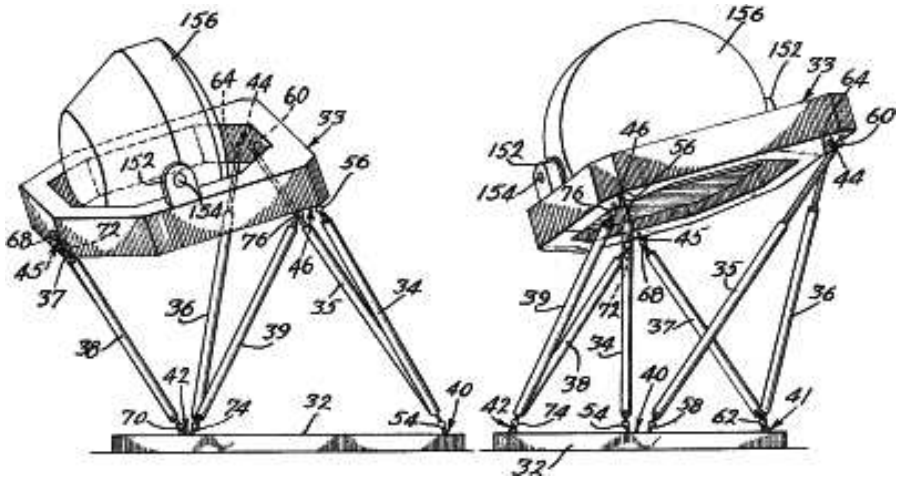
Resolución de Sistemas de Ecuaciones Polinomiales

Santiago Laplagne

Buenos Aires, 29 de septiembre de 2006

Aplicaciones - Robots paralelos



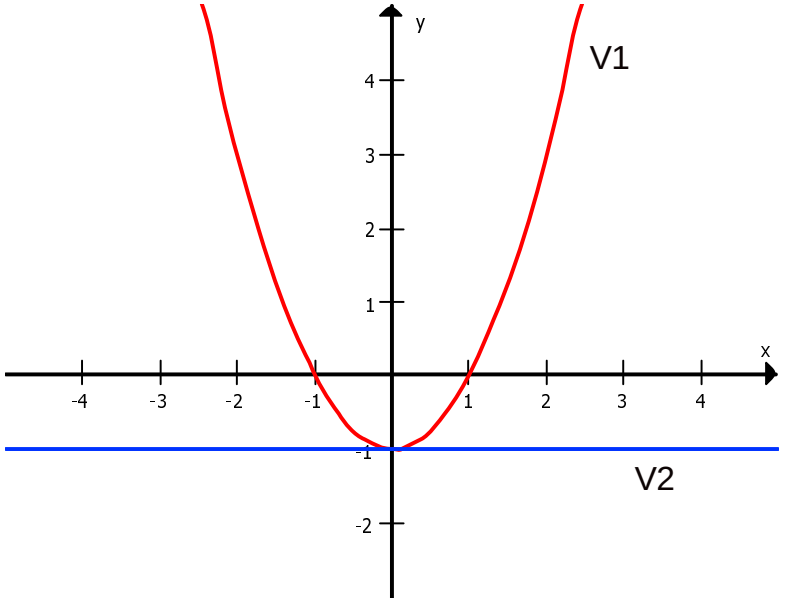
Se usan en simuladores de vuelo, cirugías, y...

¿Qué quiere decir "resolver"?

Queremos resolver

$$\begin{cases} f_1 &= (x^2-(y+1))(y+1)^2 = 0 \\ f_2 &= (x^2-(y+1))(x^2+(y+1))(y+1) = 0 \end{cases}$$

