Ecuaciones Polinomiales y Algoritmos

Teresa Krick
Universidad de Buenos Aires & CONICET

elENA IX, 29/7 al 2/8, 2019

El caso de una variable

- $f_1, \ldots, f_s \in K[X]$ ¿tienen un cero en común $x \in K$?

$$\begin{cases} f_1(x) = 0 \\ \quad \vdots \\ f_s(x) = 0 \end{cases} \iff \operatorname{mcd}(f_1, \ldots, f_s)(x) = 0$$

$\Longrightarrow$ **Sí** si $\operatorname{mcd}(f_1, \ldots, f_s) \neq 1$ y K algebraicamente cerrado

- $f \in K[X]$ ¿f se anula en los ceros comunes de $f_1, \ldots, f_s$?

$\iff \sqrt{\operatorname{mcd}(f_1, \ldots, f_s)} \mid f$ si K algebraicamente cerrado

- ¿$f \in \langle f_1, \ldots, f_s \rangle$? $\leftarrow$ *ideal* generado por $\{f_1, \ldots, f_s\}$

$f \in \langle f_1, \ldots, f_s \rangle \iff \operatorname{mcd}(f_1, \ldots, f_s) \mid f$ en $K[X]$

El caso lineal

- $$\begin{cases} f_1 = a_{11}X_1 + \cdots a_{1n}X_n - b_1 \\ \quad \vdots \\ f_s = a_{s1}X_1 + \cdots a_{sn}X_n - b_s \end{cases}$$

  ¿tienen un cero en común $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$?

  $$\exists\, \mathbf{x} \in K^n \text{ t.q. } A\,\mathbf{x} = b \iff \mathrm{Rg}(A) = \mathrm{Rg}(A|b)$$

- $f \in K[\mathbf{X}]$ ¿f se anula en los ceros comunes de $f_1, \ldots, f_s$?

  $$\iff f(\mathbf{x}) = 0,\ \forall\, \mathbf{x} \in \mathcal{S} = \mathcal{S}_0 + \mathbf{y}$$

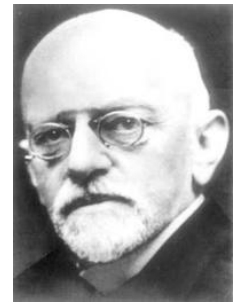
- ¿$f \in \langle f_1, \ldots, f_s \rangle$?

  $$f \in \langle f_1, \ldots, f_s \rangle \iff f \in \langle g_1, \ldots, g_t \rangle$$

  con $g_1, \ldots, g_t$ sistema escalonado (reducido) ...

El caso general

$f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ ¿tienen un cero en común $\mathbf{x} \in K^n$?



Teorema de los Ceros de Hilbert $\sim$ **1890**

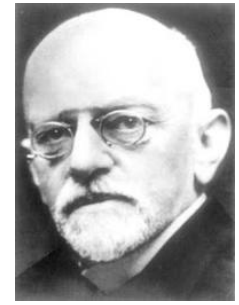
Si K es algebraicamente cerrado

$$\nexists\, \mathbf{x} \in K^n \text{ t.q. } \begin{cases} f_1(\mathbf{x}) = 0 \\ \vdots \\ f_s(\mathbf{x}) = 0 \end{cases} \iff 1 \in \langle f_1, \ldots, f_s \rangle$$

El caso general

$f \in K[X_1, \ldots, X_n]$ ¿f se anula en los ceros comunes de $f_1, \ldots, f_s$?

