La Columna de Matemática Computacional

Sección a cargo de

Tomás Recio

En este número...

En este número de *La Gaceta*, presentamos un artículo del profesor Antonio Montes, Profesor Titular de Matemática Aplicada de la Universidad Politécnica de Cataluña, en el que describe un algoritmo que proporciona, de modo compacto y canónico, el estudio de casos en la resolución de un sistema de ecuaciones polinómicas en varias variables y parámetros.

Se trata de un problema fundamental, que aparece en contextos elementales y avanzados, teóricos y aplicados. Discutir, en función de los parámetros a, b, la solución de la ecuación $ax - b = 0$, es inmediato, aunque engorroso: si a no es cero, $x = b/a$; si $a = 0$, entonces, si $b = 0$, la ecuación tiene infinitas soluciones (digamos, sobre los racionales); si $a = 0$ pero $b \neq 0$, entonces no tiene solución. Si, en vez de una ecuación lineal en una variable, consideramos una ecuación genérica de grado dos $ax^2 + bx + c = 0$, el lector sabrá apreciar cómo se complica la propia idea de «caso»: si a es distinto de cero la ecuación (digamos, sobre los complejos) tiene siempre solución, pero ¿hemos de distinguir también el caso de dos soluciones distintas y el caso de una sola (doble)? ¿Y el que corresponde a la existencia de soluciones reales?

Por otra parte, si tomamos un sistema con varias ecuaciones, tal como $\{ax^2 + bx + c = 0,\ 2ax + b = 0\}$, observamos que no tiene solución en general, para valores arbitrarios de a, b, c, por lo que dicho sistema es, genéricamente, equivalente a $\{1 = 0\}$. Pero esta forma simplificada no representa a dicho sistema en el caso particular en el que los valores de los parámetros cumplan las condiciones $\{a \neq 0, b^2 - 4ac = 0\}$. En este caso, para cualesquiera valores de a, b, c que verifiquen estas condiciones, el sistema *especializado* en tales valores es equivalente (tiene las mismas soluciones) a la sola ecuación $\{2ax + b = 0\}$, con la que visualizamos inmediatamente la solución del sistema en este caso particular.

Estas consideraciones elementales quieren mostrar al lector la importancia, en la discusión de los sistemas con parámetros, de cuatro aspectos: la complejidad de la discusión (y, por tanto, la conveniencia de su automatización); la necesidad de establecer un criterio sobre lo que debe entenderse por «caso» (y, en consecuencia, el carácter canónico de la discusión); el interés —para la obtención de la solución o soluciones— de presentar, en cada caso, un sistema simplificado equivalente, válido para todos los valores de los parámetros implicados en dicho caso; por último, la exigencia de cálculos no triviales para la descripción de los casos (así, en el ejemplo

Antonio Montes (centro), M. Wibmer (izda.) y M. Manubens (dcha.).

anterior —con sólo dos ecuaciones de grado a lo más dos y en una variable— aparece de manera natural el discriminante de una ecuación de segundo grado; pensemos en el supuesto de varias variables, muchas ecuaciones y grados más altos). Todos estos aspectos se estudian convenientemente en el artículo de Montes que aparece en esta sección de *La Gaceta*.

El profesor Montes, que cumplirá 70 años dentro de unos meses, es uno de los mayores expertos internacionales en el tratamiento automático de sistemas de ecuaciones con parámetros, con más de una década de trabajos en este campo, diversas publicaciones sobre los mismos en la revista de Álgebra Computacional de referencia, el *Journal of Symbolic Computation* e implementaciones en *Maple* y *Singular* de sus algoritmos. Ha dirigido recientemente, en este tema, la tesis doctoral de Montserrat Manubens y ha colaborado con el joven doctor por Heidelberg, Michael Wibmer, con el que ha realizado la publicación [21] que es la base del trabajo que se presenta a continuación.

El profesor Montes es, desde hace años, un activo miembro del comité científico de la Red Española de Álgebra Computacional y Aplicaciones (Red EACA) y responsable de su nodo en Cataluña.

Discusión de sistemas polinómicos con parámetros

por

Antonio Montes*

Resumen. Se detalla brevemente el desarrollo histórico de los algoritmos para la discusión de sistemas de ecuaciones polinómicas con parámetros y se dan los elementos esenciales para comprender y poder utilizar el nuevo algoritmo del cubrimiento canónico de Gröbner (GröbnerCover) de un ideal paramétrico, introducido recientemente por el autor y por Michael Wibmer, de la Universidad de Aachen. A fin de que los no especialistas puedan comprender bien su significado e interés, antes de abordar el tema se hace una introducción elemental a la teoría de las bases de Gröbner, que subyace a este nuevo algoritmo. Posteriormente se dan ejemplos donde puede apreciarse su utilidad para resolver problemas en los que aparecen ecuaciones polinómicas con parámetros.

Introducción

Las discusiones de sistemas de ecuaciones lineales con parámetros son tan populares que es raro que no aparezca un problema de ese tipo en los exámenes de acceso a la Universidad. Sin embargo, incluso para las ecuaciones lineales, las discusiones habituales no suelen ser únicas y dependen del orden en que se consideran las condiciones.

En muchos campos técnicos, como la robótica, la química, el estudio de redes eléctricas, etc., o en la demostración automática, en el diseño geométrico, etc., aparecen ecuaciones que ya no son lineales en las variables, sino polinómicas, y contienen también parámetros.

El objetivo de este artículo es presentar una discusión completamente canónica de los sistemas de ecuaciones polinómicas con parámetros a través del nuevo algoritmo GröbnerCover que, de manera conjunta, el autor de este artículo y Michel Wibmer han desarrollado recientemente [21]. Está implementado en el programa de álgebra computacional *Singular*, en la librería `grobcov.lib`, cuya versión beta puede bajarse en la web del autor [22]. Existen algoritmos más elementales para discutir sistemas polinómicos con parámetros ([4], [27], [12]), pero ninguno de ellos es canónico ni tiene las propiedades del GröbnerCover.

En la práctica trabajaremos con polinomios en varias variables con coeficientes racionales, cuyas soluciones consideraremos sobre los números complejos. Todo el

*Parcialmente financiado por el Ministerio de Ciencia y Tecnología bajo el proyecto MTM2009-07242, y por la Generalitat de Catalunya bajo el proyecto DGR 2009SGR1040.

artículo puede entenderse en este contexto, si bien el lector más avezado puede considerar los polinomios sobre un un cuerpo K computable y las soluciones en una extensión algebraicamente cerrada $\overline{K}$.

Consideremos un sistema de ecuaciones polinómicas

$$\begin{cases} p_1(\lambda_1, \ldots, \lambda_m, x_1, \ldots, x_n) = 0, \\ \qquad\qquad \ldots \\ p_r(\lambda_1, \ldots, \lambda_m, x_1, \ldots, x_n) = 0, \end{cases}$$

con coeficientes en el cuerpo K, donde $\overline{x} = (x_1, \ldots, x_n)$ son las variables y $\overline{\lambda} = (\lambda_1, \ldots, \lambda_m)$ los parámetros. Denotaremos el sistema como $\{p_1, \ldots, p_r\} \subset K[\overline{\lambda}, \overline{x}]$ y denotaremos $\overline{a} \in \overline{K}^m$ a un conjunto de valores particulares del conjunto de parámetros $\overline{\lambda}$.

El problema consiste en conocer cómo son las soluciones de los distintos sistemas algebraicos $\{p_1(\overline{a}, \overline{x}), \ldots, p_r(\overline{a}, \overline{x})\} \subset \overline{K}[\overline{x}]$ que se obtienen al *especializar* (substituir) los parámetros $\overline{\lambda}$ por valores concretos $\overline{a} \in \overline{K}^m$. Es decir, se trata de estudiar el comportamiento de los distintos sistemas obtenidos a partir del dado mediante especialización de los parámetros por valores numéricos, reflejando diferentes aspectos de dichos sistemas, tales como el poseer un número finito de soluciones, o —en otro caso— el número de grados de libertad, etc.