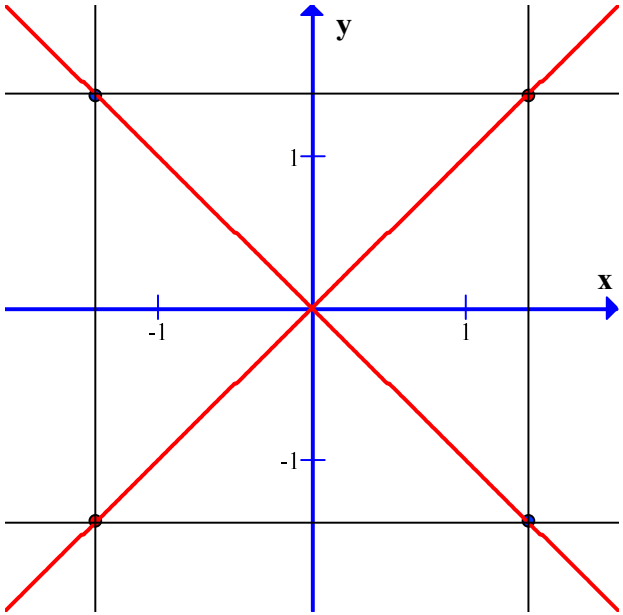
- $I = \langle f_1, f_2 \rangle$
- $V(I) = \{y = x^2 - 1\} \cup \{y = -1\}$
- $\sqrt{I} = \langle (y - x^2 - 1)(y+1) \rangle =$
  $\langle y - x^2 - 1 \rangle \cap \langle y + 1 \rangle$
  (descomponemos la variedad)
- $I = \langle y - x^2 - 1 \rangle \cap \langle y + 1 \rangle \cap$
  $\langle (y+1)^3, x^2 \rangle$
  (descomponemos el ideal)



Las variedad pueden tener varios puntos

Queremos resolver

$$I = \langle x^2 - 2, y^2 - 2 \rangle$$



$$\begin{aligned} S_1 =& \{x = \sqrt{2}, y = \sqrt{2}\} \cup \\ & \{x = \sqrt{2}, y = -\sqrt{2}\} \cup \\ & \{x = -\sqrt{2}, y = \sqrt{2}\} \cup \\ & \{x = -\sqrt{2}, y = -\sqrt{2}\} \end{aligned}$$

$$\begin{aligned} S_2 =& \{x = 1.41, y = 1.41\} \cup \\ & \{x = 1.41, y = -1.41\} \cup \\ & \{x = -1.41, y = 1.41\} \cup \\ & \{x = -1.41, y = -1.41\} \end{aligned}$$

$$\begin{aligned} S_3 =& \{x^2 = 2, x = y\} \cup \\ & \{x^2 = 2, x = -y\} \end{aligned}$$

Gröbner básico

Las bases de Gröbner son un sistema especial de generadores del ideal. Permiten calcular:

- *Pertenencia al ideal.* $f \in I$ sii el resto de dividir a f por los polinomios en una base de Gröbner de I es 0.
- *Intersección de ideales.*
- *Eliminación de variables.* Para calcular $I \cap k[x_{s+1}, \ldots, x_n]$, calcular una base de Gröbner usando un orden especial y quedarse con los polinomios en esas variables.
- *Saturación.*
  $I : f^\infty = \{g \in k[\boldsymbol{x}] / g f^s \in I \text{ para algún } s\} = \langle I, tf - 1\rangle \cap k[\boldsymbol{x}]$.
- *Pertenencia al radical.* $f \in \sqrt{I}$ sii $I : f^\infty = \langle 1\rangle$.

Primos minimales - El caso 0-dimensional

$I \subset k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, un ideal 0-dimensional:

- Tiene finitas soluciones.
- $\exists f_i(x_i) \in I \quad \forall 1 \leq i \leq n.$