$\overbrace{\text{Variedad de } \{f_1, \ldots, f_s\}}$



Teorema de los Ceros de Hilbert $\sim$ **1890**

Si K es algebraicamente cerrado

$$f \text{ se anula en los ceros comunes de } f_1, \ldots, f_s$$
$$\Updownarrow$$
$$f \in \sqrt{\langle f_1, \ldots, f_s \rangle}$$

donde $\sqrt{\langle f_1, \ldots, f_s \rangle}$ es el **radical** *del ideal* $\langle f_1, \ldots, f_s \rangle$*:*

$$\sqrt{\langle f_1, \ldots, f_s \rangle} := \left\{ g \in K[\mathbf{X}] : \exists\, N \in \mathbb{N} \text{ t.q. } g^N \in \langle f_1, \ldots, f_s \rangle \right\}$$

El caso general

¿$f \in \langle f_1, \ldots, f_s \rangle$?

Algoritmo de División de Hironaka $\sim$ **1954**

En cualquier cuerpo K

Dividir $f = X^2Y + XY^2 + Y^2$ por $\{f_1 = Y^2 - 1, f_2 = XY - 1\}$

Se necesita un orden de monomios $\prec$
total, compatible con el producto, y $1 \prec \mathbf{X}^\alpha$, $\forall\, \alpha \neq \mathbf{0}$

Orden monomial

$\prec$ orden monomial en el conjunto de monomios si

- orden total
- compatible con el producto:

$$\mathbf{X}^{\alpha} \prec \mathbf{X}^{\beta} \Rightarrow \mathbf{X}^{\alpha+\gamma} \prec \mathbf{X}^{\beta+\gamma},\ \forall\, \gamma \in \mathbb{N}_0^n$$

- $1 \prec \mathbf{X}^{\alpha},\ \forall\, \alpha \neq \mathbf{0}$

Ejemplo: Orden lexicográfico puro con $X_1 \succ \cdots \succ X_n$

Propiedades: ($M_{\prec}(f)$ monomio de cabeza de f para $\prec$)

- $\prec$ es un buen orden
- $\mathbf{X}^{\alpha} \mid \mathbf{X}^{\beta} \ \Rightarrow\ \mathbf{X}^{\alpha} \preceq \mathbf{X}^{\beta}$
- $M_{\prec}(f+g) \leq \max\{M_{\prec}(f), M_{\prec}(g)\}$
- $M_{\prec}(f \cdot g) = M_{\prec}(f) \cdot M_{\prec}(g)$

Algoritmo de División de Hironaka

Dado $\prec$ orden lexicográfico con $X \succ Y$,

Dividir $f = X^2Y + XY^2 + Y^2$ por $\{f_1 = Y^2 - 1, f_2 = XY - 1\}$

- $f = (X+1) \cdot f_1 + X \cdot f_2 + r_1$ con $r_1 = 2X + 1$
- $f = 1 \cdot f_1 + (X+Y) \cdot f_2 + r_2$ con $r_2 = X + Y + 1$

$$\Longrightarrow \quad r_1 - r_2 = X - Y = -X \cdot f_1 + Y \cdot f_2 \in \langle f_1, f_2 \rangle$$

Pero por el algoritmo $\quad X - Y = 0 \cdot f_1 + 0 \cdot f_2 + (X - Y)$

Algoritmo de División

Dados $f, f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ y $\prec$ orden monomial

Divide f por $\{f_1, \ldots, f_s\}$

y obtiene

$$q_1, \ldots, q_s, r \in K[X_1, \ldots, X_n]$$

tales que

- $f = q_1 \cdot f_1 + \cdots + q_s \cdot f_s + r$
- Ningún monomio de r es divisible por algún $M_\prec(f_i)$, $1 \leq i \leq s$
- $M_\prec(q_i f_i) \preceq M_\prec(f)$ si $q_i \neq 0$

$$\Longrightarrow \quad M_\prec(r) \preceq M_\prec(f) \ \text{ si } \ r \neq 0$$

Bases de Gröbner

$$I = \langle f_1, \ldots, f_s \rangle \subset K[X_1, \ldots, X_n] \quad , \quad \prec$$

