Escuela de Invierno: Bases y Abanicos de Gröbner

Lara Bossinger

Universidad Nacional Autónoma de México, Unidad Oaxaca

Enero 2021

§1 Bases de Gröbner

Contenido

Ordenes parciales y totales

Definición 1

Para un conjunto P un orden parcial es una relación $\leq$ en P tal que para todos $x, y, z \in P$ tenemos

1. $x \leq x$ *(reflexividad);*
2. $x \leq y$ *y* $y \leq x$ *implica* $x = y$ *(antisimetría);*
3. $x \leq y$ *y* $y \leq z$ *implica* $x \leq z$ *(transitividad).*

Un orden total en P es un orden parcial tal que para todos $x, y \in P$ tenemos $x \leq y$ o $y \leq x$.

Monomios y ordenes monomiales

Sea k un cuerpo y $k[\mathbb{x}] = k[x_1, \ldots, x_n]$ el anillo de polinomios en las variables $x_1, \ldots, x_n$. Los monomios en $k[\mathbb{x}]$ son elementos de la forma

$$x^a := x_1^{a_1} \cdots x_n^{a_n}, \quad \text{con} \quad a = (a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}.$$

Sea $Mon \subset k[\mathbb{x}]$ el conjunto de monomios.

Definición 2

Un orden parcial en Mon se llama un buen orden si cumple

1. $1 \leq x^a$ *para todos* $1 \neq x^a \in Mon$;
2. *si* $x^a, x^b \in Mon$ *y* $x^a < x^b$ *también* $x^a x^c < x^b x^c \;\; \forall \;\; x^c \in Mon$.

Un orden monomial (o también orden de términos/monomios) es un orden total que es un buen orden.

Ejercicio 1

Sea $<$ *un orden monomial. Prueba que para ningún* $x^a \in Mon$ *existe una secuencia infinita descendiente de la forma* $x^a = x^{a_0} > x^{a_1} > x^{a_2} > \ldots$

El orden lexicografico y lexicografico reverso

El orden lexicografico $<_{lex}$ es el orden monomial definido como $x^a <_{lex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico graduado $<_{deglex}$ es el orden monomial definido como $x^a <_{deglex} x^b$ si y solo si

1. $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, o
2. $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ y $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico reverso $<_{revlex}$ es el orden monomial definido como $x^a <_{revlex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \max\{i : a_i - b_i \neq 0\}$.

Ejercicio 2

1. *¿Puedes dar una definición del orden lexicografico reverso graduado $<_{degrevlex}$?*
2. *Ordena todos los monomios de $k[x_1, x_2, x_3]$ con grado menos o igual a 3 con respeto a los ordenes $<_{lex}, <_{deglex}$ y $<_{revlex}, <_{degrevlex}$.*

Formas y ideales iniciales

Definición 3

Sea $<$ *un orden de monomios y* $f = \sum_{i=1}^{m} c_i x^{a_i} \in k[\mathbb{x}]$. *Definimos la forma inicial (o también el leading term) de* f *con respeto a* $<$ *como* $in_<(f) := c_j x^{a_j}$ *con* $x^{a_j} = \max_<\{x^{a_i} : c_i \neq 0\}$. *El coeficiente principal (o leading coefficient) es* c_j *y* x^{a_j} *es el leading monomial. Para un ideal* $I \subset k[\mathbb{x}]$ *definimos* $in_<(I) := \langle in_<(f) : 0 \neq f \in I\rangle$, *su ideal inicial con respeto a* $<$.

Ejercicio 3

Verifica lo siguiente para $x^a, x^b \in Mon$ *y* $f, g \in k[\mathbb{x}]$:

1. *si* x^a *divide* x^b, *entonces* $x^a \leq x^b$;
2. $in_<(x^a f) = x^a in_<(f)$;
3. $in_<(fg) = in_<(f) in_<(g)$;
4. $in_<(f+g) \leq \max\{in_<(f), in_<(f)\}$ *con igualdad si* $in_<(f) \neq in_<(g)$.

Base de Gröbner

Definición 4

Sea $I \subset k[\mathbb{x}]$ *un ideal y* $<$ *un orden monomial. Un conjunto finito* $\{g_1, \ldots, g_s\}$ *de elementos en* I *se llama una* ***base de Gröbner*** *de* I *con respeto a* $<$ *si*

$$in_<(I) = (in_<(g_1), \ldots, in_<(g_s)).$$

Ejemplo 1

Sea $<=<_{lex}$ *el orden lexicografico en* $S = k[x_1, \ldots, x_7]$ *con respeto a* $x_1 > \cdots > x_7$ *y sean* $f = x_1x_4 - x_2x_3$ *y* $g = x_4x_7 - x_5x_6$*. Entonces,* $in_<(f) = x_1x_4$ *y* $in_<(g) = x_4x_7$*. El conjunto* $\{f, g\}$ *no es una base de Gröbner para el ideal* $I = (f, g)$*:*
toma $h = x_7f - x_1g$*, pues* $in_<(h) = x_1x_5x_6 \notin (in_<(f), in_<(g))$ *(¡Verifícalo!).*

Verificar si un conjunto es una base de Gröbner es un ejercicio más complicado. Lo vamos a resolver de manera algoritmica en las siguientes clases.

Bases de Gröbner son conjuntos de generadores

Teorema 1

Sea I un ideal en $k[\mathbb{x}]$ y $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de I con respeto a un orden monomial $<$. Entonces G es un conjunto de generadores para I.

Prueba: Vamos a mostrar que cada $f \in I$ es un elemento en el ideal (G) de manera algoritmica. El Ejercicio 1 va a asegurar que nuestro algoritmo termina.
Sea $0 \neq f \in I$, entonces $in_<(f) \in in_<(I) = (in_<(g_1), \ldots, in_<(g_s))$. En particular, existe un $g_{i_0} \in G$ tal que $in_<(g_{i_0})$ divide $in_<(f)$[1].
Sea $x^{a_0} \in Mon$ tal que $in_<(f) = cx^{a_0} in_<(g)$ para algún $c \in k$.

[1] Ejercicio: Sea J un ideal generado de monomios $\{x^{\mathbf{a_1}}, \ldots, x^{a_t}\}$. Muestra que un monomio x^b partenece a J si y solo si existe un monomio x^c tal que $x^b = x^c x^{a_i}$ para algun $1 \leq i \leq t$.

Continuación: Definimos

$$h_0 = f - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0} \in I$$

donde c_0 y c_{i_0} son los coeficientes principales de f y de g_{i_0}. Nota que el monomio inicial de f ya no es presente en h_0. Con Ejercicio 3.3 concluimos $in_<(x^{a_0} g_{i_0}) = x^{a_0} in_<(g_{i_0})$ que implica $in_<(h_0) < in_<(f)$. Si $h_0 = 0$ tenemos $f \in (g_1, \ldots, g_s)$. Si $h_0 \neq 0$ continuamos con h_0 en el lugar de f. Obtenemos

$$h_1 = f - c_{i_1}^{-1} c_1 x^{a_1} g_{i_1} - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0},$$

donde $g_{i_1} \in G$ tal que $in_<(g_{i_1})$ divide $in_<(h_0) = c' x^{a_1} in_<(g_{i_1})$, con $c' \in k$. Además c_{i_1} y c_1 son los coeficientes principales de g_{i_1} y h_0. Como antes, $in_<(h_1) < in_<(h_0)$. Si $h_1 = 0$ tenemos $f \in (g_1, \ldots, g_s)$. Si $h_1 \neq 0$ continuamos.

Del Ejercicio 1 sabemos que este procedimiento va a acabar. Entonces nos da una expresión

$$f = \sum_{q=0}^{N} c_{i_q}^{-1} c_q x^{a_q} g_{i_q} \in (g_1, \ldots, g_s). \qquad \blacksquare$$

El teorema de la base de Hilbert

Como corolario inmediatamente obtenemos el famoso resultado de Hilbert:

Corolario 1

Cada ideal en el anillo de polinomios tiene un conjunto de generadores finito.

Vectores de peso

Definición 5

Sea $w \in \mathbb{R}^n$ *(un vector de peso) y* $f = \sum_{i=1}^{m} c_i x^{a_i} \in k[\mathbb{x}]$. *Definimos la forma inicial de* f *con respeto a* w*:*

$$in_w(f) = \sum_{j:\ w \cdot a_j = \max\{w \cdot a_i\}} c_j x^{a_j}.$$

El valor $w \cdot a \in \mathbb{R}$ *se llama el* w*-peso de* x^a. *Para un ideal* $I \subset k[\mathbb{x}]$ *el ideal inicial de* I *con respeto a* w *es* $in_w(I) := (in_w(f) : 0 \neq f \in I)$.