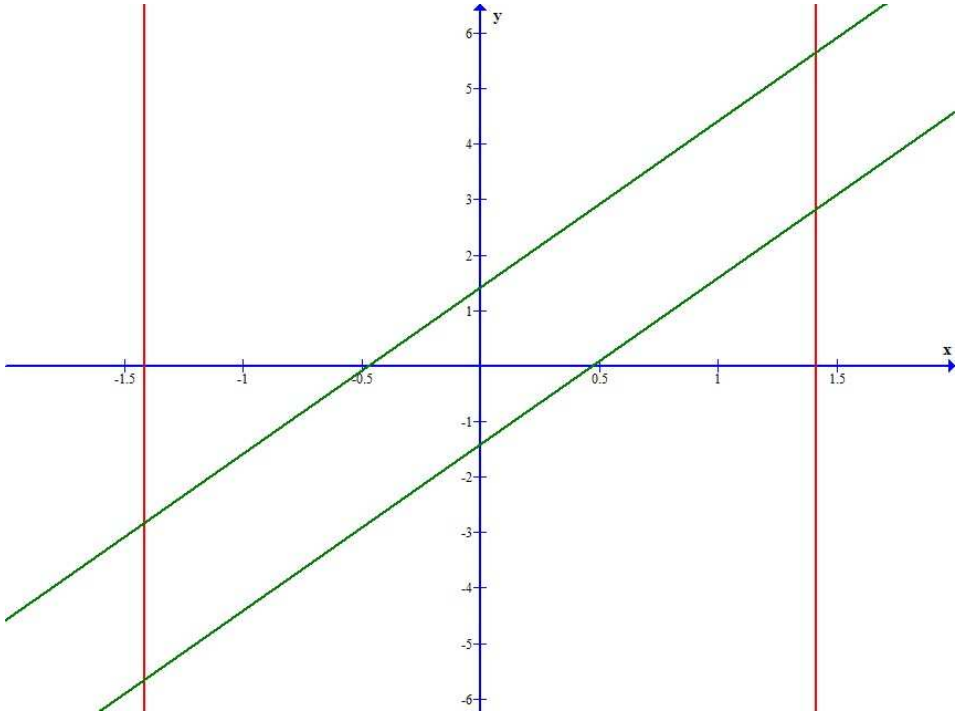
$\langle g \rangle = I \cap k[x_n]$, $g = g_1^{m_1} \ldots g_t^{m_t}$, la factorización.

$$I = \cap_{i=1}^{t} \langle I, g_i^{m_i} \rangle$$

Si x_n *separa puntos*, $\langle I, g_i \rangle$ son los primos minimales asociados.

Ejemplo.

- $I = \langle x^2 - 2, (y + 3x)^2 - 2 \rangle$
- $I \cap k[y] = y^4 - 40y^2 + 256 = (y^2 - 8)(y^2 - 32)$
- $I = \langle I, y^2 - 8 \rangle \cap \langle I, y^2 - 32 \rangle$



Primos minimales - El caso 0-dimensional

Si x_n no separa puntos, el algoritmo puede fallar.

A veces ninguna variable separa puntos. Se requiere un cambio de coordenadas al azar.

Ejemplo

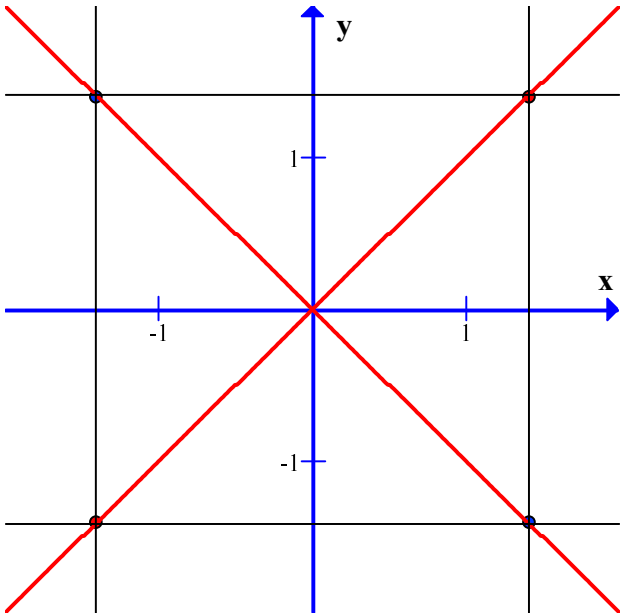
$I = \langle x^2 - 2, y^2 - 2 \rangle \subset \mathbb{Q}[x, y]$

$I \cap \mathbb{Q}[y] = \langle y^2 - 2 \rangle$

$I \cap \mathbb{Q}[x] = \langle x^2 - 2 \rangle$

Los dos polinomials son irreducibles.

