Universidad de Cantabria

Facultad
de
Ciencias

BASES DE GRÖBNER

(Gröbner Bases)

Trabajo de Fin de Grado
para acceder al
GRADO EN MATEMÁTICAS

Autor: David Ignacio Alcántara García

Director: Luis Felipe Tabera Alonso

Julio - 2023

Abstract

Las bases de Gröbner son una herramienta esencial en la geometría algebraica computacional moderna, pues permiten trabajar algorítmicamente con ideales de polinomios en varias variables. Fueron introducidas en paralelo por Hironaka (1964) y Bruno Buchberger (1965), quien les dió el nombre de su tutor Wolfgang Gröbner.

En este trabajo, motivamos la introducción de las bases de Gröbner, damos su definición formal, y discutimos algunas aplicaciones a la teoría de la eliminación, la implicitación de variedades algebraicas, la resolución de un problema mecánico, y la deducción automática de teoremas geométricos, que requieren introducir la nociones de bases comprensivas de Gröbner y el recubrimiento de Gröbner. Finalmente, discutimos algunos aspectos sobre la complejidad computacional de los problemas que involucran bases de Gröbner, y las limitaciones que conllevan en la práctica.

Gröbner bases are an essential tool in modern computational algebraic geometry, as they allow to operate algorithmically with ideals of polynomials in several variables. They were introduced in parallel by Hironaka (1964) and Bruno Buchberger (1965), who named them after his tutor Wolfgang Gröbner.

In this document, we motivate the introduction of Gröbner bases, give their formal definition, and we discuss some applications to elimination theory, the implicization of algebraic varieties, the resolution of a mechanical problem, and the automatic deduction of geometric theorems (ADGT), which require introducing the notions of comprehensive Gröbner bases and the Gröbner cover. Finally, we discuss some aspects about the computational complexity of problems involving Gröbner bases, and the limitations these entail in practice.

Keywords: Gröbner basis, Gröbner cover, Elimination Theory, Automatic Deduction of Geometric Theorems (ADGT).

Índice

1 Introducción **1**
- 1.1 Definiciones Preliminares . . . 1
- 1.2 Motivación . . . 3
- 1.3 División con resto . . . 4

2 Bases de Gröbner **7**
- 2.1 Órdenes monomiales . . . 7
- 2.2 Algoritmo de división multivariada con resto . . . 10
- 2.3 Ideales monomiales . . . 11
- 2.4 Bases de Gröbner y sizigias . . . 13
- 2.5 El algoritmo de Buchberger . . . 17
- 2.6 Operaciones elementales con ideales . . . 19
- 2.7 Especialización . . . 20
- 2.8 Bases y Sistemas Comprensibles de Gröbner . . . 21

3 Aplicaciones de las Bases de Gröbner **25**
- 3.1 Teoría de la Eliminación . . . 25
  - 3.1.1 Paso de Eliminación . . . 27
  - 3.1.2 Paso de Extensión . . . 28
- 3.2 Implicitación . . . 29
- 3.3 Problema Cinemático Inverso . . . 31
- 3.4 Deducción Automática de Teoremas Geométricos . . . 34
  - 3.4.1 Deducción Automática del Teorema del Arco Capaz . . . 34
- 3.5 Descubrimiento de Hipótesis Adicionales . . . 40
  - 3.5.1 Búsqueda de Hipótesis para un Resultado Geométrico . . . 40

4 Complejidad Computacional **45**
- 4.1 Mejoras del algoritmo de Buchberger . . . 49

Capítulo 1

Introducción

Las bases de Gröbner se han convertido en una herramienta esencial para la geometría algebraica computacional, pues permiten trabajar algorítmicamente con ideales de polinomios en varias variables [12].

Fueron introducidas por primera vez por Hironaka (1964) en su trabajo sobre la resolución de singularidades en $\mathbb{C}$, con el nombre de "*bases estándar*", si bien en términos de series de potencias en vez de polinomios [1]. De forma independiente, fueron definidas por Bruno Buchberger (1965) en su tesis doctoral, con el nombre de bases de Gröbner en honor de su tutor Wolfgang Gröbner, junto con un algoritmo para determinarlas.

Estas bases han encontrado su camino a multitud de aplicaciones, tanto prácticas como teóricas, si bien sus aplicaciones prácticas están severamente limitadas por la complejidad computacional que conlleva, tanto determinarlas como trabajar con ellas.

En este trabajo, vamos a introducir las bases de Gröbner siguiendo los pasos de [12] y [2], así como las bases de Gröbner comprensivas, siguiendo su definición original [10]. Antes de introducir estos conceptos, daremos una breve introducción a la Geometría Algebraica. Finalmente, veremos algunas aplicaciones de las bases de Gröbner tomadas de [12], [2] y [5].

Todos los ejemplos y figuras del trabajo son de elaboración propia. Las figuras han sido generadas usando GeoGebra, salvo las de la sección 3.3, generadas con Sage.

Al comenzar a realizar este trabajo no tenía mayores conocimientos sobre las bases de Gröbner que su definición. El trabajo está planteado de tal forma que cualquier graduado en matemáticas pueda leerlo sin dificultad. Los conceptos clave se introducen con definiciones y ejemplos, y se recuerdan algunos de los vistos en las asignaturas optativas de cuarto de grado *Ampliación de Álgebra* y *Geometría Proyectiva y Algebraica*.

1.1 Definiciones Preliminares

La Geometría Algebraica es una rama de las matemáticas que ha despertado un gran interés desde su concepción por la elegancia con la que une los mundos del Álgebra Abstracta y la Geometría.

Las aplicaciones de las bases de Gröbner que veremos en el Capítulo 3 están relacionadas con esta área de las matemáticas, por lo que en primer lugar introducimos brevemente algunas nociones y resultados fundamentales con el objetivo de fijar notación.

Definición 1.1.1. Escribiremos $I = \langle f_1, ..., f_s \rangle$ para denotar el **ideal generado por los polinomios** $f_1, ..., f_s$, es decir,

$$\langle f_1, ..., f_s \rangle \coloneqq \{g_1 f_1 + \cdots + g_s f_s : g_1, ..., g_s \in \mathbb{K}\}.$$

Definición 1.1.2. Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado, e $I \subseteq \mathbb{K}[\mathbf{x}] \coloneqq \mathbb{K}[x_1, ..., x_n]$ un ideal, definimos el **conjunto algebraico de** I como el conjunto de ceros del ideal, es decir,

$$\mathcal{V}(I) = \{u \in \mathbb{K}^n : \forall f \in I, f(u) = 0\}.$$

En general, decimos que un subconjunto $S \subseteq \mathbb{K}^n$ es un **conjunto algebraico** si existe un ideal I tal que $S = \mathcal{V}(I)$. A los conjunto algebraicos irreducibles, en el sentido de que no pueden escribirse como unión de subconjuntos algebraicos propios se los denomina **variedades algebraicas**.

Análogamente, dado un subconjunto $S \subseteq \mathbb{K}^n$, definimos el **ideal de** S como el conjunto de polinomios que se anulan en V, es decir,

$$\mathcal{I}(S) = \{f \in \mathbb{K}[x_1, ..., x_n] : \forall u \in S, f(u) = 0\}.$$

Si bien estos dos operadores no son inversos el uno del otro, lo son para ideales y variedades concretos, los definidos a partir de estas correspondencias.

Proposición 1.1.1. *Sean I un ideal y $S \subseteq \mathbb{K}^n$ un subconjunto, entonces $\mathcal{I}(\mathcal{V}(\mathcal{I}(S))) = \mathcal{I}(S)$ y $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) = \mathcal{V}(I)$.*

En particular, los ideales que provienen de variedades de esta forma son los ideales radicales.

Definición 1.1.3. Sea $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideal, diremos que es **radical** si para todo $f \in \mathbb{K}[\mathbf{x}]$ tal que existe un $n \in \mathbb{N}$ con $f^n \in I$, se tiene que $f \in I$.

Si I es un ideal, el **radical de** I es el conjunto $\sqrt{I} \coloneqq \{f \in \mathbb{K}[\mathbf{x}] : \exists n \in \mathbb{N}, f^n \in I\}$, que se sabe que es un ideal radical.

Proposición 1.1.2. *Sea $S \subseteq \mathbb{K}^n$ un subconjunto, entonces $\mathcal{I}(S)$ es un ideal radical.*

Demostración. Es suficiente probar la contención $\sqrt{\mathcal{I}(S)} \subseteq \mathcal{I}(S)$. Por definición, $\sqrt{\mathcal{I}(S)}$ es $\{f \in \mathbb{K}[\mathbf{x}] : \exists n \in \mathbb{N}, \forall u \in S f^n(u) = 0\}$, pero, si $f^n(u) = 0$ con $u \in S$, dado que $\mathbb{K}$ es un cuerpo, también $f(u) = 0$, por lo que, si $f \in \sqrt{\mathcal{I}(S)}$, también $f \in \mathcal{I}(S)$. □

Estas nociones también permiten definir una topología sobre $\mathbb{K}^n$, menos fina que la topología usual si $\mathbb{K}$ es $\mathbb{C}$.

Definición 1.1.4. La **topología de Zariski** sobre $\mathbb{K}^n$ es la topología cuyos cerrados son los conjuntos algebraicos.

Otras propiedades fundamentales de esta forma de pasar de ideales a variedades y viceversa son las siguientes, para cuyas demostraciones nos remitimos al capítulo §4.3 de [2].

Proposición 1.1.3. *Sean $J_1, J_2 \subseteq \mathbb{K}[\mathbf{x}]$ ideales y $S_1, S_2 \subseteq \mathbb{K}^n$ variedades, entonces*

i) $\mathcal{V}(0) = \mathbb{K}^n$

ii) $\forall c \in \mathbb{K} \setminus \{0\} : \mathcal{V}(c) = \emptyset$

iii) $\mathcal{V}(J_1 + J_2) = \mathcal{V}(J_1) \cap \mathcal{V}(J_2)$

iv) $\mathcal{V}(J_1 \cdot J_2) = \mathcal{V}(J_1 \cap J_2) = \mathcal{V}(J_1) \cup \mathcal{V}(J_2)$

Estas propiedades justifican la notación $\mathcal{V}(f_1, ..., f_s) := \mathcal{V}(\langle f_1, ..., f_s \rangle) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_s)$.