Ejercicio 4

Muestra que $in_w(f \cdot g) = in_w(f) \cdot in_w(g)$ *para cada* $f, g \in k[\mathbb{x}]$ *y* $w \in \mathbb{R}^n$.

Ejemplo 2

El ideal inicial con respeto a un vector de peso no necesariamente es generado de monomios. Por ejemplo, si $in_{(2,1)}(x_1 - x_2^2) = x_1 - x_2^2$.

Ejercicio: Espacio lineal

Ejercicio 5

1. *Sea $I \subset k[\mathbb{x}]$ un ideal homogéneo*[a]*. Toma $w = (1, \ldots, 1) \in \mathbb{R}^n$ y muestra que $in_w(I) = I$.*
2. *Para un ideal $I \subset k[\mathbb{x}]$ definimos su espacio lineal:*

$$\mathcal{L}(I) := \{w \in \mathbb{R}^n : in_x(I) = I\}.$$

Muestra que $\mathcal{L}(I)$ es un subespacio vectorial de $\mathbb{R}^n$. ¿Puedes dar un ejemplo de un ideal cuyos espacio lineal tiene dimensión más que uno?

[a] El grado total de un monomio x^a es $\sum_{i=1}^{n} a_i$. Un $f \in k[\mathbb{x}]$ es homogéneo, si todos los monomios de f tienen el mismo grado total. Un ideal $I \subset k[\mathbb{x}]$ es homogéneo si existe un conjunto de generadores $\{f_1, \ldots, f_t\}$ de I tal que cada f_j es homogéneo.

Orden monomial y vector de peso

Sea $w = (w_1, \ldots, w_n) \in \mathbb{R}^n_{\geq 0}$ y $<$ un orden de monomios para *"romper empates"*. Podemos definir un orden de monomios $<_w$ de la siguente manera: $x^a <_w x^b$ si y solo si

1. $\sum_{i=1}^n w_i(a_i - b_i) < 0$, o
2. $\sum_{i=1}^n w_i(a_i - b_i) = 0$ y $x^a < x^b$.

Ejercicio 6

Prueba que para cada ideal $I \subset k[\mathbb{x}]$ y cada $w \in \mathbb{R}^n$ tenemos $in_<(in_w(I)) = in_{<_w}(I)$. Se dice: el orden $<_w$ refine el vector de peso w.

Corolario 2

Sea $w \in \mathbb{R}^n_{\geq 0}$ y $I \subset k[\mathbb{x}]$ un ideal.

1. *Si G es una base de Gröbner para I con respeto a $<_w$, entonces $\{in_w(g) : g \in G\}$ es una base de Gröbner para $in_w(I)$ con respeto a $<$.*
2. *Si $in_w(I)$ es un ideal monomial, entonces $in_w(I) = in_{<_w}(I)$.*

Referencias §1

1. Herzog, Jürgen; Hibi, Takayuki: Monomial ideals. Graduate Texts in Mathematics, 260. Springer-Verlag London, Ltd., London, 2011. xvi+305 pp. ISBN: 978-0-85729-105-9
2. Bernd Sturmfels: Gröbner bases and convex polytopes, Volume 8 of American Mathematical Soc.1996

§2 Geometría poliedral

Contenido

Poliedros, politopos y conos

Definición 6

Un semiespacio cerrado (resp. abierto) en $\mathbb{R}^n$ *es un conjunto de puntos* $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ *que satisface*

$$a \cdot x = a_1 x_1 + \cdots + a_n x_n \geq b \quad (\textit{resp.} \quad a \cdot x > b)$$

para $a \in \mathbb{R}^n$ *y* $b \in \mathbb{R}$ *fijo.*

Definición 7

Un poliedro es una intersección de un numero finito de semiespacios cerrados en $\mathbb{R}^n$*. Se puede escribir como* $P = \{x \in \mathbb{R}^n : A \cdot x \leq b\}$ *donde* $A \in \mathbb{R}^{m \times n}$ *y* $b \in \mathbb{R}^m$*. Si* P *es acotado se llama un politopo. Si* $b = 0$*, existen vectores* $u_1, \ldots, u_m \in \mathbb{R}^n$ *tal que*

$$P = \mathrm{pos}(u_1, \ldots, u_m) := \{\lambda_1 u_1 + \cdots + \lambda_m u_m : \lambda_1, \ldots, \lambda_m \in \mathbb{R}_{\geq 0}\}.$$

En este caso P *se llama un cono (poliedral).*

Cada politopo se puede escribir como una envolvente convexa de un conjunto finito de puntos:

$$Q = \operatorname{conv}(v_1, \ldots, v_m) := \left\{ \sum_{i=1}^{m} \lambda_i v_i : \lambda_i \in \mathbb{R}_{\geq 0} \quad y \quad \sum_{i=1}^{m} \lambda_i = 1 \right\}.$$

Ejemplo 3

En $\mathbb{R}^3$ *el cuadrante es un cono:* $C = \{x \in \mathbb{R}^3 : \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \cdot x \geq 0\}$. *Si agregamos tres condiciones más, obtenemos un politopo:*

$$Q = \left\{ x \in \mathbb{R}^3 : \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \cdot x \geq \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \\ -1 \\ -1 \end{pmatrix} \right\}$$

De hecho, Q *es el cubo. Como envolvente convexa tenemos* $Q = \operatorname{conv}(0, e_1, e_2, e_3, e_1 + e_2, e_1 + e_3, e_2 + e_3, e_1 + e_2 + e_3)$ *donde* $\{e_1, e_2, e_3\}$ *es la base estándar de* $\mathbb{R}^3$*.*

Caras, dimensión y codimensión

Sea $P \subset \mathbb{R}^n$ un poliedro y $w \in \mathbb{R}^n$.

$$face_w(P) := \{u \in P : w \cdot u \geq w \cdot v \text{ para todos } v \in P\}.$$

Cada subconjunto de P que es de esta forma se llama una cara de P. En particular, $P = face_0(P)$ es una cara.

Ejercicio 7

¿Cuantas caras tiene el cubo Q del ejemplo anterior?

La dimensión de una cara de P es la dimensión del espacio afín que genera. La codimensión de una cara F de P es $\mathrm{codim}_P(F) := \dim P - \dim F$. Una cara de codimensión 1 se llama una faceta. Las caras de dimensión 0 se llaman las vértices y las de dimensión 1 son los bordes. Cada politopo es la envolvente convexa de sus vértices.

La suma de Minkowski

Definición 8

Para dos poliedros $P_1, P_2 \subset \mathbb{R}^n$ definimos su suma de Minkowski como

$$P_1 + P_2 := \{p_1 + p_2 : p_1 \in P_1, p_2 \in P_2\}.$$

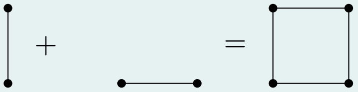
Ejercicio 8

Verifica que $face_w(P_1 + P_2) = face_w(P_1) + face_w(P_2)$. En particular, si v es un vértice de $P_1 + P_2$ existen vértices únicos $p_1 \in P_1$ y $p_2 \in P_2$ tal que $v = p_1 + p_2$.

Ejemplos

Ejemplo 4

1. *La suma de Minkowki de los dos politopos* $P_1 = conv(0, e_1) \subset \mathbb{R}^2$ *y* $P_2 = conv(0, e_2)$ *de dimensión una es el cuadrado* $Q = conv(0, e_1, e_2, e_1 + e_2)$ *de dimensión 2:*



2. *La suma de Minkowski del cuadrado* $Q \subset \mathbb{R}^2$ *con si mismo es el cuadrado más grande*

$$Q + Q = 2Q = conv(0, 2e_1, 2e_2, 2(e_1 + e_2)).$$

Nota que no toda suma de vértices es un vértice de la sume de Minkowski. Por ejemplo, $e_1 + e_2$ *no es vértice es* $2Q$.

