SISTEMAS DE ECUACIONES POLINOMIALES

Alicia Dickenstein

Minicurso UMA, octubre de 1995

1 Introducción

Dado un sistema de ecuaciones polinomiales en varias variables

$$\begin{aligned} p_1(x_1,\ldots,x_n) &= 0 \\ p_2(x_1,\ldots,x_n) &= 0 \\ &\vdots \\ p_s(x_1,\ldots,x_n) &= 0 \end{aligned}$$

nos proponemos contestar efectivamente, entre otras, las siguientes preguntas:

- ¿El sistema tiene soluciones?
- En caso afirmativo, ¿tiene finitas soluciones?
- ¿Cómo "eliminar" variables para encontrar las soluciones? Es decir, ¿cómo "triangular" el sistema?
- ¿Cómo determinar si las soluciones satisfacen una cierta condición polinomial SIN necesidad de calcularlas?
- ¿Cómo lograr que una computadora decida estas cuestiones por nosotros? (Es decir, buscamos soluciones algorítmicas de los problemas planteados)

Veamos algunos ejemplos de sistemas de ecuaciones polinomiales:

1) Un sistema de ecuaciones lineales es un caso particular de sistema polinomial, en el que todos los polinomios involucrados tienen grado 1. Para estos sistemas, el álgebra lineal da respuestas "sencillas" a todas las preguntas anteriores.

2) Sean A, B, C, D, E, F puntos en el plano. Las siguientes afirmaciones geométricas pueden ser expresadas como la anulación de una o más ecuaciones polinomiales:

i) El segmento $\overline{AB}$ es paralelo al segmento $\overline{CD}$.

ii) El segmento $\overline{AB}$ es perpendicular al segmento $\overline{CD}$.

iii) A, B, C son colineales.

iv) La distancia AB de A a B es igual a la distancia CD de C a D.

v) C cae en la circunferencia con centro A y radio AB.

vi) C es el punto medio de $\overline{AB}$.

vii) El ángulo agudo $< ABC$ es igual al ángulo agudo $< DEF$.

viii) $\overline{BD}$ bisecta el ángulo $< ABC$

ix) El teorema del círculo de Apolonio: *Sea $\triangle ABC$ un triángulo rectángulo en el plano, con ángulo recto en A. Los puntos medios de los tres lados y el pie de la altura dibujada desde A hasta $\overline{BC}$ pertenecen a una misma circunferencia.*

Ejercicio: Verificarlo. Referencia: [C-L-O], capítulo 6, parágrafo 4.

3) Supongamos que buscamos los puntos críticos de una función polinomial f de tres variables x, y, z restringida a la cáscara de la esfera S de radio r. Entonces, S coincide con el conjunto de ceros del polinomio $g(x, y, z) = x^2 + y^2 + z^2 - r^2$, y por el método de *multiplicadores de Lagrange*, la respuesta a nuestro problema son aquellos puntos $P = (x, y, z)$ en S para los cuales el gradiente de f en P es un múltiplo del gradiente de g en P. Es decir que buscamos los puntos P para los cuales existe un valor de λ de tal modo que se satisface el siguiente sistema de ecuaciones polinomiales:

$$\begin{array}{rcl} g(x,y,z) & = & 0 \\ \frac{\partial f}{\partial x}(x,y,z) & = & \lambda \frac{\partial g}{\partial x}(x,y,z) \\ \frac{\partial f}{\partial y}(x,y,z) & = & \lambda \frac{\partial g}{\partial y}(x,y,z) \\ \frac{\partial f}{\partial z}(x,y,z) & = & \lambda \frac{\partial g}{\partial z}(x,y,z) \end{array}$$

Lo que nos interesa hacer es "eliminar" la variable λ, cuyo valor no nos importa, y calcular los valores de x, y, z.

4) Decidir si un polinomio p en una variable tiene raíces múltiples corresponde a decidir si el sistema:

$$p(x) = p'(x) = 0$$

tiene o no solución.

5) Consideremos un brazo de robot que se mueve en un plano consistente de dos barras de longitudes ℓ_1 y ℓ_2, con uno de los extremos de la primer barra fijo a un punto que consideramos el origen, con posibilidad de girar en cualquier dirección, y la segunda barra unida al extremo de la primera, también con posibilidad de girar en cualquier dirección. Si denotamos por (u, v) las coordenadas del extremo de la primer barra, y con (x, y) las coordenadas del extremo del brazo del robot (es decir del extremo libre de la segunda barra), el llamado *espacio de configuraciones* del robot es el conjunto de 4-uplas (u, v, x, y) que verifican el sistema polinomial:

$$\begin{array}{rcl} u^2 + v^2 - \ell_1^2 & = & 0 \\ (x-u)^2 + (y-v)^2 - \ell_2^2 & = & 0 \end{array}$$

6) La *flor de cuatro pétalos* dada en coordenadas polares del plano por la ecuación

$$r = |\text{sen}(2\theta)|$$

(unión el origen) puede describirse como el conjunto de ceros de un polinomio en dos variables.

Ejercicio: Verificarlo.

7) Supongamos dado el polinomio $p(x) = x^6 - 7\,x^5 - 6\,x^4 + 77\,x^3 + 51\,x^2 - 160\,x - 100$, y nos preguntamos si todas las raíces de p verifican la ecuación $x^5 - 5\,x^4 - 4\,x^3 + 21\,x^2 - 3\,x - 10 = 0$. Si el polinomio $q = x^5 - 5\,x^4 - 4\,x^3 + 21\,x^2 - 3\,x - 10$ fuera un múltiplo de p, la respuesta sería obviamente SI. Pero esto seguro que no sucede en este caso ya que el grado de p es mayor que el grado de q. Sin embargo, SIN calcular las raíces de p, podemos hallar algebraicamente (Ejercicio: ¿Cómo?) el polinomio $p_1 = x^4 - 4\,x^3 - 8\,x^2 + 13\,x + 10$, con las mismas raíces que p pero simples. Usando el algoritmo de división para polinomios en una variable podemos verificar que p_1 divide a q, y entonces la respuesta buscada es efectivamente SI.

8) Un polinomio en n variables se llama *simétrico* si permanece invariante por un reordenamiento (o renumeración) arbitrario de las variables. Un conocido teorema que se remonta a Gauss y Hilbert dice que todo polinomio simétrico $p(x_1, \ldots, x_n)$ puede expresarse como un (único) polinomio q en las funciones simétricas elementales $\sigma_1 = x_1 + \ldots + x_n, \sigma_2 = \sum_{1 \le i < j \le n} x_i x_j, \ \ldots \ , \sigma_n = \prod_{i=1}^{n} x_i$ de $x_1, \ldots, x_n$. Las herramientas que desarrollaremos permiten hallar efectivamente tal polinomio q .