Un resultado clave en esta relación entre ideales y conjuntos algebraicos es el Teorema de los Ceros de Hilbert, uno de los resultados más importantes de finales del siglo XIX, que permite establecer una correspondencia entre estos conceptos.

Teorema 1.1.4 (El Nullstellensatz Débil)**.** *Si $\mathbb{K}$ es un cuerpo algebraicamente cerrado e $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideal tal que $\mathcal{V}(I) = \emptyset$, entonces I es el ideal total, $\mathbb{K}[\mathbf{x}]$, es decir, $1 \in I$ [2, §4.1].*

Esta versión del teorema permite probar la versión más conocida.

Teorema 1.1.5 (El Nullstellensatz de Hilbert)**.** *Si $\mathbb{K}$ es un cuerpo algebraicamente cerrado, e $I = \langle f_1, ..., f_s \rangle \subseteq \mathbb{K}[\mathbf{x}] := \mathbb{K}[x_1, ..., x_n]$, es un ideal finitamente generado (f.g.), entonces*

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

La contención de derecha a izquierda es inmediata. Por otro lado, una de las pruebas más elegantes de este este teorema a partir de su versión débil se debe a Rabinowitsch [9], utilizando el *truco* que lleva su nombre, que consiste en introducir una nueva variable, y.

Demostración. Si $f \in \mathcal{I}(\mathcal{V}(I))$, entonces $(1 - yf)$ y $f_1, ..., f_s$ no tienen ceros en común, por lo que, en virtud del Nullstellensatz débil, $1 \in \langle 1 - yf, f_1, ..., f_s \rangle$, y por tanto, existen $a_0, ..., a_s \in \mathbb{K}[\mathbf{x}][y]$ tales que $1 = a_0(1 - yf) + a_1 f_1 + \cdots + a_s f_s$.

Sustituyendo y por $1/f$ y eliminando los denominadores, se deduce la existencia de una potencia $m \in \mathbb{N}$, tal que $f^m = b_1 f_1 + \cdots + b_s f_s$ en $\mathbb{K}[\mathbf{x}]$, con $b_i(\mathbf{x}) = a_i(\mathbf{x}, 1/f) f^m$, por lo que $f \in \sqrt{I}$. □

Como consecuencia, existe una correspondencia biyectiva entre los conjuntos algebraicos de $\mathbb{K}^n$ y los ideales radicales de $\mathbb{K}[x_1, ..., x_n]$. Un ideal es radical si y solo si es el ideal del conjunto algebraico que define.

1.2 Motivación

En las siguientes secciones vamos a exponer una motivación para la definición de las bases de Gröbner que se verá en el próximo capítulo. Tanto esta motivación como la definición que daremos de las bases de Gröbner en el Capítulo 2 siguen las exposiciones dadas en el Capítulo 21 de *Modern Computer Algebra* [12] y el Capítulo 2 de *Ideals, Varieties and Algorithms - An introduction to computational algebraic geometry and commutative algebra* [2].

En este trabajo limitaremos nuestro estudio de las bases de Gröbner a anillos de polinomios, por lo que, en general, trabajaremos en el anillo $R = \mathbb{K}[\mathbf{x}]$, donde $\mathbb{K}$ es un cuerpo.

Algunas preguntas importantes que nos podemos hacer sobre un ideal de R son:

- Dado un polinomio $f \in \mathbb{K}[\mathbf{x}]$, ¿pertenece al ideal?
- ¿Es un ideal propio?

En general, no pediremos que el cuerpo $\mathbb{K}$ sea algebraicamente cerrado, aunque en ocasiones, particularmente cuando nos interesa el conjunto algebraico de un ideal, haremos distinciones.

En anillos de polinomios univariados, estas preguntas son de fácil respuesta, pues al ser $\mathbb{K}[x]$ dominio Euclídeo, y, en particular, dominio de ideales principales, se tiene que

$$\langle f_1, ..., f_s \rangle = \langle \gcd(f_1, ..., f_s) \rangle \tag{1.1}$$

lo que nos permite asumir que $s = 1$. Además, la división Euclídea nos permite responder a la pregunta de pertenencia al ideal, pues sean $f, g \in \mathbb{K}[x]$, podemos encontrar $q, r \in \mathbb{K}[x]$ tales que $f = qg + r$ y $\deg(r) < \deg(g)$, de forma que

$$f \in \langle g \rangle \iff r = 0,$$

y el ideal es propio si y solo si $g \neq 1$. Si $\mathbb{K}$ es algebraicamente cerrado, y g factoriza como $(x - u_1) \cdots (x - u_d)$, entonces $\mathcal{V}(g) = \{u_1, ..., u_d\}$.

Sin embargo, en el caso de anillos multivariados, la Igualdad 1.1 deja de satisfacerse. Basta considerar el ideal $\langle x, y \rangle \subseteq \mathbb{K}[x, y]$, que no es trivial ($1 \notin \langle x, y \rangle$) pero $\gcd(x, y) = 1$. Una de las principales motivaciones de las bases de Gröbner es recuperar de algún modo estas propiedades, como la división con resto para determinar la pertenencia a un ideal.

1.3 División con resto

Uno de los problemas que aparecen al extender la idea de división a múltiples variables es que ya no es suficiente con dividir por un único polinomio.

En el caso univariado, la división Euclídea responde a la pregunta de cómo encontrar $q \in \mathbb{K}[x]$ tal que $f = qg$, i.e., $f \in \langle g \rangle$. En $\mathbb{K}[\mathbf{x}]$ nuestro objetivo es encontrar $q_1, ..., q_s$ tales que

$$f = \sum_{i=1}^{s} q_i g_i,$$

i.e., $f \in \langle g_1, ..., g_s \rangle$. Por tanto, la forma de generalizar la división que nos interesa necesita ser capaz de dividir por múltiples polinomios, obteniendo múltiples cocientes.

La forma natural de definir esta división por múltiples polinomios consiste en aplicar la división Euclídea por cada polinomio, mientras sea posible.

Ejemplo 1.3.1. *Consideramos uno de los casos más sencillos, cuando $I = \langle x, y \rangle \subseteq \mathbb{K}[x, y]$. En el siguiente diagrama se muestra como podríamos extender la división Euclídea cuando se tienen dos divisores, x e y. En el diagrama aparece una columna por cada divisor, y, a diferencia de la división Euclídea habitual, escribimos cada término de los cocientes en la fila en la que se ha obtenido por claridad.*

$x^2y + xy^2 + y + 1$	x	y
$-\ x^2y$	xy	
$xy^2 + y + 1$		
$-\ xy^2$	y^2	
$y + 1$		
$-\ y$		1
1		

El resultado de esta división es $x^2y + xy^2 + y + 1 = (xy + y^2)x + (1)y + 1$.

Al resto que queda en cada paso en la columna del dividendo lo denominaremos ***resto parcial****, salvo al último, que denominamos resto.*

Esta idea parece funcionar. Un polinomio solo tendrá resto 0 *por* x, y *si su término independiente es* 0*, que es equivalente a la condición de pertenecer a* $\langle x, y\rangle$.

No obstante, aparece un problema que no existía en el caso univariado, el resultado no es único. En los primeros dos pasos podríamos haber dividido por y *en vez de* x*, obteniendo*

$$x^2y + xy^2 + y + 1 = (x^2 + x + 1)y + 1 = (xy + y^2)x + (1)y + 1.$$

Si bien la no unicidad de los cocientes es inevitable, un problema más preocupante es la no unicidad del resto, pues es lo que nos interesa para determinar la pertenencia al ideal.

Ejemplo 1.3.2. *Por ejemplo, si consideramos* $f = xy^2 - x$, $f_1 = xy + 1$ *y* $f_2 = y^2 - 1$,

$xy^2 - x$	$xy + 1$	$y^2 - 1$
$-xy^2 \quad -y$	y	
$-x - y$		

$xy^2 - x$	$xy + 1$	$y^2 - 1$
$-xy^2 + x$		x
0		

Dividiendo primero por f_1 *obtenemos como resto* $(-x - y)$*, pero dividiendo primero por* f_2 *se obtiene resto* 0*, luego concluimos que* $f \in \langle f_1, f_2\rangle$*. Si solo hubiéramos dividido primero por* f_1 *no habríamos podido llegar a la misma conclusión.*

En el próximo capítulo veremos como podemos resolver el problema de la no unicidad del resto estableciendo un orden entre los divisores, y como, para ciertos conjuntos, las bases de Gröbner, esta forma de dividir polinomios nos permite responder a la pregunta de si un polinomio pertenece a un ideal, al igual que la división Euclídea nos permitía en $\mathbb{K}[x]$.

Capítulo 2

Bases de Gröbner

2.1 Órdenes monomiales

Para poder definir apropiadamente un orden en el proceso de división anterior, necesitamos definir algunas ideas. Sea $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$, definimos su monomio asociado como

$$x^\alpha = x_1^{\alpha_1}, ..., x_n^{\alpha_n} \in \mathbb{K}[\mathbf{x}].$$

Esta asociación establece una correspondencia entre el conjunto de monomios de $\mathbb{K}[\mathbf{x}]$ y $\mathbb{N}^n$, por lo que, para ordenar monomios nos basta con tener una forma de ordenar $\mathbb{N}^n$. En primer lugar, tenemos que definir lo que es un orden.

Un **orden** $\leq$ sobre un conjunto S es una relación reflexiva, transitiva y antisimétrica, i.e., para todos $\alpha, \beta, \gamma \in S$:

$$\alpha \leq \alpha, \qquad \alpha \leq \beta \leq \gamma \Longrightarrow \alpha \leq \gamma, \qquad \alpha \neq \beta \wedge \alpha \leq \beta \Longrightarrow \beta \not\geq \alpha.$$

Diremos que el orden es **total** si relaciona a todos los elementos, i.e., para todos $\alpha, \beta \in S$ se tiene $\alpha \leq \beta$ o $\beta \leq \alpha$, y en caso contrario diremos que es parcial.