Complejos poliédricos y abanicos

Definición 9

Un complejo poliédrico Δ *es una colección finita de poliedra en* $\mathbb{R}^n$ *tal que*

1. *si* $P \in \Delta$ *y* F *es una cara de* P*, entonces* $F \in \Delta$*;*
2. *si* $P_1, P_2 \in \Delta$*, entonces* $P_1 \cap P_2$ *es una cara de* P_1 *y de* P_2*.*

El soporte de Δ *es* $|\Delta| := \bigcup_{p \in \Delta} P$*. Si cada* $P \in \Delta$ *es un cono,* Δ *se llama un abanico. Si un abanico* Δ *cumple* $|\Delta| = \mathbb{R}^n$ *se llama completo.*

Podemos asociar un abanico a cada poliedro de la siguente manera: sea $P \subset \mathbb{R}^n$ un poliedro y F una cara de P. El cono normal de F en P es

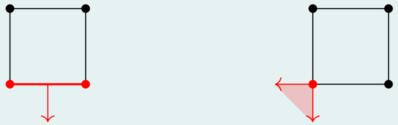
$$\mathcal{N}_P(F) := \{w \in \mathbb{R}^n : face_w(P) = F\}.$$

Ejemplo

Ejemplo 5

Para el cubo $Q = conv(0, e_1, e_2, e_1 + e_2)$ *y la cara* $F = conv(0, e_1)$ *tenemos* $face_{(0,-a)}(Q) = F$ *para todos* $a \in \mathbb{R}_{>0}$. *Entonces, el cono normal de* F *en* P *es* $\mathcal{N}_Q(F) = pos(-e_2)$.

Para el vértice $v = (0, 0)$ *de* Q *tenemos* $face_{(-a,-b)}(Q) = v$ *para todos* $a, b \in \mathbb{R}_{\geq 0}$. *Entonces* $\mathcal{N}_Q(v) = pos(-e_1, -e_2)$.



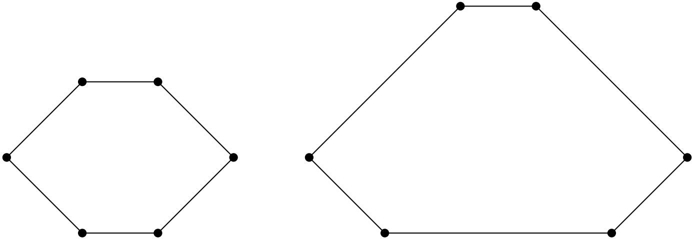
Sean F, F' dos caras del poliedro P. Entonces, F' es una cara de F si y solo si $\mathcal{N}_P(F)$ es una cara de $\mathcal{N}_P(F')$. En particular, la colección de todos los conos normales de caras de P es un abanico $\mathcal{N}(P)$, se llama el abanico normal de P.

Isomorfia

Definición 10

Dos politopos Q, Q' son fuertemente isomorfos si $\mathcal{N}(Q) = \mathcal{N}(Q')$.

Por ejemplo, los siguientes dos politopos en $\mathbb{R}^2$ son fuertemente isomorfos:



Politopos de Newton

Sea k un cuerpo y $k[\mathbb{x}] = k[x_1, \ldots, x_n]$ el anillo de polinomios en las variables $x_1, \ldots, x_n$. Los monomios en $k[\mathbb{x}]$ son elementos de la forma

$$x^a := x_1^{a_1} \cdots x_n^{a_n}, \quad \text{con} a = (a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}.$$

Para cada polinomio $f = \sum_{i=1}^m c_i x^{a_i} \in k[\mathbb{x}]$ asociamos su politopo de Newton:

$$New(f) := \text{conv}(a_i : i = 1, \ldots, m) \subset \mathbb{R}^n.$$

Ejercicio 9

Muestra que para cada $w \in \mathbb{R}^n$ y $f \in k[\mathbb{x}]$ tenemos $face_w(New(f)) = New(in_w(f))$.

Politopo de Newton y suma de Minkowksi

Lemma 1

Para $f, g \in k[\mathbb{x}]$ tenemos $New(f \cdot g) = New(f) + New(g)$.

Prueba del Lema 1: Es suficiente verificar que $New(f \cdot g)$ y la suma de Minkowskii $New(f) + New(g)$ tienen los mismos vértices. Nota que eso es claro si f y g son monomios porque $x^a x^b = x^{a+b}$.
Toma $w \in \mathbb{R}^n$ tal que $face_w(New(f \cdot g))$ y $face_w(New(f) + New(g))$ son vértices. En este caso también $in_w(f)$ y $in_w(g)$ son monomios (Ejercicio 9). Escoge w de esta manera es posible porque tenemos lo siguiente para cada polihedro P

$$face_{w'}(face_w(P)) = face_{w+\epsilon w'}(P), \text{ para } \epsilon > 0 \text{ suficientemente pequeño.}$$

Continuación: Calculamos

$$
\begin{aligned}
face_w(New(f \cdot g)) &\overset{\text{Ejercicio 9}}{=} New(in_w(f \cdot g)) \\
&\overset{\text{Ejercicio 4}}{=} New(in_w(f) \cdot in_w(g)) \\
&\overset{\text{monomios}}{=} New(in_w(f)) + New(in_w(g)) \\
&\overset{\text{Ejercicio 9}}{=} face_w(New(f)) + face_w(New(g)) \\
&\overset{\text{Ejercicio 8}}{=} face_w(New(f) + New(g)).
\end{aligned}
$$

Escogiendo varios $w \in \mathbb{R}^n$ vamos a encontrar a todos los vértices de los dos politopos. Entonces, concluimos que son iguales. ■

Comentario 1

Generalizar el politopo de Newton de polinomios a ideales vamas a llegar a los politopos de estado que es muy importante para los abanicos de Gröbner.

Ejercicios

1. Instala `polymake` en tu computadora (`https://polymake.org`)
2. Ver las funciones básicas que tiene, por ejemplo aqui: `https://www.math.ucdavis.edu/~deloera/TEACHING/RMMC2011/polymake_reference.html`
3. Usando polymake, verifica Lema 1 para $f = 2x^2y + xy^3 + 4z^4$ y $g = (x - y)(1 + z^2)$. (Puedes proceder como en la prueba y verificar que $New(f \cdot g)$ y $New(f) + New(g)$ tienen los mismos vértices.)
4. Usando polymake, verifica que los dos politopos abajo de la Definición 10 son fuertemente isomorfos. (Primero, da les coordenadas)

Referencias §2

1. Bernd Sturmfels: Gröbner bases and convex polytopes, Volume 8 of American Mathematical Soc.1996
2. Rekha R. Thomas: Lectures in Geometric Combinatorics, Student Mathematical Library, 33. IAS/Park City Mathematical Subseries. American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2006. viii+143 pp. ISBN: 0-8218-4140-8

y para profundizar el tema:

- Günter Ziegler: Lectures on polytopes. Graduate Texts in Mathematics, 152. Springer-Verlag, New York, 1995. x+370 pp. ISBN: 0-387-94365-X

§3 Algoritmos

Contenido

El Algoritmo de división

Teorema 2

Sean $<$ un orden de monomios en $k[\mathbb{x}]$ y $g_1, \ldots, g_s \in k[\mathbb{x}]$ no cero. Para cada polinomio $f \in k[\mathbb{x}]$ existen polinomios $f_1, \ldots, f_s, f' \in k[\mathbb{x}]$ con

$$f = f_1 g_1 + f_2 g_2 + \cdots + f_s g_s + f', \quad \textit{tal que}$$

1. *si $f' \neq 0$ tenemos para cada x^a monomio de f' que $x^a \notin (in_<(g_1), \ldots, in_<(g_s))$;*
2. *si $f_i \neq 0$ tenemos $in_<(f) \geq in_<(f_i g_i)$.*

Definición 11

*En la notación del teorema, la expresión $f_1 g_1 + f_2 g_2 + \cdots + f_s g_s + f'$ de f se llam a la **expresión estándar** de f con respeto a $g_1, \ldots, g_s$. El polinomio f' se llama el **resto** de f con respeto a $g_1, \ldots, g_s$. Si $f' = 0$ digamos que f **reduce a cero** con respeto a $\{g_1, \ldots, g_s\}$.*

Prueba del Teorema 2: Como en la prueba del Teorema 1 vamos a usar el Ejercicio 1 y proceder de manera algorítmica.
Sea $I := (in_<(g_1), \dots, in_<(g_s))$. Si ningún monomio de f esta en I toma $f' = f$ y $f_1 = \cdots = f_s = 0$.
Suponga que existe un monomio x^a de f que esta en I y sea x^{a_0} el monomio más grande (con respeto a $<$) de f que esta en I. Entonces existe un g_{i_0} y un monomio x^{b_0} tal que $in_<(g_{i_0})x^{b_0} = x^{a_0}$. Escribimos

$$f = c_0' c_{i_0}^{-1} x^{b_0} g_{i_0} + h_1$$

donde c_0' es el coeficiente de x^{a_0} en f y c_{i_0} es el coeficiente principal de g_{i_0}.
Entonces,

$$in_<(x^{b_0} g_{i_0}) = x^{b_0} in_<(g_{i_0}) = x^{a_0} \leq in_<(f).$$

Si $h_1 = 0$ o, si $h_1 \neq 0$ pero ningún monomio de h_0 esta en I, entonces $f = c_0' c_{i_0}^{-1} x^{b_0} g_{i_0} + h_1$ es una expresión estándar de f con respeto a $g_1, \dots, g_s$.