Si hacemos el cambio de variables $\tilde{y} = y + 3x$, obtenemos el ejemplo de la transparencia anterior.



El caso general - Reduccion al caso 0-dimensional

Conjuntos independientes maximales

$\boldsymbol{u} \subset \boldsymbol{x}$ es *indepeniente* si

$$I \cap k[\boldsymbol{u}] = \langle 0 \rangle.$$

$\boldsymbol{u}$ es un *conjunto independiente maximal* si no está propiamente incluido en ninguno otro conjunto independiente.

Reducción. Si $\boldsymbol{u}$ es un conjunto independiente maximal,

$$Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$$

es 0-dimensional en $k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$. $Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$ se puede descomponer por el caso 0-dimensional.

Ejemplo. Sea

$$I = \langle y+z, xz^2w, x^2z^2 \rangle \subset \mathbb{Q}[x, y, z, w].$$

$\boldsymbol{u} = \{x, w\}$ es un conjunto independiente maximal.

$$I\ \mathbb{Q}(x, w)[y, z] = \langle y + z, z^2 \rangle$$

es 0-dimensional en $\mathbb{Q}(x, w)[y, z]$.

$$\sqrt{I\ \mathbb{Q}(x, w)[y, z]} = \langle y, z \rangle$$

es el único primo minimal asociado a $I\ \mathbb{Q}(x, w)[y, z]$.

¿Cómo usar el caso 0-dimensional?

$I = Q_1 \cap \cdots \cap Q_t$ (desconocida) s.t.

$Q_i \cap k[\boldsymbol{u}] = \{0\}$ para $1 \leq i \leq s$ y

$Q_i \cap k[\boldsymbol{u}] \neq \{0\}$ para $s+1 \leq i \leq t$

$Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] = \tilde{Q}_1 \cap \cdots \cap \tilde{Q}_{s'}$

Entonces:

- $s = s'$ y $P_i := \sqrt{Q_i} = \sqrt{\tilde{Q}_i} \cap k[\boldsymbol{x}]$, $\forall 1 \leq i \leq s$.
- La intersección $\sqrt{\tilde{Q}_i} \cap k[\boldsymbol{x}]$ se puede calcular (por saturación).
- Falta considerar $\sqrt{Q_{s+1}} \cap \cdots \cap \sqrt{Q_t}$.

El algoritmo de Gianni-Trager-Zacharias (1989)

Para todo h vale

$$\sqrt{I} = \sqrt{I : h^\infty} \cap \sqrt{(I, h)}$$

$\exists h \in k[\boldsymbol{u}]$ tal que
$J := Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] \cap k[\boldsymbol{x}] = (I : h^\infty)$
Ahora $\boldsymbol{u}$ no es independiente con respecto a $\langle I, h\rangle$.
Podemos descomponer $\sqrt{\langle I, h\rangle}$ por inducción en el número de conjuntos independientes.

Ejemplo. Tenemos

- $I = \langle y + z, xz^2w, x^2z^2\rangle$.
- $\sqrt{I\ \mathbb{Q}(x, w)[y, z]} \cap \mathbb{Q}[\boldsymbol{x}] = \langle y, z\rangle$.
- Podemos tomar $h := xw$.
  $I : h^\infty = \langle y + z, z^2\rangle = Ik(x, w)[y, z]$.
- $\sqrt{I} = \langle y, z\rangle \cap \sqrt{\langle I, xw\rangle}$.
- Siguiendo con el algoritmo, obtnenemos $\sqrt{\langle I, xw\rangle} = \langle y + z, x\rangle \cap \langle w, y, z\rangle$.