Ejemplo 1. Dada la ecuación genérica de una cónica, de la forma $x^2 + 2cxy + by^2 + 2dx + 2ey + f = 0$, deseamos discutir para qué valores de los parámetros b, c, d, e, f dicha cónica tiene puntos singulares y cuáles son las características de dichas singularidades. El sistema completo a considerar será, pues, el siguiente:

$$\begin{cases} x^2 + 2cxy + by^2 + 2dx + 2ey + f = 0, \\ 2x + 2cy + 2d = 0, \\ 2cx + 2by + 2e = 0. \end{cases}$$

La aplicación del algoritmo GröbnerCover, al que hemos hecho referencia antes y cuya divulgación vamos a realizar en las páginas siguientes, arroja una discusión en cuatro casos diferenciados. Cada caso viene dado por un conjunto de valores de los parámetros —constituyendo diferentes *segmentos*, en la terminología que utilizaremos— y por un sistema equivalente simplificado —o *base*, en dicha terminología—. El resultado es el siguiente:

Caso 1: caso genérico, sin puntos singulares (cónica no degenerada)
Segmento: $\mathbb{C}^5 \setminus \{(b, c, d, e, f) : bd^2 - bf + c^2 f - 2cde + e^2 = 0\}$.
Base: $\{1\}$.

Caso 2: un punto singular (dos rectas que se cortan)
Segmento: $\{(b, c, d, e, f) : bd^2 - bf + c^2 f - 2cde + e^2 = 0\}$.
$\setminus \{(b, c, d, e, f) : cd - e, b - c^2 = 0\}$
Base: $\left\{ y + \dfrac{e - cd}{b - c^2},\ x + \dfrac{bd - ce}{b - c^2} \right\}$.

Caso 3: sin puntos singulares (dos rectas paralelas)
Segmento: $\{(b,c,d,e,f) : cd - e = 0, b - c^2 = 0\}$
$\setminus \{(b,c,d,e,f) : d^2 - f = 0, cf - de = 0, cd - e = 0, b - c^2 = 0\}$.
Base: $\{1\}$.

Caso 4: recta singular (recta doble)
Segmento: $\{(b,c,d,e,f) : d^2 - f = 0, cf - de = 0, cd - e = 0, b - c^2 = 0\}$.
Base: $\{x + cy + d\}$.

Se trata de una discusión completa y precisa, en la cual los distintos segmentos vienen dados como diferencia de conjuntos de soluciones de sistemas de ecuaciones; y cada caso corresponde a tipos (según el criterio tradicional) de soluciones diferentes. Además, en el ejemplo, se ve fácilmente que los casos son disjuntos y, aunque ocurre que dos de tales casos (el 1 y el 3) tienen un mismo sistema simplificado equivalente y no tienen puntos singulares, corresponden a tipos distintos de cónicas.

En lo que sigue, y a fin de desarrollar esta propuesta de discusión automática de casos, necesitaremos describir someramente, en la sección 1, la teoría de las bases de Gröbner, que es el método por excelencia para el estudio algorítmico de los sistemas polinómicos. Dentro de dicha sección reservamos una subsección (la 1.1) a detallar la relación de las bases de Gröbner y lo que podríamos llamar la *tipología* de las soluciones de un sistema dado.

En la sección 2 abordaremos el estudio sistemático de los sistemas con parámetros. Tras una breve reseña histórica introduciremos la noción de *cobertura de Gröbner canónica* para un sistema homogéneo con parámetros y también para un sistema no-homogéneo y enunciaremos los teoremas de existencia y de validez del algoritmo GröbnerCover para obtenerla. A tal fin presentaremos en dicha sección ejemplos que justifican la necesidad de considerar, en primer lugar, los sistemas homogéneos y, también, de generalizar el concepto de polinomio ordinario mediante la introducción de la idea de *función regular*.

Los distintos casos que produce la cobertura canónica de Gröbner consisten en un conjunto de valores de los parámetros —lo que denominaremos un *segmento*— y un sistema simplificado —denominado *base*— que es equivalente al sistema dado para todos los valores de los parámetros dentro del mismo segmento. Por ello en la sección 3 se estudiarán las posibles formas de representar ambos tipos de objetos —segmentos y bases— a fin de que se puedan comprender bien las opciones elegidas y, en consecuencia, el carácter canónico de los resultados obtenidos con el algoritmo.

Por último, en la sección 4, daremos un ejemplo no trivial de la potencia y utilidad del algoritmo, estudiando un caso de deducción automática de teoremas geométricos, *descubriendo* las condiciones para que el triángulo órtico de un triángulo dado sea isósceles.

1. Bases de Gröbner para sistemas sin parámetros

Esta sección puede obviarse si el lector está familiarizado con el concepto de base de Gröbner. Las bases de Gröbner para sistemas de ecuaciones (sin parámetros)

fueron estudiadas desde una perspectiva computacional por B. Buchberger en 1960 y han sido objeto de múltiples estudios desde entonces. Una introducción muy legible aparece en los excelentes libros de texto [1, 3].

Consideremos un sistema polinómico ordinario sin parámetros. Dado un sistema de ecuaciones determinado por los polinomios $\{p_1, \ldots, p_r\} \subset K[\overline{x}]$, podemos substituir dicho conjunto de ecuaciones por otro equivalente (por ejemplo añadiendo combinaciones polinómicas de dichas ecuaciones y eliminado ecuaciones que sean consecuencia de las que tenemos). Dicho en términos algebraicos, el sistema $\{p_1, \ldots, p_r\} \subset K[\overline{x}]$ define un *ideal* $I = \langle p_1, \ldots, p_r \rangle \subset K[\overline{x}]$, y existen muchas bases (sistemas equivalentes) que definen el mismo ideal. Cada una de tales bases determina el mismo *ideal* $I = \langle p_1, \ldots, p_r \rangle = \{\sum_{k=0}^{r} h_k p_k \in K[\overline{x}] : h_k \in K[\overline{x}]\}$, como el conjunto de polinomios que son combinación lineal con coeficientes polinómicos del sistema dado, y la *variedad* asociada $\mathbb{V}(p_1, \ldots, p_r) = \{\overline{a} \in \overline{K}^n : p_1(\overline{a}) = 0, \ldots, p_r(\overline{a}) = 0\}$, o conjunto de soluciones de dicho sistema, es decir, los puntos de $\overline{K}^n$ donde se anulan todos los polinomios del ideal. Nótese que tomamos los polinomios sobre un cuerpo computable K, a fin de poder hacer cálculos exactos con ellos, mientras que las variedades las consideraremos en $\overline{K}^n$ para poder usar el Teorema Fundamental del Álgebra o Teorema de los Ceros, sobre la existencia de soluciones (*Nullstellensatz*).

Entre las muchas bases posibles de un ideal, y a fin de obtener aquéllas que tengan las mejores propiedades, es preciso introducir un orden $\succ$ en el conjunto de monomios $\{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha \in \mathbb{Z}_{\geq 0}^n\}$ con las siguientes propiedades: (i) $\succ$ es un orden total; (ii) para todo monomio x^γ, si $x^\alpha \succ x^\beta$ entonces $x^{\alpha+\gamma} \succ x^{\beta+\gamma}$; (iii) $\succ$ es un buen orden.

En función del orden elegido, cada polinomio $f \in K[\overline{x}]$ tendrá un *monomio principal* $\mathrm{lpp}(f)$ (*leading power product*). Entre los muchos órdenes monomiales posibles, los más usados son el lexicográfico, $\mathrm{lex}(x_1, \ldots, x_n)$, y el graduado inverso lexicográfico, $\mathrm{grevlex}(x_1, \ldots, x_n)$. El orden lex se define estableciendo que $\alpha \succ_{\mathrm{lex}} \beta$ si la primera entrada no nula por la izquierda del vector $\alpha - \beta$ es positiva. Para el orden grevlex se tiene $\alpha \succ_{\mathrm{grevlex}} \beta$ si los grados de los monomios correspondientes cumplen $\mathrm{grad}(\alpha) > \mathrm{grad}(\beta)$ o si $\mathrm{grad}(\alpha) = \mathrm{grad}(\beta)$ y la primera entrada no nula por la derecha de $\alpha - \beta$ es negativa.