Continuación: Falta el caso $h_1 \neq 0$ y existe un monomio de h_1 que esta en I. Sea x^{a_1} el monomio más grande de ellos. Tenemos $x^{a_0} > x^{a_1}$. Nota que ningún monomio de h_1 que pertenece a I puede ser más grande que x^{a_0} y x^{a_0} no puede ser monomio de h_1.
Seguimos como con el primer monomio y obtenemos una expresión

$$f = c_0' c_{i_0}^{-1} x^{b_0} g_{i_0} + c_1' c_{i_1}^{-1} x^{b_1} g_{i_1} + h_2$$

donde $x^{a_0} = x^{b_0} in_<(g_{i_1})$ para algún $g_{i_1} \in \{g_1, \ldots, g_s\}$, c_1' es el coeficiente de x^{a_1} en f y c_{i_1} es el coeficiente principal de g_{i_1}. Tenemos

$$in_<(x^{b_1} g_{i_1}) < in_<(x^{b_0} g_{i_0}) \leq in_<(f).$$

Continuando este procedimiento obtenemos una secuencia $x^{a_0} > x^{a_1} > x^{a_2} > \ldots$ que según Ejercicio 1 termina después de N pasos para algún N.

Ejercicio 10

Para finalizar la prueda, verifica que esta secuencia nos da una expresión estándar de f con respeto a $g_1, \ldots, g_s$.

Unicidad del resto

En general el resto de un polinomio f no es único.

Ejercicio 11

¿Puedes dar un ejemplo de f y $\{g_1, \dots, g_s\}$ tal que el resto de f no es único?

Lemma 2

Sea $\mathcal{G} = \{g_1, \dots, g_s\}$ es una base de Gröbner para $I = (g_1, \dots, g_s)$ con respeto a $<$. En este caso cada polinomio $f \in k[\mathbb{x}]$ tiene un resto único con respeto a $\mathcal{G}$.

Prueba: Supongamos que existen dos restos $f' \neq f''$ de f con respeto a $\mathcal{G}$. Una consecuencia del Teorema 2 es que $f' - f'' \in I$. Entonces, $h := in_<(f' - f'') \in in_<(I)$. El monomio h es un monomio no cero en f' o f''. Pero f' y f'' son restos de f con respeto a $\mathcal{G}$. En particular, eso implica que ninguno de los monomios $in_<(g_1), \dots, in_<(g_s)$ divide h. Entonces, $h \notin (in_<(g_1), \dots, in_<(g_s))$, que es una contradicción. ∎

Aplicación: Pertenencia a un ideal

El siguiente Corolario muestra la utilidad de bases de Gröbner para resolver el problema de la pertenencia a un ideal:

Corolario 3

Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ es una base de Gröbner para $I = (g_1, \ldots, g_s)$ con respeto a $<$. Entonces, $f \in I$ si y solo si el resto único de f con respeto a $\mathcal{G}$ es cero.

Ejercicio 12

1. *Muestra el Corolario 3.*
2. *¿Conoces algún problema que se puede reformular como el problema de la pertenencia a un ideal? Si no, da le una búsqueda en google.*

Bases de Gröbner reducidas, minimales y universales

Definición 12

Una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_s\}$ se llama

- *reducida si satisface:*
  1. *el coeficiente principal de g_i es 1 para $1 \leq i \leq s$,*
  2. *si $i \neq j$ ningún monomio de g_j es divisible por $in_<(g_i)$;*
- *minimal si ningún monomio en el conjunto $\{in_<(g) : g \in G\}$ es redundante;*
- *universal si es una base de Gröbner para cada orden monomial $<$ simulaneamente.*

Teorema 3

Para cada ideal I y cada orden monomial $<$ existe una única base de Gröbner reducida (sea $\mathcal{G}_{\mathrm{red}}(I;<)$). Además, para dos ideal I y J tenemos

$$I = J \Leftrightarrow \mathcal{G}_{\mathrm{red}}(I;<) = \mathcal{G}_{\mathrm{red}}(J;<).$$

S-polinomios

Sean $f, g \in k[\mathbb{x}]$ y c_f, c_g los coeficientes de $in_<(f), in_<(g)$ en f, g, y sea $lcm(in_<(f), in_<(g))$ el *mínomo común múltiplo* de $in_<(f)$ y $in_<(g)$.

Definición 13

El S-polinomio de f y g es

$$S(f,g) := \frac{lcm(in_<(f), in_<(g))}{c_f\, in_<(f)} f - \frac{lcm(in_<(f), in_<(g))}{c_g\, in_<(g)} g.$$

Ejemplo 6

Como en el Ejemplo 1 toma $f = x_1x_4 - x_2x_3$ y $g = x_4x_7 - x_5x_6$ y $<=<_{lex}$. Entonces, $in_<(f) = x_1x_4$ y $in_<(g) = x_4x_7$. Pues $lcm(in_<(f), in_<(g)) = x_1x_4x_7$ y

$$S(f,g) = \frac{x_1x_4x_7}{x_1x_4} f - \frac{x_1x_4x_7}{x_4x_7} g = x_7 f - x1g = -x_2x_3x_7 + x_1x_5x_6.$$

Entonces, $S(f,g) \in (f,g)$ pero $in_<(S(f,g)) \notin (in_<(f), in_<(g))$.

El criterio de Buchberger

Ejercicio 13

Sean $0 \neq f, g \in k[\mathbb{x}]$ tal que $lcm(in_<(f), in_<(g)) = in_<(f)in_<(g)$ (se dice $in_<(f)$ y $in_<(g)$ son coprimos). Entonces, $S(f,g)$ reduce a cero con respeto a $\{f,g\}$.

El siguiente es el resultado más importante el la teoría de Gröbner:

Teorema 4 (El criterio de Buchberger)

Sea I un ideal no cero de $k[\mathbb{x}]$ y $\mathcal{G} = \{g_1, \ldots, g_s\}$ un conjunto de generadores de I. Entonces $\mathcal{G}$ es una base de Gröbner si y solo si

$$\forall\ i \neq j, \quad S(g_i, g_j) \quad \text{reduce a cero con respeto a } \mathcal{G}. \tag{0.1}$$

Prueba del Teorema 4:

$\Rightarrow$ Si $\mathcal{G}$ es una base de Gröbner cada $f \in I$ reduce a cero con respeto a $\mathcal{G}$ (Corolario 3). Entonces, $S(g_i, g_j) \in I$ reduce a cero.

$\Leftarrow$ Ejercicio.

El algoritmo de Buchberger

Input: $I = (g_1, \ldots, g_s)$ un ideal y $<$ un orden monomial;
Output: una base de Gröbner para I y $<$;

Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ y $N = \{1, \ldots, s\}$

1. calcula $S(g_i, g_j)$ para todos $i \neq j \in N$;
2. si $S(g_i, g_j)$ reduce a cero con respeta a $\mathcal{G}$, **retorno** $\mathcal{G}$;
   ($\mathcal{G}$ es una base de Gröbner según el criterio de Buchberger)
3. si existe un $S(g_i, g_j)$ con resto g_{s+1} con respeto a $\mathcal{G}$, sustituye
   $\mathcal{G} \leftarrow \mathcal{G} \cup \{g_{s+1}\}$,
   $N \leftarrow N \cup \{s+1\}$,
   y regresa al paso (1).

Ejercicio 14

Escribe un pseudo código para el Algoritmo de Buchberger.

Mejorar el algoritmo de Buchberger

En general no es necessario calcular *todos* los S-polinomios en el algoritmo de Buchberger.

Lemma 3

Sean $0 \neq g_1, \ldots, g_s$ *polinomios tal que* $in_<(g_i)$ *son coprimos para todos* $i \neq j$. *Entonces,* $\{g_1, \ldots, g_s\}$ *es una base de Gröbner para* $I = (g_1, \ldots, g_s)$.

Prueba: Ejercicio. Muestra primero lo siguiente:
Sean $c_a x^a$ un monomio y $f_1, \ldots, f_s$ polinomios tal que $in_<(f_i) = c_a x^a$ para todos los i. Sea $g = \sum_{i=1}^{s} b_i f_i \neq 0$ con $b_i \in k$ tal que $in_<(g) < c_a x^a$.
Entonces g es una combinatión linear de los S-polinomios
$S(f_j, f_k), 1 \leq j, k \leq s$.