9) Sea S la superficie de $\mathbf{R}^3$ dada paramétricamente por

$$\begin{aligned} x &= t(u^2 - t^2) \\ y &= u \\ z &= u^2 - t^2. \end{aligned}$$

Es posible presentar la superficie S implícitamente como

$$S = \{(x, y, z) \ / \ x^2 - y^2 z^2 + z^3 = 0\}.$$

El polinomio $x^2 - y^2 z^2 + z^3$ (que expresa las relaciones algebraicas entre las coordenadas de los puntos de $\mathbf{R}^3$ que dependen de los dos parámetros t, u), se obtiene por eliminación de las variables t, u.

10) Dado un número natural N, el desarrollo en base 2 de N tiene a lo sumo n dígitos (es decir, $N \le 2^n$) si y sólo si el siguiente sistema de ecuaciones polinomiales tiene solución:

$$\begin{aligned} x_1^2 - x_1 &= 0 \\ x_2^2 - x_2 &= 0 \\ &\vdots \\ x_n^2 - x_n &= 0 \\ \textstyle\sum_{i=1}^{n} x_i 2^{i-1} - N &= 0 \end{aligned}$$

Este sistema aparentemente ingenuo y sencillo, de hecho da cuenta de algunas de las limitaciones computacionales de la eliminación de variables [H].

11) Por ejemplo en [V-V-C], pueden encontrarse sistemas de ecuaciones polinomiales que aparecen modelando equilibrio de sistemas químicos, sistemas económicos, el problema del sistema de posición inverso de brazos de robot, o aún problemas de neurofisiología.

2 Polinomios en varias variables

En estas notas nos restringiremos a polinomios con coeficientes complejos y siempre que hablemos de existencia de soluciones nos referiremos a soluciones con coordenadas complejas. Gran parte de los resultados (pero no todos) valen para polinomios con coeficientes en cualquier cuerpo. Algunos de los resultados expuestos dependen de que todo polinomio en una variable con coeficientes complejos tiene tantas raíces complejas como su grado (contadas con multiplicidad), como el teorema de los ceros de Hilbert, o de que $\mathbf{C}$ sea un cuerpo infinito, como el hecho de que si un polinomio define la función polinomial nula, entonces se trata del polinomio nulo.

Ya es hora entonces de precisar qué es un polinomio en n variables y fijar la notación que utilizaremos. Si $\alpha = (\alpha_1, \ldots, \alpha_n)$ es una n-upla de enteros no negativos, notaremos:

$$x^\alpha := x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Diremos que x^α es un *monomio* (en n variables). En particular, $x^{(1,0,\ldots,0)} = x_1$, $x^{(0,\ldots,0)} = 1$. Llamamos *polinomio en n variables con coeficientes complejos* a toda combinación lineal finita de monomios

$$p = \sum_\alpha c_\alpha \; x^\alpha, \qquad c_\alpha \in \mathbf{C}.$$

El conjunto de polinomios en n variables a coeficientes complejos se nota $\mathbf{C}[x_1, \ldots, x_n]$. Dos polinomios p y q son iguales si y sólo si tienen los mismos coeficientes. En $\mathbf{C}[x_1, \ldots, x_n]$ se definen naturalmente las operaciones de suma (coeficiente a coeficiente) y de producto (para que valga la propiedad distributiva), de modo que $\mathbf{C}[x_1, \ldots, x_n]$ es un anillo conmutativo con unidad y una $\mathbf{C}$-álgebra.

Definimos el *grado* de un monomio x^α como la suma de los exponentes a los que aparecen cada una de las variables. Notaremos

$$\mathrm{gr(x^\alpha)} := \alpha_1 + \ldots + \alpha_\mathrm{n} = |\alpha|.$$

Por ejemplo, el grado del monomio $x_1^3 x_2^5 x_4^2$ es igual a 10. Si $p = \sum_\alpha c_\alpha \; x^\alpha$ no es el polinomio cero (es decir, alguno de los coeficientes de p es no nulo), definimos el *grado* de p (notado $\mathrm{gr}(p)$) como el máximo de los grados de los monomios que aparecen en p con coeficiente no nulo. Un polinomio se dice *homogéneo* si todos sus monomios (todos aquellos con coeficiente no nulo) tienen el mismo grado.

Es sencillo probar que si f, g son polinomios no nulos, entonces $f \cdot g$ es no nulo y $\mathrm{gr(f \cdot g)} = \mathrm{gr(f)} + \mathrm{gr(g)}$. Luego, $\mathbf{C}[x_1, \ldots, x_n]$ es un dominio íntegro. Se puede probar que es un dominio de factorización única, como en el caso de una sola variable.

Para cada natural d fijo, la cantidad de monomios de grado menor o igual que d en n variables es $\binom{n+d}{n}$ (Ejercicio: probar esta afirmación. Ayuda: hay tantos monomios de grado menor o

igual que d en n variables como monomios de grado exactamente d en $n+1$ variables; se trata entonces de un problema de "bosones", repartir d bolitas en $n+1$ cajas).

Cada polinomio $p \in \mathbf{C}[x_1, \ldots, x_n]$ define por especialización una función polinomial $\tilde{p} : \mathbf{C}^n \to \mathbf{C}$. Por inducción en n puede probarse que $\tilde{p}$ es la función nula si y sólo si p es el polinomio nulo.

Diremos que un subconjunto V de $\mathbf{C}^n$ es una *variedad algebraica (afín)* si V es el conjunto de soluciones de un sistema polinomial, es decir si existen finitos polinomios $p_1, \ldots, p_s \in \mathbf{C}[x_1, \ldots, x_n]$ tales que

$$V = \{x \in \mathbf{C}^n \ / \ p_1(x) = \ldots = p_s(x) = 0\}.$$

En la introducción vimos varios ejemplos de variedades algebraicas.

Ejercicio:

a) Los siguientes subconjuntos de $\mathbf{C}^n$ son variedades algebraicas:

i)$\mathbf{C}^n$

ii) el conjunto vacío

iii) cualquier subconjunto finito

iv) cualquier variedad lineal

v) la intersección de dos variedades algebraicas

vi) la unión de dos variedades algebraicas

b) Los puntos con coordenadas enteras $\mathbf{Z}^n$ no son una variedad algebraica en $\mathbf{C}^n$.

c) Encontrar polinomios $p_1, \ldots, p_s$ que describan las siguientes variedades algebraicas:

i) El suconjunto formado por los puntos $(1, 0)$ y $(0, 1)$ en $\mathbf{C}^2$.

ii) La unión del eje z con el plano x, y en $\mathbf{C}^3$.

Observemos, por ejemplo, que el subconjunto algebraico del plano descripto por

$$V := \left\{x^2 - y = y^2 - x = x^2 + y^2 - 2y = x - 2x^3 + x^2 = 5y^4 - 10y^3 + 5y^2 = 0\right\}$$

puede en verdad describirse más simplemente como $V = \{y^2 - y = x - y = 0\}$ (Ejercicio: Probarlo), de lo cual es ahora fácil descubrir que V es el conjunto formado por los puntos $(0, 0)$ y $(1, 1)$.

