Bases de Groebner

En lo que sigue, los coeficientes de todos los polinomios pertenecen a algún cuerpo $\mathbf{k}$. El ideal generado por elementos $g_1, \ldots, g_s$ se denota por $\langle g_1, \ldots, g_2 \rangle$. Si $X = \{x_1, \ldots, x_n\}$ entonces $\mathbf{k}[X]$ denotará el anillo de polinomios $\mathbf{k}[x_1, \ldots, x_n]$.

1. División de polinomios en una indeterminada

Sea $f := f(x) := a_0 x^m + \cdots + a_m$ con $a_0 \neq 0$. Usaremos la siguiente notación $\mathrm{LT}(f) := a_0 x^m$, $\mathrm{LM}(f) := x^m$, $\mathrm{LC}(f) := a_0$ y $\deg(f) := m$. Lo que permite ir dividiendo un polinomio entre otro en el algoritmo de la división de polinomios en $\mathbf{k}[x]$ es que

$$0 \neq \deg(g(x)) \leq \deg(f(x)) \Leftrightarrow \mathrm{LT}(g(x)) \text{ divide a } \mathrm{LT}(f(x)).$$

Se puede entonces multiplicar $f(x)$ por un monomio cx^k de modo que o bien $f(x) - cx^k g(x)$ es nulo o bien tiene menor grado que $f(x)$. Sin embargo, para polinomios en dos indeterminadas esto ya es falso (por ejemplo $f(x, y) := x^2$ y $g(x, y) := xy$).

En polinomios en una indeterminada los monomios aparecen ordenados de modo natural mediante su grado, que es básicamente el mismo orden que poseen los números naturales. Dividir $f(x)$ entre $g(x)$ se basa en *reducir* $f(x)$ usando que $\mathrm{LT}(g(x))$ divide a $\mathrm{LT}(f(x))$. Así se pueden obtener polinomios $c(x)$ y $r(x)$ tales que

$$f(x) = c(x)g(x) + r(x) \quad \text{con} \quad \deg(r(x)) < \deg(g(x))$$

(asumimos que el polinomio nulo tiene grado $-\infty$) y esta expresión es única.

Saber si un polinomio en una indeterminada divide a otro es ahora sencillo ya que $f(x) = c(x)g(x)$ para algún $c(x)$ si y solamente si $r(x) = 0$ en la expresión anterior. Como $\langle g_1(x), \ldots, g_s(x) \rangle = \langle \mathrm{mcd}(g_1(x), \ldots, g_s(x)) \rangle$, también es sencillo determinar si un polinomio $f(x)$ pertenece a un ideal $\langle g_1(x), \ldots, g_s(x) \rangle$ ya que basta comprobar si es divisible por $\mathrm{mcd}(g_1(x), \ldots, g_s(x))$ pues se tiene que $\langle g_1(x), \ldots, g_s(x) \rangle = \langle \mathrm{mcd}(g_1(x), \ldots, g_s(x)) \rangle$. Sin embargo, para $n \geq 2$ $\mathbf{k}[x_1, \ldots, x_n]$, que como ya hemos mencionado se denotará por $\mathbf{k}[X]$, no es un dominio euclídeo ni un dominio de ideales principales por lo que no se dispone de modo natural de un buen algoritmo de la división.

Lo que se va a ver en este tema es una generalización de la forma de dividir en $\mathbf{k}[x]$ y del paso del cambio $\langle g_1(x), \ldots, g_s(x) \rangle$ por $\langle \mathrm{mcd}(g_1(x), \ldots, g_s(x)) \rangle$ que son de gran utilidad a la hora de enfrentarse a sistemas de ecuaciones no necesariamente lineales.

2. Algoritmo de la división en $\mathbf{k}[x_1, \ldots, x_n]$

Sea $\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ y $X := \{x_1, \ldots, x_n\}$. Se usará la notación

$$X^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathbf{k}[x_1, \ldots, x_n]$$

Se pueden identificar los monomios $\{X^\alpha\}_{\alpha \in \mathbb{N}^n}$ con $\mathbb{N}^n$. De este modo hablaremos indistintamente de un orden en el conjunto de monomios y de un orden en $\mathbb{N}^n$.

Definición 1. *Un orden monomial en* $\mathbf{k}[X]$ *es una relación de orden* $\geq$ *en* $\{X^\alpha\}_{\alpha \in \mathbb{N}^n}$ *tal que*

1) $\geq$ *es un orden total,*

2) $X^\alpha \geq X^\beta$ *implica que* $X^{\alpha+\gamma} \geq X^{\beta+\gamma}$ *para todo* $\gamma \in \mathbb{N}^n$ *y*

3) $\geq$ *es un buen orden (es decir, todo subconjunto no vacío posee mínimo).*

Ejemplos.

Orden léxico-gráfico. $X^\alpha >_{lex} X^\beta$ si y solamente si la primera componente no nula de $\alpha - \beta$ es > 0. En particular, $x_1 > x_2 > \cdots > x_n$. Por ejemplo

$$x_1^2 >_{lex} x_1 x_1^{10}, \quad x_1^3 >_{lex} x_1^2.$$

Orden grlex. $X^\alpha >_{grlex} X^\beta$ si y solamente si o bien $|\alpha| > |\beta|$ o bien $|\alpha| = |\beta|$ y $X^\alpha >_{lex} X^\beta$, donde $|\alpha| := \alpha_1 + \cdots + \alpha_n$ si $\alpha = (\alpha_1, \ldots, \alpha_n)$. En este caso

$$x_1^2 x_2 >_{grlex} x_1^2.$$

Orden grevlex. $X^\alpha >_{grevlex} X^\beta$ si y solamente si o bien $|\alpha| > |\beta|$ o bien $|\alpha| = |\beta|$ y la última componente no nula de $\alpha - \beta$ es negativa. En particular $x_1 > \cdots > x_n$. Por ejemplo,

$$x_1^5 x_2 x_3 >_{grevlex} x_1^4 x_2 x_3^2.$$

Hemos de observar que al intercambiar el papel de las indeterminadas en el anillo $\mathbf{k}[x_1, \ldots, x_n]$ se obtienen muchos nuevos órdenes monomiales a partir de uno dado. Lo que iremos haciendo en este tema dependerá de un orden monomial prefijado. Más adelante se verá cómo varían algunas de estas construcciones al variar el orden prefijado.

Definición 2. *Dado* $f = \sum_\alpha a_\alpha X^\alpha \in \mathbf{k}[X]$ *no nulo y dado un orden monomial* $\geq$ *en* $\mathbf{k}[X]$ *se define*

1) el multigrado de f *como* $\mathrm{multideg}(f) := \max\{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\}$,

2) el coeficiente director de f *como* $\mathrm{LC}(f) := a_{\mathrm{multideg}(f)}$,

3) el monomio director de f *como* $\mathrm{LM}(f) := X^{\mathrm{multideg}(f)}$ *y*

4) el término director de f *como* $\mathrm{LT}(f) := LC(f)LM(f)$.

Teorema 1 (Algoritmo de la división)**.** *Sea* $\geq$ *un orden monomial en* $\mathbf{k}[X]$ *y* $f_1(X), \ldots, f_s(X) \in \mathbf{k}[X]$ *no nulos. Dado* $f(X) \in \mathbf{k}[X]$ *existen polinomios* $a_1(X), \ldots, a_x(X), r(X) \in \mathbf{k}[X]$ *tales que*

1) $f = a_1 f_1 + \cdots + a_s f_s + r$,

2) o bien $r = 0$ *o bien* r *es una combinación lineal de monomios no divisibles por ningún* $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$, *y además*

3) si $a_i f_i \neq 0$ *entonces* $\mathrm{LT}(f) \geq \mathrm{LT}(a_i f_i)$.

En particular, $\mathrm{LT}(f) > \mathrm{LT}(r)$ *si* $r \neq 0$. *Se dirá que* r *es un resto de dividir* f *por* $(f_1, \ldots, f_s)$.

Demostración. Fijamos inicialmente $a_1 := \cdots := a_s := 0$ y $r := 0$ aunque se irá actualizando su valor. También utilizamos una variable temporal r' que inicialmente definimos como f pero que irá disminuyendo durante el algoritmo hasta que finalmente sea 0. Durante todo el algoritmo se tendrá que $f = a_1 f_1 + \cdots + a_s f_s + r + r'$, y que o bien $r = 0$ o bien r es una combinación lineal de monomios no divisibles por ningún $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$, y además si $a_i f_i \neq 0$ entonces $\mathrm{LT}(f) \geq \mathrm{LT}(a_i f_i)$ (observar que inicialmente se cumplen estas condiciones). En el momento en que r' sea 0 se tendrá demostrado el teorema.

Si $r' = 0$ entonces se termina el proceso con el valor actual de $a_1, \ldots, a_s, r$. Si $r' \neq 0$ entonces o bien $\mathrm{LT}(r')$ no es divisible por ningún $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$, en cuyo caso se le añade r' a r, se fija $r' := 0$ y se termina el proceso con el valor actual de $a_1, \ldots, a_s$ y r, o bien $\mathrm{LT}(r')$ es divisible por algún $\mathrm{LT}(f_i)$, en cuyo caso se procede como sigue para actualizar los valores de $a_1, \ldots, a_s$, r y r'. Se considera el primer i que cumpla que $\mathrm{LT}(f_i)$ divide a $\mathrm{LT}(f')$. Así, $\mathrm{LT}(r') = \mathrm{LT}(f_i) c X^\alpha$ para algún $c \in \mathbf{k}$ y algún $\alpha \in \mathbb{N}^n$. Añadimos cX^α a a_i y consideramos un nuevo r'

$$r' := r' - cX^\alpha f_i$$

de modo que $f = a_1 f_1 + \cdots + a_s f_s + r + r'$ sigue siendo válido y el monomio director de r' ha sido rebajado. Reiterando este paso se va disminuyendo r' con múltiplos de $f_1, \ldots, f_s$ (observa que todos los monomios de estos múltiplos son $\leq \mathrm{LM}(f)$) obteniendo cada vez un polinomio con menor monomio director. Como $\{X^\alpha \mid X^\alpha \leq \mathrm{LM}(f)\}$ posee mínimo (tercera propiedad en la definición de orden monomial) entonces en algún momento se debe obtener un r' tal que o bien $r' = 0$ o bien $\mathrm{LM}(r')$ no sea divisible por ningún $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. En este último caso actualizamos r sumándole $\mathrm{LT}(r')$ y también actualizamos r' restándole $\mathrm{LT}(r')$, y volvemos a repetir el proceso con este nuevo r'.

En cada iteración de este proceso reducimos el monomio director de r' (si es que $r' \neq 0$) por lo que tras un número finito de pasos se llegará a que $r' = 0$. □

Definición 3. *Un* r *que cumpla las propiedades 1), 2) y 3) del teorema anterior se dirá que es un resto de reducir* f *mediante* $\{f_1, \ldots, f_s\}$.

Ejemplo. Sea $I = \langle xy + 1, y^2 - 1 \rangle$. Vamos a reducir $f := xy^2 - x$ mediante $\{f_1 := xy + 1, f_2 := y^2 - 1\}$. Para ello fijamos un orden lex en $\mathbf{k}[x, y]$ con $x > y$.

El término director de f es xy^2 y lo podemos eliminar usando o bien f_1 o bien f_2. Si usamos f_1 tenemos que $f - yf_1 = -y - x$. Este polinomio tiene término

director $-x$, que no es divisible ni por $\mathrm{LT}(f_1)$ ni por $\mathrm{LT}(f_2)$ por lo que $-y-x$ es un resto de reducir f mediante $\{f_1, f_2\}$. Sin embargo también podíamos haber usado f_2. En tal caso $f - xf_2 = 0$ nos habría proporcionado como resto 0. Esto muestra que **el resto de reducir un polinomio mediante un conjunto depende fuertemente del proceso seguido y no es en general único.** □.

Las demostraciones del lema y del corolario siguientes se puede encontrar en el libro de Cox, Little y O'Shea: *Ideals, varieties and algorithms*, Springer, 2007.

Lemma 1 (Lema de Dickson)**.** *Sea I un ideal de $\mathbf{k}[X]$ generado por algún conjunto de monomios S. Se tiene que existe un subconjunto finito $S_0 \subseteq S$ tal que $I = \langle S_0 \rangle$.*

Corolario 1. *Sea $\geq$ una relación de orden en $\mathbb{N}^n$ tal que*

1) $\geq$ es un orden total.

2) $\alpha \geq \beta$ implica que $\alpha + \gamma \geq \beta + \gamma$.

En tal caso $\geq$ es un buen orden si y solamente si $\alpha \geq (0, \ldots, 0)$ para todo $\alpha \in \mathbb{N}^n$.

El corolario anterior simplifica la forma de comprobar que un orden es monomial aunque el tipo de órdenes que usaremos son trivialmente monomiales.

Definición 4. *Dado un ideal no nulo I de $\mathbf{k}[X]$ definimos*

- $\mathrm{LT}(I) := \{cX^\alpha \mid \exists f \in I \text{ tal que } \mathrm{LT}(f) = cX^\alpha\}$ *(aquí c denota escalares en $\mathbf{k}$).*
- $\langle \mathrm{LT}(I) \rangle$ *el ideal generado por el conjunto de términos* $\mathrm{LT}(I)$.

Teorema 2 (Teorema de la base de Hilbert)**.** *Todo ideal I de $\mathbf{k}[X]$ posee algún conjunto finito de generadores*

Demostración. Si $I = \{0\}$ el resultado es obvio. Si $I \neq \{0\}$ entonces por el Lema de Dickson $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$ para ciertos $g_1, \ldots, g_s \in I$. El teorema quedará probado si demostramos que $I = \langle g_1, \ldots, g_s \rangle$.

Dado $f \in I$ dividimos f por $(g_1, \ldots, g_s)$ obteniendo $a_1, \ldots, a_s$ y r tales que

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

y de modo que o bien $r = 0$ o bien $\mathrm{LT}(r)$ no es divisible por ninguno de los términos $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Puesto que $r = f - a_1 g_1 - \cdots - a_s g_s \in I$ entonces si $r \neq 0$ tendríamos que $\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, lo que no es cierto. Así pues $r = 0$ y por lo tanto $I \in \langle g_1, \ldots, g_s \rangle$. Puesto que el otro contenido es inmediato queda probado el teorema. □

3. Bases de Groebner

Dado un ideal I de $\mathbf{k}[X]$ vamos a buscar un conjunto de generadores (no tiene por qué coincidir con el que nos den) de modo que podamos emular muchos de los cálculos disponibles para polinomios en una indeterminada. Recuerda que $X := \{x_1, \ldots, x_n\}$ es un conjunto de indeterminadas y que $\mathbf{k}[X] := \mathbf{k}[x_1, \ldots, x_n]$ no es en general ni un dominio euclídeo ni un dominio de ideales principales (a menos que $n = 1$).

En esta sección fijamos algún orden monomial $\geq$ en $\mathbf{k}[X]$ para que tenga sentido el concepto de término director.

Definición 5. *Un subconjunto $G = \{g_1, \ldots, g_t\}$ de un ideal I de $\mathbf{k}[X]$ se dice base de Groebner (de I con respecto al orden $\geq$) si $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.*

Es decir, si para cualquier polinomio no nulo de I su término director queda divido por el término director de alguno de los polinomios de la base de Groebner.

Hay que observar que al demostrar el Teorema de la base de Hilbert hemos probado que todo ideal no nulo de $\mathbf{k}[X]$ posee alguna base de Groebner y que si G es una base de Groebner de I entonces el ideal generado por G es exactamente I.

Fijar una base de Groebner G para un ideal I es una buena idea como veremos ya que el resto de reducir un polinomio mediante G no dependerá de cómo se haya obtenido tal resto.

Proposición 1 (Formal normal $\mathrm{N}_G(f)$ relativa a G)**.** *Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner de un ideal I de $\mathbf{k}[X]$ y sea $f \in \mathbf{k}[X]$. Existe un único $\mathrm{N}_G(f) \in \mathbf{k}[X]$ tal que*

1) *$f = g + \mathrm{N}_G(f)$ con $g \in I$ y*
2) *si $\mathrm{N}_G(f)$ no es nulo entonces ningún término de $\mathrm{N}_G(f)$ es divisible por ninguno de los términos $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.*

En particular, cualquier resto de reducir f mediante G debe coincidir con $\mathrm{N}_G(f)$, y da igual cómo se calcule tal resto.

Demostración. Sabemos que existe algún polinomio r (todavía no lo llamamos $\mathrm{N}_G(f)$ ya que desconocemos su unicidad) que cumple las propiedades 1) y 2) del enunciado (cualquier resto de dividir f entre G las cumple). Lo único que hemos de probar es la unicidad de tal r. Si $f = g + r = g' + r'$ con $g, g' \in I$ y de modo que ningún término no nulo de r ni de r' es divisible por ningún $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$ entonces $r - r' = g' - g \in I$ y ninguno de los términos no nulos en la expresión $r - r'$ es dividido por ningún $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Por la definición de base de Groeber esto implica necesariamente que $r - r' = 0$, por lo que $r = r'$. □

La existencia de formas normales tiene dos consecuencias muy importantes

Corolario 2. *Sea G una base de Groebner de un ideal I de $\mathbf{k}[X]$. Se tiene que*

$$f \in I \Leftrightarrow \mathrm{N}_G(f) = 0.$$

Corolario 3. *Sea G una base de Groebner de un ideal I de $\mathbf{k}[X]$. El conjunto*

$$B := \{X^\alpha + I \mid \nexists g \in G \text{ tal que } \mathrm{LT}(g)|X^\alpha\}$$

es una base del $\mathbf{k}$-espacio vectorial cociente $\mathbf{k}[X]/I$.