El siguiente resultado reduce todavía más el número de S-polinomios cuyos calculó es necesario:

Proposición 1

Sea I un ideal en $k[\mathbb{x}]$ y $\mathcal{G} = \{g_1, \ldots, g_s\}$ un conjunto de generadores. Definimos un epimorfismo de $k[\mathbb{x}]$-módulos:

$$\epsilon : k[\mathbb{x}]^s \twoheadrightarrow (in_<(g_1), \ldots, in_<(g_s)), \quad con \quad e_i \mapsto in_<(g_i),$$

donde $\{e_1, \ldots, e_s\}$ es la base estándar de $k[\mathbb{x}]^s$. Entonces tenemos

1. $\forall\ 1 \leq i < j \leq s$ *los elementos $r_{i,j}$ generan el núcleo de ϵ donde*

$$r_{i,j} := \frac{lcm(in_<(g_i), in_<(g_j))}{in_<(g_j)} e_j - \frac{lcm(in_<(g_i), in_<(g_j))}{in_<(g_i)} e_i$$

2. *Sea $\mathcal{R}$ un subconjunto de los $r_{i,j}$ tal que $\mathcal{R}$ genera el núcleo de ϵ. Entonces, $\mathcal{G}$ es una base de Gröbner si y solo si para cada $r_{i,j} \in \mathcal{R}$ el S-polinomio $S(g_i, g_j)$ reduce a cero con respeto a $\mathcal{G}$.*

Ejercicios: Computaciones en Macaulay2

1. Instala `Macaulay2` en tu computadora. Para Windows: `https://gist.github.com/eivan/cab0b0a29eebd91d767ea6ad7448368e` Alternativamente hay una versión en línea: `http://habanero.math.cornell.edu:3690/`
2. En M2: define un anillo de polinomios y especifica un orden de monomios (ver `MonomialOrder`[2]);
3. Usando las funciones `lcm`[3] y `leadTerm`[4] calula los S-polinomios;
4. Usando la función `gb` calcula una base de Gröbner;

For example for the ideal $I = (x_1x_3 - x_2^2 - 1, x_2x_4 - x_3 - 1, x_3x_5 - x_4^2 - 1, x_4x_6 - x_5 - 1, x_1x_5 - x_6^2 - 1, x_2x_6 - x_1 - 1) \subset \mathbb{Q}[x_1, \ldots, x_6]$.

[2] `http://www2.macaulay2.com/Macaulay2/doc/Macaulay2/share/doc/Macaulay2/Macaulay2Doc/html/___Monomial__Order.html`

[3] `https://faculty.math.illinois.edu/Macaulay2/doc/Macaulay2/share/doc/Macaulay2/Macaulay2Doc/html/_lcm.html`

[4] `https://faculty.math.illinois.edu/Macaulay2/doc/Macaulay2/share/doc/Macaulay2/Macaulay2Doc/html/_lead__Term.html`

Referencias §3

1. Herzog, Jürgen; Hibi, Takayuki: Monomial ideals. Graduate Texts in Mathematics, 260. Springer-Verlag London, Ltd., London, 2011. xvi+305 pp. ISBN: 978-0-85729-105-9
2. Bernd Sturmfels: Gröbner bases and convex polytopes, Volume 8 of American Mathematical Soc.1996

§4 Abanicos de Gröbner

Contenido

Bases de monomios estándar

Definición 14

Sean $<$ *un orden de monomios y* I *un ideal. Los monomios* $x^a \notin in_<(I)$ *se llaman monomios estándar. El conjunto*

$$\mathbb{B}_< := \{\bar{x}^a \in k[\mathbb{x}]/I : x^a \notin in_<(I)\}$$

se llama una base de monomios estándar.

Ejercicio 15

Muestra que $\mathbb{B}_<$ *es una* k*-base (como espacio vectorial) de* $k[\mathbb{x}]/in_<(I)$ *y de* $k[\mathbb{x}]/I$ *para cada ideal* I *y cada orden monomial* $<$*.*

Conos de vectores de peso

Recuerda el ideal inicial con respeto a un vector de peso.

Definición 15

Sea $I \subset k[\mathbb{x}]$ un ideal. Dos vectores de peso $v, w \in \mathbb{R}^n$ se llaman equivalente *(con respeto a I) si $in_v(I) = in_w(I)$. La clase de equivalencia de un $w \in \mathbb{R}^n$ sea $C[w]$.*

Proposición 2

Para cada $w \in \mathbb{R}^n$ su clase de equivalencia $C[w]$ es un cono convexo poliédrico relativamente abierto en $\mathbb{R}^n$, o equivalentemente $C[w]$ es la intersección de un numero finito de semi espacios abiertos y hiperplanos.

Prueba: Sea $<$ un orden monomial y $<_w$ el orden inducida por w y $<$. Sea $\mathcal{G}$ la base de Gröbner reducida de I con respeto a $<_w$.

Afirmación: $C[w] = \{v \in \mathbb{R}^n : in_v(g) = in_w(g) \ \forall \ g \in \mathcal{G}\} =: C_{\mathcal{G}}[w]$.
Prueba de la afirmación: Tenemos que probar lo siguiente:

1. $C_{\mathcal{G}}[w]$ es una intersección finita de hiperplanos y semiespacios abiertos,
2. $C[w] \supseteq C_{\mathcal{G}}[w]$, y
3. $C[w] \subseteq C_{\mathcal{G}}[w]$.

1. Nota que $v \in C_{\mathcal{G}}[w]$ si y solo si cumple para cada $g \in \mathcal{G}$:

$$\begin{cases} v \cdot a = v \cdot b & \forall \ x^a, x^b \text{ monomio no cero en } in_w(g), \text{ y} \\ v \cdot a > v \cdot c & \quad \forall \ x^c \text{ monomio en } g \text{ y no en } in_w(g). \end{cases} \tag{0.2}$$

   Los igualdades definen hiperplanos en $\mathbb{R}^n$ y los desigualdades definen semiespacios abiertos en $\mathbb{R}^n$.

2. Sea $v \in C_{\mathcal{G}}[w]$. Recuerda de Ejercicio 6: $in_{<_w}(I) = in_<(in_w(I))$ y de Corolario 2(1): $\{in_w(g) : g \in \mathcal{G}\}$ es una base de Gröbner de $in_w(I)$ con respeto a $<$. Entonces,

$$in_w(I) = (in_w(g) : g \in \mathcal{G}) = (in_v(g) : g \in \mathcal{G}) \subseteq in_v(I).$$

Continuación: Supongamos $in_w(I) \subsetneq in_v(I)$. Eso implica que también

$$in_{<_w}(I) = in_<(in_w(I)) \subsetneq in_<(in_v(I)) = in_{<_v}(I),$$

lo cual es una contradicción al Ejercicio 15.

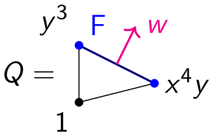
3. Sea $v \in C[w]$ y $g \in \mathcal{G}$. Como $\mathcal{G}$ es la base de Gröbner *reducida* de $in_w(I) = in_v(I)$ y $<$ tenemos que $in_v(g)$ reduce a cero con respeto a $in_w(\mathcal{G}) := \{in_w(g) : g \in \mathcal{G}\}$. Entonces, el monomio $in_{<_w}(g)$ tiene que estar presente en $in_<(g)$, porque ningún otro monomio de g esta en $in_{<_w}(I) = in_<(in_w(I))$. Escribe

$$in_w(g) = in_<(g) + h \quad \text{y} \quad in_v(g) = in_<(g) + h',$$

donde h, h' son combinaciones k-lineares de monomios estándar. Aplicamos el algoritmo de división a $in_v(g)$ con respeto a $in_w(\mathcal{G})$. Ya sabemos que $in_v(g)$ reduce a cero, entonces después del primer paso el algoritmo nos da $h' - h \in in_w(I)$ como resto. Pero ningún monomio en $h' - h$ esta en $in_{<_w}(I) = in_<(in_w(I))$. Entonces, no podemos reducir más y $h' - h = 0$, que implica $in_v(g) = in_w(g)$ y $v \in C_{\mathcal{G}}[w]$. ■

El cono $C[w]$ y el politopo de Newton

Sea $g = y^3 + x^4y + 1 \in k[x, y]$ y $w = (1, 2)$. Entonces $in_w(g) = y^3 + x^4y$ y $C[w] = \{v \in \mathbb{R}^2 : in_v(g) = in_w(g)\}$. Sea $Q = New(g)$ y $F = face_w(Q) = \{a \in Q : w \cdot a \geq w \cdot b \;\forall\; b \in Q\}$:



calculamos:

$$\begin{aligned} C[w] &= \{v \in \mathbb{R}^2 : in_v(g) = in_w(g)\} \\ &= \{v \in \mathbb{R}^2 : face_v(Q) = F\} \\ &= N_Q(F) \end{aligned}$$

Ejercicio 16

Sea I un ideal, w un vector de peso, $<_w$ el orden monomial, y $\mathcal{G}$ la base de Gröbner reducida de I y $<_w$. Muestra la siguiente ecuación:

$$C[w] = \mathcal{N}_Q(face_w(Q)), \quad con \quad Q = New(\prod_{g \in \mathcal{G}} g) = \sum_{g \in \mathcal{G}} New(g).$$

El abanico de Gröbner

Sean I y w como antes.