Fijado un orden monomial es posible introducir una división entre polinomios. Para ello, y dado que los ideales de polinomios multivariables no son necesariamente principales sino que están generados por un conjunto finito de polinomios, se define una división de un polinomio $f \in K[\overline{x}]$ entre un conjunto $\{g_1, \ldots, g_s\} \subset K[\overline{x}]$ de polinomios, siendo el resultado un resto $r \in K[\overline{x}]$ y con conjunto de cocientes $\{q_1, \ldots, q_s\} \subset K[\overline{x}]$, de manera que se cumpla:

1. $f = q_1 g_1 + \cdots + q_s g_s + r$,
2. ningún término del resto r es divisible por ninguna potencia principal $\mathrm{lpp}(g_i)$, para ningún i,
3. $\mathrm{lpp}(f) \succeq \mathrm{lpp}(q_i g_i)$ para todo i.

Esta división ya no tiene tantas propiedades como la división de polinomios univariados y, aunque el resultado no es único, es obvio que, si el resto es cero, el polinomio

f pertenece al ideal $\langle g_1, \ldots, g_s \rangle$ generado por el conjunto de polinomios $\{g_1, \ldots, g_s\}$. Pero el recíproco no es cierto.

Pues bien, dado un ideal I y un orden monomial $\succ$, una base de Gröbner G de I es una base de I tal que el resto de la división por ella es único. Con ello recuperamos la propiedad que permite saber si un polinomio f pertenece al ideal I. Si G es base de Gröbner de I, entonces f pertenece a I si y sólo si el resto de dividir f por la base G es cero. Sea $G = \{g_1, \ldots, g_s\}$ y denotemos

$$\mathrm{lpp}(G) = \{\mathrm{lpp}(g_1), \ldots, \mathrm{lpp}(g_s)\}$$

al conjunto de los monomios principales de G. Se demuestra que G es una base de Gröbner de I si el conjunto $\mathrm{lpp}(G)$ de monomios principales de G genera el conjunto de monomios principales de todos los polinomios de I:

$$\langle \mathrm{lpp}(G) \rangle = \mathrm{lpp}(I).$$

Para ilustrar estos conceptos consideremos, por ejemplo, $H = \{3x+2y-1, x-y-2\}$ e $I = \langle H \rangle \subset K[x, y]$, y tomemos un orden monomial en el que $x \succ y$. H no es una base de Gröbner de I, ya que el único monomio principal de H es x, y sin embargo, eliminando x entre los dos polinomios, resulta el polinomio $y + 1 = 1/5(3x+2y-1) - 3/5(x-y-2)$, que pertenece a I y tiene un $\mathrm{lpp}(y+1) = y$ que no pertenece a $\langle \mathrm{lpp}(H) \rangle = \langle x \rangle$. Es claro que $G = \{x-1, y+1\}$ es una base de Gröbner de I, ya que el monomio principal de cualquier polinomio de I es divisible bien por x o bien por y, puesto que ningún polinomio constante pertenece a I. Además G es la base de Gröbner reducida de I en el sentido de que ningún monomio de ninguno de los polinomios de G es divisible por ninguno de los monomios principales de G. A fin de que la base reducida sea única se exige, también, que sus polinomios sean mónicos, lo que se puede obtener normalizando, esto es, dividiendo cada uno de ellos por su coeficiente principal. Se demuestra entonces, fácilmente, que existe una única base de Gröbner reducida para un ideal dado. Por lo tanto, dados dos ideales I_1 e I_2, calculando las respectivas bases de Gröbner reducidas determinamos si éstos son iguales o no.

Como ya sugiere el ejemplo anterior, las bases de Gröbner dan información sobre las soluciones del sistema. En este caso vemos que la solución es única, ya que los monomios principales de G son precisamente todas las variables implicadas en el sistema. En la subsección 1.1 detallamos la relación existente entre los lpp de la base de Gröbner de un sistema de ecuaciones y el tipo de solución: si no tiene solución, o si existe un número finito de puntos solución, o cuántos grados de libertad tiene la solución. Ésta es la razón del interés en conocer la base de Gröbner de un ideal. Existe un algoritmo (Buchberger) que, dada una base de un ideal, permite calcular una base de Gröbner y después reducirla para obtener la única base de Gröbner reducida del ideal.

Pongamos otro ejemplo para dar una idea más clara de la potencia de las bases de Gröbner. Sea $H = \{xy + xz - 2, x^2 + y^2 + z^2 - 3, xyz - 2y - x^3 - xz^2 + 3x\}$ e $I = \langle H \rangle$. Tomando el orden lexicográfico $\succ = \mathrm{lex}(x, y, z)$, la base de Gröbner reducida resulta ser $G = \{y^4 + 2y^3z + 2y^2z^2 - 3y^2 + 2yz^3 - 6yz + z^4 - 3z^2 + 4,$

$2x + y^3 + y^2z + yz^2 - 3y + z^3 - 3z\}$. Tenemos $\mathrm{lpp}(G) = \{y^4, x\}$. Dado que no hay ningún lpp que sea una potencia de la variable más pequeña z, esto indica que la variable z es libre. Fijado z, el primer polinomio con $\mathrm{lpp}(g_1) = y^4$ indica que hay 4 soluciones parciales sobre $\overline{K}$ en y para cada z, que podemos representar como $y_i(z)$, $i = 1, \ldots, 4$. Finalmente, fijados $z, y_i(z)$, el último polinomio determina unívocamente una solución $x(z, y_i(z))$ en la variable x, dependiendo de z y de la solución $y_i(z)$ elegida. Esta discusión no es aparente empleando directamente la base H, que contiene 3 polinomios y 3 incógnitas, con lo que podría parecer que existe un número finito de soluciones en lugar de tener, como ocurre realmente, un grado de libertad y cuatro soluciones para cada valor de z.

El principal problema de las bases de Gröbner es la complejidad de su cálculo, que hace a veces desaconsejable su determinación.

Antes de concluir esta sección dedicaremos unas líneas a explicar de qué manera el conjunto mínimo de $\mathrm{lpp}(G)$ determina el tipo de solución del sistema.

1.1. Caracterización de la solución de un sistema mediante los lpp

Sea G la base de Gröbner reducida de un sistema de ecuaciones polinómicas (definido por el ideal I) y denotemos por $\mathrm{lpp}(G)$ el conjunto de sus lpp, que por la definición de base de Gröbner es un conjunto minimal de generadores de $\mathrm{lpp}(I)$.

Los tipos de solución más relevantes de un sistema son los siguientes:

(i) el sistema no tiene solución, es decir, $\mathbb{V}(I) = \emptyset$;

(ii) el sistema tiene un número finito de soluciones, es decir $|\mathbb{V}(I)| < \infty$;

(iii) $\mathbb{V}(I)$ es infinito, en cuyo caso interesa conocer la dimensión (o grados de libertad) de $\mathbb{V}(I)$.

Recordemos que, si bien los ideales (o los conjuntos de polinomios que los definen) tienen coeficientes en K, las variedades las tomamos siempre sobre $\overline{K}^n$, una extensión algebraicamente cerrada. Con ello podemos utilizar el *Nullstellensatz* de Hilbert. Por lo tanto, el sistema no tiene solución (caso (i)) si y sólo si $G = \{1\}$.

El caso (ii) de un número finito de soluciones queda cubierto por el siguiente Teorema de Finitud:

Teorema 2 (Finitud, [3, cap. 5, pág. 230]). *Sea $I \subset K[\overline{x}]$ un ideal, $\succ$ un orden monomial y G una base de Gröbner de I. Entonces, las siguientes afirmaciones son equivalentes:*

(i) *La variedad $\mathbb{V}(I)$ es un conjunto finito.*

(ii) *Para cada $1 \leq i \leq n$ existe algún $r_i > 0$ tal que $x_i^{r_i} = \mathrm{lpp}(g)$, para algún $g \in G$.*

(iii) *La dimensión del K-espacio vectorial $K[\overline{x}]/I$ es finita.*

(iv) *El conjunto de términos x^α tales que $x^\alpha \notin \langle \mathrm{lpp}(I) \rangle$ es finito.*

Con el teorema anterior queda cubierto el tipo de solución (ii), ya que una vez calculada la base de Gröbner podemos detectar inmediatamente si la variedad es finita o no.