Demostración. Por la proposición, B genera el espacio vectorial cociente $\mathbf{k}[X]/I$. Para comprobar que realmente B es una base de este espacios vectorial solamente hemos de comprobar su independencia lineal. Sea $\sum_{X^\alpha+I\in B} a_\alpha X^\alpha + I = 0 + I$ una relación de dependencia lineal entre los elementos de B (con coeficientes posiblemente nulos). En tal caso $f := \sum a_\alpha X^\alpha \in I$ por lo que $\mathrm{N}_G(f)$ es necesariamente 0, pero también es claro que $r := f$ es un resto de reducir f mediante G por lo que necesariamente $f = 0$ y por lo tanto $a_\alpha = 0$ para todo α. □

Ejemplo. Sea $I := \langle xy + 1, y^2 - 1\rangle$ y $f := xy^2 - x$. Por abreviar definimos nuevamente $f_1 := xy+1, f_2 := y^2-1$. En el ejemplo anterior vimos que $f - yf_1 = -y - x$ es un resto de reducir f mediante $\{f_1, f_2\}$ y que y que $f - xf_2 = 0$. Esto muestra que $-y - x \in I$ aunque no parezca a primera vista natural ya que los generadores $\{f_1, f_2\}$ tienen grado mayor que 1. El problema es que se pueden combinar de modo que el resultado pertenezca a I y posea grado menor que el de ambos. Con las bases de Groebner vamos a poder solucionar este problema y decidir de forma clara si un polinomio pertenece o no a I, pero todavía no sabemos cómo calcular estas bases. □

Ahora que sabemos que los ideales poseen bases de Groebner y que tales bases son de gran ayuda para determinar si un polinomio dado pertenece o no al ideal (y para otras muchas cosas que iremos viendo en los siguientes temas) sería también deseable disponer de algún algoritmo que permita determinar alguna base de Groebner para un ideal dado. Hay que observar desde este momento que el concepto de base de Groebner depende del orden que se haya fijado. Al considerar otro orden, una base de Groebner para el orden inicial puede dejar de serlo para el nuevo orden. También puede ocurrir que calcular una base de Groebner para un ideal sea mucho más sencillo usando un orden que usando otro. Todo esto se estudiará en los siguientes temas, así que por ahora simplemente nos centraremos en describir un método práctico para calcular bases de Groebner.

Una obstrucción para que un subconjunto G de un ideal I sea una base de Groebner es que existan $g_1, g_2 \in G$ tales que al "combinarlos"sin salirnos de I se pierda multigrado y quede algún polinomio con término director que no sea divisible por ningún $\mathrm{LT}(g)$, $g \in T$. Con mayor precisión:

Definición 6. *Sean $f, g \in \mathbf{k}[X]$, $\alpha := \mathrm{multideg}(f)$, $\beta := \mathrm{multideg}(g)$ y $\gamma := (\gamma_1, \ldots, \gamma_n)$ con $\gamma_i := \max\{\alpha_i, \beta_i\}$ $i = 1, \ldots, n$. Diremos que X^γ es el mínimo común múltiplo (*mcm*) de $\mathrm{LM}(f)$ y $\mathrm{LM}(g)$. Llamaremos S-polinomio de f y g al polinomio*

$$S(f, g) := \frac{X^\gamma}{\mathrm{LT}(f)} f - \frac{X^\gamma}{\mathrm{LT}(g)} g.$$

Hay que observar que en la definición anterior $\mathrm{LT}(f)$ divide a X^γ por lo que $\frac{X^\gamma}{\mathrm{LT}(f)}$ tiene sentido, y lo mismo ocurre con la otra fracción en la definición de $S(f,g)$. También hay que observar que si f, g pertenecen a algún ideal I entonces $S(f,g)$ también pertenece a I.

Como nos muestra el siguiente lema, los S-polinomios son los responsables de que en las combinaciones lineales de polinomios podamos acabar accidentalmente con un polinomio con menor término director que los polinomios que combinamos.

Recuerda que con la identificación natural entre monomios y N^n el orden de los monomios pasa a $\mathbb{N}^n$, es decir $\alpha \geq \beta$ si y solamente si $X^\alpha \geq X^\beta$.

Lemma 2. *Sea $c_1f_1+\cdots+c_sf_s$ una combinación lineal de polinomios $f_1,\ldots,f_s \in \mathbf{k}[X]$ con coeficientes $c_1,\ldots,c_s \in \mathbf{k}$. Si $\mathrm{multideg}(c_if_i) = \delta$ para todo $i = 1,\ldots,s$ pero $\mathrm{multideg}(c_1f_1+\cdots,c_sf_s) < \delta$ entonces*

$$c_1f_1+\cdots+c_sf_s = \sum_{i,j=1}^{s} c_{ij}S(f_i,f_j)$$

para ciertos $c_{ij} \in \mathbf{k}$ y $\mathrm{multideg}(S(f_i,f_j)) < \delta$ para todo $i,j \in \{1,\ldots,s\}$.

Demostración. Sea $d_i := \mathrm{LC}(f_i)$ el coeficiente director de f_i. Claramente $c_1d_1+\cdots+c_sd_s = 0$. Sea $p_i = \frac{f_i}{d_i}$. Se tiene que $\mathrm{LC}(p_i) = 1$. Escribimos la combinación lineal $c_1f_1+\cdots+c_sf_s$ del siguiente modo:

$$\begin{aligned} c_1f_1+\cdots+c_sf_s &= c_1d_1p_1+\cdots+c_sd_sp_s \\ &= c_1d_1(p_1-p_2)+(c_1d_1+c_2d_2)(p_2-p_3)+\cdots+(c_1d_1+\cdots \\ &\quad \cdots+c_{s-1}d_{s-1})(p_{s-1}-p_s)+(c_1d_1+\cdots+c_sd_s)p_s \\ &= c_1d_1(p_1-p_2)+(c_1d_1+c_2d_2)(p_2-p_3)+\cdots+(c_1d_1+\cdots \\ &\quad \cdots+c_{s-1}d_{s-1})(p_{s-1}-p_s). \end{aligned}$$

Puesto que $\mathrm{multideg}(c_if_i) = \delta$ tenemos que $\mathrm{mcm}(\mathrm{LM}(f_i),\mathrm{LM}(f_j)) = X^\delta$ por lo que

$$S(f_i,f_j) = \frac{X^\delta}{\mathrm{LT}(f_i)}f_i - \frac{X^\delta}{\mathrm{LT}(f_j)}f_j = \frac{f_i}{\mathrm{LC}(f_i)} - \frac{f_j}{\mathrm{LC}(f_j)} = p_i - p_j$$

que tiene multigrado $< \delta$. Sustituyendo en la expresión que hemos obtenido anteriormente para $c_1f_1+\cdots+c_sf_s$ se tiene que $c_1f_1+\cdots+c_sf_s = c_{12}S(f_1,f_2)+\cdots+c_{s-1,s}S(f_{s-1},f_s)$ para ciertos $c_{12},\ldots,c_{s-1s} \in \mathbf{k}$. □

Realmente son solamente los S-polinomios formados a partir del conjunto que deseamos comprobar si es base de Groebner los que hay que estudiar para saber si ese conjunto es una base de Groebner.

Teorema 3 (Criterio de Buchberger para determinar si un conjunto es base de Groebner)**.** *El conjunto $G = \{g_1,\ldots,g_t\}$ es una base de Groebner $\Leftrightarrow$ para todo $i < j$ al reducir $S(g_i,g_j)$ mediante $\{g_1,\ldots,g_t\}$ de todas las formas posibles siempre se obtiene resto 0 $\Leftrightarrow$ para todo $i < j$ al reducir $S(g_i,g_j)$ mediante $\{g_1,\ldots,g_t\}$ de alguna forma particular se obtiene resto 0.*

Demostración. La primera implicación $\Rightarrow$ es obvia ya que $S(g_i, g_j) \in I := \langle g_1, \ldots, g_t \rangle$ y sabemos que, al ser G una base de Groebner, independientemente del proceso seguido al reducir un polinomio el resto es único, y ese resto es 0 en caso de que el polinomio pertenezca a I. La segunda implicación $\Rightarrow$ es obvia.

Demostremos ahora la implicación $\Leftarrow$ que cierra el círculo de implicaciones. Es decir, asumimos que para todo $i < j$ al reducir $S(g_i, g_j)$ mediante $\{g_1, \ldots, g_t\}$ de alguna forma particular se obtiene resto 0 y probaremos que G es una base de Groebner.

Sea $0 \neq f \in I$. Veamos que necesariamente $\mathrm{LT}(f)$ queda dividido por algún $\mathrm{LT}(g_i)$. Escribimos $f = h_1 g_1 + \cdots + h_t g_t$ para ciertos $h_1, \ldots, h_t \in \mathbf{k}[X]$. Sea $m(1) := \mathrm{multideg}(h_1 g_1), \ldots, m(t) := \mathrm{multideg}(h_t g_t)$ y $\delta := \max\{m(1), \ldots, m(t)\}$. De hecho podemos elegir $h_1, \ldots, h_t$ tales que este δ se mínimo entre todos los posibles δ que se obtienen al considerar los distintos $h_1, \ldots, h_t \in \mathbf{k}[X]$ que cumplen que $f = h_1 g_1 + \cdots + h_t g_t$. Esta elección será relevante en lo siguiente. Claramente $\mathrm{multideg}(f) \leq \delta$. Si no hubiese cancelaciones en el multigrado, es decir, si $\mathrm{multideg}(f) = \delta$ entonces $\mathrm{multideg}(f) = \delta = \mathrm{multideg}(h_i g_i)$ para algún i y así $\mathrm{LT}(g_i)$ divide a $\mathrm{LT}(f)$ quedando probado lo que buscábamos. Nos centramos pues en el caso en que sí hay cancelaciones y $\mathrm{multideg}(f) < \delta$. Lo que vamos a probar es que debido a la minimalidad en la elección de δ esto no será posible, por lo que quedará probado el teorema.

Primero aislamos los sumandos que contribuyen a las cancelaciones

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned}$$

Todos los monomios del segundo y tercer sumatorio tiene multigrado $< \delta$. El primer sumatorio también tiene multigrado $< \delta$ ya que todos los términos con multigrado δ se cancelan entre sí. Para estos últimos escribimos $\mathrm{LT}(h_i) := c_i X^{\alpha(i)}$ con $c_i \in \mathbf{k}$, así

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i X^{\alpha(i)} g_i$$

Aplicando el lema anterior tenemos que

$$\begin{aligned} \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i &= \sum_{i,j} c_{ij} S(X^{\alpha(i)} g_i, X^{\alpha(j)} g_j) \\ &= \sum_{i,j} c_{ij} X^{\delta - \gamma_{ij}} S(g_i, g_j) \end{aligned}$$

donde $X^{\gamma_{ij}} := \mathrm{mcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$. Por hipótesis existe alguna forma de reducir $S(g_i, g_j)$ mediante $\{g_1, \ldots, g_t\}$ que proporciona resto 0. Es decir, existen polinomios a_{ijk} tales que $S(g_i, g_j) = \sum a_{ijk} g_k$ donde $\mathrm{multideg}(a_{ijk} g_k) \leq \mathrm{multideg}(S(g_i, g_j))$. Esto nos permite escribir

$$X^{\delta - \gamma_{ij}} S(g_i, g_j) = \sum b_{ijk} g_k \text{ con } \mathrm{multideg}(b_{ijk} g_k) < \delta$$

para ciertos polinomios b_{ijk}. Por lo tanto

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_{ijk} c_{ij}b_{ijk}g_k = \sum_k \tilde{h}_k g_k$$

para adecuados $\tilde{h}_k$ tales que $\mathrm{multideg}(\tilde{h}_k g_k) < \delta$. Así pues, finalmente podemos escribir $f = h'_1 g_1 + \cdots + h'_t g_t$ con $\mathrm{multideg}(h'_i g_i) < \delta$ para todo i, lo que no es posible por la minimalidad en la elección de δ. □

4. Algoritmo de Buchberger

Ahora que disponemos de un criterio un poco más práctico que la mera definición para determinar si un conjunto de polinomios es o no una base de Groebner vamos a probar que realmente en este criterio está encerrado un método para construir bases de Groebner.

La idea es que si en algún momento no podemos reducir $S(g_i, g_j)$ mediante $G = \{g_1, \ldots, g_t\}$ hasta dejar resto 0 esto es posiblemente debido a que nos faltan polinomios, por lo que le añadimos $S(g_i, g_j)$ a G y volvemos a comprobar si el nuevo conjunto ya es base de Groebner. Concretando, dado $I = \langle f_1, \ldots, f_s\rangle$ un ideal de $\mathbf{k}[X]$ consideramos inicialmente $G' := \{f_1, \ldots, f_s\}$ y vamos calculando $S(f_i, f_j)$ con $i < j$ hasta encontrar una pareja f_i, f_j tal que el resto de reducir $S(f_i, f_j)$ mediante G' no sea nulo (si no existe tal pareja es que G' ya es una base de Groebner). Añadimos este resto a G' obteniendo un conjunto generador G de I con un elemento más que G'. Al reducir $S(f_i, f_j)$ mediante G, como ahora el resto al que habíamos llegado ya pertenece a G, podemos terminar la reducción y llegar a un resto nulo. Volvemos a repetir el proceso con G en lugar de G', añadiendo cada vez un polinomio hasta que tengamos finalmente una base de Groebner.

Cabe preguntarse si el proceso anterior acabará o si estaremos añadiendo polinomios indefinidamente. Si observamos que al añadir un nuevo polinomio a G' para formar G se tiene que $\langle \mathrm{LT}(G')\rangle \subset \langle \mathrm{LT}(G)\rangle$ (contenido estricto) ya que el término director del resto que hemos añadido para formar G no era dividido por ningún término director de polinomios en G' vemos que si el proceso no acabase tendríamos una cadena estrictamente creciente de ideales $I_1 \subset I_2 \subset \cdots \subset \mathbf{k}[X]$, pero esto no es posible gracias al siguiente resultado

Teorema 4 ($\mathbf{k}[X]$ es noetheriano)**.** *Si $I_1, I_2, \ldots$ son ideales de $\mathbf{k}[X]$ tales que $I_1 \subseteq I_2 \subseteq \cdots$ entonces existe un $N \in \mathbb{N}$ tal que $I_N = I_{N+1} = \cdots$.*

Demostración. Sea $I := \cup I_i$. Este conjunto es claramente un ideal de $\mathbf{k}[X]$ ya que los ideales I_i forman una cadena creciente. Por el Teorema de la base de Hilbert, $I = \langle f_1, \ldots, f_t\rangle$ para ciertos polinomios $f_1, \ldots, f_t$. Claramente existe un N suficientemente grande tal que $f_1, \ldots, f_t \in I_N$. Así, $I = \langle f_1, \ldots, f_t\rangle \subseteq I_N \subseteq I$. Es decir, $I = I_N$. Para cualquier I_M con $M \geq N$ se tendrá que $I_N \subseteq I_M \subseteq I = I_N$ por lo que la cadena de ideales se estabiliza a partir de I_N. □

Ejemplo. Continuando con el ejemplo anterior, sea $I := \langle xy+1, y^2-1\rangle$ $f_1 := xy+1$ y $f_2 := y^2-1$ y fijemos el orden lex con $x > y$. Vamos a calcular una base de Groebner de I a partir de $\{f_1, f_2\}$. Comenzamos con $G' := \{f_1, f_2\}$ y comprobamos si se pueden reducir los S-polinomios correspondientes hasta 0. En primer lugar $S(f_1, f_2) = yf_1 - xf_2 = x + y$ que no puede ser reducido más mediante G'. Esto nos obliga a añadir $x + y$ a G'. Así pues consideramos un nuevo $G' := \{f_1, f_2, x + y\}$ y comprobamos nuevamente si ahora sí se pueden reducir los S-polinomios. Claramente $S(f_1, f_2)$ sí puede reducirse a 0 al haber añadido $x+y$ pero ahora hay nuevos S-polinomios que hemos de comprobar. En primer lugar $S(f_1, x+y) = f_1 - y(x+y) = 1 - y^2 \overset{f_2}{\to} 0$ donde $\overset{f_2}{\to}$ indica un paso de reducción en el que hemos restado f_2 para reducir el orden de los monomios. Así pues, este S-polinomio sí se puede reducir a 0. También

$$S(f_2, x+y) = xf_2 - y^2(x+y) = -x - y^3 \overset{-(x+y)}{\to} y - y^3 \overset{-yf_2}{\to} 0.$$

Concluimos que $G := \{xy+1, y^2-1, x+y\}$ es una base de Groebner de I.

Podemos comprobar como ahora sí que el polinomio $f = xy^2 - x$ se reduce a 0 necesariamente mediante G. En efecto

$$xy^2 - x \overset{yf_1}{\to} -y - x \overset{-(x+y)}{\to} 0.$$

De este modo no nos queda duda de que $f \in I$. También podemos calcular la dimensión del espacio vectorial cociente $\mathbf{k}[x, y]/I$. Los monomios que no son divididos por ningún $\mathrm{LT}(g)$ con $g \in G$ son exactamente $\{1, y\}$ por lo que una base de $\mathbf{k}[x, y]/I$ es $\{1 + I, y + I\}$.

Calculando la forma normal de un polinomio comprobamos si pertenece o no a I. Por ejemplo, $\mathrm{N}_G(x^2y - x^3) = 2y$ ya que

$$x^2y - x^3 \overset{-x^2(x+y)}{\to} 2x^2y \overset{2x(xy+1)}{\to} -2x \overset{-2(x+y)}{\to} 2y.$$

Como el término director de $2y$ no es divisible por ningún término director de elementos de G, hemos llegado a la forma normal de $x^2y - x^3$. □

Aunque ya se puede proceder a aplicar el anterior algoritmo para obtener bases de Groebner de cualquier ideal I a partir de un conjunto de generador, sin embargo vamos a mejorar un poco esta base de modo que podamos garantizar una cierta unicidad de la misma. En general un ideal puede tener muchas bases de Groebner pero si exigimos algunas condiciones extra nada descabelladas veremos que solamente hay una que las cumpla (hay que recalcar nuevamente que todo esto es con un orden prefijado ya que al cambiar de orden un conjunto que antes era base de Groebner puede dejar de serlo y otro que no lo era ya lo es). Esto es muy útil por ejemplo cuando se usan paquetes de software para calcular bases de Groebner ya que en tal caso independientemente del paquete la base que se ha de obtener es siempre la misma, a no ser que se cambie el orden monomial.

Definición 7. *Una base de Groebner minimal G de un ideal I es una base de Groebner G de I tal que para todo $g \in G$ se cumple*

1) $\mathrm{LC}(g) = 1$

2) $\mathrm{LT}(g)$ *no es dividido por ningún* $\mathrm{LT}(g')$ $g' \in G \setminus \{g\}$.