Definición 16

Sea $\overline{C[w]}$ la cerradura del cono $C[w]$ en $\mathbb{R}^n$. Definimos el abanico de Gröbner $GF(I)$ del ideal I como el conjunto de los conos cerrados $\overline{C[w]}$ para todos $w \in \mathbb{R}^n$. Si existe un politopo P tal que $GF(I) = \mathcal{N}(P)$, P se llama politopo de estado.

Proposición 3

El abanico de Gröbner es un abanico.

Prueba: Primero analizamos el cono cerrado $\overline{C[w]}$: sea $v \in \overline{C[w]}$. De las ecuaciones (0.2) concluimos que $in_w(I)$ es un ideal inicial de $in_v(I)$. Entonces existe un orden monomial $<$ tal que $in_{<_v}(I) = in_{<_w}(I)$. Sea $\mathcal{G}$ la base de Gröbner reducida para $<_v$ y $Q = \sum_{g \in G} New(g)$.

Continuación: Note que $\mathcal{G}$ tambien es base de Gröbner para $<_w$ y

$$C[w] = \mathcal{N}_Q(face_w(Q)) \quad \text{y} \quad C[v] = \mathcal{N}_Q(face_v(Q)).$$

Si $in_w(I)$ es ideal de $in_v(I)$ eso implica que $face_w(Q)$ es una cara de $face_v(Q)$. De la definición del cono normal concluimos entonces que $\overline{C[v]}$ es una cara de $\overline{C[w]}$.

Tenemos que mostrar que $GF(I)$ cumple las axiomas de un complejo:

1. si $C \in GF(I)$ y C' es una cara de C, entonces $C' \in GF(I)$;
2. si $C_1, C_2 \in GF(I)$, entonces $C_1 \cap C_2$ es una cara de C_1 y de C_2.

Sea C' una cara de $\overline{C[w]}$. Si v es un vector en el relativamente interior de C' tenemos $C' = \overline{C[v]}$ que es una cara de $\overline{C[w]}$. Entonces, $GF(I)$ cumple (1).

Para (2) sean $v, w \in \mathbb{R}^n$ y $P := \overline{C[v]} \cap \overline{C[w]}$. Ya vimos que para cada $u \in P$ el cono $\overline{C[u]}$ es una cara de $\overline{C[w]}$ y de $\overline{C[v]}$. Entonces, P es una unión finita de conos $\overline{C[u]}$ que son caras simultaneas. Pero una unión de caras diferentes de un cono no es un cono convexo. Entonces, P es una sola cara simultánea de $\overline{C[w]}$ y $\overline{C[v]}$. ∎

Un politopo de estado

Sea $deg(x^a) := \sum_{i=1}^{n} a_i$ el grado de un monomio x^a. Con I_d anotamos el subespacio vectorial de polinomios homogéneos del grado d en I. Para un ideal monomial J definimos

$$\sum J_d := \sum_{a \in \mathbb{Z}^n_{\geq 0} \text{ y } x^a \in J_d} a \in \mathbb{Z}^n_{\geq 0}.$$

Ejemplo: Sea $J = (x, y^2) \subset k[x, y]$. Pues J_4 tiene base $\{x^4, x^2y^2, y^4\}$. Entonces $\sum J_4 = (4,0) + (2,2) + (0,4) = (6,6)$.

Definición 17

Sea I un ideal y $\mathcal{U}$ una base de Gröbner universal minimal de I. Definimos

$$State_d(I) := conv\left\{\sum in_<(I)_d : < \text{ cualquier orden monomial}\right\}.$$

Sea $D = \max\{deg(g) : g \in \mathcal{U}\}$. Definimos

$$State(I) := State_1(I) + \cdots + State_D(I).$$

Ejemplo 7

Sea $I = (g)$ *y* $g = xy^2 + x^2y + y^3$. *Solo hay tres tipos de ordenes monomiales relevantes:*

$$in_{<_1}(g) = xy^2, in_{<_2}(g) = x^2y, in_{<_3}(g) = y^3.$$

En particular, $\{g\}$ *es una base de Gröbner universal minimal de* I *y* $D = 3$. *Tenemos* $\sum in_{<_1}(I) = (1,2), \sum in_{<_2}(I) = (2,1)$ *y* $\sum in_{<_1}(I) = (0,3)$. *Entonces,* $State_3(I) = conv\{(1,2),(2,1),(0,3)\}$. *Note que* $State_i(I)$ *es vacío para* $i < 3$. *Pues en este caso tenemos*

$$State(I) = State_3(I) = New(g).$$

Lemma 4

Para cada $w \in \mathbb{R}^n$ tenemos $face_w(State_d(I)) = State_d(in_w(I))$

Prueba: Primero tratamos el caso de w genérico. Entonces, $in_w(I)$ es un ideal monomial y $face_w(State(I))$ es un vértice. Fijamos un orden monomial tal que $in_<(I) = in_w(I)$. Sean $x^{a_1}, \ldots, x^{a_m}$ todos los monomios del grade d en $k[\mathbb{x}]$ y define $r := \dim(I_d)$. Tenemos $r \leq m$ (I_d es un subespacio de $k[\mathbb{x}]_d$).
Recuerda la base de monomios estándar $\mathbb{B}_<$ de $k[\mathbb{x}]/I$. Su existencia implica que $\dim(I)_d = \dim(in_<(I)_d)$. (Ejercicio: Verifica la igualdad.)
Pues podemos suponer que $x^{a_1}, \ldots, x^{a_r}$ son los monomios (no estándar) en $in_<(I)_d$. Existen expresiones únicos de cada $x^{a_i}, 1 \leq i \leq r$ en la base de monomios estándar modulo I. En particular,

$$x^{a_i} - \sum_{j=r+1}^{m} c_{ij} x^{a_j} \in I_d$$

Nota que $w \cdot a_i > w \cdot a_j$ cuando $c_{ij} \neq 0$ ($x^{a_i} \in in_w(I) \not\ni x^{a_j}$). Observa que $State_d(in_w(I)) = \{a_1 + \cdots + a_r\}$ porque $in_w(I)$ ya es monomial.

Continuación: Observa que $State_d(in_w(I)) = \{a_1 + \cdots + a_r\}$ porque $in_w(I)$ ya es monomial.
El vertice $face_w(State_d(I))$ es (por definición) igual a $\sum in_{<'}(I)_d$ para algún orden monomial $<'$. Sean $x^{a_{j_1}}, \ldots, x^{a_{j_r}}$ los monomios en $in_{<'}(I)_d$.
Supongamos que $face_w(State_d(I)) \neq State_d(in_w(I))$. Por definición de cara entonces tenemos

$$w \cdot (a_{j_1} + \cdots + a_{j_r}) > w \cdot (a_1 + \cdots + a_r)$$

Sea $B = \{a_1, \ldots, a_m\}$. Tenemos dos bases para $(k[\underline{x}]/I)_d$:
$A' = B - \{a_{j_1}, \ldots, a_{j_r}\}$ y $A = B - \{a_1, \ldots, a_r\}$. Podemos pasar de A a A' con una secuencia de intercambios $a_i \mapsto a_j$ con $c_{ij} \neq 0$ (El Lema de intercambio de Steinitz). Sea A_s el conjunto despues de s intercambios.
Vimos que $w \cdot a_i > w \cdot a_j$ cuando $c_{ij} \neq 0$, entonces

$$w \cdot (\sum_{a \in A_s} a) < w \cdot (\sum_{a \in A_{s+1}} a).$$

Pero eso contradice la definición de cara. Eso muestra el lema para vértices.

Ejercicio 17

Acaba la prueba del Lema 4 usando el caso de vertices, la igualdad $face_v(face_w(P)) = face_{w+\epsilon v}(P)$ para $\epsilon > 0$ suficientemente pequeño, y la igualdad $in_v(in_w(I)) = in_{w+\epsilon v}(I)$ para $\epsilon > 0$ suficientemente pequeño.

Corolario 4

Sean $<$ y $<'$ dos ordenes monomiales diferentes. Entonces

$$in_<(I)_d \neq in_{<'}(I)_d \quad \Rightarrow \quad \sum in_<(I)_d \neq \sum in_{<'}(I)_d.$$

El abanico de Gröbner de un ideal homogeneo

Teorema 5

Sea I un ideal homogéneo en $k[\mathbb{x}]$. Entonces existe un politopo de estado, es decir existe un politopo $P \subset \mathbb{R}^n$ tal que $GF(I) = \mathcal{N}(P)$. Además cada politopo de estado de I es fuertemente isomorfo a $State(I)$.