Otra propiedad importante de un orden es que nos proporcione un criterio para elegir elementos. Si para todo subconjunto no vacío de S, este subconjunto tiene mínimo, decimos que el orden es un **buen orden**.

Ejemplo 2.1.1. *Un ejemplo de orden que no es un buen orden es el orden habitual sobre los números racionales,* $\leq$*, ya que el subconjunto* $\{1/n : n \in \mathbb{N}_+\} \subseteq \mathbb{Q}$ *no tiene elemento mínimo para* $\leq$*, solo ínfimo, el* 0*.*

Respecto a nuestro problema, diremos que una relación $\preccurlyeq$ en $\mathbb{N}^n$ es un **orden monomial** de $\mathbb{K}[\mathbf{x}]$ si

i) Es un buen orden (y, por tanto, orden total)

ii) Es invariante por traslación, i.e., para todos $\alpha, \beta, \gamma \in \mathbb{N}^n$ con $\alpha \preccurlyeq \beta$ se tiene $\alpha + \gamma \preccurlyeq \beta + \gamma$.

El buen orden más fácil de definir en $\mathbb{N}^n$ es el lexicográfico, que compara en orden las coordenadas una a una:

$$\alpha \preceq_{lex} \beta \Longleftrightarrow \alpha = \beta \vee \text{la primera coordenada no nula de } \alpha - \beta \text{ es negativa.}$$

Podemos entender el orden lexicográfico como la composición de los órdenes naturales en cada coordenada, eligiendo el primero que desambigüe los elementos. En general, es posible definir un orden lexicográfico por cada permutación de S_n, reordenando las coordenadas.

Cuando queramos denotar el orden lexicográfico dado por una permutación concreta de índices o variables, $x_{i_1}, ..., x_{i_n}$, escribiremos $lex(x_{i_1}, ..., x_{i_n})$.

Esta forma de combinar distintos órdenes es una herramienta muy utilizada para definir nuevos órdenes, ya que se corresponde con la idea natural de ordenar siguiendo una lista de criterios para desambiguar la comparación. Por este motivo, es de utilidad darle un nombre, que también es usado en [5, p. 42].

Definición 2.1.1. Sean $\leq_1$ y $\leq_2$ dos órdenes parciales sobre algún conjunto S, denotamos por $\leq_1 \cdot \leq_2$ al *orden producto* de $\leq_1$ y $\leq_2$, dado por

$$\alpha \ (\leq_1 \cdot \leq_2) \ \beta \iff (\alpha \leq_1 \beta) \vee (\beta \not\leq_1 \alpha \wedge \alpha \leq_2 \beta)$$

Lema 2.1.1. *El producto de órdenes preserva la propiedad de ser orden total, i.e., si $\leq_1$ o $\leq_2$ son totales, $\leq_1 \cdot \leq_2$ también lo es.*

Demostración. Si $\leq_1$ es total, el producto coincide con $\leq_1$, pues $\alpha \not\leq_1 \beta$ implica $\beta \leq_1 \alpha$. Por otro lado, si $\leq_2$ es total, sean $\alpha, \beta \in S$, se dan dos casos. Si bien $\alpha \leq_1 \beta$, o bien $\beta \leq_1 \alpha$, se tiene que $\alpha \ (\leq_1 \cdot \leq_2) \ \beta$ o respectivamente $\beta \ (\leq_1 \cdot \leq_2) \ \alpha$. En caso contrario, el orden se reduce a $\leq_2$, que es total, por lo que el producto también lo es. □

Como es habitual, si $\leq$ (resp. $\preccurlyeq$) es una relación de orden, denotamos por $<$ (resp. $\prec$) a su relación de orden estricta, dada por $\alpha < \beta \Leftrightarrow \alpha \leq \beta \wedge \alpha \neq \beta$. Existe una correspondencia directa entre relaciones de orden y relaciones de orden estrictas, por lo que es habitual intercambiarlas arbitrariamente o definir relaciones de orden por sus relaciones estrictas, cuando esto permite simplificar la notación. También, denotamos por $\geq$ (resp. $\succcurlyeq$) a la relación de orden inversa de $\leq$ (resp. $\preccurlyeq$), dada por $\alpha \geq \beta \Leftrightarrow \alpha \not< \beta$.

Dado que un orden es una relación binaria, todo orden sobre un conjunto es también orden sobre cualquier subconjunto. Otra observación importante es que un orden se puede extender fácilmente como orden parcial a conjuntos más grandes, o a conjuntos en los que existen una o varias inyecciones naturales. En particular, es posible extender un orden de manera natural al producto cartesiano, a partir de su relación de orden estricta.

Definición 2.1.2. Sea $<_A$ un orden (estricto) definido sobre un conjunto A, y B otro conjunto, denotamos también por $<_A$ a la *extensión natural* de $<_A$ tanto a $A \times B$, como a $B \times A$. Si $a_1, a_2 \in A$ y $b_1, b_2 \in B$, estas relaciones vienen dadas por

$$(a_1, b_1) <_A (a_2, b_2) \iff a_1 <_A a_2 \iff (b_1, a_1) <_A (b_2, a_2).$$

También denotamos por $\leq_A$ a la relación de orden no estricta asociada a $<_A$ en $A \times B$ y $B \times A$.

Si denotamos por $\leq_1, ..., \leq_n$ a las extensiones del orden de $\mathbb{N}$ a cada coordenada de $\mathbb{N}^n$, podemos escribir $\preceq_{lex} := \leq_1 \cdots \leq_n$.

El orden lexicográfico tiene una propiedad desafortunada, no nos permite acotar siempre el número de elementos por debajo de un elemento cualquiera, una propiedad muy útil en el estudio de la terminación de algoritmos.

Por ejemplo, si tomamos $n = 2$, el elemento $(1, 0)$ tiene infinitos elementos menores que él de acuerdo a $\preceq_{lex}$, todos los de la forma $(0, p)$ con $p \in \mathbb{N}$.

Una forma de evitar este problema es combinando el orden anterior con el grado, obteniendo el **orden graduado lexicográfico**, $\preceq_{grlex} := \preceq_{gr} \cdot \preceq_{lex}$, donde $\preceq_{gr}$ es el orden graduado, dado por

$$\alpha \prec_{gr} \beta \iff \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i,$$

un orden parcial que sí permite acotar el número de elementos por debajo de un elemento cualquiera.

Otro orden relevante es el orden graduado lexicográfico inverso, $\preceq_{grevlex} := \preceq_{gr} \cdot \succcurlyeq_{lex}$, producto del orden graduado con el orden lexicográfico invirtiendo el orden.

Proposición 2.1.2. *Los órdenes $\preceq_{lex}$, $\preceq_{grlex}$ y $\preceq_{grevlex}$ son órdenes monomiales.*

Demostración. La totalidad de $\preceq_{lex}$ es trivial, pues, si $\alpha, \beta \in \mathbb{N}^n$ con $\alpha \neq \beta$, entonces difieren en al menos una componente, es decir, $\alpha - \beta$ tiene alguna componente no nula, y, por tanto, $\alpha \preceq_{lex} \beta \vee \beta \preceq_{lex} \alpha$.

Entonces, la totalidad de $\preceq_{grlex}$ y $\preceq_{grevlex}$ es consecuencia del Lema 2.1.1 y la totalidad de $\preceq_{lex}$.

Respecto a la propiedad de buen orden, los casos de $\preceq_{grlex}$ y $\preceq_{grevlex}$ son inmediatos, pues el número de elementos acotados superiormente por un grado cualquiera es finito, lo que garantiza la existencia de un mínimo para cualquier subconjunto.

En el caso de $\preceq_{lex}$, sea $S \subseteq \mathbb{N}^n$ no vacío, consideramos los conjuntos $S_0, ..., S_n$ definidos inductivamente como $S_0 := S$, y para todo $i \in \{1, \dots, n\}$, $S_i := \{\alpha \in S_{i-1} : \forall \beta \in S_{i-1}, \alpha_i \leq \beta_i\}$, i.e., los conjuntos de elementos del anterior que minimizan la coordenada i-ésima.

Al ser S no vacío, se deduce por inducción que S_n es no vacío, y, por la propiedad de buen orden de $\leq$ sobre $\mathbb{N}$, en cada conjunto S_i las primeras i coordenadas coinciden para todos los elementos, por lo que, en particular, S_n tiene un único elemento, el mínimo de S.

Finalmente, para la propiedad (ii), se tienen las siguientes igualdades elementales,

$$\alpha = \beta \iff \alpha + \gamma = \beta + \gamma, \quad \alpha - \beta = (\alpha + \gamma) - (\beta + \gamma),$$
$$\sum_{i=1}^{n} \alpha_i \leq \sum_{i=1}^{n} \beta_i \iff \sum_{i=1}^{n} (\alpha_i + \gamma_i) \leq \sum_{i=1}^{n} (\beta_i + \gamma_i). \qquad \square$$

El objetivo de los órdenes monomiales es establecer una forma de ordenar los términos de un polinomio que sea compatible con las operaciones. Esto nos permite introducir las siguientes definiciones.

Definición 2.1.3. Sea $f = \sum_{\alpha \in S} c_\alpha x^\alpha \in \mathbb{K}[\mathbf{x}]$ un polinomio distinto de 0, i.e., con soporte $S \subseteq \mathbb{N}^n$ finito, y $c_\alpha \in \mathbb{K} \setminus \{0\}$ para todo $\alpha \in S$. Fijado un orden monomial $\preccurlyeq$, definimos

i) Cada $c_\alpha x^\alpha$ con $c_\alpha \neq 0$ se denomina **término** de f.

ii) El **multigrado** de f es $\operatorname{mdeg}(f) = \max_{\preccurlyeq} S$, que existe al ser el soporte finito.

Y, por su utilidad, definimos también:

iii) El **coeficiente principal** de f es $\operatorname{LC}(f) = c_{\operatorname{mdeg}(f)} \in F \setminus \{0\}$ (del inglés, "*leading coefficient*").

iv) El **monomio principal** de f es $\operatorname{LM}(f) = x^{\operatorname{mdeg}(f)} \in \mathbb{K}[\mathbf{x}]$.

v) El **término principal** de f es $\operatorname{LT}(f) = \operatorname{LC}(f) \cdot \operatorname{LM}(f) \in \mathbb{K}[\mathbf{x}]$.