La última componente es redundante.

$$\sqrt{I} = \langle y, z\rangle \cap \langle y + z, x\rangle$$

Un nuevo algoritmo

$J := Ik(\boldsymbol{u})[\boldsymbol{x} \smallsetminus \boldsymbol{u}] \cap k[\boldsymbol{x}]$

$\sqrt{I} = \sqrt{J} \cap \sqrt{Q_{s+1} \cap \cdots \cap Q_t}$

Si $\sqrt{I} \neq \sqrt{J}$, $\exists g$ en cualquier conjunto de generadores de $\sqrt{J}$ tal que $g \notin \sqrt{I}$.

Entonces $\exists P$ primo minimal tal que $g \notin P$ y

$$(I : g^\infty) = \bigcap_{g \notin P_i} Q_i$$

es la intersección de algunas de las componentes $Q_{s+1}, \ldots, Q_t$.

Ejemplo.

- $I = \langle y + z, xz^2w, x^2z^2 \rangle$.
- $\sqrt{I : h^\infty} = \langle y, z \rangle$.
- Buscamos $g \in \langle y, z \rangle$ tal que $g \notin \sqrt{I}$ (usando Pertenencia al radical).
  Tomamos $g := z \notin \sqrt{I}$.
- $(I : z^\infty) = \langle y + z, xw, x^2 \rangle$ intersección de nuevas componentes primarias de I.

El nuevo algoritmo, la iteración

$J := Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}]$
Haciendo la reducción a dimensión 0 con $(I : g^\infty)$, obtenemos nuevas componentes de I: $P_1, \ldots, P_s$.
Tomamos $J := J \cap P_1 \ldots P_s$.
Buscamos $g \in J \setminus \sqrt{I}$.
Tomamos $(I : g^\infty)$ e iteramos.

- $I = \langle y + z, xz^2w, x^2z^2 \rangle$.
- $\langle y, z \rangle$ primo asociado.
- $I_2 := I : z^\infty = \langle y + z, xw, x^2 \rangle$ contiene sólo componentes primas nuevas de I.
- $\boldsymbol{u} := \{z, w\}$ es independiente maximal de I_2.
- $\sqrt{I_2\ \mathbb{Q}(z,w)[x,y]} \cap \mathbb{Q}[w,x,y,z] = \langle y + z, x \rangle$.
- $J = \langle y, z \rangle \cap \langle y + z, x \rangle = \langle y + z, xz \rangle$.
- Todos los generadores de J están en $\sqrt{I}$. Entonces, $\sqrt{I} \subset J \subset \sqrt{I}$.
- $\sqrt{I} = \langle y, z \rangle \cap \langle y + z, x \rangle$.

Table 1: Comparaciones de tiempos (en Singular)

Fuente	Código	Dim	Comps. prim.	Prim. min.	Comps. emb.	Nuevo	GTZ	Comentarios
DGP	1	3	4	4	0	39	41	
DGP	2	3	16	15	1	56	39	
DGP	5	3	9	7	2	*	*	
DGP	6	3	3	3	0	59	50	
DGP	12	1	25	25	0	138	125	
DGP	14	1	8	2	6	8	7	
DGP	16	8	4	4	0	1252	1227	
DGP	20	4	2	1	1	19	13	
DGP	21	9	9	1	8	3	3	
DGP	22	2	9	7	2	33	25	
DGP	25	5	7	5	2	96	81	
DGP	27	4	3	3	0	12	9	
DGP	28	7	2	2	0	30	28	
DGP	29	2	12	1	11	4	3	
DGP	30	1	14	14	0	314	573	
DGP	31	1	1	1	0	9	10	
DGP	32	2	17	8	9	21	14	
DGP	33	2	3	3	0	10	8	
CCT	L	7		8		522	5670	
CCT	M	5	3	3	0	55	49	
CCT	83	5	3	3	0	384	618	
CCT	C	5	4	4	0	201	750	
CCT	O	2	5	5	0	21	209	
NEW	8	9	4	4	0	281	*	From DGP25 & DGP28
NEW	9	3	11	8	3	120	*	From DGP31 & DGP32
NEW	10	3	11	8	3	69	*	From DGP31 & DGP32