Prueba: Vamos a mostrar que $\mathcal{N}(State(I)) = GF(I)$. Ya sabemos que $GF(I)$ es un abanico, en particular un complejo poliédrico (Proposición 3). Pues todas las caras de $GF(I)$ son determinadas de las caras máximas. Entonces, $GF(I)$ y $\mathcal{N}(State(I))$ son iguales si y solo si sus conos máximales (abiertos) son iguales.
Los conos máximales de $\mathcal{N}(State(I))$ corresponden a las vértices de $State(I)$, y los conos máximales de $GF(I)$ corresponden a ideales iniciales monomiales. Entonces tenemos que mostrar que para $v, w \in \mathbb{R}^n$ genéricos:

$$face_v(State(I)) = face_w(State(I)) \quad \Leftrightarrow \quad in_v(I) = in_w(I). \qquad (0.3)$$

Continuación: Pues ideales homogéneos son generados de polinomios homogéneos, dos ideales homogéneos son iguales si y solo si son iguales en cada grado. El numero D es una cota superior universal para los grados de generadores minimales de I. Entonces,

$$in_v(I) = in_w(I) \quad \Leftrightarrow \quad in_v(I)_d = in_w(I)_d \; \forall \; d = 1, \ldots, D. \tag{0.4}$$

Recuerda también la propiedad de la sume de Minkowski de Ejercicio 8:

$$face_w(State(I)) = \sum_{d=1}^{D} face_w(State_d(I)) \tag{0.5}$$

Ejercicio 18

Verifica que la dirección $\Leftarrow$ de (0.3) es una consecuencia de las observaciones (0.4), (0.5) y del Lema 4.

Continuación: Para la dirección $\Rightarrow$ supongamos que

$$face_v(State(I)) = face_w(State(I)) \quad \text{para} \quad v, w \quad \text{genéricos.}$$

La genericidad implica que $face_v(State(I))$ y $face_w(State(I))$ son vértices, y las ideales iniciales $in_w(I)$ y $in_v(I)$ son monomiales. Pues podemos encontrar ordenes monomiales $<$ y $<'$ con $in_<(I) = in_w(I)$ y $in_{<'}(I) = in_v(I)$. La prueba se completa con el siguiente ejercicio:

Ejercicio 19

Verifica que la dirección $\Rightarrow$ ahora es una consecuencia de Ejercicio 8 y del Corolario 4.

Un politopo de estados de politopos de Newton

Vimos en Ejemplo 7 que $State((g)) = New(g)$ para $g = xy^2 + x^2y + y^3$.
Eso no fue coincidencia:

Proposición 4

Sea f un polinomio homogéneo y $I = (f)$. Entonces, $New(f)$ es un politopo de estado para I.

Corolario 5

Sea $\mathcal{U}$ una base de Gröbner universal de I que también es base de Gröbner reducida para cada orden monomial. Entonces $\sum_{g \in \mathcal{U}} New(g)$ es un politopo de estado de I.

Ejercicio 20

Muestra la Proposición 4 y el Corolario 5.

Referencias §4

1. Bernd Sturmfels: Gröbner bases and convex polytopes, Volume 8 of American Mathematical Soc.1996

§5 La Tropicalización

Contenido

Geometría tropical

La geometría tropical es un área de las matemáticas joven. En términos generales se trata de estudiar objetos geométricos sobre el semianillo tropical:

$$\begin{aligned} \mathbb{R}^T &:= (\mathbb{R} \cup \{-\infty\}, \oplus, \otimes) \\ a \oplus b &:= \max\{a, b\}, \\ a \otimes b &:= a + b \quad \forall a, b \in \mathbb{R} \cup \{-\infty\}. \end{aligned}$$

Uno puede pasar de la geometría algebraica a la geometría tropical, este proceso se llama tropicalización.

Hipersuperficie tropical

Sea k un campo con $char(k) = 0$. Para simplificar trabajamos solo con polinomios y ideales homogéneos.

Definición 18

Sea $f \in k[\mathbb{x}]$ un polinomio (homogéneo). La hipersuperficie tropical de f es el conjunto

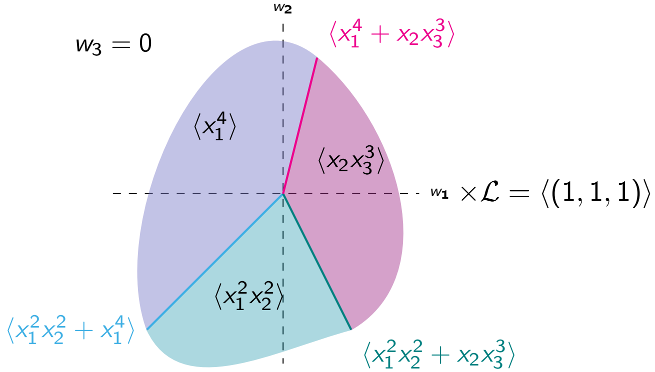
$$Trop(f) = \{w \in \mathbb{R}^n : in_w(f) \text{ no es un monomio}\}.$$

Ejercicio 21

Verifica que los conos máximales de $Trop(f)$ corresponden a los conos de codimensión 1 en $\mathcal{N}(New(f))$.

Ejemplo

Sea $J = \langle x_1^2 x_2^2 + x_1^4 + x_2 x_3^3 \rangle \subset \mathbb{C}[x_1, x_2, x_3]$. Entonces $GF(J)$ es $\mathbb{R}^3$ con la siguiente estructura de abanico:



La tropicalización de J consiste de los trés rayos y el espacio lineal $\mathcal{L}$.

(Pre-)Variedad tropical

Definición 19

Una prevariedad tropical es una intersección finita de hipersuperficies tropicales: $Trop(f_1) \cap \cdots \cap Trop(f_s)$, *para* $f_1, \ldots, f_s \in k[\mathbb{x}]$ *(homogéneos).*

Definición 20

Sea $I \subset k[\mathbb{x}]$ *un ideal homogéneo. Su tropicalización es*

$$Trop(I) := \bigcap_{f \in I} Trop(f) \subset \mathbb{R}^n.$$

El conjunto $Trop(I)$ *se llama una variedad tropical.*

Definición 21

Sean $f_1, \ldots, f_s \in I$ *tal que* $Trop(I) = Trop(f_1) \cap \cdots \cap Trop(f_s)$. *En este caso* $\{f_1, \ldots, f_s\}$ *se llama una base tropical de* I.

Bases tropicales

Teorema 6

Cada ideal $I \subset k[\mathbb{x}]$ tiene una base tropical.

Prueba: Sea $\mathcal{F}$ un conjunto de generadores de I que no es una base tropical. Escoja un cono (abierto) $C[w]$ en el $GF(I)$ tal que

1. la intersección $C[w] \cap (\cap_{f \in \mathcal{F}} Trop(f))$ no es vacía;
2. el ideal inicial $in_w(I)$ contiene un monomio x^m.

Sea $<_w$ un orden monomial que refine w y sea $\mathcal{G}_{<_w}$ la base de Gröbner reducida. Sea h una expresión estándar de x^m con respeto a $\mathcal{G}_{<_w}$ y $f := x^m - h$. Nota que x^m reduce a cero con respeto a $\{in_{<_w}(g) : g \in \mathcal{G}_{<_w}\}$. Entonces, cada monomio de h tiene w-peso más pequeño que $w \cdot m$ (el w-peso de x^m). Nota también que h solo depende de $\mathcal{G}_{<_w}$, no del peso w. Entonces, tenemos que para cada $v \in C[w]$ igualmente $x^m = in_v(f)$. Eso implica que $C[w]$ no es un cono en $Trop(I)$.

Continuación: Reemplazamos $\mathcal{F}$ por $\mathcal{F}' := \mathcal{F} \cup \{f\}$ y repetimos el procedimiento anterior. De esta manera vamos a pasar por todo el abanico de Gröbner eliminando conos cuyos ideal inicial contiene algún monomio. Como es abanico de Gröbner tiene un numero finito de conos (Teorema 5), este proceso termina en tiempo finito. ■

Comentario 2

Aún existen, las bases tropicales pueden ser muy grandes. Por ejemplo, para cada $1 \leq d \leq n$ existe un ideal linear en $k[\mathbb{x}]$ tal que cualquier base tropical de formas lineares en I tiene al menos $\frac{1}{n-d+1}\binom{n}{d}$ elementos [Teorema 2.19 en BJSST].