Base de Gröbner, Buchberger $\sim$ 1966

$G = \{g_1, \ldots, g_t\}$ es base de Gröbner de I para $\prec$ si

- $G \subset I$
- $f \in I \iff r_G(f) = 0$

Bases de Gröbner

Teorema de la base de Hilbert $\sim$ 1888, Lema de Dickson

Sea $M \subset K[X_1, \ldots, X_n]$ un *ideal monomial*, i.e.

$$M = \langle \mathbf{X}^\alpha : \alpha \in A \subset \mathbb{N}_0^n \rangle$$

Entonces M está generado por finitos de los $\mathbf{X}^\alpha,\ \alpha \in A$

$$I = \langle f_1, \ldots, f_s \rangle \subset K[X_1, \ldots, X_n], \quad M_\prec(I) := \langle M_\prec(f) : f \in I \rangle$$

Otra caracterización de base de Gröbner

$G = \{g_1, \ldots, g_t\}$ es base de Gröbner de I para $\prec$ si

- $G \subset I$
- $M_\prec(I) = \langle M_\prec(g_1), \ldots, M_\prec(g_t) \rangle$

Primeras propiedades de bases de Gröbner

Sea $G = \{g_1, \ldots, g_t\}$ base de Gröbner de I para $\prec$. Entonces

- $G \subset I$
- $M_\prec(I) = \langle M_\prec(g_1), \ldots, M_\prec(g_t)\rangle$
- $f \in I \iff r_G(f) = 0$
- $r_G(f)$ no depende del algoritmo de división elegido
- $I = \langle g_1, \ldots, g_t\rangle$

Algoritmo de construcción de base de Gröbner

$$X(Y^2-1)-Y(XY-1) = -X+Y$$
$$=: S(Y^2-1, XY-1) \quad \in \; I = \langle Y^2-1, XY-1\rangle$$

Los S-polinomios (o Polinomios de cancelación)

$f = a\,\mathbf{X}^{\alpha} + \overline{f}$ con $M_{\prec}(f) = \mathbf{X}^{\alpha}$, $g = b\,\mathbf{X}^{\beta} + \overline{g}$ con $M_{\prec}(g) = \mathbf{X}^{\beta}$

Sea

$$\mathbf{X}^{\gamma} = \text{mcm}\left(\mathbf{X}^{\alpha}, \mathbf{X}^{\beta}\right)$$

i.e. $\gamma_i = \max\{\alpha_i, \beta_i\}$, $1 \le i \le n$.
Entonces

$$S(f,g) := \frac{\mathbf{X}^{\gamma-\alpha}}{a}\cdot f - \frac{\mathbf{X}^{\gamma-\beta}}{b}\cdot g \quad \in \langle f, g\rangle$$

Algoritmo de construcción de base de Gröbner

Criterio de Buchberger

$G = \{g_1, \ldots, g_t\}$ es base de Gröbner de $\langle g_1, \ldots, g_t \rangle$ para $\prec$

$$\Updownarrow$$

$$\forall\ g, h \in G, \quad \exists\ q_1, \ldots, q_t \quad \text{t.q.}$$

- $S(g, h) = q_1 \cdot g_1 + \cdots + q_t \cdot g_t$
- $M_\prec(q_i \cdot g_i) \preceq M_\prec(S(g, h))$ si $q_i \neq 0$

$\rightsquigarrow$ **induce directamente un algoritmo!**

Construcción de base de Gröbner

$I = \langle f_1 = Y^2 - 1, f_2 = XY - 1 \rangle \in K[X, Y]$, $\prec$ o.lex. con $X \succ Y$

- $S(f_1, f_2) = -X + Y$

  $$r_{\{f_1, f_2\}}(-X + Y)) = -X + Y =: f_3$$

- $S(f_1, f_3) = -X + Y^3$

  $$r_{\{f_1, f_2, f_3\}}(-X + Y_3) = 0 : \quad -X + Y^3 = Y \cdot f_1 + f_3$$

- $S(f_2, f_3) = Y^2 - 1$

  $$r_{\{f_1, f_2, f_3\}}(Y^2 - 1) = 0 : \quad Y^2 - 1 = 1 \cdot f_1$$

$$\Longrightarrow \quad G_\prec = \{Y^2 - 1, XY - 1, -X + Y\}, \quad G'_\prec = \{Y^2 - 1, X - Y\}$$