Podemos precisar más, utilizando las siguientes proposiciones:

Proposición 3 ([3]). *Sea $I \subset K[\overline{x}]$ un ideal cero dimensional. Entonces el número de puntos de $\mathbb{V}(I)$ es, como máximo,* $\dim(K[\overline{x}]/I)$*, es decir, como máximo el número de monomios que son irreducibles módulo I o, lo que es lo mismo, el número de* lpp*'s que no son divisibles por ningún* $\mathrm{lpp}(G)$.

Ejemplo 4. Sea un sistema cuya base de Gröbner reducida respecto al orden $\mathrm{lex}(x, y)$ es:

$$\begin{aligned} G = \{&y^4 - 7y^3 + 11y^2 + 7y - 12, \\ &xy^2 - x - 2y^3 + 4y^2 + 2y - 4, \\ &4x^2y - 4x^2 - 9y^3 + 24y^2 + 5y - 20, \\ &8x^3 - 24x^2 - 8x - 11y^3 + 36y^2 + 11y - 12\}. \end{aligned}$$

Sus monomios principales son $\{y^4, xy^2, x^2y, x^3\}$. La base del K-espacio vectorial $K[\overline{x}]/I$ es el conjunto de monomios que no son divisibles por ningún monomio principal, es decir: $\{1, y, y^2, y^3, x, xy, x^2\}$ (ver figura 1). Por lo tanto tiene como máximo 7 soluciones. En este ejemplo es fácil ver que las soluciones son $\{(4, 4), (2, 3), (3, 1), (1, 1), (-1, 1), (1, -1), (-1, -1)\}$ que son, efectivamente, 7.

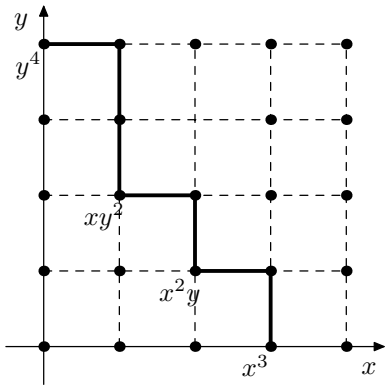

Figura 1: Monomios principales y base de $K[x]/I$ del ejemplo 4.

Veamos ahora el caso (iii), correspondiente a infinitas soluciones. En el supuesto de un tipo particular de ideales, los ideales de monomios, se tiene la siguiente

Proposición 5 ([3]). *Sea $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \subset K[\overline{x}]$ un ideal de monomios. Para $1 \leq j \leq s$, denotemos*

$$M_j = \{k \in \{1, \ldots, n\} : x_k \textit{ divide al monomio } x^{\alpha_j}\}$$

al conjunto de índices de las variables que figuran con exponente positivo en el monomio x^{α_j} (nótese que todos los M_j son no vacíos siempre que $I \neq K[\overline{x}]$). Si

$$M = \{J \subset \{1, \ldots, n\} : J \cap M_j \neq \emptyset \textit{ para todo } 1 \leq j \leq s\},$$

entonces

$$\dim(\mathbb{V}(I)) = n - \text{mín}\{|J| : J \in M\}.$$

Esta proposición permite, utilizando la base de Gröbner, determinar igualmente la dimensión de la variedad de un ideal cualquiera:

Teorema 6 (de la Dimensión, [3]). *Sea $I \subset K[\overline{x}]$ un ideal. Si $\succ$ es un orden monomial graduado y G es una base de Gröbner de I, entonces*

$$\dim(\mathbb{V}(I)) = \dim(\mathbb{V}(\text{lpp}(I)) = \dim(\mathbb{V}(\text{lpp}(G)).$$

Ejemplo 7. Veamos un ejemplo donde la dimensión del ideal no sea 0. Consideremos el sistema cuyas soluciones son $V = \mathbb{V}(x^2z+y^2z-z, x^3y+xy^3-xy)$. Tomando el orden graduado grevlex(x, y, z) observamos que el sistema $\{x^2z + y^2z - z, x^3y + xy^3 - xy\}$ ya es la base de Gröbner reducida del ideal que genera. Así pues, en este caso se tiene $\text{lpp}(G) = \{x^2z, x^3y\}$ y, con la notación anterior, se tiene $M_1 = \{1, 3\}$, $M_2 = \{1, 2\}$. El subconjunto de $\{1, 2, 3\}$ con menos elementos que tiene intersección no nula con todos los M_j es $M = \{1\}$, que tiene un único elemento. Por lo tanto la dimensión de V es $\dim(V) = 3 - 1 = 2$.

Nota. Utilizando el algoritmo de descomposición primaria de un ideal [9],[1] se puede ver que la variedad consta de un cilindro y dos rectas: $V = \mathbb{V}(x^2 + y^2 - 1) \cup \mathbb{V}(x, z) \cup \mathbb{V}(x, y)$. Por lo tanto, su dimensión, que es la máxima de las dimensiones de las variedades irreducibles que contiene, es la del cilindro, que es 2.

2. Cobertura de Gröbner de un sistema con parámetros

Consideremos ahora sistemas con parámetros. El primero en aplicar la teoría de las bases de Gröbner a dichos sistemas fue Weispfenning [28]. El problema fundamental de las bases de Gröbner en el estudio de sistemas con parámetros es que, en general, una base de Gröbner en $K[\overline{\lambda}, \overline{x}]$ no se convierte, cuando substituimos $\overline{\lambda}$ por valores numéricos $\overline{a}$, en una base de Gröbner del correspondiente sistema evaluado. Weispfenning demostró la existencia de un tipo especial de base con esta propiedad, la denominada *Base de Gröbner Comprehensiva*, dando un algoritmo para su cálculo. Desde entonces muchos otros autores han contribuido al estudio de este problema. Entre las contribuciones más importantes citemos [8, 28, 11, 5, 18, 7, 29, 25, 23, 15, 26, 30, 14, 16, 12]. Otros autores han aplicado con éxito dichos algoritmos a problemas concretos (véase, por ejemplo, [10, 17, 6, 24, 2, 19, 13, 20]).

El algoritmo más eficiente para abordar el problema de la falta de conservación por especialización de las bases de Gröbner es, en general, [12], que mejora el algoritmo [26]. Sin embargo, ni éste ni otros algoritmos propuestos tienen determinadas propiedades que serían interesantes en el contexto de la discusión de sistemas con parámetros. Deseamos obtener una discusión lo más compacta y canónica posible, únicamente dependiente del ideal dado y del orden monomial. Éste es el objetivo

[1] Dicho algoritmo utiliza bases de Gröbner y existe una muy buena implementación en *Singular*, en la librería `primedec.lib`.

de nuestro algoritmo GröbnerCover [21], cuya presentación describimos con un poco de detalle a continuación.

El algoritmo canónico GröbnerCover tiene una larga historia de diez años ([18, 15, 14, 16]) y es el resultado de una fructífera conjunción de ideas entre el algoritmo MCCGS *Minimal Canonical Comprehensive Gröbner System* ([16]) y las ideas teóricas de Michael Wibmer en su tesis doctoral en la Universidad de Heidelberg, publicadas en [30]. El algoritmo GröbnerCover utiliza parte de esos algoritmos previos e introduce nuevos y más precisos algoritmos, basados en los resultados de M. Wibmer. Se trata de un algoritmo muy complicado por lo que nuestro objetivo en esta sección es presentar las ideas fundamentales y, sobre todo, aquellos aspectos que contribuyan a facilitar su utilización y comprensión de los resultados del mismo. Para más detalles recomendamos al lector consultar el artículo [21].

Dejando aparte los problemas de eficiencia, la cuestión crucial en este contexto es dilucidar cómo representar de la manera más simple y canónica todas las bases de Gröbner reducidas que resultan al especializar un sistema.

Fijemos un orden monomial $\succ_{\overline{x}}$ en las variables y un ideal $I \subset K[\overline{\lambda}][\overline{x}] = K[\overline{\lambda}, \overline{x}]$ generado por el conjunto de polinomios $\{p_1, \ldots, p_r\}$.