Modificar una base de Groebner para que sea reducida es trivial ya que basta con dividir todos los polinomios que su coeficiente director para que cumplan 1) e ir quitando los que no cumplen 2) ya que un tal g es superfluo a la hora de reducir puesto que se puede usar g'. De hecho $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(G) \setminus \{g\} \rangle$ en tal caso por lo que obviamente g es superfluo.

Definición 8. *Una base de Groebner reducida de un ideal* I *de* $\mathbf{k}[X]$ *es una base de Groebner* G *de* I *tal que para todo* $g \in G$ *se tiene que*

1) $\mathrm{LC}(g) = 1$ *y*

2) ningún monomio de g *es dividido por ningún* $\mathrm{LT}(g')$ *con* $g' \in G \setminus \{g\}$.

Obviamente, una base reducida es automáticamente minimal. También es sencillo transformar una base base de Groebner cualquiera de un ideal I en una reducida. Si hay algún g que no cumpla 2) lo cambiamos por $g - cX^\alpha g'$ para un $c \in \mathbf{k}$ y X^α adecuado de modo que el monomio de g divisible por $\mathrm{LT}(g')$ desaparezca y quede a cambio una combinación lineal de términos menores. Puesto que al hacer estos cambios se rebaja el orden de los monomios el proceso debe acabar en un número finito de pasos. Una vez terminado se normaliza para que todos los polinomios de la base sean mónicos y así se cumpla 1) también.

Sin embargo, la importancia de las bases reducidas va más allá debido a que son únicas (siempre teniendo presente que dependen del orden monomial prefijado).

Teorema 5. *Sea* $\geq$ *un orden monomial en* $\mathbf{k}[X]$. *Cualquier ideal no nulo* I *de* $\mathbf{k}[X]$ *posee una única base de Groebener reducida relativa al orden* $\geq$.

Demostración. Hemos observado ya que I posee alguna base de Groebner reducida ya que cualquier base de Groebner puede modificarse hasta obtener una reducida. Lo que vamos a probar es la unicidad de tales bases.

Sean $G := \{g_1, \ldots, g_t\}$ y $\tilde{G} := \{\tilde{g}_1, \ldots, \tilde{g}_s\}$ bases de Groebner reducidas. Ordenamos estas bases de modo que $\mathrm{LT}(g_1) < \mathrm{LT}(g_2) < \cdots < \mathrm{LT}(g_t)$ y análogamente para $\tilde{G}$. Vamos a demostrar primero que $t = s$ y que $\mathrm{LT}(g_1) = \mathrm{LT}(\tilde{g}_1), \ldots, \mathrm{LT}(g_t) = \mathrm{LT}(\tilde{g}_t)$.

Empezamos probando que $\mathrm{LT}(g_1) = \mathrm{LT}(\tilde{g}_1)$. En efecto, al ser G y $\tilde{G}$. bases de Groebner, existen i, j tales que $\mathrm{LT}(g_i)$ divide a $\mathrm{LT}(\tilde{g}_1)$ y $\mathrm{LT}(\tilde{g}_j)$ divide a $\mathrm{LT}(g_i)$. En particular $\mathrm{LT}(\tilde{g}_j)$ divide a $\mathrm{LT}(\tilde{g}_1)$. Al ser $\tilde{G}$ reducida esto implica que necesariamente $j = 1$. Por lo tanto $\mathrm{LT}(g_i) = \mathrm{LT}(\tilde{g}_1)$ ya que todos los polinomios en G y $\tilde{G}$ son mónicos. Así pues, $\mathrm{LT}(\tilde{g}_1) \geq \mathrm{LT}(g_1)$. Por simetría entre G y $\tilde{G}$ concluimos que $\mathrm{LT}(g_1) = \mathrm{LT}(\tilde{g}_1)$.

Podría ocurrir que existiese algún $i \leq \min\{t, s\}$ tal que $\mathrm{LT}(g_i) \neq \mathrm{LT}(\tilde{g}_i)$. Si esto fuese así tomaríamos el menor de tales i (que será ≥ 2). Sin pérdida de generalidad podemos suponer que $\mathrm{LT}(\tilde{g}_i) > \mathrm{LT}(g_i)$. Observamos que al ser

$\tilde{G}$ una base de Groebner, existe un j tal que $\mathrm{LT}(\tilde{g}_j)$ divide a $\mathrm{LT}(g_i)$. Al haber ordenado $\tilde{G}$ esto implica que $j < i$ pero en tal caso la minimalidad de i nos dice que $\mathrm{LT}(\tilde{g}_j) = \mathrm{LT}(g_j)$ y por lo tanto $\mathrm{LT}(g_j)$ dividiría a $\mathrm{LT}(g_i)$, lo que no es posible por ser G reducida. Así pues $\mathrm{LT}(g_1) = \mathrm{LT}(\tilde{g}_1), \mathrm{LT}(g_2) = \mathrm{LT}(\tilde{g}_2), \ldots$.

El problema es que quizás $t \neq s$. Si esto ocurriese entonces, sin pérdida de generalidad podríamos asumir que $t < s$. Nos fijamos en $\tilde{g}_{s+1}$. Como G es base de Groebner entonces $\mathrm{LT}(\tilde{g}_{s+1})$ queda dividido por algún $\mathrm{LT}(g_i) = \mathrm{LT}(\tilde{g}_i)$, pero como $\tilde{G}$ es reducida esto no puede darse.

Concluimos en este punto que $t = s$ y que $\mathrm{LT}(g_i) = \mathrm{LT}(\tilde{g}_i)$ $i = 1, \ldots, t$. Sin embargo todavía no hemos probado que $G = \tilde{G}$. Solamente hemos probado que los términos directores de los polinomios de G coinciden con los de $\tilde{G}$. Supongamos ahora que hay algún i tal que $\tilde{g}_i \neq g_i$. En ese caso $\tilde{g}_i - g_i$ tendrá término director no nulo y menor que $\mathrm{LT}(g_i) = \mathrm{LT}(\tilde{g}_i)$. Como $\tilde{g}_i - g_i \in I$, esto implica que algún término de g_i o de $\tilde{g}_i$ menor que $\mathrm{LT}(g_i)$ ha de se divisible por algún término en $\mathrm{LT}(G \setminus \{g_i\}) = \mathrm{LT}(\tilde{G} \setminus \{\tilde{g}_i\})$, lo que no es posible debido a que tanto G como $\tilde{G}$ son reducidas. □

Ejemplo. Para terminar con el ejemplo que venimos desarrollando, vamos a convertir la base de Groebner $G = \{xy + 1, y^2 - 1, x + y\}$ en una (la única para el orden lex con $x > y$) reducida. Observamos que $\mathrm{LT}(xy + 1) = xy$ es múltiplo de $\mathrm{LT}(x + y) = x$ por lo que podemos prescindir de $xy + 1$ y así nos quedamos con $G := \{x + y, y^2 - 1\}$. Ahora sí que ningún monomio de los polinomios que forman G es divisible por el término director de polinomios en G, por lo que se cumple la segunda condición en la definición de base de Groebner reducida. Como además los polinomios de G son mónicos también se cumple la primera condición y $\{x + y, y^2 - 1\}$ es una base de Groebner reducida. □

Transformación de bases de Groebner

Aunque el orden lex es muy útil para llevar a cabo la eliminación de indeterminadas en sistemas de ecuaciones polinómicas, el cálculo de bases de Groebner de ideales usando este orden es costoso. Se han estudiado otros algoritmos más rápidos que el algoritmo de Buchberger como por ejemplo el F5 de Faugère. También se están estudiado técnicas que permiten transformar bases de Groebner relativas a un orden en bases de Groebner relativas a otro orden distinto.

Teorema 6 (Cainglia e al, 1988, 1991)**.** *Sea $I = \langle f_1, \ldots, f_s \rangle$ un ideal de $\mathbf{k}[X]$ y $d = \max\{\deg(f_i) \mid i = 1, \ldots, s\}$. Si $|V(I)| < \infty$ entonces se puede calcular una base de Groebner relativa al grevlex con un coste polinomial en d^{n^2} mientras que para el orde lex el coste sería polinomial en d^{n^3}.*

Un banco de pruebas popular para contrastar avances computacionales es la resolución del siguiente sistema de ecuaciones

$$\left.\begin{array}{rcl} x_1 + \cdots + x_n &=& 0 \\ x_1x_2 + \cdots + x_{n-1}x_n + x_nx_1 &=& 0 \\ &\vdots& \\ x_1 \cdots x_{n-1} + \cdots + x_nx_1 \cdots x_{n-2} &=& 0 \\ x_1 \cdots x_n &=& 1 \end{array}\right\}$$

Este problema es muy complejo para $n \geq 8$. El número de soluciones para distintos valores de n son: 6 ($n = 3$), ∞ ($n = 4$), 70 ($n = 5$), 156 ($n = 6$), 924 ($n = 7$), ∞ ($n = 8$), ∞ ($n = 9$), 34940 ($n = 10$), 184756 ($n = 11$), ∞ ($n = 12$). Faugère resolvió el caso $n = 9$ en 1999.

5. Algoritmo FGLM

Teorema 7 (Faugère, Gianni, Lazard, Mora, 1994)**.** *Si $|V(I)| < \infty$ entonces usando el algoritmo FGLM se puede calcular una base de Groebner relativa a cualquier un orden monomial con un coste polinomial en d^{n^2}.*

El algoritmo FGLM propuesto por Faugère, Gianni, Lazard y Mora en 1994 permite, por ejemplo, obtener una base de Groebner reducida para un orden lex a partir de una base de Groebner relativa a otro orden. Desafortunadamente, si $\dim \mathbf{k}[X]/I = \infty$ el algoritmo puede no terminar.

Sea G una base de Groebner de I. Vamos a construir una base de Groebner G_{lex} relativa a un orden lex y una base B_{lex} del espacio vectorial $\mathbf{k}[X]/I$ aprovechando para ello la rapidez de los algoritmos del álgebra lineal. Para ello comenzamos fijando $G_{lex} = \emptyset = B_{lex}$. Habrá monomios que sí incluiremos en B_{lex} y otros que no.

Comenzamos analizando el monomio $X^\alpha = 1$. Calculamos $\overline{\mathrm{N}_G(X^\alpha)} \in \mathbf{k}[X]/I$.

- (Paso 1a) Si es linealmente independiente con $\overline{B_{lex}}$ entonces añadimos X^α a B_{lex} y vamos directamente al paso 2.
- (Paso 1b) Si no es linealmente independiente con $\overline{B_{lex}}$ entonces es que existe $g = X^\alpha - \sum c_\beta X^\beta \in I$ para ciertos $X^\beta \in B_{lex}$ y $c_\beta \in \mathbf{k}$. En este caso añadimos g a B_{lex} y realizamos el siguiente test de finalizado para saber si ya hemos de parar: si X^α es una potencia de la mayor indeterminada x_i (en el nuevo orden) terminamos el proceso. En otro caso vamos al paso 2.
- (Paso 2) Reemplazamos X^α por el siguiente monomio (en el nuevo orden) que no sea divisible por ningún $\mathrm{LT}(g)$ con $g \in G_{lex}$ y retornamos al paso 1a. (Notar que las potencias de x_i no lo son o habríamos terminado ya.)

Se observa que si $\dim_{\mathbf{k}} \mathbf{k}[X]/I < \infty$ (I tiene dimensión cero) entonces el conjunto B_{lex} no puede crecer indefinidamente. También se observa que si en un punto determinado $G_{lex} = \{g_1, \ldots, g_r\}$ entonces, debido al aso 2, $\mathrm{LT}(g_1) < \cdots < \mathrm{LT}(g_r)$ y $\mathrm{LT}(g_i)$ no divide a $\mathrm{LT}(g_j)$ si $i \neq j$. Debido a esto y al Lema de Dickson el conjunto G_{lex} tampoco puede crecer indefinidamente. Así pues, el algoritmo FGLM termina.

Para ver que realmente $G_{lex} = \{g_1, \ldots, g_r\}$ es una base de Groebner relativa al nuevo orden asumamos que existe $0 \neq f \in I$ de modo que $\mathrm{LT}(f)$ no es divido por ningún $\mathrm{LT}(g_j)$. Si $\mathrm{LT}(f) >_{lex} \mathrm{LT}(g_r) = x_i^{\alpha_i}$, como x_i es la mayor indeterminada en el nuevo orden, $\mathrm{LT}(f)$ debe tener exponente mayor que α_i en x_i, por lo que $\mathrm{LT}(g_r)$ divide a $\mathrm{LT}(f)$, lo que no es cierto. Todos los términos en f son necesariamente menores que $\mathrm{LT}(g_r)$ en el orden $>_{lex}$. Reduciéndolos mediante G_{lex} podemos asumir además que ninguno de estos términos queda dividido por $\mathrm{LT}(g_j)$ $j = 1, \ldots, r$. Es decir, todos los monomios que componen a f forman parte de B_{lex} ya que han tenido que ser procesados por el algoritmo antes de que se procese $\mathrm{LT}(g_k)$. Sin embargo esto es imposible ya que los elementos de $\overline{B_{lex}}$ son linealmente independientes en $\mathbf{k}[X]/I$ pero $[f] = [0]$ muestra que son linealmente dependientes.

Ejemplo. Sea $I = \langle x^2 + 2y^2 - y - 2z, x^2 - 8y^2 + 10z - 1, x^2 - 7yz \rangle$. El conjunto $G = \{980z^2 - 18y - 201z + 13, 35yz - 4y + 2z - 1, 8y^2 - 7yz - 10z + 1, x^2 - 7yz\}$ es una base de Groebner relativa al orden grevlex con $x > y > z$. Vamos a transformarla en una base relativa al orden lex:

- $\mathrm{N}_G(1) = 1$ por lo que ahora $B_{lex} = \{1\}$ y pasamos a analizar z.
- $\mathrm{N}_G(z) = z$ por lo que ahora $B_{lex} = \{1, z\}$ y pasamos a analizar z^2.
- $\mathrm{N}_G(z^2) = \frac{9}{490}y + \frac{201}{980}z - \frac{13}{980}$ por lo que ahora $B_{lex} = \{1, z, z^2\}$ y pasamos a analizar z^3.
- $\mathrm{N}_G(z^3) = \frac{2817}{480200}y + \frac{26653}{960400}z - \frac{2109}{960400}$ que, módulo I, depende linealmente de B_{lex}. Definimos entonces $g_1 = z^3 - \frac{313}{980}z^2 + \frac{37}{980}z + \frac{1}{490}$ y $G_{lex} = \{g_1\}$. Al no ser z^3 potencia de x (la mayor variable) seguimos. El siguiente monomio no divisible por z^3 es y.

- $\mathrm{N}_G(y) = y$ que, módulo I, depende linealmente de B_{lex}. Esto nos proporciona $g_2 = y - \frac{980}{18}z^2 + \frac{201}{18}z - \frac{13}{18}$ y $G_{lex} = \{g_1, g_2\}$. Como tampoco se cumple la condición para terminar analizamos el siguiente monomio, que es x.
- $\mathrm{N}_G(x) = x$ por lo que ahora $B_{lex} = \{1, z, z^2, x\}$ y pasamos a analizar x^2.
- $\mathrm{N}_G(x^2) = \frac{4}{5}y - \frac{2}{5}z + \frac{1}{5}$ que, módulo I, depende linealmente de B_{lex}. Definimos $g_3 = x^2 - \frac{392}{9}z^2 + \frac{84}{9}z - \frac{7}{9}$ y $G_{lex} = \{g_1, g_2, g_3\}$. Puesto que ahora sí se cumple la condición para parar, el proceso termina.

El resultado es que $G_{lex} = \{g_1, g_2, g_3\}$ es la base de Groebner reducida de I relativa al orden lex con $x > y > z$ y que $\{\bar{1}, \bar{z}, \bar{z}^2, \bar{x}\}$ es una base de $\mathbf{k}[x, y, z]/I$. □

6. Abanicos de Groebner

Sabemos que a cada orden monomial le corresponde una única base de Groebner reducida. Puede ocurrir que dos órdenes distintos proporcionen la misma base de Groebner reducida, o incluso que como conjuntos las bases sean las mismas pero los términos directores no ya que los órdenes son distintos. Una **base de Groebner marcada** es una base de Groebner en la que hemos marcado los términos directores de sus elementos para distinguirlos.

El problema computacional de calcular bases de Groebner reducidas sugiere que deberíamos conocer mejor cuántas bases de Groebner reducidas tiene un ideal y cómo transformar unas en otras, y no solo para ideales de dimensión cero. Este problema esta muy relacionado con el estudio del siguiente conjunto

$$\mathrm{Mon}(I) = \{\langle \mathrm{LT}_>(I)\rangle \mid \text{ es un orden monomial}\}.$$

ya que

Lemma 3. *Dos bases de Groeber $G_>$ y $G'_{>'}$ reducidas marcadas tales que $\langle \mathrm{LT}_>(G)\rangle = \langle \mathrm{LT}_{>'}(G')\rangle$ son iguales como bases marcadas.*

Demostración. Dado $g \in G$, existe $g' \in G'$ tal que $\mathrm{LT}_{>'}(g')$ divide a $\mathrm{LT}_>(g)$, pero también existe $g_1 \in G$ tal que $\mathrm{LT}_>(g_1)$ divide a $\mathrm{LT}_{>'}(g')$. Al ser G reducida se sigue que $\mathrm{LT}_>(g) = \mathrm{LT}_{>'}(g')$. Por lo tanto $\mathrm{LT}_>(G) = \mathrm{LT}_{>'}(G')$. Más aún, si $\mathrm{LT}_{>'}(g) \neq \mathrm{LT}_>(g)$ entonces un término de g, distinto del director, sería dividido por $\mathrm{LT}_>(g_1)$, lo que no es posible. Por lo tanto $\mathrm{LT}_>(g) = \mathrm{LT}_{>'}(g)$.

