Computational Algebraic Geometry

Lecture II - Division & Hidden Equations

Juliette Bruce (Dartmouth)

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

② $$\mathbb{V}_{\mathbb{K}}(I) = \{ \bar{x} \in \mathbb{K}^n \mid f(\bar{x}) = 0 \ \forall f \in I \}$$ "variety"

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

③ Thm: (Hilbert's Nullstenstatz): If $\mathbb{K} = \overline{\mathbb{K}}$ then $\mathbb{V}$ and $\mathbb{I}$ are mutal inveses, Inclusion revesing bijections

$$\begin{tikzcd} \left\{ \begin{matrix} \text{varieties} \\ \text{in } \mathbb{K}^n \end{matrix} \right\} \arrow[r, shift left, "\mathbb{I}"] & \left\{ \begin{matrix} \text{radical ideals in} \\ \mathbb{K}[x_1, \ldots, x_n] \end{matrix} \right\} \arrow[l, shift left, "\mathbb{V}"] \end{tikzcd}$$

④ Friends:

- Circle · Parabola : $\langle x^2 - y, x^2 + y^2 - 1 \rangle \subseteq \mathbb{K}[x,y]$
- Affine Twisted Cubic: $\mathbb{K} \longrightarrow \mathbb{K}^3 \quad t \longmapsto (t, t^2, t^3)$

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

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

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

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

$f \in I \iff \exists\, g_1, \dots g_t \in I$ such that

$f = g_1 h_1 + \dots + g_t h_t$ for some h_i

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

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

For every $f \in \Bbbk[x]$ there exists unique polynomials $q, r \in \Bbbk[x]$ such that

$$f = gq + r \quad \& \quad \deg(r) < \deg(g)$$

q = quotient, remainder

Input: f and g

Output: q and r

Process: ⓪ $p = f$ and $q = 0$

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

$$m = \frac{LT(p)}{LT(g)} \qquad q = q + m \qquad p = p - mg$$

③ Output q and $r = p$

Cor: ① Every ideal in $\mathbb{k}[x]$ is principal i.e $I = \langle g \rangle$

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

$\langle y - x^2, z - xy \rangle \subseteq \mathbb{k}[x, y, z]$ Twisted Cubic

① this is not principal! $\longrightarrow$ Divide by lists

② $xz - y^2 = y(x^2 - y) - x(xy - z)$

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

what is the lead term?

$\longrightarrow$ Need extra data to define lead terms

- **Def:** A monomial ord $\leq$ on $\mathbb{k}[x_1, \ldots x_n]$ (or $\preceq$ on $\mathbb{Z}^n_{\geq 0}$) is a relation $\leq$ on the set of monomial (a relation $\preceq$ on $\mathbb{Z}^n_{\geq 0}$) such that

① $\leq$ is strict total order $m_1 \leq m_2,\ m_1 = m_2,\ m_2 \leq m_1$	① $\preceq$ is strict well order
② if $m_1 \leq m_2$ and m is monomial then $mm_1 \leq mm_2$	② $\alpha \preceq \beta$ then $\alpha + \gamma \preceq \beta + \gamma$

③ $\leq$ wellorder

every subset has a min. elem

③ $\leq$ well ordering

there are bijections

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

(Graded Lex) $\beta <_{grlex} \alpha$ iff $\sum \alpha_i > \sum \beta_i$

or if $\sum \alpha_i = \sum \beta_i$

then $\alpha >_{lex} \beta$

$\rightsquigarrow$ We can define $LT_{<}(f)$ for any $f \in k[x_1, \dots x_n]$

with respect to a monomial order $\leq$

Thm: : Given a monomial order $\leq$ on $k[x_1, \dots x_n]$ and ordered list $(g_1, g_2, \dots g_s)$ of non-zero polynomials there is a division algorithm such

<u>input</u>: $f \in k[x_1, \dots x_n]$ and $(g_1, \dots g_s)$

<u>output</u>: $(q_1, \dots, q_s)$ and r

such that

① $f = q_1 g_1 + q_2 g_2 + \cdots q_s g_s + r$

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

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

Cor: If remainder $r = 0 \Rightarrow f \in \langle g_1, \ldots g_s \rangle$

$\not\Leftarrow$

• **Def**: Let $\leq$ be monomial order on $k[x_1, \ldots x_n]$. If I is an ideal. The initial ideal of I w/r/t $\leq$

$$\mathrm{in}_{\leq}(I) = \langle LT_{\leq}(f) \mid \underset{f \neq 0}{f \in I} \rangle$$

① $\mathrm{in}_{\leq}(I)$ is a monomial ideal

② if $I = \langle g_1, \ldots g_s \rangle$ it can be the case

$$\langle LT_{\leq}(g_1), \ldots LT_{\leq}(g_s) \rangle \subsetneq \mathrm{in}_{\leq}(I)$$

Ex: $\langle \underset{g_1}{y - x^2}, \underset{g_2}{z - xy} \rangle \subset$

$$\langle LT(g_1), LT(g_2) \rangle = \langle x^2, xy \rangle$$

$f = xz - y^2 \in \langle g_1, g_2 \rangle$

$LT(f) = xz \notin$

Def: Let $I \subseteq \mathbb{K}[x_1,\dots x_n]$ 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

$$\langle LT(g_1), \dots, LT(g_s)\rangle = in_<(I).$$

Thm: Let $I \subseteq \mathbb{K}[x_1, \dots x_n]$ 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 divide G is 0 then $f \in I$

2) $f \in I \iff rem_G(f) = 0$

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: $\langle x^2 - y \rangle \xrightarrow{\text{Lex}} \langle x \rangle = in_< \langle x^2 - y\rangle$