El *espacio de parámetros* es $\overline{K}^m$ y lo consideraremos como un espacio topológico con la $\overline{K}$-topología de Zariski. Así, un subconjunto es *cerrado* si es de la forma

$$S = \mathbb{V}(\mathfrak{a}) := \{\overline{a} \in \overline{K}^m \,:\, g(\overline{a}) = 0,\ g \in \mathfrak{a}\},$$

para algún conjunto $\mathfrak{a}$ de $K[\overline{\lambda}] = K[\lambda_1, \ldots, \lambda_m]$; y es *localmente cerrado* si es diferencia de dos conjuntos cerrados $\mathbb{V}(\mathfrak{a}) \setminus \mathbb{V}(\mathfrak{b})$ o variedades.

Objetivo. Dado $\overline{a} \in \overline{K}^m$, denotemos $I_{\overline{a}} \subset \overline{K}[\overline{x}]$ al ideal generado por todos los $p(\overline{a}, \overline{x}) \in \overline{K}[\overline{x}]$ con $p \in I$. El objetivo es describir de la mejor manera posible, en función de $\overline{a} \in \overline{K}^m$, las bases de Gröbner de $I_{\overline{a}}$ (respecto al orden $\succ_{\overline{x}}$). En este sentido deseamos dividir el espacio de parámetros $\overline{K}^m$ en el menor número posible de segmentos S_i disjuntos, que sean localmente cerrados ($S_i = \mathbb{V}(\mathfrak{a}_i) \setminus \mathbb{V}(\mathfrak{b}_i)$), y de tal manera que sobre cada uno de dichos segmentos los lpp de las bases de Gröbner reducidas de $I_{\overline{a}}$ con $\overline{a} \in S_i$ sean iguales y podamos describir todas estas bases como especialización de una única expresión, utilizando polinomios en $K[\overline{\lambda}][\overline{x}]$.

En esta dirección aparecen dos problemas que mostramos en los dos ejemplos siguientes.

Ejemplo 8. Sea $I = \langle ax + by, cx + dy\rangle \subset \mathbb{C}[a, b, c, d][x, y]$ y consideremos el orden $\succ_{\overline{x}} = \mathrm{lex}(x, y)$. Resulta fácil obtener la partición del espacio de parámetros de acuerdo a los lpp de la base de Gröbner especializada correspondiente, como se muestra a continuación:

	Segmento	lpp	Base
S_1	$\mathbb{C}^4 \setminus \mathbb{V}(ad - bc)$	$[y, x]$	$\{y, x\}$
S_2	$\mathbb{V}(ad - bc) \setminus \mathbb{V}(a, c)$	$[x]$	$\{x + \left\{\frac{b}{a}, \frac{d}{c}\right\} y\}$
S_3	$\mathbb{V}(a, c) \setminus \mathbb{V}(a, b, c, d)$	$[y]$	$\{y\}$
S_4	$\mathbb{V}(a, b, c, d)$	$[\,]$	$\{\,\}$

Vemos que hay cuatro lpp-segmentos diferentes. Sin embargo, para el segmento S_2 no es suficiente tomar sólo una de las expresiones $x + \frac{b}{a}y$ o $x + \frac{d}{c}y$ para describir la base correspondiente. En efecto, basta considerar los puntos de S_2 para los que $a \neq 0$, $c = 0$, $ad - bc = 0$, donde el polinomio $x + \frac{d}{c}y$ no está definido; y los puntos de S_2 para los cuales $a = 0$, $c \neq 0$, $ad - bc = 0$, donde $x + \frac{b}{a}y$ no está definido. Obviamente ambos coinciden en los puntos del segmento S_2 donde ambos están definidos (pues $ad - bc = 0$ en ese segmento). Por lo tanto, para dar una descripción correcta de la base de Gröbner reducida en todo el lpp-segmento, necesitamos ambos polinomios. Para ello consideraremos los «polinomios» en $\mathcal{O}(S_2)[\overline{x}]$, donde $\mathcal{O}(S)$ es una ampliación del conjunto de funciones racionales sobre S al conjunto de funciones regulares sobre S, que definiremos en la subsección 3.2. Así, si $f : S_2 \to \mathbb{C}$ es la función regular dada por $f(a, b, c, d) = \frac{b}{a}$ si $a \neq 0$ y $f(a, b, c, d) = \frac{d}{c}$ si $c \neq 0$ (ambas expresiones son iguales en los demás puntos de S_2, ya que $ad - bc = 0$ en S_2), entonces el polinomio $F = x + fy \in \mathcal{O}(S_2)[\overline{x}]$ determina precisamente la base de Gröbner deseada para todos los puntos del lpp-segmento. Obsérvese que, para representar el polinomio mónico $F \in \mathcal{O}(S_2)[\overline{x}]$, podemos utilizar el par de polinomios $(ax+by, cx+dy)$, ya que cada uno de ellos, si no es nulo en un punto $(a_0, b_0, c_0, d_0) \in S_2$, especializa (una vez normalizado) al correspondiente polinomio de la base de Gröbner de $I_{(a_0,b_0,c_0,d_0)}$; y, además, siempre se tiene que en cada punto de S_2 al menos uno de los dos polinomios no es nulo. En la subsección 3.2 explicaremos qué son y cómo se representan convenientemente los elementos de $\mathcal{O}(S_i)[\overline{x}]$.

La segunda dificultad aparece cuando tratamos con sistemas no homogéneos en las variables $\overline{x}$, como en el ejemplo siguiente.

Ejemplo 9. Sea el ideal no-homogéneo $I = \langle ax+1, bx+1\rangle \subset \mathbb{C}[a, b][x]$. Es inmediato obtener la partición del espacio de parámetros respecto a los lpp:

	Segmento	lpp	Base
1	$\big(\mathbb{C}^2 \setminus \mathbb{V}(a-b)\big) \cup \mathbb{V}(a, b)$	$[1]$	$\{1\}$
2	$\mathbb{V}(a-b) \setminus \mathbb{V}(a, b)$	$[x]$	$\{x + \frac{1}{b}\}$

El primer segmento con base $\{1\}$ no es localmente cerrado, es decir, no es diferencia entre dos conjuntos cerrados o variedades, sino unión de dos conjuntos localmente cerrados. Si queremos que los segmentos sean localmente cerrados hemos de separar ese segmento en dos. Podemos hacerlo de forma canónica, homogeneizando el sistema y deshomogeneizando el resultado, a costa de perder la propiedad de tener un único segmento para cada lpp. Veámoslo en este ejemplo.

Homogeneizando el sistema resulta $\langle ax+t, bx+t\rangle$. Ahora el segmento 1 se divide en dos segmentos $1a$ y $1b$ con lpp diferentes del modo siguiente:

	Segmento	lpp	Base	Base deshomogeneizada
$1a$	$\big(\mathbb{C}^2 \setminus \mathbb{V}(a-b)\big)$	$[x, t]$	$\{x, t\}$	$\{1\}$
$1b$	$\mathbb{V}(a, b)$	$[t]$	$\{t\}$	$\{1\}$
2	$\mathbb{V}(a-b) \setminus \mathbb{V}(a, b)$	$[x]$	$\{x + \frac{t}{b}\}$	$\{x + \frac{1}{b}\}$

Haciendo $t = 1$ en las bases de los segmentos $1a$ y $1b$, después de reducir las bases, ambos tienen base $\{1\}$; a cambio, ambos segmentos son ahora localmente cerrados.

Es posible superar estos dos escollos y construir la cobertura canónica de Gröbner para sistemas homogéneos y también, empleando la técnica de homogeneizar el ideal y deshomogeneizar después, para sistemas no-homogéneos. Nos restringimos, en primer lugar, a sistemas homogéneos y consideramos polinomios de $\mathcal{O}(S)[\overline{x}]$ para poder solventar ambos problemas.