Dado $f \in I$, al ser G' base de Groebner existe $g' \in G'$ tal que $\mathrm{LT}_{>'}(g')$ divide a $\mathrm{LT}_{>'}(f)$. Como $\mathrm{LT}_>(G) = \mathrm{LT}_{>'}(G')$ entonces G es base de Groebner relativa al orden $>'$. También G es reducida relativa a $>'$. El lema es ya consecuencia de la unicidad de las bases reducidas para un orden dado. □

Puesto que se considerarán distintos órdenes al mismo tiempo es conveniente a veces introducir en la notación el orden $>$ en relación al cual se realizan las definiciones.

Contrariamente a lo que puede parecer, resulta que $\mathrm{Mon}(I)$ es finito.

Teorema 8. $\mathrm{Mon}(I)$ *es finito.*

Demostración. Asumamos que $\mathrm{Mon}(I)$ es infinito. Esto implica en particular que $I \neq 0$. Tomamos $0 \neq f \in I$. Cada $M \in \mathrm{Mon}(I)$ contiene un término de f por lo que debe existir un término m_1 de f de modo que $\Sigma_1 = \{M \in \mathrm{Mon}(I) \mid m_1 \in M\}$ es infinito. Cada ideal $M \in \Sigma_1$ contiene a $J_1 = \langle m_1 \rangle$, así que existe $M = \langle \mathrm{LT}_>(I) \rangle \in \Sigma_1$ tal que $J_1 \subset M$ (contenido estricto). El término $\mathrm{LT}_>(g)$ con $g \in I$, $\mathrm{LT}_>(g) \in M \setminus J_1$ debe ser linealmente dependiente, módulo I, con los monomios no pertenecientes a M ya que estos monomios proporcionan una base de $\mathbf{k}[X]/I$. Esto prueba que existe $0 \neq f_2 \in I$ tal que ninguno de sus términos pertence a J_1. De nuevo existe un término m_2 de f_2 tal que

$$\Sigma_2 = \{M \in \Sigma_1 \mid m_2 \in M\}$$

es infinito. Formando $J_2 = \langle m_1, m_2 \rangle$ se obtiene un ideal J_2 generado por monomios tal que $J_1 \subset J_2$. Reiterando con J_2 y Σ_2 y usando la noetherianidad de $\mathbf{k}[X]$ se obtiene una contradicción. □

Corolario 4. *El conjunto de bases de Groebner reducidas marcadas de I está en correspondencia biyectiva con* $\mathrm{Mon}(I)$ *y es, por tanto, finito.*

Demostración. La aplicación $G \mapsto \langle$términos marcados en los elementos de $G\rangle$ entre el conjunto de bases de Groebner reducidas marcadas y $\mathrm{Mon}(I)$ es suprayectiva. La inyectividad se sigue del lema previo al teorema □

Una base de Groebner se dice **base de Groebner universal** si es base de Groebner para todos los posibles órdenes monnomiales a la vez. Basta unir las finitas bases de Groebner reducidas para obtener una. Hay sin embargo otros algoritmos para calcularlas.

Dada una matriz $M \in M_{m,n}(\mathbb{R}_{\geq 0})$ tal que $\ker(M) = \{b \in \mathbb{R}^n \mid Mb = 0\}$ corte trivialmente a $\mathbb{Z}^n$ el orden

$$X^\alpha >_M X^\beta \text{ si la primera componente no nula de } M(\alpha - \beta) \text{ es positiva}$$

resulta ser monomial, y de hecho todo orden monomial es de este tipo (Robbiano: *Term orderings on the polynomial ring*, 1985). Es interesante observar que en estos órdenes matriciales si $>_M =>_{M'}$ entonces la primera fila w de M y la primera fila w' de M' están relacionadas mediante $w = \lambda w'$ con $\lambda > 0$. Le vamos a asociar a $>$ muchos más vectores.

Sea G una base de Groebner reducida marcada de I, $G = \{g_1, \ldots, g_r\}$, $X^{\alpha(i)} = \mathrm{LT}(g_i)$, $g_i = X^{\alpha(i)} + \sum c_{i,\beta} X^\beta$. Si M es una matriz tal que $>_M =>$ y w es su primera fila entonces $w \cdot (\alpha(i) - \beta) \geq 0$ si $c_{i,\beta} \neq 0$ por ser $X^{\alpha(i)}$ el término director. Sea

$$C_{G_>} = \{w \in \mathbb{R}^n_{\geq 0} \mid w \cdot \alpha(i) \geq w \cdot \beta \text{ si } c_{i,\beta} \neq 0\}$$

Este conjunto es la intersección finita de semiespacios de $\mathbb{R}^n$ delimitados por hiperplanos que pasan por el origen, es decir es un **cono poliédrico convexo cerrado con vértice en el origen**.

Teorema 9. *Sea I ideal de $\mathbf{k}[X]$ y $G_>$ una base de Groebner reducida marcada de I relativa al orden $>$. Se tiene que:*

i) $\mathrm{Int}(C_G)$ *es un abierto no vacío de* $\mathbb{R}^n$.

ii) Si $M \in M_{m,n}(\mathbb{R}^+_{\geq 0})$ *y* $>_M$ *es un orden monomial tal que la primera fila de* M *pertenece a* $\mathrm{Int}(C_G)$ *entonces* G *es la base de Groebner reducida marcada de* I *relativa a* $>_M$.

iii) Si G' *es otra base de Groebner reducida marcada de* I *distinta de* G *entonces* $C_G \cap C_{G'}$ *está contenido en un hiperplano frontera de* C_G *y* $C_{G'}$.

iv) $\bigcup_{G'} C_{G'} = \mathbb{R}^n_{\geq 0}$ *donde* G' *recorre todas las bases de Groebner reducidas marcadas de* I.

Demostración. i) Sea M una matriz tal que G es base de Groebner reducida marcada relativa a $>_M$ y $w_1, \ldots, w_m$ las filas de M. Consideramos el vector

$$w_\epsilon = w_1 + \epsilon w_2 + \cdots + \epsilon^{m-1} w_m$$

para valores positivos de ϵ cercanos a 0. Si $X^\alpha > X^\beta$ entonces la tupla $(w_1 \cdot (\alpha - \beta), \ldots, w_m \cdot (\alpha - \beta))$ tiene positiva su primera componente no nula. Si ϵ es pequeño entonces $w_\epsilon \cdot (\alpha - \beta) > 0$ ya que las componentes posteriores a la primera componente no nula se ven afactadas de mayor potencia de ϵ. Puesto que hay un número finito de $c_{i,\beta} \neq 0$ entonces existe un ϵ común que nos asegura que $w_\epsilon \cdot \alpha(i) > w_\epsilon \cdot \beta$ si $c_{i,\beta} \neq 0$. Si $\alpha = (0 \ldots, 1, \ldots, 0)$ y $\beta = (0, \ldots, 0)$ el mismo argumento muestra que las componentes de w_e oin positivas. Así pues $w_\epsilon \in \mathrm{Int}(C_G)$.

ii) Asumamos que la primera fila de M pertenece a $\mathrm{Int}(C_G)$. Esto implica que $\mathrm{LT}_{>_M}(g_i) = X^{\alpha(i)}$ para todo i. Por lo tanto $\langle X^{\alpha(1)}, \ldots, X^{\alpha(r)} \rangle \subseteq \langle \mathrm{LT}_{>M}(I) \rangle$. Por lo tanto $\langle LT_>(I) \rangle \subseteq \langle \mathrm{LT}_{>_M}(I) \rangle$. Los monomios que no pertencen a $\langle LT_>(I) \rangle$ forman una base de $\mathbf{k}[X]/I$, lo mismo que los que no pertenecen a $\langle \mathrm{LT}_{>_M}(I) \rangle$, así que forzosamente se ha de tener que $\langle LT_>(I) \rangle = \langle \mathrm{LT}_{>_M}(I) \rangle$. Por la correspondencia biyectiva entre estos ideales y las bases marcadas se sigue que G es la base de Groebner reducida marcada relativa a $>_M$.

iii) Si $C_G \cap C_{G'}$ contuviese un punto en $\mathrm{Int}(C_G)$ entonces, por i), contendría $w \in \mathrm{Int}(C_G) \cap \mathrm{Int}(C_{G'})$. Eligiendo M con primera fila igual a w y tal que $>_M$ sea monomial se seguría por ii) que G y G' coinciden como bases de Groebner marcadas.

iv) Dado $w \in \mathbb{R}^n_{\geq 0}$ podemos encontrar M con primera fila igual a w de modo que $>_M$ sea monomial. Esto nos asegura que w pertenece al cono asociado a alguna base de Groebner reducida marcada. □

Un **abanico** es un conjunto finito de conos poliédricos convexos cerrados con vértice en el origen tal que cumple

(1) Una cara de un cono en el abanico está en el abanico también.

(2) La intersección de dos conos del abanico es una cara de ambos.

Se puede probar que el conjunto formado por todos los conos C_G, al recorrer G todas las bases de Groebner reducidas marcadas, junto con sus caras es un abanico [ver Cox et al]. Este abanico se llama **abanico de Groebner** y codifica información acerca de las posibles bases de Groebner reducidas.

El siguiente ejemplo se ha tomado de [Freeke].

Ejemplo. Sea $I = \langle x^7 - y, x^4 - y^3, x^3y^2 - 1\rangle$.

- Una base de Groebner reducida para el orden grevlex con $x > y$ es $G_1 = \{x^4 - y^3, y^5 - x, x^3y^2 - 1\}$- El correspondiente cono es

$$C_{G_1} = \{(a, b) \in \mathbb{R}^2_{\geq 0} \mid 4a \geq 3b, 5b \geq a, 3a + 2b \geq 0\}.$$

- Para el orden lex con $x > y$ obtenemos $G_2 = \{y^{17} - 1, x - y^5\}$ y un cono

$$C_{G_2} = \{(a, b) \in \mathbb{R}^2_{\geq 0} \mid 17b \geq 0, a \geq 5b\}.$$

- Para el orden lex con $y > x$ obtenemos $G_3 = \{x^{17} - 1, y - x^7\}$ y un cono

$$C_{G_3} = \{(a, b) \in \mathbb{R}^2_{\geq 0} \mid 17a \geq 0, b \geq 7a\}.$$

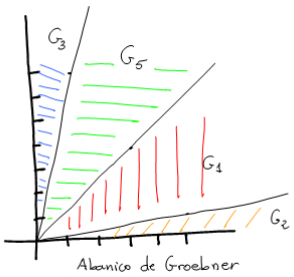
- Para el orden grevlex con $y > x$ volvemos a obtener el cono C_{G_1}.

En la figura vemos que todavía no hemos podido agotar todas las posibles bases de Groebner reducidas. Vamos a hacer trampa (para descubrir una nueva forma de calcular bases de Groebner con Singular). Elegimos el vector $w = (1, 2)$ que no pertenece a ninguno de los conos que nos han aparecido. Completamos este vector hasta una matriz $M = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ para que w esté en el interior del cono asociado al orden $>_M$. Una base de Groebner reducida para este orden es $G_5 = \{y^3 - x^4, x^3y^2 - 1, x^7 - y\}$. El cono asociado es

$$C_{G_5} = \{(a, b) \in \mathbb{R}^2_{\geq 0} \mid 3b \geq 4a, 3a + 2b \geq 0, 7a \geq b\}.$$

Puesto que los conos que tenemos hasta el momento rellenan todo $\mathbb{R}^2_{\geq 0}$, hemos encontrado todas las posibles bases reducidas punteadas para el ideal I.

□



7. Rutas de Groebner (Collart, Kalkbrener, Mall, 1997)

El objetivo es calcular una base de Groebner respecto de un orden $>_t$ conocida una respecto de otro orden $>_s$. El orden $>_t$ lo representamos como $>_{M_t}$ usando alguna matriz M_t cuya primera fila la denotaremos por w_t. Hacemos lo mismo con $>_s$. La idea es intentar movernos del cono que contiene a w_s al que contiene w_t. Durante la ruta cruzaremos de un cono al siguiente y transformaremos la base de Groebner correspondiente al cono antiguo en la base de Groebner del nuevo cono.

Empezamos cruzando los conos. Estamos en el cono C_{old} con base G_{old}, matriz M_{old} con primera fila w_{old}. Sea w_{new} el último punto que nos encontrarmos en el tramo de ruta situado detro de C_{old}. Sea $>_{\text{new}}$ el orden asociado a la matriz

$$\begin{pmatrix} w_{\text{new}} \\ M_t \end{pmatrix}$$

y C_{new} el nuevo cono (en [Cox et al.]. encotrarás un algoritmo de determinar el punto w_{new}).

Una vez que hemos cambiado de cono vamos a transformar la base que representa al cono C_{old} en una para el cono C_{new}. Como w_{new} está en la frontera de C_{old}, hay algún elemento $g \in G_{\text{old}}$ cuyo monomio director tiene el mismo w_{new}-peso que alguno de sus términos (el w-peso de X^α es $w \cdot \alpha$). La **forma inicial** de f relativa a w se define como

$$\text{ini}_w(f) = \text{suma de todos los términos de } f \text{ de } w\text{-peso máximo.}$$

Análogamente $\text{ini}_w(S) = \{\text{ini}_w(f) \mid f \in S\}$.

Teorema 10. *Sea H una base de Groebner mónica de $\langle \text{ini}_{w_{new}}(G_{old})\rangle$ con respecto al orden matricial $>_{new}$ representado por la matriz $\begin{pmatrix} w_{new} \\ M_t \end{pmatrix}$. Escribimos cada $h_j \in H$ como*

$$h_j = \sum_{g \in G_{old}} p_{i,g}\, \text{ini}_{w_{new}}(g).$$

Se tiene que los polinomios $\bar{h}_j = \sum_{g \in G_{old}} p_{j,g} g$ *forman una base de Groebner de* I *relativa a* $>_{new}$.

En general la base que se obtiene del teorema no es reducirla así que hay que reducirla para seguir el proceso. En principio se espera que el cálculo de H no sea costoso. Los polinomios $p_{j,g}$ se pueden obtener dividiendo h_j por $\mathrm{ini}_{w_{\mathrm{new}}}(G_{\mathrm{old}})$ usando $>_{\mathrm{old}}$.

Ejemplo. Consideremos de nuevo el ideal $I = \langle x^7 - y, x^4 - y^3, x^3y^2 - 1\rangle$. Vamos a transformar una base de Groebner relativa al orden grevlex en otra relativa al orden lex con $y > x$. Este orden lex se puede caracterizar como un orden matricial mediante $M_t = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}$.

Iremos siguiendo la horizontal desde el cono C_{G_1} hasta el punto $(0, 4)$, así que inicialmente el cono C_{old} será C_{G_1} y la base $G_{\mathrm{old}} = \{x^4 - y^3, y^5 - x, x^3y^2 - 1\}$. El último punto por el que pasamos para abandonar el cono C_{G_1} es $w_{\mathrm{new}} = (3, 4)$. La matriz M_{new} es $M_{\mathrm{new}} = \begin{pmatrix} 3 & 4 \\ 0 & 4 \\ 1 & 0 \end{pmatrix}$ (observar que la última fila es superflua) y empezamos...

- El conjunto $\mathrm{ini}_{\mathrm{new}}(G_{\mathrm{old}})$ es $\{x^4 - y^3, y^5, x^3y^2\}$;
- una base de Groebner relativa a $>_{\mathrm{new}}$ de $\langle \mathrm{ini}_{\mathrm{new}}(G_{\mathrm{old}})\rangle$ es $H = \{y^3 - x^4, x^3y^2, x^7\}$. Calculamos la expresión de cada uno de los h_j propuesta en el teorema:
  - $h_1 = y^3 - x^4 = -1(x^4 - y^3)$ proporciona $\bar{h}_1 = -1(x^4 - y^3)$,
  - $h_2 = x^3y^2 = 1x^3y^2$ proporciona $\bar{h}_2 = x^3y^2 - 1$,
  - $h_3 = x^7 = x^3(x^4 - y^3 + y(x^3y^2)$ proporciona $\bar{h}_3 = x^3(x^4 - y^3) + y(x^3y^2 - 1)$.
- Al reducir estos vectores para obtener una base de Groebner relativa a $>_{\mathrm{new}}$ obtenemos $G_{\mathrm{new}} = \{y^3 - x^4, x^3y^2 - 1, x^7 - y\}$.

Ahora ya estamos en el siguiente cono, pero todavía hemos de seguir avanzando. La siguiente parada en la ruta es el punto $w_{\mathrm{new}} = (4/7, 4)$, así que ahora $M_{\mathrm{new}} = \begin{pmatrix} 4/7 & 4 \\ 0 & 4 \\ 1 & 0 \end{pmatrix}$ mientras que $G_{\mathrm{old}} = \{y^3 - x^4, x^3y^2 - 1, x^7 - y\}$.

- El conjunto $\mathrm{ini}_{\mathrm{new}}(G_{\mathrm{old}})$ es $\{y^3, x^3y^2, x^7 - y\}$;
- una base de Groebner relativa a $>_{\mathrm{new}}$ de $\langle \mathrm{ini}_{\mathrm{new}}(G_{\mathrm{old}})\rangle$ es $H = \{y - x^7, x^{17}\}$. Calculamos la expresión de cada uno de los h_j propuesta en el teorema:
  - $h_1 = y - x^7 = -1(x^7 - y)$ proporciona $\bar{h}_1 = y - x^7$,

- $h_2 = x^{17} = (x^{10} + x^3y)(x^7 - y) + x^3y^2$ proporciona $\bar{h}_2 = (x^{10} + x^3y)(x^7 - y) + x^3y^2 - 1 = x^{17} - 1$.

- Al reducir estos vectores para obtener una base de Groebner relativa a $>_{\text{new}}$ llegamos a $G_{\text{new}} = \{y - x^7, x^{17} - 1\}$.

De este modo se ha convertido la base de Groebner original en una para el orden lex.

□.

En el ejemplo se ha usado solamente dos variables por sencillez, lo que limita el número de rutas "diferentes"para ir de un cono a otro. Con un mayor número de variables tiene interés buscar estrategias que permitan optimizar este método.

8. Referencias

- Cox, Little, O'Shea: *Using Algebraic Geometry*. Springer, 2005.

- Freeke: *Linking Gröbner bases and toric varieties*, 2009 (master project).