Finalmente, por completitud y conveniencia, extendemos estas definiciones al 0 de forma natural, $\operatorname{LT}(0) = \operatorname{LM}(0) = \operatorname{LC}(0) = 0$, y $\operatorname{mdeg}(0) = -\infty$.

La notación usada para denotar los términos principales (y sus partes) varía con frecuencia en la literatura. Otras notaciones existentes en la literatura son HT (del inglés, "*head term*"), HC, HM [10, p. 5], o lpp (del inglés, "*leading power product*") como alternativa de LM [5, p. 3].

En ocasiones, resulta de utilidad especializar a una variable o conjunto de variables concretos. Si $f \in \mathbb{K}[x_1, ..., x_n]$, y $X \subseteq \mathbf{x}$ es un subconjunto de variables, denotaremos por $\operatorname{mdeg}_X(f)$ al multigrado de f como polinomio de $\mathbb{K}[\mathbf{x} \setminus X][X]$, y análogamente escribimos $\operatorname{LC}_X(f)$, $\operatorname{LM}_X(f)$ y $\operatorname{LT}_X(f)$.

También es frecuente considerar el conjunto de coeficientes o términos principales de un conjunto de polinomios, por lo que, si S es un conjunto de polinomios, en general denotaremos la imagen $\{\operatorname{LC}(f) : f \in S\}$ por $\operatorname{LC}(S)$, y análogamente para $\operatorname{LM}(S)$ y $\operatorname{LT}(S)$.

2.2 Algoritmo de división multivariada con resto

Retomando nuestra idea inicial para dividir por múltiples polinomios, ahora sí estamos en condiciones de definir un algoritmo.

La idea será ir eliminando el término principal del dividendo, de acuerdo a un orden monomial, y en caso de no ser posible, añadirlo al resto y seguir dividiendo. A diferencia del caso de la división euclídea, al dividir por varios polinomios, es posible que tras añadir un término al resto, los de menor grado sean aún divisibles.

Algoritmo 1 División con resto multivariada

Entrada: $f, f_1, ..., f_s \in \mathbb{K}[\mathbf{x}]$

Salida: $q_1, ..., q_s, r \in \mathbb{K}[\mathbf{x}]$ tales que $f = q_1 f_1 + \cdots + q_s f_s + r$, y ningún término de r es divisible por ningún término principal de $f_1, ..., f_s$

1: $r \leftarrow 0$
2: $p \leftarrow f$
3: $q_1, ..., q_s \leftarrow 0, ..., 0$
4: **while** $p \neq 0$ **do**
5: **if** $\exists i \in \{1, \dots, s\} : \operatorname{LT}(f_i) \mid \operatorname{LT}(p)$ **then**
6: $i \leftarrow \min\{i \in \{1, \dots, s\} : \operatorname{LT}(f_i) \mid \operatorname{LT}(p)\}$
7: $q_i \leftarrow q_i + \frac{\operatorname{LT}(p)}{\operatorname{LT}(f_i)}$
8: $p \leftarrow p - \frac{\operatorname{LT}(p)}{\operatorname{LT}(f_i)} f_i$
9: **else**
10: $r \leftarrow r + \operatorname{LT}(p)$
11: $p \leftarrow p - \operatorname{LT}(p)$

Para probar la corrección de este algoritmo, observamos que en cada iteración se mantienen las siguientes invariantes:

i) $\operatorname{mdeg}(p) \preccurlyeq \operatorname{mdeg}(f)$ y $f = p + q_1 f_1 + \cdots + q_s f_s + r$.

ii) Para todo $i \in \{1, \dots, s\}$, $\operatorname{mdeg}(q_i f_i) \preccurlyeq \operatorname{mdeg}(f)$.

iii) Ningún término de r es divisible por ningún término principal de $f_1, ..., f_s$.

Por otro lado, para probar la terminación del algoritmo, basta observar que en cada iteración del bucle de la línea 4 se reduce el multigrado de p, independientemente de la rama que se tome en la línea 5, pues:

i) Si existe $i \in \{1, \dots, s\}$ con $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$, $\mathrm{LT}(p) = \mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right)$, luego $\mathrm{mdeg}\left(p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right) \prec \mathrm{mdeg}(p)$, por lo que el multigrado de p disminuye en la línea 8.

ii) En caso contrario, el multigrado de p disminuye en la línea 11.

Al ser $\preccurlyeq$ un buen orden, eventualmente se alcanza $\mathrm{mdeg}(p) = -\infty$ y $p = 0$, con lo que el algoritmo termina.

Ejemplo 2.2.1. *Sea $f = x^2y + xy^2 + 2x$, y $f_1 = xy + 1$, $f_2 = y + 1$, tomando $\preceq_{grlex}$ como orden monomial el algoritmo de la división con resto multivariada actúa con los siguientes pasos:*

	$xy+1$	$y+1$	resto
$x^2y + xy^2 + 2x$			
$-x^2y \quad - x$	x		
$xy^2 + x$			
$-xy^2 \quad - y$	y		
$x - y$			
$-x$			x
$-y$			
$y+1$		-1	
1			1

con lo que $f = (x + y) \cdot f_1 + (-1) \cdot f_2 + (x + 1)$.

Esta división es equivalente a la Euclídea cuando $s = 1$. Sin embargo, para $s \geq 2$, ya hemos visto que este algoritmo no responde a la pregunta de pertenencia al ideal, pues en el Ejemplo 1.3.2 al aplicar el algoritmo obtenemos $xy^2 - x = y(xy+1) + (-x-y)$, a pesar de que $xy^2 - x = x(y^2 - 1)$.

Más adelante veremos que las bases de Gröbner son sistemas de generadores para los que el resto obtenido por este algoritmo es único, y nos da la respuesta al problema de pertenencia del ideal.

2.3 Ideales monomiales

Un ideal monomial $I \subseteq R = \mathbb{K}[\mathbf{x}]$ es un ideal generado por monomios de R, i.e., tal que existe un subconjunto $A \subseteq \mathbb{N}^n$ con

$$I = \langle x^A \rangle = \langle \{x^\alpha : \alpha \in A\} \rangle.$$

El problema de pertenencia de un ideal monomial se puede caracterizar fácilmente. Sea $I = \langle x^A \rangle \subseteq R$ un ideal monomial y $\beta \in \mathbb{N}^n$, entonces:

$$x^\beta \in I \iff \exists \alpha \in A : x^\alpha \mid x^\beta$$

Además, sea $f \in R$, la pertenencia de f en I queda determinada por sus términos, i.e.,

$$f \in I \iff f = \sum_{\beta \in B \subseteq \mathbb{N}^n} c_\beta x^\beta, \text{ con } x^\beta \in I \ \ \forall \beta \in B.$$

La demostración se deduce inmediatamente de la definición de $I = \left\{\sum_{\alpha\in A} q_\alpha x^\alpha : q_\alpha \in R\right\}$.

A continuación se presenta el Lema de Dickson, que es de utilidad para probar el Teorema de la base de Hilbert, pues nos garantiza la existencia de un número finito de generadores para ideales monomiales.

Lema 2.3.1 (de Dickson)**.** *Todo ideal monomial está generado por un conjunto finito de monomios, i.e., sea $A \subseteq \mathbb{N}^n$, existe un subconjunto finito $B \subseteq A$ tal que $\langle x^A\rangle = \langle x^B\rangle$.*

Demostración. La demostración de este resultado es combinatoria. Si A es vacío, el resultado es trivial. En caso contrario, definimos el orden parcial $\leq^n$ sobre $\mathbb{N}^n$. Sean $\alpha, \beta \in \mathbb{N}^n$,

$$\alpha \leq^n \beta \iff \forall i \in \{1, \dots, n\} : \alpha_i \leq \beta_i \iff x^\alpha \mid x^\beta$$

Con este orden, consideramos el conjunto de elementos minimales para $\leq^n$,

$$B = \{\alpha \in A : \forall \beta \in A, \beta \not<^n \alpha\}.$$

Dado $\alpha \in \mathbb{N}^n$ solo existe una cantidad finita de elementos dominados por α según $\leq^n$. De hecho, su número está acotado por el número de elementos tales que la suma de sus coordenadas es menor o igual a la de α. Por tanto, no puede existir una cadena infinita descendente de grados a partir de α, con lo que existe un elemento minimal $\beta \in B$ con $\beta \leq^n \alpha$.

Para probar que B es finito razonamos por inducción sobre n. Si $n = 1$, el orden coincide con el de los naturales, luego B contiene un único elemento. Si $n \geq 2$, definimos

$$A^* = \left\{(\alpha_1, ..., \alpha_{n-1}) \in \mathbb{N}^{n-1} : \exists \alpha_n \in \mathbb{N}, (\alpha_1, ..., \alpha_n) \in A\right\}.$$

Por hipótesis de inducción, su conjunto de elementos minimales, B^*, es finito. Entonces, para cada $\beta = (\beta_1, ..., \beta_{n-1}) \in B^*$, elegimos $b_\beta \in \mathbb{N}$ con $\left(\beta_1, ..., \beta_{n-1}, b_\beta\right) \in A$.

Si tomamos $b = \max\left\{b_\beta : \beta \in B^*\right\}$, veamos que cualquier $\alpha = (\alpha_1, ..., \alpha_n) \in B$ tiene $\alpha_n \leq b$. Por definición de B^*, existe $\beta = (\beta_1, ..., \beta_{n-1}) \in B^*$ tal que $\beta \leq^{n-1} (\alpha_1, ..., \alpha_{n-1})$. Si suponemos por reducción al absurdo que $\alpha_n > b$, necesariamente

$$\left(\beta_1, ..., \beta_{n-1}, b_\beta\right) \leq (\beta_1, ..., \beta_{n-1}, b) < \alpha,$$

lo cual contradice la minimalidad de α. Análogamente, pueden encontrarse cotas para cada coordenada de los elementos minimales, con lo que su cantidad debe ser finita.