Supongamos que tenemos en general una variedad algebraica $V = \{x \in \mathbf{C}^n \ / \ p_1(x) = \ldots = p_s(x) = 0\}$. Si g es una combinación lineal con coeficientes polinomiales de $p_1, \ldots, p_s$, es decir, si existen polinomios $h_1, \ldots, h_s$ tales que $g = \sum_{i=1}^{s} h_i p_i$, entonces es fácil ver que $V \subseteq \{g = 0\}$, es decir que g se anula en todos los ceros comunes de $p_1, \ldots, p_s$. Suele decirse que g es una "consecuencia polinomial" de $p_1, \ldots, p_s$.

Diremos que un subconjunto I de $\mathbf{C}[x_1, \ldots, x_n]$ es un *ideal* si es no vacío y contiene todas las consecuencias polinomiales de los polinomios de I. Precisamente, I es un ideal sii:

i) I no es vacío

ii) $f + g \in I$, para todo par de polinomios f, g en I.

iii) Si $f \in I$ y h es cualquier polinomio, entonces el producto $h \cdot f$ está en I.

Es fácil ver que I es un ideal si y sólo si $0 \in I$, y para cualquier elección de $p_1, \ldots, p_s \in I$ y $h_1, \ldots, h_s \in \mathbf{C}[x_1, \ldots, x_n]$, el polinomio $\sum_i h_i p_i$ está en I.

Ejemplos de ideales:

1) (EL ejemplo) Dado cualquier subconjunto S de $\mathbf{C}^n$, el conjunto $I(S)$ de todos los polinomios que se anulan en todos los puntos de S es un ideal. No todos los ideales son de esta forma; por ejemplo, los múltiplos del polionomio x^2.

2) $\mathbf{C}[x_1, \ldots, x_n]$ y $\{0\}$ son ideales.

3) El conjunto de todas las combinaciones polinomiales de un conjunto finito de polinomios $p_1, \ldots, p_s$. En este caso notamos:

$$I =< p_1, \ldots, p_s >= \{\sum_{i=1}^{s} h_i p_i\}$$

y decimos que I es el ideal generado por $p_1, \ldots, p_s$, o bien que $p_1, \ldots, p_s$ son un sistema de generadores de I.

4) Ejercicio: En el caso $n = 1$, cualquier ideal admite un solo generador. Más explícitamente,

$$< p_1, \ldots, p_s >=< q >,$$

donde q es el máximo común divisor de los polinomios $p_1, \ldots, p_s$. Es decir, cualquier ideal consiste de los múltiplos de un cierto polinomio. Luego, toda variedad algebraica propia se reduce a un número finito de puntos.

Esto no es cierto para más de una variable. Por ejemplo, si $n \geq 2$, el ideal generado por $x_1, \ldots, x_s$ no admite un único generador (para cualquier s entre 2 y n), y los ceros en $\mathbf{C}^n$ del ideal generado por un único polinomio no constante, forman una variedad algebraica con infinitos puntos.

5) $I := \{f \in \mathbf{C}[x, y] / f(0,0) = f_x(0,0) = f_y(0,0) = 0\}$ es un ideal, que puede generarse por los polinomios x^2, y^2 y $x \cdot y$

Observemos que el conjunto de ceros comunes de un conjunto finito de polinomios $p_1, \ldots, p_s$ es igual al conjunto de ceros comunes de todos los polinomios en el ideal generado $< p_1, \ldots, p_s >$. Notaremos $V(I) = \{x \in \mathbf{C}^n \ / p(x) = 0 \ \ \forall p \in I\}$ el conjunto de ceros del ideal I. Notemos en particular que si $< p_1, \ldots, p_s >=< q_1, \ldots, q_k >$, los sistemas $p_1 = \ldots = p_s = 0$ y $q_1 = \ldots = q_t = 0$ tienen las mismas soluciones (Ejercicio: No vale la recíproca, es decir, si dos conjuntos finitos de polinomios tienen las mismas soluciones, no es cierto necesariamente que los ideales generados sean iguales).

Vamos a admitir sin demostración el Teorema de la Base de Hilbert, que dice que todo ideal del anillo de polinomios $\mathbf{C}[x_1, \ldots, x_n]$ admite un sistema finito de generadores. De aquí se deduce que cualquier subconjunto V de $\mathbf{C}^n$ que pueda expresarse como el conjunto de ceros comunes de un conjunto cualquiera de polinomios, es una variedad algebraica (es decir, puede expresarse

como el conjunto de ceros comunes de un conjunto finito de polinomios (de cualquier conjunto finito de generadores del ideal de todos los polinomios que se anulan en V)).

Diremos que un ideal I es *radical*, si

$$f^m \in I \text{ para algún } m \Rightarrow f \in I.$$

Observemos que todos los ideales de la forma $I(S)$ son radicales. El ideal formado por todos los múltiplos de x^2, en cambio, no es radical.

Ejercicio : Probar que el ideal I generado por $x^2 - y, x^3 - z$ en $\mathbf{C}[x, y, z]$ es radical. (Ayuda: $V(I) = \{(t, t^2, t^3),\ t \in \mathbf{C}\}$)

Observemos que si bien un ideal es un $\mathbf{C}$-subespacio lineal de $\mathbf{C}[x_1, \ldots, x_n]$, se pierde la noción de " independencia" lineal cuando se trata de combinaciones lineales con coeficientes polinomiales. Para cualquier par de polinomos f, g vale la igualdad: $g \cdot f + (-f) \cdot g = 0$, con lo que si un polinomio es una combinación polinomial de dos o más polinomios, hay siempre infinitas maneras de escribirlo como combinación lineal polinomial de ellos.

El principal problema que nos proponemos resolver algorítmicamente es el de determinar la pertenencia de un polinomio f a un ideal $I =< p_1, \ldots, p_s >$, es decir, decidir si existen polinomios $h_1, \ldots, h_s$ tales que $f = \sum h_i p_i$. Esta pregunta está muy relacionada con el problema de describir las soluciones del sistema

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ p_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ p_s(x_1, \ldots, x_n) &= 0. \end{aligned}$$

En el caso $n = 1$, el algoritmo de división y el algoritmo de Euclides, basado en él, para calcular el máximo común divisor entre dos polinomios, son suficientes para decidir efectivamente la pertenencia a un ideal $I =< p_1, \ldots, p_s >$. En efecto, teniendo en cuenta el ejercicio en el ítem 4) más arriba, basta calcular iteradamente $q = \text{mcd}(\text{mcd}(p_1, \ldots, p_{s-1}), p_s)$, y entonces un polinomio dado g pertenece a $I \Leftrightarrow g$ es un múltiplo de $q \Leftrightarrow$ el resto de la división de g por q es 0.

El algoritmo de Euclides provee además una manera de escribir el máximo común divisor q de dos (o más, por aplicación reiterada) polinomios p_1, p_2 en el ideal que generan, es decir, permite encontrar polinomios a_1 y a_2 tales que $q = a_1 p_1 + a_2 p_2$. Luego, en el caso de una sola variable, las siguientes afirmaciones son equivalentes:

i) Los polinomios $p_1, \ldots, p_s$ no tienen ceros comunes.

ii) $\text{mcd}(p_1, \ldots, p_s\ ) = 1$

iii) Existen polinomios $h_1, \ldots, h_s$ tales que $1 = \sum_i h_i p_i$. (es decir, $1 \in < p_1, \ldots, p_s >$, con lo que $< p_1, \ldots, p_s >= \mathbf{C}[x]$).