Teoría de la eliminación (mediante bases de Groebner)

9. Eliminacion de indeterminadas

La eliminación de indeterminadas en sistemas de ecuaciones polinómicas es una técnica similar al proceso de eliminación gaussiana. Descomponemos el conjunto $X = \{x_1, \ldots, x_n\}$ en una unión disjunta $X = X' \cup X''$ con $X' \neq \emptyset \neq X''$. Un **orden de eliminación** en $\mathbf{k}[X]$ (para el cual las indeterminadas en X' son mayores que las indeterminadas en X'') es un orden monomial con la siguiente propiedad:

$$X'^{\alpha} X''^{\beta} > X'^{\gamma} X''^{\delta} \text{ si } \begin{cases} X'^{\alpha} > X'^{\gamma} \\ \text{ó} \\ X'^{\alpha} = X'^{\gamma} \text{ pero } X''^{\beta} > X''^{\delta} \end{cases}$$

Teorema 11 (Teorema de eliminación)**.** *Sea $>$ un orden de eliminación en $\mathbf{k}[X]$ para el cual las indeterminadas en X' son mayores que las de X''. Dado un ideal I de $\mathbf{k}[X]$ y una base de Groebner G de I relativa al orden $>$ se tiene que $G \cap \mathbf{k}[X'']$ es base de Groebner de $I \cap \mathbf{k}[X'']$ (**ideal de eliminación**).*

Demostración. Dado $0 \neq f \in I$ existe $g \in G$ tal que $\mathrm{LT}(g)$ divide a $\mathrm{LT}(f)$. Cualquier monomio que contenga indeterminadas en X' es mayor que los términos de f, por lo que $g \in \mathbf{k}[X'']$. Así pues, los términos directores de elementos en $I \cap \mathbf{k}[X'']$ son divididos por términos directores de elementos en $G \cap \mathbf{k}[X'']$. Esto prueba el resultado. □

Dado $S \subseteq \mathbf{k}[X]$ sea $V(S) = \{(a_1, \ldots, a_n) \in \mathbf{k}^n \mid f(a_1, \ldots, a_n) = 0 \quad \forall_{f \in S}\}$ el **conjunto algebraico afín** determinado por S. Observamos que $V(S) = V(I)$ donde $I = \langle S \rangle$. Si $G = \{g_1, \ldots, g_t\}$ es base de Groebner de I entonces $V(S) = \{z \in \mathbf{k}^n \mid g_1(z) = 0, \ldots, g_t(z) = 0\}$. El teorema anterior sugiere que $g_1(z) = 0, \ldots, g_t(z) = 0$ es una "versión escalonada"del sistema de ecuaciones determinado por S.

Al eliminar las variables, digamos $x_1, \ldots, x_l$ quedan ecuaciones solamente en $x_{l+1}, \ldots, x_n$. Encontrar $(a_{l+1}, \ldots, a_n)$ que las cumplan no significa que se exista $(a_1, \ldots, a_n)$ que cumpla todas las ecuaciones del sistema, ni siquiera aunque el cuerpo sea algebraicamente cerrado.

Teorema 12 (Teorema de extensión)**.** *Dado $I = \langle f_1, \ldots, f_s \rangle$ un ideal de $\mathbf{k}[X]$ consideramos la decomposición*

$$f_i = g_i(x_2, \ldots, x_n) x_1^{N_i} + \text{ términos de menor grado en } x_1$$

con $g_i(x_2, \ldots, x_n) \neq 0$. Si $(a_2, \ldots, a_n) \in V(I \cap \mathbf{k}[x_2, \ldots, x_n])$ y $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_s)$ entonces existe $a_1 \in \mathbb{C}$ tal que $(a_1, \ldots, a_n) \in V(I)$.

Las hipótesis del teorema se cumplen trivialmente si algún q_i es una constante no nula.

Ejemplo. Sea $I = \langle (x-y)^3 - z^2, (z-x)^3 - y^2, (y-z)^3 - x^2 \rangle$. Usando un orden de eliminación para eliminar las variables x, y como por ejemplo el lex con $x > y > z$ se obtiene que $I \cap \mathbb{Q}[z] = \langle p(z) \rangle$ donde $p(z) = 15625z^8 + 3750z^6 + 452z^4 + 8z^2 \rangle$. Por simetría en los generadores de I se tiene que $I \cap \mathbb{Q}[x] = \langle p(x) \rangle$ e $I \cap \mathbb{Q}[y] = \langle p(y) \rangle$. Esto obviamente limita el número de elementos de $V(I)$ a 8^3, pero todavía esta cota se puede mejorar.

□.

Fijemos la notación

$$\mathrm{I}(V) = \{ f \in \mathbf{k}[X] \mid f(a_1, \ldots, a_n) = 0 \quad \forall_{(a_a, \ldots, a_n) \in V} \}.$$

El conjunto $\mathrm{I}(V)$ es un ideal de V.

Teorema 13 (Teorema débil de los ceros de Hilbert)**.** *Sea $\bar{\mathbf{k}}$ un cuerpo algebraicamente cerrado e I un ideal de $\bar{\mathbf{k}}[X]$. Si $V(I) = \emptyset$ entonces $I = \bar{\mathbf{k}}[X]$.*

Teorema 14 (Teorema de los ceros de Hilbert)**.** *Sea $\bar{\mathbf{k}}$ un cuerpo algebraicamente cerrado e I un ideal de $\bar{\mathbf{k}}[X]$. Se tiene que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in V(I)$ si y solamente si existe un $m \geq 1$ tal que $f^m \in I$.*

El conjunto

$$\sqrt{I} = \{ f \in \mathbf{k}[X] \mid \exists m \geq 1 \text{ tal que } f^m \in I \}$$

se llama **radical** del ideal I y es también un ideal que contiene a I. Obviamente $\sqrt{\sqrt{I}} = \sqrt{I}$ y

$$V(\sqrt{I}) = V(I).$$

Los ideales que coinciden con su radical se llaman **ideales radicales**. El Teorema de los ceros de Hilbert implica que si $\bar{\mathbf{k}}$ es algebraicamente cerrado entonces la correspondencia

$$\begin{array}{rcl} \{\text{ideales radicales de } \bar{\mathbf{k}}[X]\} & \leftrightarrow & \{\text{conjuntos algebraicos afines } \bar{\mathbf{k}}^n\} \\ I & \rightarrow & V(I) \\ \mathrm{I}(V) & \leftarrow & V \end{array}$$

es biyectiva.

Eliminar variables es, en cierto sentido, similar a proyectar. Sea $\pi \colon \mathbb{C}^n \to \mathbb{C}^{n-l}$ la proyección en las últimas $n-l$ coordenadas. Sea $I_l = I \cap \mathbb{C}[x_{l+1}, \ldots, x_n]$ y $V = V(I)$. Claramente $\pi_l(V) \subseteq V(I_l)$. Si nos fijamos en uno solo de los pasos en la eliminación de variables y usamos la notación del Teorema de extensión vemos que

$$V(I_1) = \pi_1(V) \cup (V(g_1, \ldots, g_s) \cap V(I_1))$$

ya que o bien $(a_2, \ldots, a_n)$ se extiende (y así pertenece a $\pi_1(V)$) o bien no lo hace y así pertenece a $V(g_1, \ldots, g_s)$ por el Teorema de extensión.

Teorema 15 (Clausura de la proyección)**.** *Sea* $V = V(f_1, \ldots, f_s) \subseteq \mathbb{C}^n$, $I = \langle f_1, \ldots, f_s \rangle$ *e* $I_l = I \cap \mathbf{k}[x_{l+1}, \ldots, x_n]$. *Se tiene que*

$$V(I_l) \text{ es el menor conjunto algebraico afín que contiene a } \pi_l(V).$$

Demostración. Sea W un conjunto algebraico afín que contiene a $\pi_l(V)$. Dado un polinomio $h(x_{l+1}, \ldots, x_n) \in \mathrm{I}(W)$ se tiene que $h(a_{l+1}, \ldots, a_n) = 0$ para cualquier $(a_1, \ldots, a_n) \in V$. Si vemos $h(x_{l+1}, \ldots, x_n)$ como un polinomio en $\mathbb{C}[X]$ entonces $h(a_1, \ldots, a_n) = 0$ por lo que existe $m \geq 1$ tal que $h^m(x_{l+1}, \ldots, x_n) \in I_l$. Por lo tanto $h(x_{l+1}, \ldots, x_n) \in \sqrt{I_l}$. Así pues, $\mathrm{I}(W) \subseteq \sqrt{I_l}$. La correspondencia entre conjuntos algebraicos afines e ideales implica finalmente que $V(I_l) = V(\sqrt{I_l}) \subseteq V(\mathrm{I}(W)) = W$. Esto demuestra el teorema. □

10. Sistemas de ecuaciones polinomiales con un número finito de soluciones

Dado un ideal I de $\mathbf{k}[X]$ y $U \subseteq X$ se dice que U es **algebraicamente independiente** módulo I si $\mathbf{k}[U] \cap I = 0$. La **dimensión** de I se define como la mayor de las cardinalidades de los subconjuntos algebraicamente independientes de X.

Teorema 16. *Equivalen*

i) $\dim I = 0$

ii) $\dim_{\mathbf{k}} \mathbf{k}[X]/I < \infty$

iii) Toda base de Groebner G *de* I *cumple que para todo* $i = 1, \ldots, n$ *existe* $g_i \in G$ *y* $m_i > 0$ *con* $\mathrm{LM}(g_i) = x_i^{m_i}$.

iv) Existe una base de Groebner G *de* I *tal que para todo* $i = 1, \ldots, n$ *existe* $g_i \in G$ *y* $m_i > 0$ *con* $\mathrm{LM}(g_i) = x_i^{m_i}$.

v) Si además $\mathbf{k}$ *es algebraicamente cerrado entonces las condiciones anteriores equivalen a que* $|V(I)| < \infty$.

Demostración. La dimensión I es cero si y solamente si $I \cap \mathbf{k}[x_i] \neq 0$ para todo $i = 1, \ldots, n$, y esto equivale a que $\dim \mathbf{k}[X]/I < \infty$ y obviamente también equivale a que en toda base de Groebner y para cualquier x_i debe existir algún elemento con monomio director potencia de x_i o a que exista alguna de tales bases. Asi pues, los cuatro primeros puntos del teorema son equivalentes. También es obvio que iv) implica v).

Asumamos ahora que $|V(I)| < \infty$. Si $V(I) = \emptyset$ el Teorema de los ceros de Hilbert en su versión débil implica que $I = \mathbf{k}[X]$ y así iv) es cierta. Si $V(I) = \{z_1, \ldots, z_k\}$ y $z_i = (a_{i1}, \ldots, a_{in})$ el polinomio $f(x_j) = \prod_{i=1}^{k}(x_j - a_{ij})$ se anula en $V(I)$ y por lo tanto existe m tal que $f^m \in I$. Así pues, toda base de Groebner debe contener algún elemento cuyo monomio director divida a $\mathrm{LT}(f) = x_i^k$, lo que prueba que iv) implica iii). □

Teorema 17. *Sea $\bar{\mathbf{k}}$ algebraicamente cerrado e I un ideal de $\bar{\mathbf{k}}[X]$ de dimensión cero. Se tiene que*

$$|V(I)| \leq \dim_{\bar{\mathbf{k}}} \bar{\mathbf{k}}[X]/I.$$

La igualdad se da si y sololamente si $I = \sqrt{I}$.

Demostración. Sea $V(I) = \{z_1, \ldots, z_k\}$. Si z_1 no es proporcional a z_2 entonces existe un polinomio lineal que cumple que $f(z_1) = 1$ mientras que $f(z_2) = 0$. Si $z_1 = \lambda z_2$ con $z_2 \neq (0, \ldots, 0)$ y $\lambda \neq 1$ elegimos una componente a_i no nula de z_2. El polinomio $f = (x_i - a_i)/(\lambda a_i - a_i)$ también cumple que $f(z_1) = 0$ mientras que $f(z_2) = 0$. Usando este tipo de polinomios podemos concluir que existen polinomios $f_i \in \bar{\mathbf{k}}[X]$ tales que $f_i(z_j) = \delta_{ij}$. Con ellos se define la aplicación

$$\begin{array}{rcl} \varphi\colon \bar{\mathbf{k}}[X]/I & \to & \bar{\mathbf{k}}^k \\ [f] & \mapsto & (f(z_1), \ldots, f(z_k)) \end{array}$$

es suprayectiva. Por lo tanto $k = |V(I)| \leq \dim_{\bar{\mathbf{k}}} \bar{\mathbf{k}}[X]/I$. Usando el Teorema de los ceros de Hilbert vemos que $\ker \varphi = [\sqrt{I}]$. Finalmente observamos que $I = \sqrt{I} \Leftrightarrow \varphi$ es inyectiva $\Leftrightarrow \dim_{\bar{\mathbf{k}}} \bar{\mathbf{k}}[X]/I = k = |V(I)|$. □

Puesto que para saber el número exacto de soluciones de un sistema de ecuaciones polinomiales sobre un cuerpo algebraicamente cerrado hemos de utilizar $\sqrt{I}$ en lugar de I veamos cómo calcularlo.

Proposición 2. *Sea $\mathbf{k}$ un cuerpo perfecto, $I = \langle f_1, \ldots, f_r \rangle$ un ideal de $\mathbf{k}[X]$ y $\mathbf{k}[x_i] \cap I = \langle p_i(x_i) \rangle$. Sea $g_i(x_i)$ la parte libre de cuadrados de $g_i(x_i)$. Se tiene que*

$$\sqrt{I} = \langle f_1, \ldots, f_r, g_1, \ldots, g_n \rangle.$$

Demostración. El ideal $J = \langle f_1, \ldots, f_r, g_1, \ldots, g_n \rangle$ está contenido en $\sqrt{I}$ por lo que $\sqrt{J} \subseteq \sqrt{I}$. Como también $\sqrt{I} \subseteq \sqrt{J}$, se tiene que $\sqrt{I} = \sqrt{J}$. Si probamos que J es un ideal radical habrá quedado probada la proposición. Lo que vamos a probar es que J es intersección de ideales maximales. Un ideal maximal es también un ideal primo, por lo que es un ideal radical, y como la intersección de ideales radicales es radical, habremos acabado.

Los polinomios g_i cumplen que, al ser $\mathbf{k}$ perfecto, $\mathrm{mcd}(g_i, g_i') = 1$, donde g_i' denota la derivada de g_i. Así, el resultado será consecuencia del siguiente lema.

Lemma 4 (Lema de Seidenberg)**.** *Sea J un ideal de dimensión cero. Si para toda x_i existe $g_i \in J \cap k[x_i]$ tal que $\mathrm{mcd}(g_i, g_i') = 1$ el ideal J es intersección de ideales maximales.*

Demostración. El lema se prueba por inducción en n. Si $n = 1$ el ideal J es principal $J = \langle g \rangle$ con g libre de cuadrados ya que g_1 lo es. Descomponiendo $g = h_1 \cdots h_s$ en producto de polinomios irreducibles se tiene que $\langle g \rangle = \langle h_1 \rangle \cap \cdots \langle h_s \rangle$. Como en $\mathbf{k}[x_1]$ el ser ideal maximal es equivalente a ser un ideal generado por un polinomio irreducible el resultado quedaría probado. Asumamos ahora que es cierto hasta $n-1$. Puesto que los polinomios $g/h_1, \ldots, g/h_n$ son primos entre

sí podemos econtrar una descomposición $1 = p_1 g/h_1 + \cdots + p_s g/h_s$. Consideramos $\mathbf{k}[x_1]/\langle g_1\rangle$ que es isomorfo a un producto cartesiano de cuerpos $\mathbf{k}[x_1]/\langle h_1\rangle \times \cdots \times \mathbf{k}[x_1]/\langle h_s\rangle = K_1 \times \cdots \times K_s$. Sea $\varphi_1 \colon \mathbf{k}[x_1] \to K_i$ la i-ésima proyección. Extendemos φ_i hasta un epimorfismo $\varphi_i \colon \mathbf{k}[x_1, \ldots, x_n] \to K_i[x_2, \ldots, x_n]$. La imagen $J_i = \varphi_i(J)$ es un ideal de $K_i[x_2, \ldots, x_n]$. El ideal J_i contiene a los elementos $\varphi_i(g_2), \ldots, \varphi_i(g_n)$, que coinciden con $g_2, \ldots, g_n$ si vemos estos últimos como polinomios con coeficientes en el cuerpo K_i extensión de $\mathbf{k}$. Puesto que el máximo común divisor y el polinomio derivada no dependen de si se calculan en un cuerpo o en una extensión, se cumplen las condiciones para aplicar la hipótesis de inducción. Concluimos que J_i es una intersección de ideales maximales. Esto prueba que también $M_i = \varphi_i^{-1}(J_i) = J + \ker \varphi_i = J + \langle h_i\rangle$ lo es. Bastará ahora probar que $J = \cap_i M_i$. Si $x \in \cap_i M_i$ entonces $xg/h_i \in J + \langle g\rangle \subseteq J$, así que $x = x1 = \sum p_i(xg/h_i) \in J + \langle g\rangle$. Asi pues, $\cap_i M_i \subseteq J \subseteq \cap_i M_i$. □

Queda probado el teorema □

Ejemplo. Volvamos al ejemplo $I = \langle (x-y)^3 - z^2, (z-x)^3 - y^2, (y-z)^3 - x^2\rangle$. Habíamos visto que $I \cap \mathbf{k}[z] = \langle p(z)\rangle$ con $p(z) = 15625z^8 + 3750z^6 + 452z^4 + 8z^2$. La parte libre de cuadrados de este polinomio es $g(z) = 15625z^7 + 3750z^5 + 452z^3 + 8z$. Añadiendo $g(x), g(y), g(z)$ a los generadores del ideal y calculando una base de Groebner de $\sqrt{I}$ observamos que $\dim \mathbb{C}[x,y,z]/\sqrt{I} = 7$, por lo que $V(I)$, visto dentro de $\mathbb{C}^3$, contiene 7 puntos. Si además hemos usado un orden de eliminación (el orde lex lo es) observaremos que $V(I)$ está determinado por las ecuaciones

$$\left.\begin{aligned} 15625z^7 + 3750z^5 + 425z^3 + 8z &= 0 \\ 8y + 3125z^6 + 1250z^5 + 750z^4 + 250z^3 + 65z^2 + 24z &= 0 \\ 8x - 3125z^6 + 1250z^5 - 750z^4 + 250z^3 - 65z^2 + 24z &= 0 \end{aligned}\right\}$$

Este sistema lo podriamos resolver por sustitución regresiva si supiésemos resolver la primera ecuación (que no es difícil), aunque hay que observar que si esta ecuación se resuelve solo de forma aproximada los errores se propagarán al resto de variables.