Finalmente, $x^A \subseteq \langle x^B\rangle$ se deduce por construcción de B, ya que $\alpha \leq \beta \iff x^\alpha \mid x^\beta$. Por tanto, $\langle x^A\rangle = \langle x^B\rangle$, ya que $B \subseteq A$. □

Lema 2.3.2. *Sea $I \subseteq R = \mathbb{K}[\mathbf{x}]$ un ideal, y $G \subseteq I$ es un conjunto finito que genere los términos principales de I (respecto a un orden monomial), i.e., tal que $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. Entonces $\langle G\rangle = I$, i.e., G es un sistema de generadores del ideal.*

Demostración. Sean $G = \{g_1, ..., g_s\}$ y $f \in I$. Aplicando la división con resto, $f = q_1 g_1 + \cdots + q_s g_s + r$, con $q_1, ..., q_s, r \in R$, de modo que, o bien $r = 0$, o ninguno de sus términos es divisible por los términos principales $\langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s)\rangle$.

Sin embargo, $r = f - q_1 g_1 - \cdots - q_s g_s \in I$, con lo que $\mathrm{LT}(r) \in \mathrm{LT}(I) \subseteq \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s)\rangle$. Por tanto, solo cabe que $r = 0$, i.e., $f \in \langle g_1, ..., g_s\rangle = \langle G\rangle$, como queríamos. □

Aplicando estos resultados a $\text{LT}(I)$, es posible dar una prueba del Teorema de la base de Hilbert en el caso de anillos de polinomios sobre un cuerpo.

Teorema 2.3.3 (Teorema de la Base de Hilbert)**.** *Todo ideal $I \subseteq R = \mathbb{K}[\mathbf{x}]$ es finitamente generado, i.e., R es Noetheriano.*

Demostración. El teorema afirma la existencia de un conjunto finito $G \subseteq I$ tal que $\langle G \rangle = I$. Dado que $\langle \text{LT}(I) \rangle$ es un ideal monomial, el Lema de Dickson nos garantiza la existencia de un subconjunto finito de generadores $G_t \subseteq \langle \text{LT}(I) \rangle$.

Al ser los elementos de G_t términos principales de elementos de I, para cada $g_t \in G_t$ existe $g \in I$ tal que $g_t = \text{LT}(g)$, de modo que existe un subconjunto finito $G \subseteq I$ con $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$, por lo que el lema anterior nos permite concluir que $\langle G \rangle = I$.

□

Nótese que la demostración anterior no es constructiva.

Corolario 2.3.3.1. *Sea $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ una cadena ascendente de ideales en R, esta cadena se estabiliza. Es decir, existe $n \in \mathbb{N}$ tal que $I_n = I_{n+1} = \cdots$ (condición de Noetherianidad).*

Demostración. Consideramos la unión de la cadena, $I = \bigcup_{j \geq 1} I_j$, que es un ideal de R, y, por tanto, finitamente generado, i.e., $I = \langle g_1, ..., g_s \rangle$. Basta tomar $n = \min \left\{ j \geq 1 : g_1, ..., g_s \in I_j \right\}$. □

2.4 Bases de Gröbner y sizigias

Esta prueba del Teorema de la base de Hilbert motiva la siguiente definición.

Definición 2.4.1. Sea $\preccurlyeq$ un orden monomial, e $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideal. Un conjunto finito $G \subseteq I$ es una **base de Gröbner** de I con respecto a $\preccurlyeq$ si $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$.

En general, denotamos el conjunto de bases de Gröbner de I respecto de $\preccurlyeq$ como $\text{GRÖB}_{\preccurlyeq}(I)$, o $\text{GRÖB}(I)$ cuando el orden monomial no sea relevante, y escribiremos $G \in \text{GRÖB}_{\preccurlyeq}(I)$ por brevedad.

Como hemos visto anteriormente, una base de Gröbner también es base del ideal. Es decir, $G \in \text{GRÖB}(I) \implies \langle G \rangle = I$. El Teorema de la Base de Hilbert también tiene como consecuencia el siguiente corolario.

Corolario 2.4.0.1. *Todo ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ tiene una base de Gröbner.*

Finalmente, veamos que las bases de Gröbner son la respuesta a nuestro problema inicial para garantizar la unicidad del resto de la división multivariada.

Lema 2.4.1. *Sea $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideal, $G \in \text{GRÖB}(I)$ y $f \in \mathbb{K}[\mathbf{x}]$, entonces existe un único polinomio $r \in \mathbb{K}[\mathbf{x}]$ tal que:*

i) $f - r \in I$.

ii) Ningún término de r es divisible por ningún monomio de $\text{LT}(G)$.

Demostración. La existencia se deduce de la corrección del algoritmo de división con resto multivariada. Para probar la unicidad, suponemos que $f = h_1 + r_1 = h_2 + r_2$ con r_1, r_2 en las condiciones del lema. Entonces, $r_1 - r_2 = h_2 - h_1 \in I$, y $\text{LT}(r_1 - r_2) \in \text{LT}(G)$, pero por hipótesis, ningún término de r_1 ni r_2 son divisibles por ningún monomio de $\text{LT}(G)$, con lo que $r_1 - r_2 = 0$. □

Dado que el resto de la división multivariada por una base de Gröbner es único, escribiremos

$$r = f \text{ rem } G$$

Además, hemos alcanzado finalmente un algoritmo para responder al problema de pertenencia al ideal.

Teorema 2.4.2. *Sea $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideal, $G \in \text{GRÖB}(I)$ y $f \in \mathbb{K}[\mathbf{x}]$, $f \in I$ si y solo si f rem $G = 0$.*

Demostración. La demostración es consecuencia de la unicidad de $r = f$ rem G. El algoritmo de la división con resto nos permite escribir $f = h + r$ con $h \in I$. Si $r = 0$, es inmediato que $f = h \in I$.

Por otro lado, si $r \neq 0$, al no ser ningún término de r divisible por ningún $\text{LT}(G)$, tenemos que $r \notin \langle G \rangle = I$, pero si suponemos por reducción al absurdo que $f \in I$, tendríamos que $f - h = r \in \mathbb{K}[\mathbf{x}]$. Por tanto, $r \neq 0$, por lo que $f \notin I$. □

De hecho, esta propiedad es equivalente a ser una base de Gröbner.

Proposición 2.4.3. *Sea $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideal, $G = \langle g_1, ..., g_s \rangle \subseteq I$ un conjunto finito, entonces $G \in \text{GRÖB}(I)$ si y solo si para todo $f \in \mathbb{K}[\mathbf{x}]$, $f \in I \iff f$ rem $G = 0$.*

Demostración. La implicación directa es consecuencia del teorema anterior. Por otro lado, si para todo $f \in \mathbb{K}[\mathbf{x}]$, $f \in I \iff f$ rem $G = 0$, veamos que $\langle \text{LT}(I) \rangle = \langle \text{LT}(G) \rangle$, para lo que solo es necesario probar que $\langle \text{LT}(I) \rangle \subseteq \langle \text{LT}(G) \rangle$.

Sea $f \in I$, por hipótesis, aplicando el algoritmo de división, existen $f_1, ..., f_n$ tales que f viene dado por una suma $\sum q_i g_i$ en la que no ocurren cancelaciones de términos principales, pues el multigrado del término eliminado en cada paso de la división es distinto, por lo que se tiene que $\text{LT}(f) \in \langle g_1, ..., g_s \rangle$, de donde se deduce que $\text{LT}(I) \subseteq \langle \text{LT}(G) \rangle$, y, por tanto, $\langle \text{LT}(I) \rangle \subseteq \langle \text{LT}(G) \rangle$. □

Sin embargo, la existencia de bases de Gröbner para un ideal depende de la demostración no constructiva dada del Teorema de la Base de Hilbert. Esta demostración no nos proporciona un algoritmo para determinar la base de Gröbner de un ideal dado.

Para construir este algoritmo, debemos estudiar por qué motivos puede un conjunto generador de un ideal no ser base de Gröbner. Una de estas razones es porque una combinación de dos polinomios, $g, h \in G$, dada por $ax^\alpha g + bx^\beta h$ para algunos $a, b \in \mathbb{K}$ y $\alpha, \beta \in \mathbb{N}^n$ puede tener un término principal que no sea divisible por ningún elemento de $\text{LT}(G)$ si los términos principales de g y h se cancelan.

Vamos a intentar estudiar bajo qué condiciones pueden producirse estas cancelaciones.

Definición 2.4.2. Sean $g, h \in \mathbb{K}[\mathbf{x}]$ polinomios no nulos, una **sizigia** de los términos principales de g y h es una tupla de términos, $S = (s_1, s_2)$, que producen la cancelación de términos principales en la combinación $s_1 g + s_2 h = 0$.

En general, si $\alpha = (\alpha_1, ..., \alpha_n) = \text{mdeg}(g)$, $\beta = (\beta_1, ..., \beta_n) = \text{mdeg}(h)$, y definimos

$$\gamma = (\max\{\alpha_1, \beta_1\}, ..., \max\{\alpha_n, \beta_n\}),$$

entonces $\left(\frac{x^\gamma}{\text{LT}(g)}, -\frac{x^\gamma}{\text{LT}(h)}\right)$ es una sizigia de $\text{LT}(g)$ y $\text{LT}(h)$, y denotamos por $S(g, h)$ a la combinación de g y h asociada a esta sizigia, i.e.,

$$S(g, h) = \frac{x^\gamma}{\text{LT}(g)} g - \frac{x^\gamma}{\text{LT}(h)} h \in \mathbb{K}[\mathbf{x}]. \tag{2.1}$$

A esta expresión se la denomina en ocasiones S**-polinomio** de g y h, y nos permite determinar nuevos términos principales que pueden aparecer en las combinaciones de g y h como resultado de cancelaciones.

Lema 2.4.4. *Sea f un polinomio de $\langle g_1, ..., g_s \rangle$ dado por*

$$f = \sum_{i=1}^{s} c_i x^{\alpha_i} g_i \in \mathbb{K}[\mathbf{x}], \tag{2.2}$$

con $\alpha_1, ..., \alpha_s \in \mathbb{N}^n$ y $c_1, ..., c_s \in \mathbb{K}\backslash\{0\}$, y de manera que existe $\delta \in \mathbb{N}^n$ tal que para todo $i \in \{1, \dots, s\}$, $\alpha_i + \operatorname{mdeg}(g_i) = \delta$, pero $\operatorname{mdeg}(f) \prec \delta$, es decir, de modo que todos los términos principales de los sumandos tengan el mismo multigrado, δ, y se cancelen.