Propiedad útil para base de Gröbner

Sea $G = \{g_1, \ldots, g_t\} \subset K[X_1, \ldots, X_n]$ t.q.

$$\text{mcd}(M_{\prec}(g_i)), M_{\prec}(g_j)) = 1, \forall\, i \neq j$$

Entonces G es base de Gröbner de $\langle g_1, \ldots, g_t \rangle$ para $\prec$

Volviendo al caso lineal:

$g_1, \ldots, g_t$ sistema escalonado es base de Gröbner de $\langle g_1, \ldots, g_t \rangle$!

Aplicaciones de bases de Gröbner

$f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ ¿tienen un cero en común $\mathbf{x} \in K^n$?

Por el Teorema de los ceros de Hilbert

para K algebraicamente cerrado

$\{f_1, \ldots, f_s\}$ no tienen cero común $\mathbf{x}$ en K^n

$\Updownarrow$

$1 \in \langle f_1, \ldots, f_s \rangle$

$\Updownarrow$

$1 \in G$ base de Grobner de $\langle f_1, \ldots, f_s \rangle$

Aplicaciones de bases de Gröbner

$f \in K[X_1, \ldots, X_n]$ ¿f se anula en los ceros comunes de $f_1, \ldots, f_s$?

Por el Teorema de los ceros de Hilbert

Para K algebraicamente cerrado

f se anula en los ceros comunes de $f_1, \ldots, f_s$

$$\Updownarrow$$

$$f \in \sqrt{\langle f_1, \ldots, f_s \rangle}$$

$$\Updownarrow$$

$$1 \in \langle f_1, \ldots, f_s, 1 - Y \cdot f \rangle \subset K[X_1, \ldots, X_n, Y]$$

Aplicaciones de bases de Gröbner

¿$f \in \langle f_1, \ldots, f_s \rangle$?

$$f \in \langle f_1, \ldots, f_s \rangle$$

$$\Updownarrow$$

$r_G(f) = 0$ para G base de Gröbner de $\langle f_1, \ldots, f_s \rangle$

Y más aún se pueden reconstruir $h_1, \ldots, h_s$ t.q.

$$f = h_1 \cdot f_1 + \cdots + h_s \cdot f_s$$

Y mucho más!!!

- Eliminación

$I = \langle f_1, \ldots, f_s \rangle \subset K[X_1, \ldots, X_n]$: ¿$I \cap K[X_2, \ldots, X_n]$?

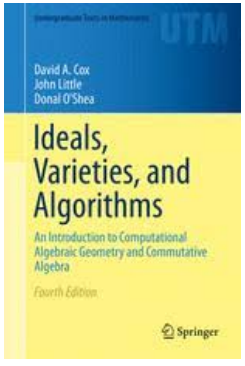
$$I \cap K[X_2, \ldots, X_n] = \langle G \cap K[X_2, \ldots, X_n] \rangle$$
donde G es una base de Gröbner de I
para el orden lexicográfico $X_1 \succ X_2 \succ \cdots \succ X_n$

- Intersección

$I = \langle f_1, \ldots, f_s \rangle, J = \langle g_1, \ldots, g_t \rangle \subset K[X_1, \ldots, X_n]$: ¿$I \cap J$?

$$I \cap J = \langle Yf_1, \ldots, Yf_s, (1-Y)g_1, \ldots, (1-Y)g_t \rangle \cap K[X_1, \ldots, X_n]$$

Referencia obligada



Ideals, Varieties and Algorithms,
David Cox, John Little & Donal O'Shea,
Springer Undergraduate Textes in Mathematics, 1996

FIN

¡Gracias!