Para $n \geq 2$, i) e iii) son equivalentes, pero ii) no, con lo que será necesario desarrollar nuevas herramientas para decidir si un sistema de ecuaciones polinomiales no tiene soluciones.

En lo que sigue, veremos cómo emular de alguna manera el algoritmo de división en el caso de un número cualquiera de variables para poder decidir efectivamente la pertenencia a ideales en el anillo de polinomios.

3 Ordenes monomiales y bases de Gröbner

Supongamos dados $g, p_1, \ldots, p_s \in \mathbf{C}[x_1, \ldots, x_n]$. Para determinar si $g \in < p_1, \ldots, p_s >$, querríamos poder encontrar un algoritmo de división por s polinomios, que proporcione cocientes $h_i,\ i = 1, \ldots, s$ y un resto r de tal modo que (como en el caso de la división por un polinomio en una variable):

1) $g = \sum_i h_i p_i + r$

2) $g \in I \Leftrightarrow r = 0$

3) r esté unívocamente determinado en algún sentido.

De hecho, existe una generalización más o menos directa del algoritmo de división en una variable que provee 1), una vez que se ha elegido un orden en los monomios con ciertas propiedades. Claramente, si $r = 0$, el polinomio g pertenece al ideal generado por $p_1, \ldots, p_s$. Sin embargo, para que valga 3) y la equivalencia en 2), es necesario reemplazar el sistema de generadores del ideal por otro, denominado " base de Gröbner" del ideal (que denotaremos GB).

Las bases de Gröbner fueron introducidas por Bruno Buchberger en su tesis doctoral en 1965, hecha bajo la direccion de Wolfgang Gröbner. Los principios básicos subyacentes a la noción de GB se remontan al fin del siglo XIX, pero la contribución principal de Buchberger ha sido la de idear un algoritmo finito que transforma un sistema de generadores dados de un ideal en una GB del ideal. Este algoritmo (mejorado) está actualmente implementado en muchos sistemas de "computer algebra" (MAPLE, MATHEMATICA, REDUCE, AXIOM, MACAULAY, COCOA, GROBNER, etc.)

Un orden total "$\prec$ " en los monomios en n variables se llama un *orden monomial* si $1 \preceq m$ para todo monomio m, y si para cualquier terna de monomios $m_1, m_2, m_3 \in \mathbf{C}[x_1, \ldots, x_n], m_1 \prec m_2 \Rightarrow m_1 \cdot m_3 \prec m_2 \cdot m_3$.

Definiendo $\alpha \prec \beta \Leftrightarrow x^\alpha \prec x^\beta$, para cualquier par de n-uplas de enteros no negativos, un orden monomial es equivalente a un orden total $\prec$ en $\mathbf{Z}^n_{\geq 0}$ que verifique que $0 \preceq \alpha$ para toda n-upla α, y para cualquier terna α, β, γ, $\alpha \prec \beta \Rightarrow \alpha + \gamma \prec \beta + \gamma$.

Ejemplos de órdenes monomiales: (Ejercicio: Probar que lo son)

i) (n=1) En $\mathbf{Z}_{\geq 0}$ (equivalentemente en $\mathbf{C}[x]$) el único orden monomial es el usual $0 \prec 1 \prec 2 \prec \ldots$ (equivalentemente, $1 \prec x \prec x^2 \prec \ldots$).

ii) Orden lexicográfico (notado lex): Decimos que $\alpha \preceq_{\text{lex}} \beta$ si la primer coordenada no nula desde la izquierda de $\alpha - \beta$ es negativa (es el orden del diccionario). En particular, $x_n \prec_{\text{lex}} \ldots \prec_{\text{lex}} x_2 \prec_{\text{lex}} x_1$. Por ejemplo, si $n = 3$, $x_1^2 x_2^2 x_3^7 \prec_{\text{lex}} x_1^2 x_2^3 x_3$. De hecho, hay $n!$ órdenes lexicográficos, uno para cada ordenación de las variables.

iii) Orden graduado lexicográfico (notado deglex): Decimos que $\alpha \preceq_{\text{deglex}} \beta$ si $\text{gr}(\alpha) < \text{gr}(\beta)$, o si $\text{gr}(\alpha) = \text{gr}(\beta)$ y la primer coordenada no nula desde la izquierda de $\alpha - \beta$ es negativa. En particular, $x_n \prec_{\text{deglex}} \ldots \prec_{\text{deglex}} x_2 \prec_{\text{deglex}} x_1$. Por ejemplo, si $n = 3$, $x_1^2 x_2^2 x_3^7 \succ_{\text{deglex}} x_1^2 x_2^3 x_3$.

iv) Orden graduado lexicografico reverso (notado grevlex): Decimos que $\alpha \preceq_{\text{grevlex}} \beta$ si $\text{gr}(\alpha) < \text{gr}(\beta)$, o si $\text{gr}(\alpha) = \text{gr}(\beta)$ y la primer coordenada no nula desde la derecha de $\alpha - \beta$ es

positiva (no es lo mismo que numerar las variables al revés y considerar deglex!). En particular, $x_n \prec_{\text{grevlex}} \ldots \prec_{\text{grevlex}} x_2 \prec_{\text{grevlex}} x_1$. Por ejemplo, si $n = 3$, $x_1 x_3^2 \prec_{\text{grevlex}} x_2^2 x_3$.

v) Si $n = 2$, por ejemplo, podemos definir el *orden de peso* con peso $(1, \sqrt{2})$ por $\alpha \prec \beta$ sii $\alpha_1 + \sqrt{2}\alpha_2 < \beta_1 + \sqrt{2}\beta_2$

vi) Si $n = 2$, por ejemplo, podemos definir un orden monomial $\prec_w$ a partir de los vectores $w_1 = (1, 2), w_2 = (3, 5)$ del siguiente modo: decimos que $\alpha \prec \beta$ sii $\alpha_1 + 2\alpha_2 < \beta_1 + 2\beta_2$, o si $\alpha_1 + 2\alpha_2 = \beta_1 + 2\beta_2$ y $3\alpha_1 + 5\alpha_2 < 3\beta_1 + 5\beta_2$.

De hecho, puede probarse que todos los órdenes monomiales pueden obtenerse de esta manera, es decir como el producto lexicográfico de n órdenes de peso (cf. [R]).

Un ideal $I \subseteq \mathbf{C}[x_1, \ldots, x_n]$ se llama *monomial* si está generado por monomios. El lema de Dickson asegura que dado un sistema de generadores cualquiera de un ideal monomial $I = < x^\alpha, \alpha \in A >$, es posible extraer un número finito $x^{\alpha_1}, \ldots, x^{\alpha_s}$ de estos generadores de modo que $I =< x^{\alpha_1}, \ldots, x^{\alpha_s} >$.