Entonces, si denotamos $x^{\gamma_{ij}} = \operatorname{lcm}\left\{\operatorname{LM}(g_i), \operatorname{LM}\left(g_j\right)\right\}$, tenemos que, para todo $1 \leq i < j \leq s$, $x^{\gamma_{ij}} \mid x^{\delta}$, y existen $c_{ij} \in \mathbb{K}$, de manera que

$$f = \sum_{1 \leq i < j \leq s} c_{ij} x^{\delta - \gamma_{ij}} S(g_i, g_j), \tag{2.3}$$

y $\operatorname{mdeg}\left(x^{\delta-\gamma_{ij}} S(g_i, g_j)\right) \prec \delta$, es decir, f se puede expresar como una combinación de S-polinomios de los g_i.

Demostración. Dado que los coeficientes c_i son arbitrarios, podemos asumir que los polinomios $g_1, ..., g_s$ son mónicos. Sean $1 \leq i < j \leq s$, el monomio $x^{\delta} = x^{\alpha_i} \operatorname{LM}(g_i) = x^{\alpha_j} \operatorname{LM}\left(g_j\right)$ es múltiplo común de $\operatorname{LM}(g_i)$ y $\operatorname{LM}\left(g_j\right)$, por lo que $x^{\gamma_{ij}} \mid x^{\delta}$. Por otra parte,

$$S(g_i, g_j) = \frac{x^{\gamma_{ij}}}{\operatorname{LT}(g_i)} g_i - \frac{x^{\gamma_{ij}}}{\operatorname{LT}\left(g_j\right)} g_j,$$

con lo que $\operatorname{mdeg}\left(S(g_i, g_j)\right) \preccurlyeq \gamma_{ij}$. Como los términos principales en la ecuación (2.1) se cancelan, tenemos que

$$\operatorname{mdeg}\left(x^{\delta-\gamma_{ij}} S(g_i, g_j)\right) = \delta - \gamma_{ij} + \operatorname{mdeg}\left(S(g_i, g_j)\right) \prec \delta - \gamma_{ij} + \gamma_{ij} = \delta.$$

Por último, probamos la ecuación (2.3) por inducción sobre s. En el caso $s = 1$ no se producen cancelaciones y la afirmación es vacua. Si $s \geq 2$, definimos $g = f - c_1 x^{\delta-\gamma_{12}} S(g_1, g_2)$,

$$g = \sum_{i=1}^{s} (c_i x^{\alpha_i} g_i) - c_1 x^{\delta-\gamma_{12}} \left(\frac{x^{\gamma_{12}}}{\operatorname{LT}(g_1)} g_1 - \frac{x^{\gamma_{12}}}{\operatorname{LT}(g_2)} g_2 \right).$$

Sacando factor común de g_1 y g_2, y teniendo en cuenta que $\delta = \alpha_1 + \operatorname{mdeg}(g_1) = \alpha_2 + \operatorname{mdeg}(g_2)$,

$$g = c_1(x^{\alpha_1} - x^{\delta - \operatorname{mdeg}(g_1)}) g_1 + (c_2 x^{\alpha_2} + c_1 x^{\delta - \operatorname{mdeg}(g_2)}) g_2 + \sum_{3 \leq i \leq s} c_i x^{\alpha_i} g_i \tag{2.4}$$

$$= (c_1 + c_2) x^{\alpha_2} g_2 + \sum_{3 \leq i \leq s} c_i x^{\alpha_i} g_i \tag{2.5}$$

$$\tag{2.6}$$

Por definición de g, $\operatorname{mdeg}(g) \preccurlyeq \max_{\prec}\left\{\operatorname{mdeg}(f), \operatorname{mdeg}\left(x^{\delta-\gamma_{12}} S(g_1, g_2)\right)\right\} \prec \delta$, luego g es una combinación en las mismas condiciones que en la ecuación (2.2), con una suma de tamaño $s-1$ si $c_1 + c_2 \neq 0$, o $s-2$ en caso contrario, por lo que, por hipótesis de inducción, tenemos que

$$g = \sum_{2 \leq i < j \leq s} c_{ij} x^{\delta - \gamma_{ij}} S(g_i, g_j),$$

entendiendo que $g = 0$ cuando $s = 2$. Entonces, tomando $c_{12} = c_1$ y $c_{1j} = 0$ para todo $j \in \{3, \ldots, j\}$, podemos reescribir

$$f = g + c_1 x^{\delta - \gamma_{12}} S(g_1, g_2) = \sum_{1 \leq i < j \leq s} c_{ij} x^{\delta - \gamma_{ij}} S(g_i, g_j),$$

como queríamos probar. □

Esta idea se puede aplicar para comprobar algorítmicamente si una base de un ideal es de Gröbner, comprobando que ninguna posible combinación de sus elementos produce una sizigia con término principal no divisible por la base.

Teorema 2.4.5. *Un conjunto finito $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{K}[\mathbf{x}]$ es una base de Gröbner de $\langle G \rangle$ si y solo si*

$$\forall 1 \leq i < j \leq s : S(g_i, g_j) \text{ rem } (g_1, \ldots, g_s) = 0.$$

Demostración. Si G es base de Gröbner, dado que $S(g_i, g_j) \in I = \langle G \rangle$ para todos $i, j \in \{1, \ldots, s\}$, el resto respecto de G debe ser 0.

Recíprocamente, veamos que G es base de Gröbner, es decir, sea $f \in I$, que asumimos distinto de 0, queremos ver que $\operatorname{LT}(f) \in \langle \operatorname{LT}(G) \rangle$.

Dado que $f \in I$, aplicando la división multivariada, escribimos $f = \sum_{1 \leq i \leq s} q_i g_i$, para algunos $q_i \in \mathbb{K}[\mathbf{x}]$, y definimos $\delta = \max_{\prec}\{\operatorname{mdeg}(q_i g_i) : 1 \leq i \leq s\}$ de modo que $\operatorname{mdeg}(f) \preccurlyeq \delta$.

Si la desigualdad es estricta, entonces la suma ha sufrido cancelación de términos principales, y

$$f^* = \sum_{\substack{1 \leq i \leq s \\ \operatorname{mdeg}(q_i g_i) = \delta}} \operatorname{LT}(q_i)\, g_i$$

es una suma en las condiciones de la ecuación (2.2), con lo que, en virtud del Lema 2.4.4, podemos escribir f^* como combinación de polinomios de la forma $x^{\alpha_{ij}} S(g_i, g_j)$, con $\alpha_{ij} \in \mathbb{N}^n$ tales que $\alpha_{ij} + \operatorname{mdeg}\left(S(g_i, g_j)\right) \prec \delta$.

Si dividimos entonces f^* por $(g_1, \ldots, g_s)$, por hipótesis el resto de $S(g_i, g_j)$ es 0, y obtenemos cocientes $q_i^* \in \mathbb{K}[\mathbf{x}]$ tales que $f^* = \sum_{1 \leq i \leq s} q_i^* g_i$, de modo que $\max_{\prec} \operatorname{mdeg}(q_i^* g_i) : 1 \leq i \leq s \prec \delta$.

Por tanto, podemos reescribir $f - f^*$ y f^* en términos de G con un valor más pequeño de δ, y, por tanto, también f. Aplicando este proceso de reemplazo tantas veces como sea necesario se alcanza un grado mínimo, pues δ decrece en cada paso y $\preccurlyeq$ es un buen orden, y acabamos con una expresión de f en la que se da la igualdad $\operatorname{mdeg}(f) = \operatorname{mdeg}(q_i g_i)$, al menos para un índice i, con lo que finalmente tenemos

$$\operatorname{LT}(f) = \sum_{\substack{1 \leq i \leq s \\ \operatorname{mdeg}(q_i g_i) = \delta}} \operatorname{LT}(q_i) \cdot \operatorname{LT}(g_i) \in \langle \operatorname{LT}(G) \rangle.$$ □

2.5 El algoritmo de Buchberger

Finalmente estamos en condiciones de describir un algoritmo que sea capaz de determinar la base de Gröbner de un ideal, partiendo de una base del ideal.

La idea detrás de este algoritmo es añadir a nuestra base cada sizigia que no cumpla la condición de clausura por términos principales.

Algoritmo 2 Algoritmo de Buchberger

Entrada: $f_1, ..., f_s \in \mathbb{K}[\mathbf{x}]$ y un orden monomial $\preccurlyeq$
Salida: $G \in \text{GRÖB}_{\preccurlyeq}(\langle f_1, ..., f_s \rangle)$, con $f_1, ..., f_s \in G$

1: $G \leftarrow \emptyset$
2: $S \leftarrow \{f_1, ..., f_s\}$
3: **while** $S \neq \emptyset$ **do**
4: $\quad G \leftarrow G \cup S$
5: $\quad S \leftarrow \emptyset$
6: $\quad$ Sean $g_1, ..., g_t$ los elementos de G ordenados por $\prec$,
7: $\quad$ **for** $i \in \{\{1, ..., t-1\}\}$, $j \in \{\{i+1, ..., t\}\}$ **do**
8: $\quad\quad r \leftarrow S(g_i, g_j)$ rem $(g_1, ..., g_t)$
9: $\quad\quad$ **if** $r \neq 0$ **then**
10: $\quad\quad\quad S \leftarrow S \cup \{r\}$

Teorema 2.5.1. *En $\mathbb{K}[\mathbf{x}]$, el algoritmo de Buchberger (Algoritmo 2) es correcto.*

Demostración. Asumiendo que el algoritmo termina, G siempre es generador de I, pues siempre contiene a $f_1, ..., f_s$, y, a partir de ahí, en el algoritmo solo se le añaden elementos de I, i.e., restos de dividir sizigias de elementos de I por elementos de I.

Por otra parte, si el algoritmo termina, todos los restos de las sizigias por la división por G son 0, luego $G \in \text{GRÖB}(I)$.