□.

En este punto ya podriamos definir dos interesantes algoritmos para calcular el radical de ideales de dimensión cero y para comprobar si un tal ideal es radical o no: basta ir calculando $I \cap \mathbf{k}[x_i] = \langle p_i\rangle$ y si para algún i se tiene que $\mathrm{mcd}(p_i, p_i') \neq 1$ entonces I no es radical, pero si siempre ocurre que $\mathrm{mcd}(p_i, p_i') = 1$ entonces el ideal es radical (de nuevo p_i' denota la derivada de p_i).

11. Transformación en ecuaciones implícitas

Consideremos $f_1, \ldots, f_n \in \mathbf{k}[t_1, \ldots, t_m]$ y

$$\begin{aligned} F \colon \mathbf{k}^m &\to \mathbf{k}^n \\ (a_1, \ldots, a_m) &\mapsto (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m)). \end{aligned}$$

Encontrar el menor conjunto algebraico afín en $\mathbf{k}^n$ que contiene a $F(\mathbf{k}^m)$ implica encontrar las ecuaciones polinomiales que satisfacen los puntos en $F(\mathbf{k}^m)$. El grafo de la aplicación F es el conjunto de puntos en $\mathbf{k}^{m+n}$ de la forma $(t_1, \ldots, t_m, x_1, \ldots, x_n)$ tales que $x_i - f_i(t_1, \ldots, t_m) = 0$ $i = 1, \ldots, n$. Es decir, el conjunto algebraico afín definido por el ideal

$$I = \langle x_1 - f_1(t_1, \ldots, t_m), \ldots, x_n - f_n(t_1, \ldots, t_m) \rangle$$

El ideal de eliminación

$$I_m = \mathbf{k}[x_1, \ldots, x_n] \cap I$$

recoge ecuaciones que cumplen los puntos $(x_1, \ldots, x_n) \in F(\mathbf{k}^m)$.

Teorema 18 (Transformación en ecuaciones implícitas)**.** *Si* $\mathbf{k}$ *un cuerpo infinito El conjunto* $V(I_m)$ *es el menor conjunto algebraico afín en* $\mathbf{k}^n$ *que contiene a* $F(\mathbf{k}^m)$*.*

Demostración. Observamos que $F(\mathbf{k}^m)$ es proyección del grafo de la aplicación F sobre las n últimas componentes. El teorema acerca de la interpretación geométrica de la eliminación de indeterminadas nos dice, si $\mathbf{k} = \mathbb{C}$ o si es algebraicamente cerrado, que $V(I_m)$ es el menor conjunto algebraico afin que que contine a $F(\mathbf{k}^m)$. El teorema es cierto también si $\mathbf{k}$ es infinito [Cox et al.]. □

Este teorema se puede extender a aplicaciones no polinomiales. Dada una aplicación $F\colon \mathbf{k}^m \setminus V(g_1, \ldots, g_n) \to \mathbf{k}^n$

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right)$$

para ciertos polinomios $f_1, \ldots, f_n, g_1, \ldots, g_n \in \mathbf{k}[t_1, \ldots, t_m]$ con $g_1 \cdots g_n \neq 0$, un argumento similar al anterior pero añadiendo una indeterminada más y y una ecuación $y g_1(t_1, \ldots, t_m) \cdots g_n(t_1, \ldots, t_m) = 1$ que codifica el que los polinomios g_i no sean nulos muestra para esta aplicación F el siguiente resultado:

Teorema 19. *Sea* $\mathbf{k}$ *es infinito,* $J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - y g_1 \cdots g_n \rangle \subseteq \mathbf{k}[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$ *y* $J_{m+1} = J \cap \mathbf{k}[x_1, \ldots, x_n]$*. Se tiene que* $V(J_{m+1})$ *es el menor conjunto algebraico afín en* $\mathbf{k}^n$ *que contiene a* $F(\mathbf{k}^m \setminus W)$*.*

Ejemplo. La clausura de Zariski del conjunto $\{(t + u, t^2 + 2tu, t^3 + 3t^2u) \mid t, u\}$ está determinada por la ecuación $4x^3z - 3x^2y^2 - 6xyz + 4y^3 + z^2 = 0$.

□

12. Aritmética de ideales

Sean I, J ideales $\mathbf{k}[X]$. Los conjuntos

$$\begin{aligned} I + J &= \{f + g \mid f \in I,\, g \in J\} \\ IJ &= \{f_1 g_1 + \cdots + f_s g_s \mid s \in \mathrm{N},\, f_1, \ldots, f_s \in I,\, g_1, \ldots, g_s \in J\} \\ I \cap J &= \{f \in I \mid f \in J\} \end{aligned}$$

son también ideales.

Proposición 3. *Se tiene que:*

i) $V(I+J) = V(I) \cap V(J)$ *y*

ii) $V(IJ) = V(I) \cup V(J) = V(I \cap J)$.

Claramente, si $I = \langle f_1, \ldots, f_s \rangle$ y $J = \langle g_1, \ldots, g_r \rangle$ se tiene que $I + J = \langle f_1, \ldots, f_s, g_1, \ldots, g_r \rangle$ e $IJ = \langle f_i g_j \mid i = 1, \ldots, s,\ j = 1, \ldots, t \rangle$. Sin embargo, calcular un conjunto generador de $I \cap J$ es más complicado. Dado $f(t) \in \mathbf{k}[t]$, consideraremos el ideal de $\mathbf{k}[t, x_1, \ldots, x_n]$

$$fI = \langle f f_1, \ldots, f f_s \rangle.$$

Este ideal está generado por $f f_1, \ldots, f f_s$ en $\mathbf{k}[t, X]$ no en $\mathbf{k}[X]$.

Proposición 4. *Sean* I, J *ideales de* $\mathbf{k}[X]$ *y* $t \notin X$ *otra indeterminda. Se tiene que*

$$I \cap J = (tI + (1-t)J) \cap \mathbf{k}[X].$$

Demostración. Cualquier elemento $f \in I \cap J$ puede escribirse como $f = tf + (1-t)f$, por lo que uno de los contenidos es evidente. Por otro lado, dado $f \in (tI + (1-t)J) \cap \mathbf{k}[X]$ escribimos $f = g(t, X) + h(t, X)$ con $g(t, X) \in tI$ y $h(t, X) \in (1-t)J$. Como f no depende de t basta evaluar en $t = 0$ y $t = 1$ la anterior expresión para concluir que $f \in I \cap J$. □

La proposición anterior muestra que si $I = \langle f_1, \ldots, f_s \rangle$ y $J = \langle g_1, \ldots, g_r \rangle$ entonces el ideal de eliminación relativo a t de $\langle tf_1, \ldots, tf_s, (1-t)g_1, \ldots, (1-t)g_r \rangle$ será $I \cap J$.

Es interesante observar que el hecho de que $\langle f \rangle \cap \langle g \rangle = \langle \mathrm{mcd}(f, g) \rangle$ y $\mathrm{mcd}(f, g) = \frac{fg}{\mathrm{mcm}(f,g)}$ permite calcular estos polinomios, aunque no de forma eficiente.

13. Cociente de ideales. Saturación

Aunque la unión de conjuntos algebraicos afines es de nuevo un conjunto algebraico afín, la diferencia no lo es en general. Sin embargo podemos determinar el sistema de ecuaciones que cumple. La clausura de Zariski de un conjunto $S \subseteq \mathbf{k}^n$ es el conjunto $\bar{S} = V(\mathrm{I}(S))$ y ya ha aparecido anteriormente. Se llama **ideal cociente** de I por J al ideal

$$I : J = \{f \mid fg \in I \quad \forall_{g \in J}\}.$$

El **ideal de saturación** de I relativo a J es el ideal $I : J^\infty = \cup_{k=1}^{\infty} I : J^k$.

Teorema 20. *Sea* $\bar{\mathbf{k}}$ *algebraicamente cerrado. Se tiene que*

$$\overline{V(I) \setminus V(J)} = V(I : J^\infty).$$

En el caso en que I *sea además un ideal radical entonces*

$$\overline{V(I) \setminus V(J)} = V(I : J).$$

Demostración. Dados $f \in I : J$ y $z \in V(I) \setminus V(J)$, existe $g \in J$ tal que $g(z) \neq 0$. Al pertenecer fg a I se tiene que $f(z)g(z) = 0$, por lo que $f(z) = 0$. Así, $f \in \mathrm{I}(V(I) \setminus V(J))$. Esto prueba que $\overline{V(I) \setminus V(J)} \subseteq V(I : J)$.

Para cualquier ideal radical I, $h \in \mathrm{I}(V(I) \setminus V(J))$ y $g \in V(J)$ el polinomio hg se anula en $V(I)$ por lo que $hg \in \sqrt{I} = I$. Esto prueba que $\mathrm{I}(V(I) \setminus V(J)) \subseteq I : J$. Por lo tanto $V(I : J) \subseteq \overline{V(I) \setminus V(J)}$.

La primera igualdad no la demostramos. □

Observamos que si $I \cap \langle g \rangle = \langle h_1, \ldots, h_p \rangle$ entonces $I : \langle g \rangle = \langle h_1/g, \ldots, h_p/g \rangle$. Se tiene asi un algoritmo para calcular $I : J$. Dados $I = \langle f_1, \ldots, f_r \rangle$, $J = \langle g_1, \ldots, g_s \rangle$: calculamos un conjunto generador de $I : \langle g_i \rangle$ usando la observación anterior. Después se aprovecha que $I : \langle g_1, \ldots, g_s \rangle = I : \langle g_1 \rangle \cap \cdots \cap I : \langle g_2 \rangle$ y ya se tiene.

En el caso particular de $J = \langle f \rangle$

$$I : f^\infty = \{g \mid \exists m \geq 0 \text{ tal que } gf^m \in I\}.$$

Es sencillo probar que si $I = \langle f_1, \ldots, f_s \rangle$ entonces $I : f^\infty = \mathbf{k}[X] \cap \langle f_1, \ldots, f_s, 1 - yf \rangle$ donde y es una nueva indeterminada.

14. Núcleo e imagen de un homomorfismo

Sea $Y = \{y_1, \ldots, y_m\}$, $X = \{x_1, \ldots, x_n\}$ y $\phi\colon \mathbf{k}[Y] \to \mathbf{k}[X]$ un homomorfismo de álgebras de polinomios determinado por $\phi(y_j) = f_j(X)$ $j = 1, \ldots, m$. Sea

$$I = \langle y_1 - f_1(X), \ldots, y_m - f_m(X) \rangle.$$

Teorema 21. *Se tiene que* $\ker \phi = I \cap \mathbf{k}[Y]$.

Demostración. Dado $g(Y) = \sum_\alpha c_\alpha Y^\alpha \in \ker \phi$ podemos escribirlo como

$$\begin{aligned} g(Y) &= g(Y) - g(f_1(X), \ldots, f_m(X)) = \sum c_\alpha (Y^\alpha - f_1(X)^{\alpha_1} \cdots f_m(X)^{\alpha_m}) \\ &= \sum c_\alpha y_1^{\alpha_1} (y_2^{\alpha_2} \cdots y_m^{\alpha_m} - f_1^{\alpha_1} \cdots f_m^{\alpha_m}) + c_\alpha (y_1^{\alpha_1} - f_1^{\alpha_1}) f_2^{\alpha_2} \cdots f_m^{\alpha_m}. \end{aligned}$$

Reiterando se tiene que $g(Y) \in I \cap \mathbf{k}[Y]$.

Consideramos ahora $g(Y) \in I \cap \mathbf{k}[Y]$. Sea $\bar{\phi}\colon \mathbf{k}[Y, X] \mapsto \mathbf{k}[X]$ el homormofismo determinado por $y_j \mapsto f_j(X)$ y $x_i \mapsto x_i$. Claramente $I \subseteq \ker \bar{\phi}$. Por lo tanto $g(Y) \in \ker \bar{\phi}$. De aquí deducimos que $\phi(g(Y)) = \bar{\phi}(g(Y)) = 0$, así que $g(Y) \in \ker \phi$. □

Teorema 22. *Sea* $>$ *un odrden de eliminación en* $\mathbf{k}[X, Y]$ *en el que las variables* x_i *son mayores que las* y_j*, y sea* G *una base de Groebner de* I *relativa a este orden. Se tiene que*

$$f(X) \in \operatorname{Im} \phi \Leftrightarrow \mathrm{N}_G(f) \in \mathbf{k}[Y].$$

En tal caso $\mathrm{N}_G(f)$ *es una preimagen de* f.

Demostración. Sea $f(x) \in \operatorname{Im}\phi$ y sea $g(Y)$ tal que $f(X) = g(f_1(X), \ldots, f_m(X))$. Siguiendo el razonamiento de la demostración de teorema anterior se deduce que $f(X) - g(Y) \in I$. Por lo tanto $\mathrm{N}_G(f) = \mathrm{N}_G(g)$. Para reducir $g(Y)$ hasta $\mathrm{N}_G(g)$ mediante G no se usan las variables $x_1, \ldots, x_n$ ya que son mayores que las de Y, así pues, $\mathrm{N}_G(f)$ pertenecerá a $\mathbf{k}[Y]$. Recíprocamente, supuesto que $\mathrm{N}_G(f) \in \mathbf{k}[Y]$, y denotando por $g(Y)$ a este polinomio, se tendrá que $f(X) - g(Y) \in I$ por lo que al sustituir y_j por $f_j(X)$ se obtendrá 0. Es decir, $f(X) = g(f_1(X), \ldots, f_m(X)) \in \operatorname{Im}\phi$. □

Este tipo de resultados se extienden a homomorfismos entre álgebras afines.

15. Referencias

- Adams y Loustaunau: *An Introduction to Gröbner Bases*, AMS, 1994.
- Cox, Little y O'Shea: *Using algebraic geometry*, Springer, 2005.
- Sturmfels: *Solving Systems of Polynomial Equations*. Disponible en internet.

Algunas aplicaciones

16. Programación entera

Sean $a_{ij} \in \mathbb{Z}$, $b_i \in \mathbb{Z}$. Vamos a buscar soluciones $(\sigma_1, \ldots, \sigma_m) \in \mathbb{N}^n$ del siguiente sistema:

$$\left.\begin{array}{rcl} a_{11}\sigma_1 + \cdots + a_{1m}\sigma_m & = & b_1 \\ \vdots & & \vdots \\ a_{n1}\sigma_1 + \cdots + a_{nm}\sigma_m & = & b_n \end{array}\right\} \tag{1}$$

de modo que además se minimice la función de costes

$$c(\sigma_1, \ldots, \sigma_m) = c_1\sigma_1 + \cdots + c_m\sigma_m$$

donde $c_1, \ldots, c_m \in \mathbb{R}$ son coeficientes fijos.

Las técnicas que hemos visto de bases de Groebner permiten una aproximación nueva a este problema. Para ello hay que interpretar este problema como un problema acerca de polinomios.

Procederemos a encontrar soluciones del sistema distinguiendo dos casos de acuerdo al signo que tengas los coeficientes del sistema. Finalmente se estudia cómo encontar las que minimicen la función de costes.

Primer caso: $a_{ij}, b_i \geq 0$**.**

Se consideran variables $x_1, \ldots, x_n$, una por cada ecuación del sistema, y se cambia la i-ésima ecuación por la siguiente ecuación polinomial equivalente

$$x_i^{a_{i1}\sigma_1 + \cdots + a_{im}\sigma_m} = x_i^{b_i}$$

o equivalentemente

$$(x_1^{a_{11}} \cdots x_n^{a_{n1}})^{\sigma_1} \cdots (x_1^{a_{1m}} \cdots x_n^{a_{nm}})^{\sigma_m} = x_1^{b_1} \cdots x_n^{b_n}.$$

Las soluciones $(\sigma_1, \ldots, \sigma_m)$ se corresponden con las preimágenes $y_1^{\sigma_1} \cdots y_m^{\sigma_m}$ de $x_1^{b_1} \cdots x_n^{b_n}$ por el homomorfismo de álgebras determinado por

$$\begin{array}{rcl} \phi\colon \mathbf{k}[y_1, \ldots, y_m] & \to & \mathbf{k}[x_1, \ldots, x_n] \\ y_j & \mapsto & x_1^{a_{1j}} \cdots x_n^{a_{nj}} \end{array}$$

Como vimos en la lección anterior, esta preimagen puede calcularse mediante técnicas de álgebra computacional.

Consideramos el ideal

$$I = \langle y_1 - f_1(X), \ldots, y_m - f_m(X) \rangle$$

donde $f_j(X) = x_i^{a_{ij}} \cdots x_n^{a_{nj}}$ y calculamos una base de Groebner reducida G de I relativa a un orden de eliminación respecto del cual las variables x_i sean mayores que las y_j. Bastará calcular $\mathrm{N}_G(x_1^{b_1} \cdots x_n^{b_n})$ y comprobar que pertenece a $\mathbf{k}[Y]$

para obtener la preimagen que se buscaba. Sin embargo, hay que comprobar que dicha preimagen es de la forma $y_1^{\sigma_1} \cdots y_m^{\sigma_m}$ para que realmente proporcione una solución de (1).

Lemma 5. *Si* $\mathrm{N}_G(x_1^{b_1} \cdots x_n^{b_n}) \in \mathbf{k}[Y]$ *entonces* $\mathrm{N}_G(x_1^{b_1} \cdots x_n^{b_n})$ *es de la forma* Y^σ *para algún* $\sigma = (\sigma_1, \ldots, \sigma_m)$.