Teorema fundamental y estructural

Definición 22

1. *La dimensión del ideal I es definida como* $\dim_{Krull}(k[\mathbb{x}]/I) = \dim_k(V(I))$ *donde* $V(I) \subset \mathbb{A}_k^n$ *es la variedad afín.*
2. *Sea* Σ *un abanico y sean* $r_1, \ldots, r_s$ *sus rayos con generadores primitivos* $\rho_1, \ldots \rho_s$. *El abanico se llama balanceado si existen* $m_1, \ldots, m_s \in \mathbb{Z}_{>0}$ *tal que* $\sum m_i \rho_i = 0$;
3. *Una faceta de* Σ *es un* $C \in \Sigma$ *que no es cara de ningún otro* $C' \in \Sigma$. *El abanico* Σ *es puro si todos sus facetas tienen la misma dimensión.*

Teorema 7

Para cada ideal primo I *de dimensión* d *tenemos*

1. $Trop(I) = \{w \in \mathbb{R}^n : in_w(I) \text{ no contiene ningún monomio}\} =: NoMon(I)$, *entonces* $Trop(I) \subset GF(I)$;
2. $Trop(I)$ *es el soporte de un abanico balanceado puro de dimensión* d.

Sobre la prueba:

1. Es parte del Teorema fundamental de la geometría tropical. Una inclusión es fácil: *$NoMon(I) \subseteq Trop(I)$:* Tomamos $w \notin Trop(I)$, entonces existe un $g \in I$ tal que su forma inicial $in_w(g)$ es un monomio. Pues $in_w(I) \ni in_w(g)$ entonces $w \notin NoMon(I)$. Para la otra inclusión: [Theorem 3.2.5 in Maclagan–Sturmfels].
2. Esto es parte del Teorema estructural para variedades tropicales. Que es un abanico de dimensión d es consecuencia de [Bieri y Groves, 1986]. Para lo demás es [Theorem 3.3.6 in Maclagan–Sturmfels].

Polinomios de Laurent

Sea $k[\mathbb{x}^{\pm}] := k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ el anillo de los polinomios de Laurent. Los monomios $Mon^{\pm} \subset k[\mathbb{x}^{\pm}]$ son en biyección con $\mathbb{Z}^n$ y son invertibles. En particular, tenemos la acción de $GL_n(\mathbb{Z})$ en $\mathbb{Z}^n$ que se extiende a $Mon^{\pm}$:

$$A \cdot x^m := x^{A \cdot m}, \quad A \in GL_n(\mathbb{Z}) \Rightarrow A \cdot m \in \mathbb{Z}^n \quad y \quad A \cdot Mon^{\pm} = Mon^{\pm}.$$

Esta acción se llama un cambio de coordenadas multiplicativo.
Para $f = \sum_{i=1}^{m} c_i x^{a_i} \in k[\mathbb{x}]$ definimos $f^{\pm} := \sum_{i=1}^{m} c_i x^{a_i} \in k[\mathbb{x}^{\pm}]$. Para un ideal $I \subset k[\mathbb{x}]$ definimos $I^{\pm} := (f^{\pm} : f \in I) \subset k[\mathbb{x}^{\pm}]$.

Muchos definiciones se extienden directamente de $k[\mathbb{x}]$ a $k[\mathbb{x}^{\pm}]$, por ejemplo:

- la forma inicial y el ideal inicial con respeto a un vector de peso;
- las hipersuperficies tropicales y las (pre-)variedades tropicales

Lemma 5

Para cada ideal $I \subset k[\mathbb{x}]$ la variedad tropical $Trop(I)$ solo depende de $I^{\pm}$.

Prueba: Primero tratamos el caso de hipersuperficies: sea $f = \sum_{i=1}^{m} c_i x^{a_i} \in k[\mathbb{x}]$ y $w \in \mathbb{R}^n$. Tenemos $in_w(f) = in_w(f^{\pm})$, entonces $Trop(f) = Trop(f^{\pm})$.
Sean I_1, I_2 dos ideales en $k[\mathbb{x}]$ tal que $I_1^{\pm} = I_2^{\pm}$ en $k[\mathbb{x}^{\pm}]$. Toma $w \notin Trop(I_1)$. Pues existe $f \in I_1$ tal que $in_w(f)$ es un monomio. Como $I_1^{\pm} = I_2^{\pm}$ sabemos que existe un monomio $x^m \in k[\mathbb{x}^{\pm}]$ tal que $x^m f \in I_2^{\pm}$. Pero $in_w(x^m f) = x^m in_w(f)$ es un monomio. Entonces $w \notin Trop(I_2)$. ■

Comentario 3

Para cada ideal $I \subset k[\mathbb{x}^{\pm}]$ y $w \in \mathbb{R}^n$ tenemos que $in_w(I)$ no contiene ningún monomio si y solo si $in_w(I) \neq (1) = k[\mathbb{x}^{\pm}]$.

Intersecciones

Definición 23

Sean I, J dos ideales y $w \in \mathbb{R}^n$ tal que $w \in Trop(I) \cap Trop(J)$. Sean $F \subset Trop(I)$ y $G \subset Trop(J)$ los conos (abiertos) con $w \in G \cap F$. Si $\mathbb{R}F \cup \mathbb{R}G = \mathbb{R}^n$ decimos que $Trop(I) \cap Trop(J)$ es transversal en w. Si existe tal w se dice que $Trop(I)$ y $Trop(J)$ se encuentran transversalmente.

Lemma 6 (Intersección transversal)

Sean I, J ideales en $k[\mathbb{x}]$ cuyos variedades tropicales $Trop(I)$ y $Trop(J)$ se encuentran transversalmente en $w \in \mathbb{R}^n$. Entonces $w \in Trop(I + J)$.

Corolario 6

Sean $I, J \subset k[\mathbb{x}]$ ideales. Entonces $Trop(I + J) \subseteq Trop(I) \cap Trop(J)$. Si además la intersección $Trop(I) \cap Trop(J)$ es transversal en cada punto que no es el origen y la intersección no contiene solo el origen, entonces $Trop(I + J) = Trop(I) \cap Trop(J)$.

Conectividad

Sea I un ideal primo de dimensión d en $k[\mathbb{x}]$. Entonces su variedad tropical $Trop(I)$ se llama irreducible.

Teorema 8

Cada variedad tropical irreducible es conectada en codimensión uno: es decir, para cada I primo de dimensión d y cada pareja de facetas $F, F' \in Trop(I)$ existe una secuencia de facetas

$$F = F_1, F_2, \ldots, F_{r-1}, F_r = F'$$

tal que $F_i \cap F_{i+1}$ es un cono de dimensión $d-1$.

Sobre la prueba: Primero, I se reemplaza por $I^{\pm}$ que también es primo. La prueba es con inducción sobre d, $d = 1$ es trivial. Para $d = 2$ uno cambia el campo K por las series de Puiseux que deja eliminar una variable y reducir al caso $d = 1$ otra vez. El paso de la inducción usa el Lema 2, un cambio de coordenadas multiplicativo y el Teorema de Bertini.

Ideales no homogéneos

Definición 24

Para $f = \sum_{i=1}^{m} c_i x^{a_i} \in k[x_1, \ldots, x_n]$ *definimos su homogenización*

$$^h f := \sum_{i=1}^{m} c_i x^{a_i} x_0^{\deg(f) - \sum_{j=1}^{n} a_{ij}} \in k[x_0, x_1, \ldots, x_n].$$

Para un ideal $I \subset k[x_1, \ldots, x_n]$ *definimos similar su homogenización* $^h I := (^h f : f \in I) \subset k[x_0, \ldots, x_n]$.

Ejercicio 22

Muestra que para $w \in \mathbb{R}^n$ *tenemos*

$$in_w(I) \text{ contiene un monomio} \quad \Leftrightarrow \quad in_{(0,w)}(^h I) \text{ contiene un monomio} .$$

En particular, con respeto a la computación, es suficiente tener algoritmos para calcular la tropicalización de un ideal homogéneo.

Referencias §5

1. Bogart, T.; Jensen, A. N.; Speyer, D.; Sturmfels, B.; Thomas, R. R.: Computing tropical varieties. J. Symbolic Comput. 42 (2007), no. 1-2, 54–73.
2. Bieri, R.; Groves, J. R. J.: A rigidity property for the set of all characters induced by valuations. Trans. Amer. Math. Soc. 294 (1986), no. 2, 425–434.
3. Maclagan, D.; Sturmfels, B.: Introduction to tropical geometry. Graduate Studies in Mathematics, 161. American Mathematical Society, Providence, RI, 2015. xii+363 pp. ISBN: 978-0-8218-5198-2