Por último, veamos que el algoritmo termina, ya que, si G' y G'' se corresponden a estados sucesivos del conjunto G, tenemos $G' \subseteq G''$, y por tanto $\langle \text{LT}(G') \rangle \subseteq \langle \text{LT}(G'') \rangle$. Es decir, los estados sucesivos de G inducen una cadena ascendente de ideales $\langle \text{LT}(G) \rangle$ de $\mathbb{K}[\mathbf{x}]$, que se estabiliza como consecuencia del Teorema de la Base de Hilbert, luego en alguna repetición del bucle se tiene que $\langle \text{LT}(G') \rangle = \langle \text{LT}(G'') \rangle$.

Queremos ver entonces que $G' = G''$, i.e., $S = G'' \setminus G' = \emptyset$. Suponemos por reducción al absurdo que $r \in S$, i.e., r es el resto de dividir alguna sizigia por G'. Como $r \in G''$, o bien $r = 0$ o $\text{LT}(r) \in \langle \text{LT}(G'') \rangle$. Sin embargo, como $\langle \text{LT}(G'') \rangle = \langle \text{LT}(G') \rangle$, y r es resto de dividir por G', necesariamente $r = 0$. No obstante, es imposible que $r = 0 \in S$, por construcción del algoritmo. □

Como consecuencia, los siguientes problemas son decidibles para ideales de $\mathbb{K}[\mathbf{x}]$, usando bases de Gröbner:

1. Pertenencia a un ideal
2. Contención en un ideal
3. Igualdad entre ideales

En general, las bases de Gröbner obtenidas por el algoritmo de Buchberger no son únicas para un ideal, ya que dependen de los generadores usados. Sin embargo, veremos que existe una forma de reducir bases de Gröbner con clausura única.

Ejemplo 2.5.1. *Sea* $I = \langle x^2y + x^2 + y, y\rangle \subseteq \mathbb{K}[x, y]$*, aplicando el algoritmo de Buchberger respecto a* $\preceq_{lex}$*, se obtiene la base de Gröbner* $G = \{x^2y + x^2 + y, y, x^2\}$*, mientras que, si aplicamos el algoritmo de Buchberger tomando como generadores* $I = \langle x^2y + x^2, y\rangle$*, el resultado del algoritmo es* $G' = \{x^2y + x^2, y, x^2\}$*.*

Lema 2.5.2. *Sea* $G \in \text{GRÖB}(I)$ *con* $I \subseteq \mathbb{K}[\mathbf{x}]$ *un ideal,* $g \in G$ *y* $\text{LT}(g) \in \langle \text{LT}(G \setminus \{g\})\rangle$*, entonces,* $G \setminus \{g\}$ *es una base de Gröbner de* I*.*

Demostración. La demostración es inmediata, pues al ser $\langle \text{LT}(G \setminus \{g\})\rangle = \langle \text{LT}(G)\rangle = \langle \text{LT}(I)\rangle$, por lo que $G \setminus \{g\} \in \text{GRÖB}(I)$. □

Dado que G es finito, este lema nos permite reducir una base de Gröbner a una minimal, eliminando elementos que no sean necesarios para generar $\langle \text{LT}(I)\rangle$.

Definición 2.5.1. Una base $G \in \text{GRÖB}_{\preccurlyeq}(I)$ se dice **minimal** para $I = \langle G\rangle$ si y solo si para todo $g \in G$:

i) $\text{LC}(g) = 1$,

ii) $\text{LT}(g) \notin \langle \text{LT}(G \setminus \{g\})\rangle$.

También diremos que un elemento g de una base de Gröbner está **reducido con respecto a** G si ningún monomio de g pertenece a $\langle \text{LT}(G \setminus \{g\})\rangle$. Consecuentemente, diremos que una base de Gröbner minimal es **reducida** si todos sus elementos están reducidos con respecto a ella.

Teorema 2.5.3. *Todo ideal de* $\mathbb{K}[\mathbf{x}]$ *tiene una única base de Gröbner reducida respecto a un orden monomial dado,* $\preccurlyeq$*.*

Demostración. La existencia es consecuencia de la existencia de bases de Gröbner generales. Sea G una base de Gröbner respecto a $\preccurlyeq$, podemos asumir que G es minimal aplicando el procedimiento de reducción del Lema 2.5.2.

Para encontrar una base reducida, veamos que podemos definir también un procedimiento de reducción que reduce cada elemento de la base secuencialmente. Para todo $i \in \{1, \dots, s\}$ consideramos

$$h_i = g_i \text{ rem } G_i \ := \ \{h_1, ..., h_{i-1}, g_{i+1}, ..., g_s\}.$$

Se puede probar por inducción sobre i que $\text{LT}(g_i) = \text{LT}(h_i)$, observando que, si G es minimal, en cada paso $\text{LT}(G_i) = \text{LT}(G) \setminus \{\text{LT}(g_i)\}$. Además, por definición, h_i es reducido con respecto a G_i, con lo que $G_s = \{h_1, ..., h_s\}$ es una base reducida.

Para probar la unicidad, consideramos dos bases reducidas de I, G y G'. Queremos ver que $\text{LT}(G) = \text{LT}(G')$. Sea $g \in \text{LT}(G)$, se tiene que $g \in \langle \text{LT}(G)\rangle = \text{LT}(I) = \langle \text{LT}(G')\rangle$, luego existe algún $g' \in G'$ con $\text{LT}(g') \mid \text{LT}(g)$, y análogamente, existe un $g'' \in G$ con $\text{LT}(g'') \mid \text{LT}(g')$. Por tanto, como G es minimal, se deduce $\text{LT}(g) = \text{LT}(g') = \text{LT}(g'') \in \text{LT}(G')$, i.e., $\text{LT}(G) \subseteq \text{LT}(G')$. Intercambiando las bases, se tiene $\text{LT}(G') \subseteq \text{LT}(G)$, y por tanto, la igualdad.

Finalmente, sea $g \in G$, tomamos $g' \in G'$ con $\text{LT}(g) = \text{LT}(g')$. Dado que ambas bases son reducidas, ningún monomio de $g - g'$ es divisible por ningún elemento de $\text{LT}(G) = \text{LT}(G')$. Por tanto, $g - g' = g - g'$ rem $G = 0$, pues $g - g' \in I$. En consecuencia, $g \in G'$, i.e., $G \subseteq G'$, e intercambiando las bases en el argumento se deduce la igualdad. □

2.6 Operaciones elementales con ideales

Como hemos visto en la sección anterior, determinar una base de Gröbner de un ideal es un proceso bastante complicado. Por este motivo, una pregunta que nos podemos hacer es si conociendo las bases de Gröbner de algunos ideales sería posible construir directamente bases de Gröbner de ideales definidos a partir de operaciones elementales entre los que conocemos. Sin embargo, como veremos, la respuesta a esta pregunta es en general negativa.

Observación 1. Sean $I, J \subseteq \mathbb{K}[\mathbf{x}]$ ideales, con respectivas bases de Gröbner $G_I \in \text{GRÖB}_{\preccurlyeq}(I)$ y $G_J \in \text{GRÖB}_{\preccurlyeq}(J)$,

i) $G_I \cup G_J$ es un sistema generador de $I + J$, sin embargo, no forma una base de Gröbner de $I + J$, pues las cancelaciones entre términos principales de elementos de G_I y G_J dan lugar a que existan términos principales en $\text{LT}(I + J)$ que no pertenezcan a $\langle \text{LT}(G_I \cup G_J) \rangle$.

ii) $G_{IJ} := \{f \cdot g : f \in G_I, g \in G_J\}$ es un sistema generador de $I \cdot J$, pero tampoco forma una base de Gröbner de $I \cdot J$, pues, si bien los términos principales de S-polinomios de elementos de G_{IJ} sí están por separado en $\text{LT}(G_I)$ y $\text{LT}(G_J)$, no están necesariamente en $\text{LT}(G_{IJ})$.

Para demostrar esta observación, basta el siguiente ejemplo.

Ejemplo 2.6.1. *Sean $I = \langle x + 1, y \rangle$ y $J = \langle x, y \rangle$ ideales de $\mathbb{K}[x, y]$, sus bases de Gröbner reducidas respecto al orden lexicográfico $\preccurlyeq := \preccurlyeq_{lex(x,y)}$ son trivialmente $G_I = \{x + 1, y\}$ y $G_J = \{x, y\}$.*

Sin embargo, $G_I \cup G_J = \{x + 1, x, y\}$ no es una base de Gröbner respecto a $\preccurlyeq$, pues $I + J = 1$ y $1 \notin \langle \text{LT}(G_I \cup G_J) \rangle$. Del mismo modo, $G_{IJ} = \{x^2 + x, xy + y, xy, y^2\}$, no es una base de Gröbner de $I \cdot J$ respecto a $\preccurlyeq$, ya que $\text{LT}((xy + y) - xy) = y \notin \langle \text{LT}(G_{IJ}) \rangle$.

Si bien no es posible obtener directamente bases de Gröbner de la suma y el producto de ideales, sí que es posible diseñar mejoras del algoritmo de Buchberger que sean capaces de aprovechar la información de estas bases de Gröbner para evitar, por ejemplo, calcular S-polinomios entre elementos de G_I o G_J en el cálculo de una base de Gröbner de $I + J$. Sin embargo, su utilidad es cuestionable.

En el caso de la intersección y cociente de ideales, tampoco es posible construir directamente una base de Gröbner a partir de los ideales conocidos.

No obstante, sí que existen formas de encontrar sistemas generadores para estos ideales utilizando bases de Gröbner, utilizando el truco de Rabinowitsch y algunos conceptos de teoría de la eliminación, que serán introducidos más adelante.

Proposición 2.6.1. *Sean $I, J \subseteq \mathbb{K}[\mathbf{x}]$ dos ideales, con $G_I \in \text{GRÖB}_{\preccurlyeq}(I)$ y $G_J \in \text{GRÖB}_{\preccurlyeq}(J)$, para un mismo orden monomial $\preccurlyeq$.*

Sea G una base de Gröbner del ideal $tI + (1-t)J \subseteq \mathbb{K}[\mathbf{x}][t]$, con respecto del orden $\preccurlyeq_* := \preccurlyeq \cdot \preccurlyeq_t$, siendo $\preccurlyeq_t$ el orden natural dado por el grado en t, entonces, $G' = G \cap \mathbb{K}[\mathbf{x}] \in \text{GRÖB}_{\preccurlyeq}(I \cap J)$.