Demostración. El ideal I está generado por los binomios $y_j - f_j(X)$. Al crear la base G siguiendo el algoritmo de Buchberger calculamos los S-polinonimos, que serán también a lo sumo binomios, y los reducimos. En cada paso de reducción el resultado es de nuevo a lo sumo un binomio. Por lo tanto al final la base de Groebner G contendrá a lo sumo binomios. Al reducir $x_1^{b_1} \cdots x_n^{b_n}$ usando estos monomios el resultado es nuevamente un monomio (o cero, que no es posible ya que $x_1^{b_1} \cdots x_n^{b_n} \notin I$). Esto demuestra el lema. □

Segundo caso: $a_{ij}, b_i \in \mathbb{Z}$**.**

Para poder usar exponente negativos se introduce una variable w y se hacen los cálculos en $\mathbf{k}[X]/J$ donde $J = \langle w x_1 \cdots x_n - 1 \rangle$. Se acumulan todos los exponentes negativos en w como sigue:

$$(a_{1j}, \ldots, a_{nj}) = (a'_{1j}, \ldots, a'_{nj}) + \alpha_j(-1, \ldots, -1)$$

para ciertos $a'_{ij} \in \mathbb{N}$. Así

$$x_1^{a_{1j}} \cdots x_n^{a_{nj}} + J = x_1^{a'_{1j}} \cdots x_n^{a'_{nj}} w^{\alpha_j} + J.$$

Se procede exactamente igual para obtener una descomposición $(b_1, \ldots, b_n) = (b'_1, \ldots, b'_n) + \beta(-1, \ldots, -1)$ con $b'_j \in \mathbb{N}$. De este modo

$$x_1^{b_1} \cdots x_n^{b_n} + J = x_1^{b'_1} \cdots x_n^{b'_n} w^{\beta} + J.$$

Del mismo modo que en el caso anterior, se define el homomorfismo

$$\begin{aligned} \phi\colon \mathbf{k}[Y] &\to \mathbf{k}[w, X]/J \\ y_j &\mapsto x_1^{a'_{1j}} \cdots x_n^{a'_{nj}} w^{\alpha_j} + J \end{aligned}$$

y buscamos una preimagen de $x_1^{b'_1} \cdots x_n^{b'_n} w^{\beta} + J$. Para ello se considera el ideal de $\mathbf{k}[w, Y, X]$

$$I = \langle y_j - x_1^{a'_{1j}} \cdots x_n^{a'_{nj}} w^{\alpha_j}, w x_1 \cdots x_n - 1 \mid j = 1, \ldots, m \rangle$$

y un orden de eliminación repecto del cual tanto $x_1, \ldots, x_n$ como w sean mayores que $y_1, \ldots, y_m$. Como para homomorfismos entre álgebras de polinomios, puede probarse qeu si G es una base de Groebner reducida relativa a este orden, existe una preimagen de $x_1^{b'_1} \cdots x_n^{b'_n} w^{\beta} + J$ si y solamente si $\mathrm{N}_G(x_1^{b'_1} \cdots x_n^{b'_n} w^{\beta}) \in \mathbf{k}[Y]$, y

que en tal caso este polinomio será de la forma $y_1^{\sigma_1}\cdots y_m^{\sigma_m}$ para alguna solución $(\sigma_1,\ldots,\sigma_m)$ del sistema de ecuaciones (1).

Inclusión de la función de costes.

Una estrategia para obtener una solución que minimice la función de costes es usar un orden adecuado. Un **orden complatible con la función de costes** en $\mathbf{k}[Y]$ es un orden monomial que cumple que si $\phi(y_1^{\sigma_1}\cdots y_m^{\sigma_m}) = \phi(y_1^{\sigma'_1}\cdots y_m^{\sigma'_m})$ y $c(\sigma_1,\ldots,\sigma_m) < c(\sigma'_1,\ldots,\sigma'_m)$ entonces $y_1^{\sigma_1}\cdots y_m^{\sigma_m} < y_1^{\sigma'_1}\cdots y_m^{\sigma'_m}$.

La siguiente proposición se enuncia para el segundo caso pero es igualmente válida para el primero sin más que prescindir de la indeterminada w.

Proposición 5. *Sea G una base de Groebner de I relativa a un orden de eliminación para el cual las indeterminadas x_i $i=1,\ldots,n$ y w son mayores que las y_j $j=1,\ldots,m$. Asumamos también que el orden inducido en $\mathbf{k}[Y]$ es compatible con la función de costes. Si $\mathrm{N}_G(x_1^{b'_1}\cdots x_n^{b'_n}w^{\beta}) = y_1^{\sigma_1}\cdots y_m^{\sigma_m}$ entonces $(\sigma_1,\ldots,\sigma_m)$ es una solución del sistema (1) que minimiza la función de costes.*

Demostración. La tupla $(\sigma_1,\ldots,\sigma_m)$ será una solución. Si no minimizase la función de costes entonces debería existir otra solución $(\sigma'_1,\ldots,\sigma'_m)$ que cumpliese $c(\sigma'_1,\ldots,\sigma'_m) < c(\sigma_1,\ldots,\sigma_m)$. Por las hipótesis acerca del orden se sigue que el polinomio $y^{\sigma_1}\cdots y^{\sigma_m} - y^{\sigma'_1}\cdots y^{\sigma'_m}$ tiene monomio director $y^{\sigma_1}\cdots y^{\sigma_m}$ y que además pertenece a $\ker\phi \subseteq I$. En particular, $y^{\sigma_1}\cdots y^{\sigma_m} - y^{\sigma'_1}\cdots y^{\sigma'_m}$ debería reducirse a cero mediante G pero $y^{\sigma_1}\cdots y^{\sigma_m}$ no puede reducirse más, lo que origina una contradicción. □

En general no es sencillo encontrar órdenes que cumplan las propiedades de la proposición [Conti y Traverso]. Un caso sencillo es el caso en que $c_j \geq 0$ $j=1,\ldots,m$ ya que por ejemplo

$$y_1^{\sigma_1}\cdots y_m^{\sigma_m} < y_1^{\sigma'_1}\cdots y_m^{\sigma'_m} \Leftrightarrow \begin{cases} c(\sigma_1,\ldots,\sigma_m) < c(\sigma'_1,\ldots,\sigma'_m) \\ \\ \text{ó} \\ \\ c(\sigma_1,\ldots,\sigma_m) = c(\sigma'_1,\ldots,\sigma'_m) \text{ y} \\ y_1^{\sigma_1}\cdots y_m^{\sigma_m} <' y_1^{\sigma'_1}\cdots y_m^{\sigma'_m} \\ \text{respecto de algún orden monomial } <' \end{cases}$$

sería un orden monomial en $\mathbf{k}[Y]$ compatible con la función de costes. Bastaría juntar este orden con cualquier otro orden monomial en $\mathbf{k}[X]$ de modo que el orden resultante sea un orden de eliminación.

Ejemplo. Cuatro factorías $F_1,\ldots,F_4$ fabrican la misma variedad de un mismo producto. Su producción se distribuye a cuatro almacenes $S_1,\ldots,S_4$ pudiendo cada factoría repartir a más de un almacén. Las cantidades del producto fabricadas por las distintas factorías han sido $220, 215, 93$ y 64. Las cantidades

solicitadas por los distintos almacenes han sido $108, 286, 71$ y 127. La distribución desde la factoría F_i hasta el almacén S_j tiene un coste w_{ij} que viene determinado por la siguiente matriz

$$w = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 4 & 3 & 2 & 1 \\ 7 & 5 & 3 & 1 \\ 10 & 7 & 4 & 1 \end{pmatrix}.$$

Hay que encontrar la forma de distribuir los productos de modo que el coste total de distribución sea el menor posible.

Sean $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ las cantidades que debe repartir la primera factoría a los almacenes en un reparto óptimo. Del mismo modo sean $\sigma_5, \ldots, \sigma_8$ las que reparte F_2; $\sigma_9, \ldots, \sigma_{12}$ las que reparte F_3 y finalmente $\sigma_{13}, \ldots, \sigma_{16}$ las que reparte F_4. Estas cantidades cumplen las relaciones

$$\begin{aligned} \sigma_1 + \sigma_2 + \sigma_3 + \sigma_4 &= 220 \\ \sigma_5 + \sigma_6 + \sigma_7 + \sigma_8 &= 215 \\ \sigma_9 + \sigma_{10} + \sigma_{11} + \sigma_{12} &= 93 \\ \sigma_{13} + \sigma_{14} + \sigma_{15} + \sigma_{16} &= 64 \\ \sigma_1 + \sigma_5 + \sigma_9 + \sigma_{13} &= 108 \\ \sigma_2 + \sigma_6 + \sigma_{10} + \sigma_{14} &= 286 \\ \sigma_3 + \sigma_7 + \sigma_{11} + \sigma_{15} &= 71 \\ \sigma_4 + \sigma_8 + \sigma_{12} + \sigma_{16} &= 127 \end{aligned}$$

y se debe minimizar la función de costes

$$\begin{aligned} &\sigma_1 + \sigma_2 + \sigma_3 + \sigma_4 + 4\sigma_5 + 3\sigma_6 + 2\sigma_7 + \sigma_8 + 7\sigma_9 + 5\sigma_{10} + \\ &\quad 3\sigma_{11} + \sigma_{12} + 10\sigma_{13} + 7\sigma_{14} + 4\sigma_{15} + \sigma_{16} \end{aligned}$$

En términos polinomiales el sistema de ecuaciones equivale a

$$\begin{aligned} &(x_1x_5)^{\sigma}_1(x_1x_6)^{\sigma_2}(x_1x_7)^{\sigma_3}(x_1x_8)^{\sigma_4}(x_2x_5)^{\sigma_5}(x_2x_6)^{\sigma_6}(x_2x_7)^{\sigma_7}(x_2x_8)^{\sigma_8}(x_3x_5)^{\sigma_9} \\ &\quad (x_3x_6)^{\sigma_{10}}(x_3x_7)^{\sigma_{11}}(x_3x_8)^{\sigma_{12}}(x_4x_5)^{\sigma_{13}}(x_4x_6)^{\sigma_{14}}(x_4x_7)^{\sigma_{15}}(x_4x_8)^{\sigma_{16}} \\ &= x_1^{220}x_2^{215}x_3^{93}x_4^{64}x_5^{108}x_6^{286}x_7^{71}x_8^{127} \end{aligned}$$

Introduciendo los datos en `Singular`

```
// Vector de pesos para que el orden sea compatible con los costes;
intvec w = 1,1,1,1,4,3,2,1,7,5,3,1,10,7,4,1;
// Anillo con las indeterminadas;
// Orden grevlex en las x_i, orden por w-peso y despues ;
// revlex en las y_j;
ring R = 0, (x(1..8),y(1..16)), (dp(8),wp(w));
// El ideal I;
```

```
ideal I = y(1)-x(1)*x(5), y(2)-x(1)*x(6),y(3)-x(1)*x(7),
y(4)-x(1)*x(8),y(5)-x(2)*x(5),y(6)-x(2)*x(6),y(7)-x(2)*x(7),
y(8)-x(2)*x(8),y(9)-x(3)*x(5),y(10)-x(3)*x(6),y(11)-x(3)*x(7),
y(12)-x(3)*x(8),y(13)-x(4)*x(5),y(14)-x(4)*x(6),y(15)-x(4)*x(7)
,y(16)-x(4)*x(8);
// Se calcula la base de Groebner;
option(redSB);
ideal GI =groebner(I);
// Se reduce el el polinomio mediante G;
poly p = x(1)^220*x(2)^215*x(3)^93*x(4)^64*x(5)^108*
x(6)^286*x(7)^71*x(8)^127;
reduce(p,GI);
```

El resultado es $y(1)^{108}y(2)^{112}y(6)^{174}y(7)^{41}y(11)^{30}y(12)^{63}y(16)^{64}$. Por lo tanto la solución del sistema inicial que minimiza el valor de la función de costes es $\sigma_i = 0$ con la excepción de $\sigma_1 = 108, \sigma_2 = 112, \sigma_6 = 174, \sigma_7 = 41, \sigma_{11} = 30, \sigma_{12} = 63$ y $\sigma_{16} = 64$.

□

Referencias

- Adams y Loustaunau: *An introduction to Göbener bases*, 1995.
- Conti y Traverso: *Buchberger algorithm and integer programming*, 1991.
- Steidel: *Singular - Tutorial*, 2008.
- Sturmelds: *Gröbner bases and convex polytopes*, 1995.

17. Bancos de filtros

La transformada de Fourier de una función integrable $f\colon \mathbb{R} \to \mathbb{C}$ es

$$\hat{f}(w) = \int_{-\infty}^{\infty} f(t) e^{-2\pi i w t} dt.$$

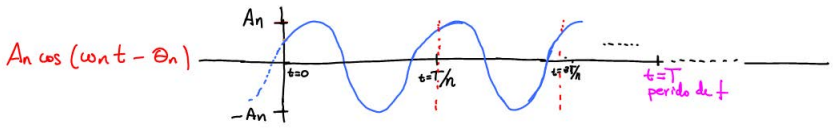
Bajo ciertas condiciones $f(t)$ se recupera como

$$f(t) = \int_{-\infty}^{\infty} \hat{f}(w) e^{2\pi i w t} dw.$$

La variable t se suele interpretar como el tiempo y la variable w como la frecuencia. El desarrollo de Fourier de una función periódica de periodo T es

$$f(t) = A_0 + \sum_{n=1}^{\infty} A_n \cos(w_n t - \phi_n) \quad \text{con } w_n = \frac{2\pi n}{T}$$

que expresa una señal de entrada en como una combinación lineal de señales más sencillas.



Para procesar digitalmente una señal se toman muestras obteniéndose una señal discreta $x(n)$. Se define la z-transformada de $x(n)$ como

$$X(z) = \sum_{k} x(k) z^{-k}.$$

Si se sustituye z por $e^{\frac{2\pi i n}{T}}$ el lado derecho de la anterior igualdad es $\sum_n x(k) e^{-\frac{2\pi i n k}{T}}$ por lo que $X(z)$ mantendrá cierta semejanza con la transformada de Fourier.

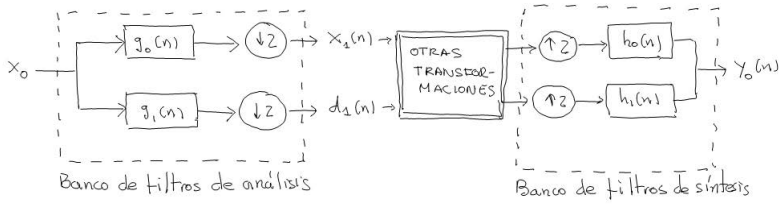
Dada otra serie $\{h(n)\}_{n\geq 0}$, la convolución y de h y x se define como

$$y(n) = (h * x)(n) = \sum_{k\geq 0} h(k) x(n-k).$$

(si existe). La z-transformada de $h * x$ es el producto $Y(z) = H(z)X(z)$ de las z-transformadas de h y x.

Los valores $h(k)$ se usan para cambiar el valor de la señal x en diferentes puntos y así obtener una nueva señal y. La transformación $x \mapsto h * x$ se llama **filtro**. Algunos de ellos se usan para eliminar de la señal componentes no deseadas, entre otros usos.

Los **bancos de filtros** pueden componerse de varios filtros. Una forma popular de construir un banco de filtros con dos canales desarrollada en los años 80 es



Al duplicar inicialmente la señal x_0 parece que se procesará el doble de datos. Para evitar esto se realizan las transformaciones $\downarrow 2$ después de aplicar los filtros g_0 y g_1. Esta transformación descarta las componentes en tiempo n impar:

$$y = \downarrow 2(x)\colon n \mapsto x(2n).$$

En principio esto podría suponer la pérdida de información. Tras realizar transformaciones a las señales x_1 y d_1 se llega al banco de filtros de síntesis donde se combinan usando dos filtros h_0 y h_1 junto con la operación:

$$y = \uparrow 2(x)\colon \begin{cases} x(n/2) \text{ si } n \text{ es par} \\ 0 \text{ si } n \text{ es impar.} \end{cases}$$

Nuevamente esto podría suponer la pérdida de más información. En el dominio de frecuencias las operaciones $\downarrow 2$ y $\uparrow 2$ se corresponden con

$$\begin{aligned} \downarrow 2 : X(z) &\mapsto Y(z) = \frac{1}{2}(X(z^{\frac{1}{2}}) + X(-z^{\frac{1}{2}},) \\ \uparrow 2 : X(z) &\mapsto Y(z) = Z(z^2). \end{aligned}$$

Un banco de filtros **PR** de reconstrucción perfecta es aquél en el que, si no se realizan más transformaciones más que las del análisis y síntesis, a la salida del banco de síntesis se obtiene la señal inicial, quizás con un desfase temporal, $x_0(n-l)$, pero sin pérdida de información. Esto asegura que al dividir la señal inicial en dos señales y realizar la operación $\uparrow 2$ no se está perdiendo información de la señal. Claramente debe haber alguna relación entre los filtros h_0, h_1 y g_0, g_1 para que el banco de filtros tenga la propiedad PR. En términos de z-transformadas se puede comprobar que esta propiedad equivale a que las z-transformadas de los filtros cumplan

$$\begin{aligned} G_0(z)H_0(z) + G_1(z)H_1(z) &= 2z^{-l} \\ G_0(z)H_0(-z) + G_1(z)H_1(-z) &= 0 \end{aligned}$$

o equivalentemente

$$\begin{pmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{pmatrix} \begin{pmatrix} G_0(z) \\ G_1(z) \end{pmatrix} = \begin{pmatrix} 2z^{-l} \\ 0 \end{pmatrix}$$

es decir,

$$G_0(z) = \frac{2z^{-l}}{D(z)} H_1(-z) \quad G_1(z) = -\frac{2z^{-l}}{D(z)} H_0(-z)$$

con $D(z) = H_0(z)H_1(-z) - H_0(-z)H_1(z)$ que asumiremos no nulo en el dominio de las z.

Al imponer que los filtros solamente tengan un número finito de componentes no nulas (filtros FIR) se puede probar, aunque no lo haremos, que "esencialmente"solamente aparecen dos casos: $D(z) = 2z^{-l}$ y $D(z) = 2z^{-l-1}$. Vamos a discutir el segundo caso ya que en la práctica permite construir más filtros.