Ejercicio: Si $I =< x^{\alpha_1}, \ldots, x^{\alpha_s} >$ es un ideal monomial, entonces:

i) Un monomio x^β está en I si y sólo si existe algún índice j tal que x^β es divisible por x^{α_j}.

ii) Un polinomio $p = \sum_\beta a_\beta x^\beta$ está en I si y sólo si para cada coeficiente a_β no nulo, el correspondiente monomio x^β está en I.

Luego, es sencillo decidir la pertenencia a un ideal monomial.

Como consecuencia del lema de Dickson, es posible probar que si $\prec$ es un orden monomial arbitrario, cualquier cadena decreciente

$$\alpha_1 \succeq \alpha_2 \succeq \ldots \succeq \alpha_j \succeq \alpha_{j+1} \succeq \ldots$$

se estaciona, es decir, toda cadena estrictamente decreciente de monomios es necesariamente finita.

Introduzcamos un poco de notación. Dado un orden monomial $\prec$, todo polinomio no nulo p puede escribirse en la forma

$$p = \sum_{j=0}^{k} a_{\alpha_i} x^{\alpha_i},$$

donde los α_j están numerados decrecientemente (respecto de $\prec$) y $a_{\alpha_0} \neq 0$. Decimos que el *multigrado* de p es α_0, (notado $\text{multideg}(p) = \alpha_0$), que el *coeficiente principal* de p es $a_{\alpha_0)}$ (notado $\text{LC}(p) = a_{\alpha_0}$), que el *monomio principal* de p es x^{α_0} (notado $\text{LM}(p) = x^{\alpha_0}$), y que el *término principal* de p es $a_{\alpha_0} x^{\alpha_0}$ (notado $\text{LT}(p) = a_{\alpha_0} x^{\alpha_0}$).

Ejercicio: Sean $f, g \in \mathbf{C}[x_1, \ldots, x_n]$ polinomios no nulos. Entonces

i) $\text{multideg}(f \cdot g) = \text{multideg}(f) + \text{multideg}(g)$

ii) Si $f + g \neq 0$, $\text{multideg}(f + g) = \text{máx}\ \{\text{multideg}(f), \text{multideg}(g)\}$.

iii) Si f no es un monomio, $\text{multideg}(f - \text{LT}(f)) \prec \text{multideg}(f)$.

Con estas consideraciones, es posible probar el siguiente teorema:

Teorema (Algoritmo de división): *Fijemos un orden monomial $\prec$ y $F := (f_1, \ldots, f_s)$ una s-upla ordenada de polinomios no nulos en $\mathbf{C}[x_1, \ldots, x_n]$. Entonces todo $f \in \mathbf{C}[x_1, \ldots, x_n]$ puede escribirse por medio del algoritmo descripto más abajo como $f = \sum_{i=1}^{s} a_i f_i + r$, con las siguientes propiedades:*

i) Ningún monomio de r es divisible por ningún monomio principal LM(f_1),...,LM(f_s), o $r = 0$.

ii) multideg($a_i f_i$) $\preceq$ multideg(f).

Algoritmo de división

Datos: $F = (f_1, \ldots, f_s)$, $\prec$

Salida: $a_1, \ldots, a_s, r$

$a_1 := 0, \ldots, a_s := 0$, $p := f$, $r := 0$
Mientras (WHILE) $p \neq 0$ *hacer (DO)*
$i = 1$
$division := falso$
Mientras (WHILE) $i \leq s$ *y* $division := falso$ *hacer (DO)*
Si (IF) LT(f_i) divide a LT(p), entonces (THEN)
$a_i := a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$, $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i$, $division := cierto$.
Si no (ELSE), $i := i + 1$ *Fin hacer (OD)*
Si (IF) $division = falso$, *entonces (THEN)*
$r := r + \mathrm{LT}(p)$, $p := p - \mathrm{LT}(p)$ *Fin hacer (OD)*
Fin (END)

Idea de la demostración: Verificar que en cada paso del algoritmo se mantiene la igualdad

$$f = a_1 f_1 + \ldots + a_s f_s + r + p,$$

y que en cada iteración el multigrado del "nuevo" p es inferior al multigrado del "viejo" p, con lo cual en un número finito de pasos el algoritmo termina.

Ejercicio: Fijemos el orden lexicográfico $\prec$ en $\mathbf{C}[x, y]$ (con $x \succ y$). Verificar que si $f = x^2y + xy^2 + y^2$, $g = xy^2 - x, f_1 = xy - 1, f2 = y^2 - 1$, el algoritmo de división recién descripto provee las siguientes escrituras:

1) Si $F := (f_1, f_2)$, $f = (x+y)f_1 + f_2 + (x+y+1)$. Si $F := (f_2, f_1)$, $f = xf_2 + (x+1)f_1 + (2x-1)$. Luego, los restos cambian al cambiar el orden de los polinomios por los cuales dividimos.

2) Si $F := (f_1, f_2)$, $g = yf_1 + 0f_2 + (-x + y)$. Si $F := (f_2, f_1)$, $g = 0f_1 + xf_2 + 0$. Luego, $g \in < f_1, f_2 >$ pero el resto de la primera división no es cero.

Agreguemos un poco de notación. Dado un ideal I y un orden monomial $\prec$, llamamos *ideal inicial de I (con respecto a $\prec$)*, al ideal monomial $\mathrm{LT}(I) =< \mathrm{LT}(f), f \in I - \{0\} >=< \mathrm{LM}(f), f \in I - \{0\} >$ generado por los términos (o monomios) principales de todos los polinomios no nulos en I.

Por el lema de Dickson, existen finitos polinomios no nulos $f_1, \ldots, f_s \in I$ tales que $\mathrm{LT}(I) = < \mathrm{LT}(f_i),\ i = 1, \ldots, s >$

Lema: *Si I es un ideal no nulo y $f_1, \ldots, f_s \in I$ son tales que $\mathrm{LT}(I) =< \mathrm{LT}(f_i),\ i = 1, \ldots, s >$, entonces $< f_1, \ldots, f_s >= I$.*

Idea de la demostración: Dado $f \in I$, por el algoritmo de división escribimos $f = \sum a_i f_i\ + r$. Notemos que $r = f - \sum a_i f_i\ \in I$. Si r no fuera 0, ninguno de sus monomios sería divisible por ninguno de los monomios iniciales de $f_1, \ldots, f_s$. Pero esto es una contradicción porque el monomio inicial de r está en $\mathrm{LT}(I) =< \mathrm{LT}(f_i),\ i = 1, \ldots, s >$.

Dado un ideal no nulo I, y un orden monomial $\prec$, llamamos *base de Gröbner* (GB) de I a cualquier subconjunto finito $f_1, \ldots, f_s$ de polinomios no nulos en I tales que $\mathrm{LT}(I) = < \mathrm{LT}(f_i),\ i = 1, \ldots, s >$. Por el lema anterior, una GB de I es un sistema de generadores de I.