Teorema 10 (Wibmer [30]). *Dados un ideal paramétrico $I \subset K[\overline{\lambda}][\overline{x}]$, homogéneo en las variables $\overline{x}$, y un orden monomial $\succ_{\overline{x}}$ en las variables, existe la cobertura canónica de Gröbner consistente en un conjunto $\{(S_1, B_1), \ldots, (S_s, B_s)\}$ de pares con las siguientes propiedades:*

(i) *Los S_i son conjuntos disjuntos dos a dos, localmente cerrados de $\overline{K}^m$ y tales que $\overline{K}^m = \bigcup S_i$.*

(ii) *Para $\overline{a}, \overline{b} \in \overline{K}^m$ es $\operatorname{lpp}(I_{\overline{a}}) = \operatorname{lpp}(I_{\overline{b}})$ si y sólo si existe un i tal que $\overline{a}, \overline{b} \in S_i$.*

(iii) *Las B_i's son conjuntos finitos de polinomios mónicos en $\mathcal{O}(S_i)[\overline{x}]$, donde $\mathcal{O}(S_i)$ denota el anillo de las funciones I-regulares sobre S_i.*

(iv) *Para $\overline{a} \in S_i$, el conjunto $\operatorname{lpp}(B_i)$ constituye el conjunto generador minimal de $\operatorname{lpp}(I_{\overline{a}})$, y evaluando cada elemento de B_i en $\overline{a} \in S_i$ se obtiene la base de Gröbner reducida de $I_{\overline{a}}$ respecto a $\succ_{\overline{x}}$.*

Los subconjuntos S_i se denominan lpp*-segmentos. Como consecuencia de las propiedades anteriores, la cobertura de Gröbner de un sistema homogéneo es canónica (independiente del algoritmo).*

En el caso de que el ideal no sea homogéneo en las variables $\overline{x}$, procedemos a determinar en primer lugar el ideal $J \subset K[\overline{x}, x_0, \overline{\lambda}]$ homogeneizado de I (es decir, el ideal que contiene todos los polinomios que se obtienen de homogeneizar un polinomio de I). Seguidamente se calcula la cobertura de Gröbner canónica del ideal homogéneo J, y finalmente se deshomogeneízan las bases y se reducen. El resultado así obtenido es la *cobertura de Gröbner canónica del ideal no homogéneo*. Con ello, la condición (ii) queda limitada a

(iib) Para $\overline{a}, \overline{b} \in S_i$ es $\operatorname{lpp}(I_{\overline{a}}) = \operatorname{lpp}(I_{\overline{b}})$,

pudiendo existir segmentos con los mismos lpp. No obstante, y debido a que el proceso de construcción es canónico, la cobertura de Gröbner para un ideal no-homogéneo también es canónica. Además, como hemos visto en el ejemplo, cuando hay más de un segmento con el mismo lpp, ello corresponde a soluciones que son de tipo diferente en el infinito:

Teorema 11. *El algoritmo* GröbnerCover (*Montes-Wibmer*) *calcula la cobertura de Gröbner canónica* (*canonical Gröbner cover*) *de $\overline{K}^m$ de un ideal $I \subset K[\overline{\lambda}][\overline{x}]$ respecto al orden $\succ_{\overline{x}}$, tanto si el ideal es homogéneo en las variables $\overline{x}$ como si no lo es.*

3. Representación de la cobertura de Gröbner canónica

Esta sección es importante para aprender a leer el resultado obtenido al aplicar el algoritmo GröbnerCover a un ideal $I \subset K[\overline{\lambda}][\overline{x}]$ respecto a un orden dado $\succ$.

Recordemos que la cobertura de Gröbner (véase la sección 2 y el teorema 10) consiste en un conjunto $\{(S_1, B_1), \ldots, (S_s, B_s)\}$ de pares, donde los S_i son subconjuntos localmente cerrados de $\overline{K}^m$ y las B_i son conjuntos de elementos de $\mathcal{O}(S)[\overline{x}]$. Los S_i representan los puntos de $\overline{K}^m$ para los cuales los elementos de B_i especializan unívocamente a la base de Gröbner reducida de I para todos los puntos $\overline{a} \in S_i$. Aunque en la mayoría de casos y sistemas las funciones I-regulares pueden ser representadas por un único polinomio, ello no es siempre posible y la correcta descripción requiere una representación más elaborada. En esta sección explicamos cómo se representan tanto las bases como los segmentos.

3.1. Representación canónica de conjuntos localmente cerrados

Un conjunto $S \subset \overline{K}^m$ localmente cerrado es una diferencia de dos variedades $\mathbb{V}(\mathfrak{a}) \setminus \mathbb{V}(\mathfrak{b})$, donde $\mathfrak{a}, \mathfrak{b}$ son subconjuntos de $K[\overline{\lambda}]$. No obstante, diferentes $\mathfrak{a}, \mathfrak{b}$ pueden describir, tomando la diferencia de sus variedades, el mismo S. Denotemos $\overline{S}$ a la clausura de Zariski de S, es decir, a la variedad más pequeña que contiene S. Se tiene la siguiente

Definición 12. Sea $S \subset \overline{K}^m$ un conjunto localmente cerrado. Entonces, existe un único par de ideales radicales $\mathfrak{a}$ y $\mathfrak{b}$ de $K[\overline{\lambda}]$ de modo que $S = \mathbb{V}(\mathfrak{a}) \setminus \mathbb{V}(\mathfrak{b})$ y $\mathfrak{a} \subset \mathfrak{b}$, tales que

- $\overline{S} = \mathbb{V}(\mathfrak{a})$ y
- $\overline{S} \setminus S = \mathbb{V}(\mathfrak{b})$.

El par $(\mathfrak{a}, \mathfrak{b})$ se denomina la *C-representación* de S (representación canónica).

Definición 13. Sea $S \subset \overline{K}^m$ un conjunto localmente cerrado. Entonces, existen ideales primos unívocamente determinados

$$\{(\mathfrak{p}_i, \{\mathfrak{p}_{ij} : 1 \leq j \leq s_i\}) : 1 \leq i \leq r\} \tag{1}$$

de $K[\overline{\lambda}]$, siendo $S = \bigcup_{i=1}^{r} \left(V(\mathfrak{p}_i) \setminus \bigcup_{j=1}^{r_i} \mathbb{V}(\mathfrak{p}_{ij}) \right)$ y $\mathfrak{p}_i \subset \mathfrak{p}_{ij}$ para todos los i, j, tales que

- $\overline{S} = \mathbb{V}(\mathfrak{p}_1) \cup \cdots \cup \mathbb{V}(\mathfrak{p}_r)$ y
- $(\overline{S} \setminus S) \cap \mathbb{V}(\mathfrak{p}_i) = \mathbb{V}(\mathfrak{p}_{i1}) \cup \cdots \cup \mathbb{V}(\mathfrak{p}_{is_i})$

son las descomposiciones mínimas en conjuntos irreducibles cerrados. Decimos que (1) es la *P-representación de* S. Llamamos a los $\mathfrak{p}_i$ *componentes de* S y a los $\mathfrak{p}_{ij}$ los *agujeros de* $\mathfrak{p}_i$ (respecto a S).

Por ejemplo, si $S = \mathbb{V}(a^3 - a^2b^2 - ab^2 + b^4) \setminus \mathbb{V}(a^2 - ab)$ tenemos

$$\begin{aligned} S &= \mathbb{V}((a-b^2)(a+b)(a-b)) \setminus \mathbb{V}(a(a-b)) \\ &= \big(\mathbb{V}(a-b^2) \setminus \mathbb{V}(a-b^2, a(a-b)\big) \cup (\mathbb{V}(a+b)) \setminus \mathbb{V}(a(a-b)), (a+b)) \\ &= \big(\mathbb{V}(a-b^2) \setminus (\mathbb{V}(a,b) \cup \mathbb{V}(a-1,b-1))\big) \cup (\mathbb{V}(a+b) \setminus \mathbb{V}(a,b)) \,. \end{aligned}$$

Resulta obvio que la última representación (la P-representación), además de canónica, es más detallada que la inicial.

Por razones de la simplicidad de interpretación, pero también por razones de cálculo, el algoritmo GröbnerCover obtiene los segmentos en forma de P-representación. Así, no solamente los lpp-segmentos que obtiene son canónicos sino que también lo es su representación. Además las variedades que aparecen son irreducibles y vienen dadas por los correspondientes ideales primos.