Una condición extra que puede imponerse para in delimitando el banco de filtros PR es que

$$g_0(n) = h_0(-n) \quad \text{y} \quad g_1(n) = h_1(-n)$$

o equivalentemente

$$G_0(z) = H_0(z^{-1}) \quad \text{y} \quad G_1(z) = H_1(z^{-1}).$$

que básicamente nos dice que los filtros de síntesis son los mismos que los de análisis pero aplicados "al revés". Los bancos de filtros que cumplen esta condición se llaman **ortogonales**. Al juntar esta condición con la condición PR nos queda que

$$\begin{aligned} H_0(z)H_0(z^{-1}) + H_1(z)H_1(z^{-1}) &= 2z^{-l} \\ H_0(-z)H_0(z^{-1}) + H_1(-z)H_1(z^{-1}) &= 0 \end{aligned}$$

Estas igualdades, junto con la condición FIR y que $D(z) = 2z^{-1-l}$ implican que

$$H_1(z) = z^{-1}H_0(-z^{-1}).$$

y que

$$H_0(z)H_0(z^{-1}) + H_0(-z)H_0(-z^{-1}) = 2z^{-l}$$

lo que ya delimita bastante el tipo de filtros que queremos. Esta ecuación también implica que l debe ser par, por lo que normalizando H_0 mutiplicándolo por $z^{l/2}$ se puede asumir que $l = 1$. Así pues, salvo desplazamiento de los coeficientes de h_0 se tiene que lo que debe cumplir el filtro h_0 es

$$\sum_{n\geq 0} h_0(n)h_o(n-2k) = \begin{cases} 2 \text{ si } k = 0 \\ 0 \text{ si } k \neq 0 \end{cases} \tag{2}$$

Los filtros h_1, g_0 y g_1 se construyen a partir de este h_0 usando las relaciones que hemos derivado anteriormente.

Dentro de la familia de filtros h_0 que cumplan (2) vamos a buscar unos concretos. La idea es que si la señal de entrada es muy suave (analíticamente hablando) entonces la componente d_1 que correspondería a filtrar frecuencias muy bajas, producidas por ejemplo por ruido, sea nula. Una forma de lograr esto es imponer que si $x_0(n)$ es una función polinomial en n de un grado digamos

$\leq K-1$ para un cierto K entonces la componente d_1 que se obtiene sea nula. Esto equivale a imponer que $(z-1)^K$ divida a $G_1(z)$ o equivalentemente a que

$$(z+1)^K \text{ divide a } H_0(z) \tag{3}$$

habida cuenta de la relación entre $G_1(z)$ y $H_0(z)$. Así pues, buscaremos filtros $H_0(z)$ del menor grado posible que cumplan todas estas condiciones (filtros **maxflat**).

Vamos a desarrollar el caso $K=4$ (**filtros de Daubechies** de longitud 8). Escribimos $H(z)=\alpha_0+\alpha_1+z+\cdots+\alpha_7 z^7$ para ciertos coeficientes $\alpha_0,\ldots,\alpha_7$ a determinar. De ellos sabemos que cumplen las condiciones (2) y (3). La condición (2) es equivalente en este caso a

$$\begin{aligned}
\alpha_0^2+\alpha_1^2+\cdots+\alpha_7^2-2 &= 0\\
\alpha_7\alpha_5+\alpha_6\alpha_4+\alpha_5\alpha_3+\alpha_4\alpha_2+\alpha_3\alpha_1+\alpha_2\alpha_0 &= 0\\
\alpha_7\alpha_3+\alpha_6\alpha_2+\alpha_5\alpha_1+\alpha_4\alpha_0 &= 0\\
\alpha_7\alpha_1+\alpha_6\alpha_0 &= 0
\end{aligned}$$

La condición (3) queda, una vez realizada la eliminación gaussiana,

$$\begin{aligned}
\alpha_0-\alpha_4+4\alpha_5-10\alpha_6+20\alpha_7 &= 0\\
\alpha_1-4\alpha_4+15\alpha_5-36\alpha_6+70\alpha_7 &= 0\\
\alpha_2-6\alpha_4+20\alpha_5-45\alpha_6+84\alpha_7 &= 0\\
\alpha_3-4\alpha_4+10\alpha_5-20\alpha_6+35\alpha_7 &= 0
\end{aligned}$$

Estos sistemas de ecuaciones pueden resolverse utilizando bases de Groebner (conviene en este caso añadir una última ecuación $\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+A=0$ donde A es otra indeterminada). Al calcular una base reducida para el orden lex (A debe ser la mayor de las indeterminadas) se observa que A solamente puede tomar ocho valores y sus opuestos, y que $\alpha_0,\ldots,\alpha_7$ se despejan en términos de A. Se logra así una familia de filtros con todas las propiedades deseadas.

En realidad, para encontrar filtros con la propiedad maxflat no es necesario el uso de bases de Groebner ya que se pueden usar otros métodos matemáticos. Sin embargo, al imponer condiciones en los filtros sí que quizás pudieran aparecer ecuaciones polinomiales que, a falta de otras técnicas teóricas, podrían ser abordadas mediante técnicas de bases de Groebner.

Referencias

- Lebrun y Selesnick: *Gröbner bases and wavelets design*, 2004.
- Strang y Ngyuen: *Wavelets and Filter banks*, 1996.

18. Invariantes de grupos finitos

Un polinomio $f(X) \in \mathbf{k}[X]$ se dice **polinomio simétrico** si $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ para toda permutación σ de $\{1, \ldots, n\}$. Los polinomios $\sigma_1 = x_1 + \cdots + x_n, \ldots, \sigma_k = \sum_{i_1 < \cdots < i_k} x_{i_1} \cdots x_{i_k}, \ldots, \sigma_n = x_1 \cdots x_n$ se llaman **funciones simétricas elementales**. Definimos $\sigma_0 = 1$.

Proposición 6.

$$(x - x_1) \cdots (x - x_n) = \sum_{k=0}^{n} (-1)^{n-k} \sigma_{n-k} x^k.$$

Teorema 23 (Teorema fundamental acerca de los polinomios simétricos)**.** *Todo polinomio simétrico en* $\mathbf{k}[X]$ *puede expresarse de forma única como un polinomio en* $\sigma_1, \ldots, \sigma_n$.

Demostración. Fijamos un orden lex en $\mathbf{k}[X]$ con $x_1 > \cdots > x_n$. Dado un polinomio simétrico no nulo f, sea $\mathrm{LT}(f) = aX^\alpha$ con $\alpha = (\alpha_1, \ldots, \alpha_n)$. Si para algún i se ocurriese que $\alpha_i < \alpha_{i+1}$ entonces, al ser f simétrico, el término $a x_1^{\alpha_1} \cdots x_i^{\alpha_{i+1}} x_{i+1}^{\alpha_i} \cdots x_n$ sería mayor que $\mathrm{LT}(f)$, lo que no puede ser. Por lo tanto $\alpha_1 \geq \cdots \geq \alpha_n$.

Sea $h = \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \cdots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}$. Puesto que $\mathrm{LT}(\sigma_k) = x_1 \cdots x_k$ podemos deducir que $\mathrm{LT}(h) = X^\alpha$. El polinomio $f - ah$ es simétrico y $\mathrm{LM}(f - ah) < LM(f)$. Reiterando se concluye que f puede expresarse como un polinomio en $\sigma_1, \ldots, \sigma_n$.

Si la expresión que hemos encontrado no fuese la única posible entonces, restando ambas expresiones, existiría un polinomio no nulo $g(y_1, \ldots, y_n)$ de tal modo que $g(\sigma_1(X), \ldots, \sigma_n(X)) = 0$. Sea Y^β un monomio de g. Al realizar la sustitución $y_i \mapsto \sigma_i(X)$ se tiene que

$$\mathrm{LT}(\sigma_1(X)^{\beta_1} \cdots \sigma_n(X)^{\beta_n}) = x_1^{\beta_1 + \cdots + \beta_n} x_2^{\beta_2 + \cdots + \beta_n} \cdots x_n^{\beta_n}.$$

El mayor monomio que aparece al desarrollar $g(\sigma_1(X), \ldots, \sigma_n(X))$ es de de esta forma para algún monomio Y^β de $g(Y)$. Sin embargo, la aplicación $\beta \mapsto (\beta_1 + \cdots + \beta_n, \beta_2 + \cdots + \beta_n, \ldots, \beta_n)$ es inyectiva por lo que el término en $g(\sigma_1(X), \ldots, \sigma_n(X))$ correspondiente a ese mononio no se cancela con ningún otro y así $g(\sigma_1(X), \ldots, \sigma_n(X)) \neq 0$, lo que es una contradicción. □

Dado un polinomio simétrico, para calcular su expresión en términos de las funciones simétricas elementales podemos usar la teoría de bases de Groebner. Consideramos el homomorfismo de álgebras

$$\begin{array}{rcl} \phi\colon \mathbf{k}[Y] & \mapsto & \mathbf{k}[X] \\ y_i & \mapsto & \sigma_i(X) \end{array}$$

Los polinomios simétricos conforman $\mathrm{Im}\,\phi$. Para expresar un polinomio simétrico $f(X)$ como polinomio en $\sigma_1(X), \ldots, \sigma_n(X)$ basta hallar la (única) preimagen de $f(X)$ por ϕ. Usando el teorema de cálculo de preimágenes visto anterioremente se tiene

Teorema 24. *Sea $I = \langle y_1 - \sigma_1(X), \ldots, y_n - \sigma_n(X)\rangle$ ideal de $\mathbf{k}[X,Y]$ y sea G una base de Groebner de I relativa a un orden de eliminación en el que las indeterminadas x_i son mayores que las y_j. Un polinomio $f(X)$ es simétrico si y solamente si $\mathrm{N}_G(f) = g(Y)$ para algún polinomio $g(Y) \in \mathbf{k}[Y]$. Además, en tal caso $f(X) = g(\sigma_1(X), \ldots, \sigma_n(X))$.*

Ejemplo. El polinomio $x_1^3+x_2^3+x_3^3 \in \mathbf{k}[x_1,x_2,x_3]$ es simétrico. Para expresarlo en términos de las funciones simétricas elementales usamos `Singular`:

```
ring R = 0, (x(1..3),y(1..3)), (lp(3),lp(3));
ideal I = y(1)-x(1)-x(2)-x(3), y(2)-x(1)*x(2)-x(1)*x(3)-
 x(2)*x(3), y(3)-x(1)*x(2)*x(3);
ideal GI = groebner(I);
reduce(x(1)^3+x(2)^3+x(3)^3,GI);
```

El resultado es $y^3 - 3y_1y_2 + 3y_3$. Así pues,

$$x_1^3+x_2^3+x_3^3 = (x_1+x_2+x_3)^3 - 3(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) + 3x_1x_2x_3$$

□

Si tienes curiosidad por conocer una base de Groebner del ideal I del Teorema consulta [Cox et al.]

Los polinomios

$$s_k = x_1^k + \cdots + x_n^k$$

son todos polinomios simétricos. Si definimos

$$\sigma(t) = \prod_{i=1}^{n}(1+x_it) \quad s(t) = \sum_{i=1}^{n}\frac{x_i}{1-tx_i} \quad \tau(t) = \prod_{i=1}^{n}\frac{1}{1-x_it}$$

podemos observar fácilmente que $\tau(t)\sigma(-t) = 1$ por lo que si derivamos respecto de t se tiene que $\tau(t)^{-1}\tau(t)'\sigma(-t) + \sigma(-t)' = 0$. Puesto que $\tau(t)^{-1}\tau(t)'$ es la derivada de $\log\tau(t)$, aprovechando que el logaritmo del producto es la suma de logaritmos, tenemos $\tau(t)^{-1}\tau(t)' = s(t)$. De este modo

$$s(t)\sigma(-t) + \sigma(-t)' = 0$$

Sustituyendo en esta igualdad las relaciones

$$\sigma(t) = \sum_{k=1}^{n}\sigma_kt^k \quad s(t) = \sum_{k=1}^{\infty}s_kt^{k-1}$$

y comparando los coeficientes de las potencias de t tenemos

Teorema 25 (Fórmulas de Newton)**.**

$$\begin{aligned}(-1)^{m-1}\sigma_{m-1}s_1 + \cdots + \sigma_0s_m &= -(-1)^m\sigma_m m \qquad si\ 1 \le m \le n\\ (-1)^n\sigma_n s_{m-n} + (-1)^{n-1}\sigma_{n-1}s_{m-n-1} + \cdots + \sigma_0 s_m &= 0 \qquad si\ m > n\end{aligned}$$

Corolario 5. *Sea* $\mathbf{k}$ *un cuerpo de característica cero. Se tiene que todo polinomio simétrico (con término independiente nulo) puede expresarse de forma única como un polinomio en* $s_1, \ldots, s_n$.

Al igual que antes la expresión que se asegura existir en el corolario se puede calcular mediante el uso de bases de Groebner.

El grupo simétrico es un caso particular de subgrupo finito de un grupo de matrices. Es natural el intentar extender los anteriores resultados a estos grupos. Cada matrix invertible $A = (a_{ij}) \in G \subseteq \mathrm{GL}_n(\mathbf{k})$ define un automorfismo de $\mathbf{k}[X]$ determinado en los generadores por

$$\begin{array}{rccl} \phi_A \colon \mathbf{k}[X] & \to & \mathbf{k}[X] \\ x_i & \mapsto & a_{i1}x_1 + \cdots + a_{in}x_n \end{array}$$

El automorfismo inverso es $\phi_{A^{-1}}$ ya que $\phi_A\phi_B = \phi_{AB}$ y ϕ_{I_n} es la aplicación identidad. Dado un grupo finito $G \subseteq \mathrm{GL}_n(\mathbf{k})$ se dice que un polinomio $p(X)$ es **invariante** por G si $\phi_A(p(X)) = p(X)$ para toda $A \in \mathrm{GL}_n(\mathbf{k})$. El conjunto de todos los polinomios invariantes por G se denota por $\mathbf{k}[X]^G$ y es una subálgebra de $\mathbf{k}[X]$. Un polinomio simétrico es un polinomio invariante para el grupo de matrices permutación.

Teorema 26 (Noether)**.** *Sea* $G \subseteq \mathrm{GL}_n(\mathbf{k})$ *un grupo finito de matrices y* $\mathbf{k}$ *un cuerpo de característica cero. El álgebra* $\mathbf{k}[x_1, \ldots, x_n]^G$ *está generada por*

$$\{R_G(X^\beta) \mid |\beta| \leq |G|\}$$

donde $R_G(p(X)) = \frac{1}{|G|}\sum_{A\in G} \phi_A(p(X))$ *y* $|\beta| = \beta_1 + \cdots + \beta_n$.

Demostración. Dado $p(X) = \sum_\alpha c_\alpha X^\alpha \in \mathbf{k}[X]^G$,

$$p(X) = R_G(p(X)) = \sum_\alpha c_\alpha R_G(X^\alpha).$$

Como $\phi_A \circ R_G = R_G$ para todo $A \in G$, los polinomios $R_G(X^\alpha)$ son polinomios invariantes. La diferencia de estos polinomios con los del enunciado es que los del enunciado tienen un grado acotado por el tamaño del grupo. Si probamos que cualquier $R_G(X^\alpha)$ pueden expresarse mediante combinaciones lineales de productos de los polinomios del enunciado entonces el resultado quedará probado.

Consideremos unos escalares genéricos $u_1, \ldots, u_n$. Observamos que

$$R_G((u_1x_1 + \cdots u_nx_n)^m) = \begin{cases} \frac{1}{|G|}\sum_{A\in G}(u_1\phi_A(x_1) + \cdots + u_n\phi_A(x_n))^m \\ \\ R_G(\sum_{|\alpha|=m} a_\alpha u^\alpha X^\alpha) \\ \quad = \sum_{|\alpha|=m} a_\alpha u^\alpha R_G(X^\alpha) \end{cases} \tag{4}$$

para ciertos $a_\alpha \in \mathbb{N}$. El polinomio $S_m = \sum_{A\in G}(u_1\phi_A(x_1) + \cdots + u_n\phi_A(x_n))^m$ es una suma de m potencias con tantos sumados como elementos tiene el grupo, así que, por el Corolario a las fórmulas de Newton, son expresables como polinomios en $S_1, \ldots, S_{|G|}$, y debido a (4) estos últimos polinomios son expresables del mismo modo en términos de $R_G(X^\beta)$ con $|\beta| \leq |G|$. Así que la parte derecha superior de (4) es una expresión polinómica en $|\beta| \leq |G|$ y en $u_1, \ldots, u_n$. Comparando el coeficiente de u^α de esta expresión con el de la expresión derecha inferior de (4) (que es $a_\alpha R_G(X^\alpha)$) obtenemos que $R_G(X^\alpha)$ tiene la forma deseada. □

Nota. Habría que justificar completamente el paso final en el que hemos igualado los coeficientes de los u^α ya que son escalares y no indeterminadas. Esto es debido, por ejemplo, a que hay infinitos escalares pero lo pasaremos por alto.

El Teorema de Noether asegura que cualquier polinomio invariante se podrá escribir como una expresión polinomial en $\{R_G(X^\beta) \mid |\beta| \leq |G|\}$. El criterio para encontrar esta expresión es similar al caso de polinomios simétricos ya que se trata de calcular una preimagen.

Referencias

- Cox, Little y O'Shea: *Ideals, varieties and algorithms*. Springer, 2007.
- Derksen y Kemper: *Computational invariant theory*. Springer, 2002.

Ejercicios

1. Determina usando técnicas de bases de Groebner si los siguientes ideales son iguales:

   - $< y^3 - z^2, xz - y^2, xy - z, x^2 - y >$
   - $< xy - z^2, xz - y^2, xy - z, x^2 - y >$
   - $< xz - y^2, x + y^2 - z - 1, xyz - 1 >$
   - $< y^2 - x^2y, z - xy, y - x^2 >$

   Puedes ayudarte del ordenador.

2. Calcula, sin usar el ordenador, mediante el algoritmo de Buchberger una base reducida del ideal $I = \langle xy + z, x^2 + y^2 \rangle$. Determina también sin usar el ordenador si la clase $[x + 1]$ es invertible en $\mathbf{k}[x, y, z]/I$.

3. Calcula el abanico de Groebner del ideal $\langle x^2 - y^3, x^3 - y^2 + x \rangle$.

4. ¿Puede escribirse $4x^4y^2 + 4y^6 - 2x^4 - 4x^2y^2 - 6y^4 + 2x^2 + 4y^2 - 1$ de la forma $h(x^2 + y^2 - 1, x^2 - y^2)$ para algún polinomio $h \in \mathbb{Q}[x, y]$?