Ejercicio: Verificar las siguientes afirmaciones.

i) $x + z,\ y - z$ son una GB (del ideal que generan) respecto de $\prec_{\mathrm{lex}}$ con $z \prec y \prec x$ en $\mathbf{C}[x, y, z]$, pero no son una GB con respecto de $\prec_{\mathrm{lex}'}$ con $x \prec y \prec z$.

ii) Los polinomios f_1, f_2 del ejercicio anterior no son una GB (del ideal que generan) respecto de $\prec_{\mathrm{lex}}$ en $\mathbf{C}[x, y]$.

iii) Los polinomios $x_1 - 1, x_1$ no son GB (del ideal que generan) para ningún orden monomial en $\mathbf{C}[x_1, \ldots, x_n]$.

iv) El polinomio 1 es una GB de $\mathbf{C}[x_1, \ldots, x_n]$.

v) Sea $\prec$ un orden monomial en $\mathbf{C}[x, y]$ y f, g dos polinomios tales que el monomio inicial de f respecto de $\prec$ es x^a y el monomio inicial de g es y^b (los monomios iniciales son coprimos). Probar que f, g es una GB.

Proposición: *Sea $G = (f_1, \ldots, f_s)$ una GB de I con respecto a un orden monomial $\prec$. Para cualquier $f \in \mathbf{C}[x_1, \ldots, x_n]$ existen únicos $g \in I$ y $r \in \mathbf{C}[x_1, \ldots, x_n]$ tales que $f = g + r$ y $r = 0$ o ningún monomio de r está en LT(I).*

Idea de la demostración: Una tal escritura existe por el algoritmo de división, y si hay dos de tales escrituras $f = g + r = g' + r'$ con esta propiedad, $r - r' \in I$ y se argumenta de modo similar a la demostración del lema previo.

Si G es una GB de I, f, g, r son como en la proposición anterior, notaremos $r = R_G(f)$ (resto de dividir f por G). Por el lema anterior, $R_G(f)$ no depende del orden de la sucesión $f_1, \ldots, f_s$ sino sólo de $\prec$. Es posible probar que $G = (f_1, \ldots, f_s)$ es una GB de I si y sólo si para todo $f \in \mathbf{C}[x_1, \ldots, x_n]$, $f \in I \Leftrightarrow R_G(f) = 0$. Entonces, sabiendo que G es una GB, el algoritmo de división nos provee una manera de testear pertenencia al ideal I.

Demos entonces una definición para poder enunciar el teorema de Buchberger. Dados $f, g \in \mathbf{C}[x_1, \ldots, x_n]$ no nulos y un orden monomial $\prec$, supongamos que el monomio inicial de f es x^α, el de g es x^β, y sea x^γ el mínimo común múltiplo entre ellos, es decir, $\gamma_i = \ \mathrm{máx}\{\alpha_i, \beta_i\}$ para todo $i = 1, \ldots, n$. Llamamos *S-polinomio de f y g* al polinomio que se obtiene cancelando los términos principales:

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

Observemos que $S(f,g) \in < f,g >$.

Teorema (Buchberger): *Sea $\prec$ un orden monomial, $I =< g_1,\ldots,g_s >$ un ideal no nulo. Entonces G es una GB $\Leftrightarrow$ $R_G(S(g_i,g_j)) = 0$ para todo par de índices distintos $i,j = 1,\ldots,s$.*
No daremos aquí una prueba de este teorema. Esta demostración, como todo el resto, puede leerse en forma accesible en [C-L-O]. Esta es la referencia más didáctica y agradable.

Corolario: Es posible chequear efectivamente la pertenencia de un dado polinomio f a un ideal polinomial $I =< f_1,\ldots,f_k > \subseteq \mathbf{C}[x_1,\ldots,x_n]$ (y en caso de que sea cierta escribir f como combinación polinomial de los generadores dados).

Idea de la demostración del corolario: Dados $f_1,\ldots,f_k$, calculamos todos los S- polinomios entre dos cualesquiera de ellos y chequeamos si el resto de la división de cada uno de ellos por $F = (f_1,\ldots,f_k)$ es nulo. Si la respuesta es sí en todos los casos, ya tenemos una GB. Si no, agregamos a la lista inicial de polinomios todos los restos de los S-polinomios calculados que no sean cero e iteramos el proceso. Si consideramos en cada paso el ideal monomial generado por los monomios iniciales de los polinomios de la lista, iremos obteniendo una cadena creciente de ideales que debe estacionarse, con lo que el proceso termina en un número finito de pasos. Una vez así obtenida una GB G de I, dado un polinomio f, basta aplicar el algoritmo de división de f por G y chequear si el resto $R_G(f)$ es o no nulo.

Una primera mejora en la implementación del algoritmo se obtiene a partir del hecho de que si dos polinomios f,g tienen monomios iniciales coprimos, entonces pueden evitarse los cálculos con $S(f,g)$. Aún con muchas mejoras, la "complejidad" del algoritmo de Buchberger en el peor caso es muy alta; sin embargo, muchos ejemplos son calculables por las computadoras actuales, siempre que el número de variables no sea grande (y grande es un número chico...), y especialmente si el ideal tiene buenas propiedades "geométricas" y los coeficientes de los polinomios involucrados no tienen problemas "aritméticos".

La "performance" del algoritmo depende, para un ideal fijo, del orden monomial utilizado. En general (y hay un argumento matemático para esto) los cálculos con grevlex son mucho más rápidos que los cálculos con órdenes lexicográficos. Existen también algoritmos "dinámicos" que van cambiando el orden monomial de manera apropiada a los datos a lo largo del proceso.

El problema de la pertenencia puede atacarse también (y de hecho ha sido estudiado) a partir de la acotación a priori de los grados de los polinomios intervinientes en una especial combinación lineal, lo que permite reducir el problema de la pertenencia a un problema de álgebra lineal (con matrices muy grandes...). Este enfoque tambien tiene una " complejidad" muy grande para ideales arbitrarios, ya que se trata de algo inherente al problema.

Ejercicio: Verificar las siguientes afirmaciones.

i) Consideremos el orden lexicográfico en $\mathbf{C}[x,y,z]$ con $x \succ y \succ z$ y sean $f = x^3 + y,\ g = x^3 + z$. Verificar que (f,g) no es una GB pero que $(f,g,S(f,g))$ sí lo es.

ii) Consideremos el orden lexicográfico en $\mathbf{C}[x,y]$ con $x \succ y$ y sean $f_1 = x^3 - y,\ f_2 = x^2 - x,\ f_3 = R_{(f_1,f_2)}(S(f_1,f_2)),\ f_4 = R_{(f_1,f_2,f_3)}(S(f_2,f_3))$. Verificar que (f_1,f_2,f_3) no es una GB de $< f_1,f_2 >$ (con lo cual (f_1,f_2) tampoco lo es), pero que $(f_1,f_2,f_3,f_4))$ sí lo es.

Diremos que una GB $G = (g_1,\ldots,g_s)$ respecto de un orden monomial es *reducida* si para todo $i = 1,\ldots,s$:

i) $\mathrm{LC}(g_i) = 1$

ii) Ningún monomio de g_i es divisible por ningún monomio inicial de g_j, para todo $j \neq i$.