3.2. Representación de las bases de Gröbner

Sea $B = \{g_1, \ldots, g_s\} \subset \mathcal{O}(S)[\overline{x}]$ la base del ideal I asociada al segmento localmente cerrado S de la cobertura de Gröbner. Desde el punto de vista teórico, los polinomios g_i son polinomios mónicos de $\mathcal{O}(S)[\overline{x}]$; es decir, son polinomios de la forma $p = \sum_\alpha c_\alpha x^\alpha$, donde los coeficientes c_α son funciones regulares $c_\alpha : S \to \overline{K}$. En muchos casos prácticos g_i puede ser representado simplemente por un polinomio $P \in K[\overline{\lambda}][\overline{x}]$, que dividido por su coeficiente principal (a fin de que sea mónico), especializa para todo $\overline{a} \in S$ al correspondiente polinomio de la base de Gröbner reducida de $I_{\overline{a}}$. Sin embargo, en ocasiones es necesaria una representación mas compleja.

Definición 14. Un conjunto $\{P_1, \ldots, P_n\} \subset K[\overline{\lambda}][\overline{x}]$ representa completamente al polinomio mónico $g \in \mathcal{O}(S)[\overline{x}]$, si

- para todo i se tiene $\mathrm{lpp}(P_i) = \mathrm{lpp}(g)$;
- para cada $\overline{a} \in S$ existe un abierto $U = S \setminus \mathbb{V}(\mathfrak{c})$, siendo $\mathbb{V}(\mathfrak{c}) < S$, con $\overline{a} \in U$, y existe un i tal que, para todo $\overline{b} \in U$,

$$g(\overline{b}, \overline{x}) = \frac{P_i(\overline{b}, \overline{x})}{\mathrm{lc}(P_i)(\overline{b})};$$

- para todo $\overline{a} \in S$ y para todo i, j se cumple

$$\mathrm{lc}(P_j)(\overline{a}) P_i(\overline{a}, \overline{x}) = \mathrm{lc}(P_i)(\overline{a}) P_j(\overline{a}, \overline{x}),$$

  esto es, cualquier P_i que no se anule en $\overline{a}$ define correctamente a g en $\overline{a}$.

Si bien la representación $\{P_1, \ldots, P_n\}$ de la función mónica $g \in \mathcal{O}(S)[\overline{x}]$ no es única, de la unicidad de las bases de Gröbner reducidas resulta inmediatamente que las funciones mónicas $g_i \in \mathcal{O}(S)[\overline{x}]$ de B asociadas a S son únicas (su valor está unívocamente determinado para cada $\overline{a} \in S$). A dicho conjunto de funciones le llamamos *base de Gröbner reducida de I sobre S*.

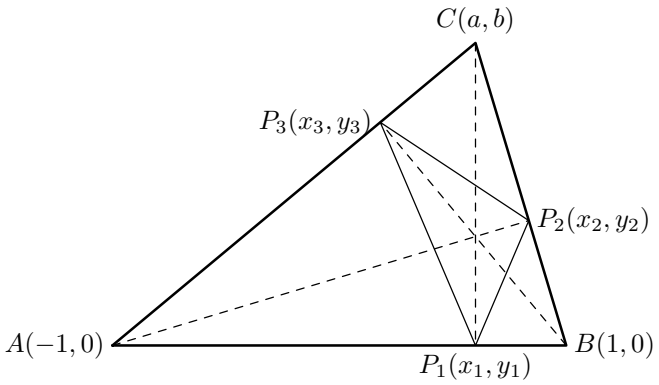

Figura 2: Triángulo órtico.

4. Aplicaciones

Entre las múltiples aplicaciones posibles del algoritmo GröbnerCover seleccionamos un ejemplo de deducción automática de teoremas geométricos [19] por su belleza.

Consideremos el problema siguiente: ¿Cuál es el lugar geométrico de los puntos (a,b) del plano para los cuales el triángulo ABC de la figura 2 tiene un triángulo órtico asociado (es decir, el triángulo que tiene como vértices P_1, P_2, P_3 los pies de las alturas) que sea isósceles, con los lados $\overline{P_1P_2} = \overline{P_1P_3}$?

Obviamente $P_1 = (a,0)$. Agrupando las ecuaciones que definen los puntos P_2 y P_3 y la condición para que el triángulo órtico sea isósceles, obtenemos el sistema de ecuaciones

$$\begin{cases} (a-1)y_2 - b(x_2-1) = 0,\ (a-1)(x_2+1) + by_2 = 0, \\ (a+1)y_3 - b(x_3+1) = 0,\ (a+1)(x_3-1) + by_3 = 0, \\ (x_3-a)^2 + y_3^2 - (x_2-a)^2 - y_2^2 = 0, \end{cases}$$

que se corresponde con el ideal

$$\begin{aligned} I = \langle &(a-1)y_2 - b(x_2-1),\ (a-1)(x_2+1) + by_2, \\ &(a+1)y_3 - b(x_3+1),\ (a+1)(x_3-1) + by_3, \\ &(x_3-a)^2 + y_3^2 - (x_2-a)^2 - y_2^2 \rangle. \end{aligned}$$

Aplicando el algoritmo GröbnerCover, obtenemos el siguiente conciso y preciso resultado:

1. Segmento con lpp = [1]	Segmento genérico
Base: $\{1\}$.	
P-representación del segmento: $\{(\langle 0\rangle, (\langle a^2-b^2-1\rangle, \langle a^2+b^2-1\rangle, \langle a\rangle))\}$.	

2. Segmento con lpp $= [y_3, y_2, x_3, x_2]$
Base:

$$\{(a^2+b^2+2a+1)y_3+(-2ab-2b),\\ (a^2+b^2-2a+1)y_2+(2ab-2b),\\ (a^2+b^2+2a+1)x_3+(-a^2+b^2-2a-1),\\ (a^2+b^2-2a+1)x_2+(a^2-b^2-2a+1)\}.$$

P-representación del segmento:

$$\{(\langle a^2+b^2-1\rangle,(\langle b,a-1\rangle,\langle b,a+1\rangle));\\ (\langle a^2-b^2-1\rangle,(\langle b,a-1\rangle,\langle b,a+1\rangle,\langle b^2+1,a\rangle));\\ (\langle a\rangle,(\langle b^2+1,a\rangle))\}.$$

3. Segmento con lpp $= [y_3, x_3, x_2^2]$
Base: $\{y_3,\ x_3-1,\ x_2^2+y_2^2-2x_2+1\}$.
P-representación del segmento: $\{(\langle b,a-1\rangle,(\langle 1\rangle))\}$.

4. Segmento con lpp $= [1]$
Base: $\{1\}$.
P-representación del segmento: $\{(\langle b^2+1,a\rangle,(\langle 1\rangle))\}$.

5. Segmento con lpp $= [y_2, x_2, x_3^2]$
Base: $\{y_2, x_2+1, x_3^2+y_3^2+2x_3+1\}$.
P-representación del segmento: $\{(\langle b,a+1\rangle,(\langle 1\rangle)\}$.

Como vemos sólo hay 5 lpp-segmentos, y únicamente hay un lpp repetido que corresponde a los segmentos 1 y 4.

Las bases de los segmentos 1 y 4 son $\{1\}$, lo que nos muestra que no existe ninguna solución en ambos casos. Sin embargo ambos casos son distintos, ya que el primero es el caso genérico y el segundo corresponde a un par de puntos complejos no interesantes para la discusión en el caso real.

