm: Let $g \in K[x], g \neq 0$.

For every $f \in K[x]$ there exists unique polynomials

$q, r \in K[x]$ such that

$$f = gq + r \quad \text{if } \deg(r) < \deg(g)$$


 $q = \text{quotient}$
 $r = \text{remainder}$

Input: f and g

Output: q and r

Process: ① $P = f$ and $q = 0$

① while $P \neq 0$ and $\deg(P) \geq \deg(g)$

$$m = \frac{LT(P)}{LT(Q)} \quad Q = Q + m \quad P = P - mQ$$

③ Output Q and $r = P$

Cor: ① Every ideal in $K[x]$ is principal i.e. $I = \langle 0 \rangle$

② $f \in \langle 0 \rangle \iff$ the remainder $r = 0$.

$\langle y - x^2, z - xy \rangle \in K[x, y, z]$ Twisted Cubic

① This is not principal! $\rightsquigarrow$ Divide by lists

$$\textcircled{2} \quad xz - y^2 = y(x^2 - y) - x(xy - z)$$

$$\Rightarrow xz - y^2 \in I$$

$\uparrow$ what is the lead term?

$\rightsquigarrow$ Need extra data to define lead terms

• Def: A monomial order $\leq$ on $K[x_1, \dots, x_n]$ (or $\leq$ on $\mathbb{Z}_{\geq 0}^n$)

is a relation $\leq$ on the set of monomial (a relation

$\leq$ on $\mathbb{Z}_{\geq 0}^n$) such that

① $\leq$ is strict total order

$$m_1 \leq m_2, m_1 = m_2, m_2 \leq m_1$$

② if $m_1 \leq m_2$ and m is

monomial then

$$mm_1 \leq mm_2$$

① $\leq$ is strict well order

$$\textcircled{2} \quad \alpha \leq \beta \text{ then } \alpha + \gamma \leq \beta + \gamma$$

③ $\leq$ wellorder

every subset has min. elem

③ $\leq$ well ordering

these are bijections

• Ex: (Lex) $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ $\beta <_{\text{lex}} \alpha$ iff left most entry of $\alpha - \beta$ is positive.

(Graded Lex)

$\beta <_{\text{graded}} \alpha$ iff $\sum \alpha_i > \sum \beta_i$

α if $\sum \alpha_i = \sum \beta_i$

then $\alpha \geq_{\text{lex}} \beta$

~> We can define $LT_{\prec}(f)$ for any $f \in K[x_1, \dots, x_n]$

with respect to a monomial order $\prec$

Thm: Given a monomial order $\prec$ on $K[x_1, \dots, x_n]$ and ordered list

$(\theta_1, \theta_2, \dots, \theta_s)$ of non-zero polynomials there is a division algorithm such

input: $f \in K[x_1, \dots, x_n]$ and $(\theta_1, \dots, \theta_s)$

output: $(q_1, \dots, q_s)$ and r

such that

$$① \quad f = q_1 \theta_1 + q_2 \theta_2 + \dots + q_s \theta_s + r$$

② No monomial appearing in r is divisible by $LT(\theta_i)$ for all i .

* Depends on both $\leq$ and the order of the list *

Cor: If remainder $r=0 \Rightarrow f \in \langle \theta_1, \dots, \theta_s \rangle$



• Def: Let $\leq$ be monomial order on $k[x_1, \dots, x_n]$. If I

is an ideal. The initial ideal of I w.r.t $\leq$

$$in_{\leq}(I) = \langle LT_{\leq}(f) \mid f \in I, f \neq 0 \rangle$$

① $in_{\leq}(I)$ is a monomial ideal

② if $I = \langle \theta_1, \dots, \theta_s \rangle$ it can be the case

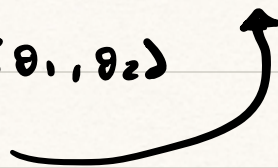
$$\langle LT_{\leq}(\theta_1), \dots, LT_{\leq}(\theta_s) \rangle \subsetneq in_{\leq}(I)$$

$$\underline{\text{Ex}}: \begin{array}{ccc} \langle y^2 - x^2, & z - xy \rangle & \subset \\ \parallel & \parallel & \\ \theta_1 & \theta_2 & \end{array}$$

$$\langle LT(\theta_1), LT(\theta_2) \rangle = \langle x^2, xy \rangle$$

$$f = xz - y^2 \in \langle \theta_1, \theta_2 \rangle$$

$$LT(f) = xz \notin$$



Def: Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal and $\leq$ be a monomial order.

A finite list $G = (g_1, \dots, g_s) \subseteq I$ is a Gröbner basis for I w.r.t $\leq$ if and only if

$$\langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle = \text{in}_<(I).$$

Thm: Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal, $G = (g_1, \dots, g_s)$ be a Gröbner basis for I w.r.t $\leq$.

1) If $f \in I$ and remainder of f divided G is 0
then $f \in I$

$$2) f \in I \iff \text{rem}_G(f) = 0$$

$$3) \langle g_1, \dots, g_s \rangle = I$$

Questions: ① Do Gröbner basis exist? Can find them?

② What is the geometry of initial ideals

Ex: $\langle x^2 - y \rangle \xrightarrow{\text{LCM}} \langle x \rangle = \text{in}_< \langle x^2 - y \rangle$