Observemos que si G es una GB de I para $\prec$ y existe $g \in G$ tal que $\mathrm{LT}(g)$ es divisible por algún $\mathrm{LT}(g')$, con $g' \in G,\ g' \neq g$, entonces $G' := G - \{g\}$ también es una GB de I. (Ejercicio: Probarlo).

Proposición: *Fijado un orden monomial $\prec$, todo ideal no nulo tiene una única base de Gröbner reducida.*

Idea de la demostración: Dada una GB G de I, procedemos en tres etapas: primero, dividimos cada uno de los polinomios de G por su coeficiente principal; luego, descartamos aquellos polinomios tales que su monomio inicial sea divisible por el de alguno de los otros (la lista de polinomios resultante sigue generando el ideal I, como acabamos de observar), y finalmente, reemplazamos cada polinomio por su resto en la división respecto de todos los demás. Este algoritmo construye una GB reducida a partir de una GB arbitraria. Faltaría probar la unicidad, pero no es difícil.

Por ejemplo, para decidir si un ideal $I =< f_1, \ldots, f_s >$ es de hecho todo el anillo $\mathbf{C}[x_1, \ldots, x_n]$, basta calcular una GB reducida de I. La respuesta es sí sii la base calculada consta solamente del polinomio 1.

En la próxima sección, veremos cómo las bases de Gröbner son "ladrillos" básicos para diseñar algoritmos algebraicos más avanzados.

4 Aplicaciones

Consistencia de un sistema de ecuaciones polinomiales: El famoso Nullstellensatz (o teorema de los ceros) de Hilbert dice en su forma débil que un ideal $I \subseteq \mathbf{C}[x_1, \ldots, x_n]$ no tiene ceros (es decir, $V(I)$ es vacío) si y sólo si $1 \in I$, es decir si y sólo si $I = \mathbf{C}[x_1, \ldots, x_n]$. Luego el sistema

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ p_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ p_s(x_1, \ldots, x_n) &= 0 \end{aligned}$$

no tiene soluciones (es inconsistente) si y sólo si el ideal $< p_1, \ldots, p_s >$ tiene por GB reducida (para cualquier orden monomial) al polinomio 1.

Condiciones polinomiales de las soluciones de un sistema: Supongamos otra vez que tenemos un sistema polinomial

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ p_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ p_s(x_1, \ldots, x_n) &= 0 \end{aligned}$$

y nos preguntamos si todas las soluciones satisfacen una cierta condición polinomial f. Agreguemos una variable más y, y consideremos el polinomio $g(x_1, \ldots, x_n, y) := 1 - yf(x_1, \ldots, x_n)$. La

pregunta es entonces equivalente al hecho de que el ideal $< g, p_1, \ldots, p_s >$ en $\mathbf{C}[x_1, \ldots, x_n, y]$ no tenga ceros. Luego basta chequear si la GB reducida de éste ideal consiste sólo del polinomio 1.

Eliminación de variables: Dado un ideal $I \subseteq \mathbf{C}[x_1, \ldots, x_n]$, llamamos k-ésimo ideal de eliminación de I al ideal de $\mathbf{C}[x_{k+1}, \ldots, x_n]$ definido por $I_k := I \cap \mathbf{C}[x_{k+1}, \ldots, x_n]$. Geométricamente, si llamamos $\pi_k : \mathbf{C}^n \to \mathbf{C}^{n-k}$ a la proyección sobre las últimas $n-k$ coordenadas, un punto $(a_{k+1}, \ldots, a_n)$ está en la imagen $\pi_k(V(I))$ de los ceros del ideal I si y sólo si existen $a_1, \ldots, a_k$ tales que el punto $(a_1, \ldots, a_n)$ pertenece a $V(I)$. Es fácil ver que $\pi_k((V(I)) \subseteq V(I_k) \subseteq \mathbf{C}^{n-k}$, y de hecho, $V(I_k)$ resulta ser la menor variedad algebraica que la contiene. En particular, si la imagen es una variedad algebraica, entonces se describe por la anulación de los polinomios de I que dependen sólo de las últimas $n-k$ variables. Esto no sucede necesariamente. Por ejemplo, si $I =< xy - 1 >$, la imagen de $V(I)$ por la proyección sobre la coordenada y es igual a $\{y \in \mathbf{C} / \ \exists x \in \mathbf{C} \text{ such that } xy = 1\} = \mathbf{C} - \{0\}$, que no es una variedad algebraica. En este caso $I_1 = \{0\}$ y $V(I_1) = \mathbf{C}$.

Teorema: *Sea $\prec$ un orden monomial tal que*

$$\alpha_1 + \ldots + \alpha_k > 0 \Rightarrow (\alpha_1, \ldots, \alpha_n) \succ (0, \ldots, 0, \beta_{k+1}, \ldots, \beta_n)$$

para toda elección de enteros no negativos $\beta_{k+1}, \ldots, \beta_n$ (Por ejemplo, el orden lexicográfico con $x_n \prec \ldots \prec x_1$). Sea I un ideal y G una GB de I respecto de $\prec$. Entonces $G \cap \mathbf{C}[x_{k+1}, \ldots, x_n]$ es una GB de I_k para el orden inducido por $\prec$ en $\mathbf{C}[x_{k+1}, \ldots, x_n]$.

Entonces, si $\prec$ es un orden como en el teorema, existe en I un polinomio no nulo que dependa sólo de las últimas $n-k$ variables si y sólo si es posible encontrar un polinomio en $\mathbf{C}[x_{k+1}, \ldots, x_n]$ en cualquier GB de I respecto de $\prec$ (y esto provee un algoritmo para hallarlo).

Por ejemplo, "triangular" el sistema

$$\begin{array}{ccccccc} x^2 & + & y & + & z & = & 1 \\ x & + & y^2 & + & z & = & 1 \\ x & + & y & + & z^2 & = & 1 \end{array}$$

corresponde a tratar de encontrar las últimas coordenadas de las soluciones, luego las segundas coordenadas que corresponden a estas últimas coordenadas, y luego las primeras coordenadas correspondientes.

Entonces consideramos el orden lexicográfico con $x \succ y \succ z$, y calculamos una GB G de $I =< x^2 + y + z - 1,\ x + y^2 + z - 1,\ x + y + z^2 - 1 >$. Con la ayuda de MAPLE obtenemos $G =< x+y+z^2-1,\ y^2-y-z^2+z,\ 2yz^2+z^4-z^2,\ z^6-4z^4+4z^3-z^2 >$. Como $z^6-4z^4+4z^3-z^2 = z^2(z-1)^2(z^2+2z-1)$, vemos que los posibles valores de z son $0, 1, -1+\sqrt{2}, -1-\sqrt{2}$. Sustituyendo estos valores en el segundo y el tercer polinomios (que no dependen de x), podemos determinar los posibles valores de y. Finalmente, es posible comprobar que el sistema tiene exactamente 5 soluciones.