El segmento importante para nuestro problema es el segmento 2, con lpp $= [y_3, y_2, x_3, x_2]$ (es decir, el conjunto completo de variables), pues nos indica que en ese segmento existe una solución única para los puntos P_2 y P_3 (que vienen determinados por la base). Dicho segmento viene dado por tres ramas (véase la figura 3)

$$\begin{aligned} R_1\colon &\quad a=0,\\ R_2\colon &\quad a^2+b^2-1=0,\\ R_3\colon &\quad a^2-b^2-1=0, \end{aligned}$$

a las que hay que restar los puntos $A=(-1,0)$ y $B=(1,0)$ correspondientes a triángulos degenerados, y dos puntos complejos $M=(i,0)$, $N=(-i,0)$. La rama R_1 representa triángulos ABC isósceles y es, por lo tanto, una solución obvia. La rama R_2 (circunferencia) representa triángulos rectángulos para los cuales el triángulo órtico es isósceles con base de longitud 0 y es también una solución obvia. Pero la rama R_3 determina los puntos de una hipérbola para la cual el triángulo dado ABC no es ni isósceles ni rectángulo, pero tiene un triángulo órtico que sí es isósceles

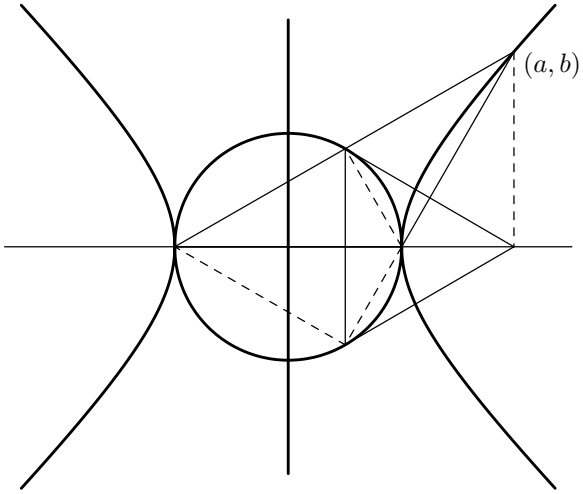

Figura 3: Las tres componentes del lugar geométrico de triángulos órticos isósceles.

y esa no es una solución obvia. Los segmentos 3 y 5 corresponden respectivamente a triángulos degenerados donde $C = A = (1, 0)$ o $C = B = (-1, 0)$. Finalmente, el segmento 4 representa los dos puntos imaginarios $C = M(0, i)$ y $C = N(0, -i)$ para los cuales no existe tampoco solución, como ocurre en los puntos del segmento 1, pero estos puntos no están incluidos en un único segmento en la cobertura canónica de Gröbner. La razón fundamental para ello es que provienen de segmentos del ideal homogeneizado con lpp diferentes. Obsérvese que la unión de los segmentos 1 y 4 no es localmente cerrada, lo que es otra buena razón para que el algoritmo no los reúna en uno solo.

Como conclusión, podemos afirmar que el *Gröbner cover* que se ha obtenido en este ejemplo ha proporcionado de una manera muy compacta un conocimiento geométrico nuevo, distinguiendo casos degenerados de no degenerados, y todos ellos de fácil interpretación. El cálculo efectuado en un sencillo ordenador portátil no ha requerido más que un segundo y ha aportado conocimientos no triviales. Hemos resulto nuevos y más interesantes problemas de descubrimiento geométrico de teoremas, como la generalización del teorema de Steiner-Lehmus [20], cuya versión completa difundiremos más adelante. Consideramos que el algoritmo puede ser muy útil en muchas otras aplicaciones.

Referencias

[1] T. Becker y V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Springer, New York, 1993.

[2] M. Coste, Classifying serial manipulators: Computer Algebra and geometric insight, *Actas* del EACA-2004 (2004), 323–323.

[3] D. Cox, J. Little y D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, New-York, 1992. 3rd edition, 2007.

[4] A. Dolzmann, A. Seidl y T. Sturm, Redlog software in Reduce, `http://redlog.dolzmann.de/`

[5] D. Duval, Évaluation dynamique et clôture algébrique en Axiom, *Journal of Pure and Applied Algebra* **99** (1995), 267–295.

[6] I. Z. Emiris, Computer algebra methods for studying and computing molecular conformations, *Algorithmica* **25** (1999), 372–402.

[7] X.S. Gao y D.K. Wang, Zero decomposition theorems for counting the number of solutions for parametric equation systems, In *Proceedings* of the 6th Asian Symposium on Computer Mathematics, Ed. Ziming Li & William Sit, *Lecture notes series on computing* **10** (2003), 129–144. World Scientific.

[8] P. Gianni, Properties of Gröbner bases under specializations, In: EUROCAL'87. Ed. J.H. Davenport, Springer *Lecture Notes Series on Computing* **378** (1987), 293–297.

[9] P.Gianni, B. Trager y G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, *Journal of Symbolic Computation* **6**:2-3 (1988), 149–167.

[10] M.J. González-López y T. Recio, The ROMIN inverse geometric model and the dynamic evaluation method, In: *Computer Algebra in Industry,* Ed. A.M. Cohen, Wiley & Sons (1993), 117–141.

[11] D. Kapur, An approach for solving systems of parametric polynomial equations, In: *Principles and Practices of Constraints Programming,* Eds. Saraswat and Van Hentenryck, MIT Press (1995), 217–244.

[12] D. Kapur, Y. Sun y D.K. Wang, A new algorithm for computing comprehensive Gröbner systems, *Proceedings* of ISSAC'2010, ACM Press (2010), 29–36.

[13] R. Losada, T. Recio y J.L. Valcarce, On the automatic discovery of Steiner-Lehmus generalizations, *Proceedings* of ADG 2010 (J. Richter-Gebert, P. Schreck, editors), München (2010), 171–174.

[14] M. Manubens, Tesis Doctoral «Parametric Polynomial System Discussion: Canonical Comprehensive Gröbner Systems», *Universitat Politècnica de Catalunya*, 2008.

[15] M. Manubens y A. Montes, Improving DISPGB algorithm using the discriminant ideal, *Journal of Symbolic Computation* **41** (2006), 1245–1263.

[16] M. Manubens y A. Montes, Minimal canonical comprehensive Gröbner systems, *Journal of Symbolic Computation* **44**:5 (2009), 463–478.

[17] A. Montes, Algebraic solution of the load-flow problem for a 4-nodes electrical network, *Mathematics and Computer in Simulations* **45** (1998), 163–174.

[18] A. Montes, New algorithm for discussing Gröbner bases with parameters, *Journal of Symbolic Computation* **33**:1-2 (2002), 183–208.

[19] A. Montes y T. Recio, Automatic discovery of geometry theorems using minimal canonical comprehensive Gröbner systems, *Proceedings* of ADG 2006, *Lecture Notes on Artificial Intelligence* **4869** (2007), 113–138. Springer.

[20] A. Montes y T. Recio, Generalizing the Steiner-Lehmus theorem using the Gröbner cover, *Proceedings* of the XIV Spanish Meeting on Computational Geometry. Alcalá, 27–30 June, 2011.

[21] A. Montes y M. Wibmer, Gröbner bases for polynomial systems with parameters, *Journal of Symbolic Computation* **45** (2010), 1391–1425.

[22] `http://www-ma2.upc.edu/~montes/`.

[23] K. Nabeshima, A computation method for ACGB-V, *Proceedings* of A3L 2005 (Conference in Honour of the 60th Birthday of V. Weispfenning), Eds. A. Dolzmann, A. Seidl, T. Sturm, 171–180. BOD Norderstedt.

[24] M. Rychlik, Complexity and applications of parametric algorithms of computational algebraic geometry, In: *Dynamics of Algorithms*, Eds. R. de la Llave, L. Petzold, J. Lorenz, IMA Volumes in Mathematics and its Applications, Springer-Verlag **118** (2000), 1–29.

[25] Y. Sato y A. Suzuki, An alternative approach to comprehensive Gröbner bases, *Journal of Symbolic Computation* **36**:3-4 (2003), 649–667.

[26] A. Suzuki y Y. Sato, A simple algorithm to compute comprehensive Gröbner bases, *Proceedings* of ISSAC 2006, ACM, 326–331.

[27] A. Suzuki y Y. Sato, Implementation of CGS and CGB on Risa/Asir and other computer algebra systems using Suzuki-Sato algorithm, *ACM Communications in Computer Algebra* **41**:3 (2007), `http://kurt.cla.kobe-u.ac.jp/~sakira/CGBusingGB/`.

[28] V. Weispfenning, Comprehensive Gröbner bases, *Journal of Symbolic Computation* **14**:1-1 (1992), 1–29.

[29] V. Weispfenning, Canonical comprehensive Gröbner bases, *Journal of Symbolic Computation* **36**:3-4 (2003), 669–683.

[30] M. Wibmer, Gröbner bases for families of affine or projective schemes, *Journal of Symbolic Computation* **42**:8 (2007), 803–834.

Antonio Montes, Dept. de Matemàtica Aplicada II, Universitat Politècnica de Catalunya
Correo electrónico: `antonio.montes@upc.edu`
Página web: `http://www-ma2.upc.edu/~montes/`