En verdad, además de un teorema de eliminación como el enunciado, hacen falta resultados que aseguren extensión de soluciones parciales.

Implicitaciones y ecuaciones de dependencia algebraica: Veremos con dos ejemplos, como puede utilizarse la eliminación efectiva de variables para resolver estos problemas.

Consideremos la superficie S formada por la unión de las rectas tangentes a la curva parametrizada por (t, t^2, t^3). Es decir,

$$S = \left\{ x = t + u,\ y = t^2 + 2tu,\ z = t^3 + 3t^2u \right\}.$$

Encontrar ecuaciones implícitas para S es lo mismo que considerar el ideal $I :=< t+u-x,\ t^2+2tu-y,\ t^3+3t^2u-z >$ en $\mathbf{C}[t,u,x,y,z]$, y eliminar las variables t,u. Para ello, basta encontrar una GB G de I con respecto al orden lexicográfico con $t \succ u \succ x \succ y \succ z$, y buscar $G \cap \mathbf{C}[x,y,z]$. Haciendo esto con la ayuda de MAPLE por ejemplo, encontramos el polinomio $p = 1-6zxy-3x^2y^2+4y^3+z^2+4zx^3$. De hecho, lo único que podemos asegurar por el momento es que $S \subseteq \{p=0\}$, y hay que seguir trabajando ad-hoc para ver que vale la igualdad.

Consideremos los polinomios en dos variables $f = y^2+x^2-1,\ g = 3xy-1, h = y-x-1$. Estos polinomios son algebraicamente dependientes, y para encontrar una ecuación de dependencia algebraica entre ellos, basta con agregar tres nuevas variables u,v,w, considerar el ideal generado por $f-u,\ g-v,\ h-w$, y eliminar x e y. Así obtenemos el polinomio $3w^2+6w+2v-3u+2$, es decir que $3h^2+6h+2g-3g+2=0$.

Polinomios invariantes: Supongamos que queremos escribir un polinomio simétrico como un polinomio en las funciones simétricas elementales. Introduzcamos nuevas variables $y_1,\ldots,y_n$ y consideremos el ideal $I =< \sigma_1 - y_1, \ldots, \sigma_n - y_n$. Sea $\prec$ un orden monomial tal que cualquier monomio que contenga alguna de las variables $x_1,\ldots,x_n$ sea mayor que cualquier monomio sólo en las variables $y_1 \ldots, y_n$. Sea G una GB de I respecto de $\prec$. Dado $p \in \mathbf{C}[x_1,\ldots,x_n]$, llamemos q al resto de la división de p por g. Puede probarse que p es simétrico si y sólo si $q \in \mathbf{C}[y_1,\ldots,y_n]$ y que si p es simétrico, $p(x_1,\ldots,x_n) = q(\sigma_1,\ldots,\sigma_n$. Es decir que el cociente de la división por G provee el polinomio buscado.

Este algoritmo puede generalizarse a polinomios invariantes respecto de grupos lineales finitos, pero hay desarrollados además otros algoritmos específicos que tienen en cuenta la invariancia durante el proceso (cf. [S]).

Sistemas con finitos ceros: Dado un ideal $I \subseteq \mathbf{C}[x_1,\ldots,x_n]$, puede probarse que $V(I)$ es finito si y sólo si para cada $i=1,\ldots,n$ existe un polinomio no nulo $p_i \in I$ que depende solamente de la variable x_i. Los ceros de I quedan contenidos en la "grilla" $\{x/\ p_1(x_1) = 0,\ \ldots, p_n(x_n) = 0\}$. Es posible decidir la existencia o no de tales polinomios considerando n órdenes de eliminación que dejen en cada caso a la variable x_i como la menor variable.

Asimismo, si $\prec$ es un orden monomial arbitrario, y G es una GB de I respecto de $\prec$, $V(I)$ es finito si y sólo si para cada $i=1,\ldots,n$ existe un polinomio $g_i \in G$ tal que el multigrado de g_i depende sólo de x_i. Esta propiedad provee otro algoritmo para decidir si un sistema polinomial tiene finitas soluciones complejas.

Invertibilidad de una aplicación polinomial: Supongamos que $F = (F_1,\ldots,F_n) : \mathbf{C}^n \to \mathbf{C}^n$ es una aplicación polinomial. Es posible chequear con la herramienta de las bases de Gröbner si la aplicación F tiene una inversa polinomial, y si la tiene, encontrar la inversa. Supongamos que los polinomios dados dependen de las variables $x_1,\ldots,x_n$, y agreguemos n nuevas variables $y_1,\ldots,y_n$. Consideremos el ideal generado por $y_1 - F_1(x_1,\ldots,x_n),\ldots,y_n - F_n(x_1,\ldots,x_n)$ en el anillo de polinomios $\mathbf{C}[x_1,\ldots,x_n,y_1,\ldots,y_n]$. Consideremos cualquier orden monomial tal que cualquier x_j sea mayor que cualquier monomio donde aparezcan sólo las variables y. Entonces F es inversible si y sólo si la GB reducida con respecto a un tal orden es de la forma $x_1 - G_1(y_1,\ldots,y_n),\ldots,x_n - G_n(x_1,\ldots,x_n)$. Además, la aplicación $(G_1,\ldots,G_n) : \mathbf{C}^n \to \mathbf{C}^n$ resulta ser la inversa de F (cf. [V]).

Bibliografía

[A-L] W. Adams and P. Loustaunau: *An Introduction to Gröbner Bases*, Volume 3/ GSM Series, Springer–Verlag, 1994.

[B-W] T. Becker and V. Weispfenning (in cooperation with H. Kredel): *Gröbner Bases*, Graduate Texts in Mathematics 141, Springer–Verlag, 1993.

[C-L-O] D. Cox, J. Little, D. O'Shea: *Ideals, Varieties and Algorithms*, Undergraduate Texts in Mathematics, Springer–Verlag, 1992.

[E] D. Eisenbud: *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics 150, Springer–Verlag, 1995.

[H-M] J. Heintz and J. Morgenstern: *On the intrinsic complexity of elimination theory*, J. of Complexity 9 (1993), 471–498.

[L] M. Lejeune–Jalabert: *Effectivité de Calculs Polynomiaux*, Cours de D.E.A. 84–85, Université de Grenoble I, Institut Fourier.

[R] L. Robbiano: *On the theory of graded structures*, J. Symb. Comp. 1 (1986), 139–170.

[S] B. Sturmfels: *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Springer–Verlag, 1993.

[V] A. Van den Essen: *A criterion to decide if a polinomial map is invertible and to compute the inverse*, Comm. Algebra 18 (10) (1990), 3183–3186.

[V-V-C] J. Verschelde, P. Verlinden and R. Cools, *Homotopies exploiting Newton Polytopes for Solving Sparse Polynomial Systems*, Siam J. Numer. Anal., Vol. 31 , No. 3, 915–930, June 1994.

Departamento de Matemática - F.C.E. y N. - Universidad de Buenos Aires
Ciudad Universitaria - Pabellón I - (1428) Buenos Aires - Argentina
alidick@dm.uba.ar