La búsqueda de una base de Gröbner del cociente de ideales se puede reducir a la de la intersección, ya que, si I, J son ideales de $\mathbb{K}[\mathbf{x}]$ con $J = \langle g_1, ..., g_s \rangle$, entonces,

$$I : J = (I : \langle g_1 \rangle) \cap \cdots \cap (I : \langle g_s \rangle) = \left(\frac{1}{g_1}(I \cap \langle g_1 \rangle) \right) \cap \cdots \cap \left(\frac{1}{g_s}(I \cap \langle g_s \rangle) \right),$$

donde si $(I \cap \langle g_i \rangle)$ está generado por $\langle h_1, ..., h_r \rangle$, g_i divide a cada h_j, y $\frac{1}{g_i}(I \cap \langle g_i \rangle)$ denota el ideal $\left\langle \frac{h_1}{g_i}, ..., \frac{h_r}{g_i} \right\rangle \subseteq \mathbb{K}[\mathbf{x}]$.

Por otro lado, el problema de la búsqueda de una base del radical de un ideal no es tan sencillo, si bien sí que es posible reducir el problema de pertenencia al radical utilizando una base de Gröbner del propio ideal y el truco de Rabinowitsch [2, p. 184], ya visto en el grado, por lo que, si solo nos interesa este problema, no es necesario determinar una base de Gröbner del radical.

Lema 2.6.2. *Sea* $I = \langle f_1, ..., f_n \rangle \subseteq \mathbb{K}[\mathbf{x}]$ *un ideal, y* $f \in \mathbb{K}[\mathbf{x}]$*,*

$$f \in \sqrt{I} \iff 1 \in J := \langle f_1, ..., f_n, 1 - tf \rangle,$$

como ideal de $\mathbb{K}[\mathbf{x}][t]$*.*

2.7 Especialización

Otra operación que podemos considerar con bases de Gröbner es la sustitución de variables por valores concretos. Es decir, nos preguntamos si la imagen de una base de Gröbner, $G \in \text{GRÖB}_{\preccurlyeq}(I)$, con $I \subseteq \mathbb{K}(t)[\mathbf{x}]$, por el homomorfismo de anillos σ_a que sustituye t por algún $a \in \mathbb{K}$ fijo, sigue siendo una base de Gröbner de $\sigma_a(I)$, como ideal de $\mathbb{K}[\mathbf{x}]$.

Podríamos esperar que esto ocurra en general, al ser σ_a homomorfismo de anillos. Sin embargo, en algunos casos, pueden existir valores de a para los que G deja de ser base de Gröbner.

Ejemplo 2.7.1. *Un ejemplo sencillo de este fenómeno es cuando el homomorfismo* σ_a *hace disminuir el grado de los polinomios de* G*, al llevar coeficientes a* 0*.*

Si en $\mathbb{K}(t)[x, y]$ *tomamos* $G = \{tx + y, y + 1\} \in \text{GRÖB}_{\preccurlyeq_{revlex}} \langle G \rangle$*, es fácil ver que la substitución* $\sigma_0 : t \mapsto 0$*, resulta en* $\sigma_0(G) = \{y, y + 1\}$*, que no es base de Gröbner, pues el ideal que genera es* $\langle 1 \rangle$*, pero* $1 \notin \text{LM}(\sigma_0(G))$*.*

Este tipo de substitución se denomina **especialización**, y en general consideraremos la posibilidad de especializar varios parámetros simultáneamente, trabajando en $\mathbb{K}(\mathbf{t})[\mathbf{x}]$.

Una forma alternativa de estudiar el problema consiste en tratar G como una base de Gröbner de I como ideal de $\mathbb{K}[\mathbf{x}, \mathbf{t}]$, respecto a un orden producto $\preccurlyeq_* := \preccurlyeq \cdot \preccurlyeq_t$, donde $\preccurlyeq$ es orden monomial de $\mathbb{K}[\mathbf{x}]$ y $\preccurlyeq_t$ de $\mathbb{K}[\mathbf{t}]$, lo que nos garantiza que $G \in \text{GRÖB}_{\preccurlyeq_*}(I)$.

Dado que el ideal también es ideal de $\mathbb{K}(\mathbf{t})[\mathbf{x}]$, no impone restricciones sobre los parámetros, luego podemos suponer que $I \cap \mathbb{K}[\mathbf{t}] = \{0\}$. Considerar el ideal en $\mathbb{K}[\mathbf{x}, \mathbf{t}]$ nos permite determinar en qué casos la especialización preserva la propiedad de ser base de Gröbner, como muestra el siguiente resultado, una versión débil de la Proposición 6.3.1 de [2].

Proposición 2.7.1. *Sea* $\mathbb{K}$ *un cuerpo, e* $I = \langle f_1, ..., f_s \rangle \subseteq \mathbb{K}[\mathbf{x}, \mathbf{t}]$ *tal que* $I \cap \mathbb{K}[\mathbf{t}] = \{0\}$*,* $\preccurlyeq := \preccurlyeq_x \cdot \preccurlyeq_t$ *un orden monomial, con* $\preccurlyeq_x$ *y* $\preccurlyeq_t$ *órdenes monomiales sobre* $\mathbb{K}[\mathbf{x}]$ *y* $\mathbb{K}[\mathbf{t}]$ *respectivamente, y* $G = \{g_1, ..., g_r\} \in \text{GRÖB}_{\preccurlyeq}(I)$*, entonces:*

i) En $\mathbb{K}(\mathbf{t})[\mathbf{x}]$*,* $G \in \text{GRÖB}_{\preccurlyeq_x}\left(\tilde{I}\right)$*, donde* $\tilde{I} := \langle f_1, ..., f_s \rangle$ *es el ideal* I *visto como ideal de* $\mathbb{K}(\mathbf{t})[\mathbf{x}]$*.*

ii) Si para todo $i \in \{1, \dots, r\}$ *denotamos por* $h_i(\mathbf{t}) := \text{LC}_{\mathbf{x}}(g_i(\mathbf{x}, \mathbf{t}))$*, y consideramos el conjunto algebraico que generan,* $W = \mathcal{V}(h_1) \cup \cdots \cup \mathcal{V}(h_r) \subsetneq \mathbb{K}^n$ *para algún* n*, entonces, para toda especialización dada por* $\mathbf{t} \mapsto a \in \mathbb{K}^n \setminus W$*, la imagen de* G*,* $\sigma_a(G) = \{g_i(\mathbf{x}, a), ..., g_i(\mathbf{x}, a)\} \in \text{GRÖB}_{\preccurlyeq_x}(\sigma_a(I))$*, en* $\mathbb{K}[\mathbf{x}]$*.*

Demostración. Para probar (i), observamos que, si $f \in \mathbb{K}[\mathbf{x},\mathbf{t}]$, dado que $I \cap \mathbb{K}[\mathbf{t}] = \{0\}$, necesariamente $\text{LM}(f) = \mathbf{x}^\alpha \mathbf{t}^\beta$ con $\alpha \neq 0$. Entonces en $\mathbb{K}(\mathbf{t})[\mathbf{x}]$, se tiene que $\text{LM}_{\mathbf{x}}(f) = \mathbf{x}^\alpha$, y, por tanto, $\text{LT}_{\mathbf{x}}(f) = c(\mathbf{t})\mathbf{x}^\alpha$ para algún $c \in \mathbb{K}[\mathbf{t}]$.

Esto implica que $\text{LM}_{\mathbf{x}}(I) \subseteq \langle \text{LM}_{\mathbf{x}}(G) \rangle$, y, dado que $\mathbb{K}(\mathbf{t})$ es cuerpo, también se sigue que, en $\mathbb{K}(\mathbf{t})[\mathbf{x}]$, $\text{LT}(I) \subseteq \langle \text{LT}(G) \rangle$.

Por otro lado, para probar (ii), veremos que para todo $\overline{f} \in \mathbb{K}[\mathbf{x}]$, $\overline{f} \in \sigma_a(I)$ si y solo si $\overline{f}$ rem $\sigma_a(G) = 0$.

Si $\overline{f} \in \sigma_a(I)$, entonces existe $f \in I$ con $\overline{f} = \sigma_a(f)$, de manera que, por (i), f rem $G = 0$, y, dado que los términos principales de G no se anulan por σ_a, el resultado de la división es el mismo, y $\overline{f}$ rem $\sigma_a(G) = 0$.

Recíprocamente, si $\overline{f}$ rem $\sigma_a(G) = 0$, existen $b_1, ..., b_r \in \mathbb{K}[\mathbf{x}]$ tales que $\overline{f} = \sum_{i=1}^{r} b_i g_i$. Entonces, queremos construir un polinomio $f \in \mathbb{K}(\mathbf{t})[\mathbf{x}]$, tal que $\sigma_a(f) = \overline{f}$ y f rem $G = 0$.

Podemos considerar como candidato inicial $f = \overline{f}$, pues también $\overline{f} \in \mathbb{K}(\mathbf{t})[\mathbf{x}]$ con $\sigma_a(\overline{f}) = \overline{f}$. Para conseguir que f rem $G = 0$ también en $\mathbb{K}[\mathbf{x},\mathbf{t}]$, necesitamos comparar el proceso de reducción de $\overline{f}$ y f por G.

La observación clave es que, en cada paso de la división multivariada, lo único que puede hacer distinta la división en $\mathbb{K}[\mathbf{x},\mathbf{t}]$ es que términos no principales de un divisor introduzcan monomios en los restos parciales de la división que no aparecían al dividir en $\mathbb{K}[\mathbf{x}]$, pues el único factor que afecta a la elección del divisor en cada paso son los monomios que aparezcan en cada resto parcial, ya que los monomios principales de los divisores coinciden por hipótesis.

Sin embargo, la condición para que esto ocurra es que dichos términos no principales se anulen por σ_a, por lo que podemos podemos sumar a nuestro candidato el término correspondiente para que se anule durante la división, sin alterar su imagen por σ_a.

Dado que el número de pasos de la división es finito, existe un polinomio f como buscábamos, y deducimos que $\overline{f} \in \sigma_a(I)$. Finalmente, aplicando la Proposición 2.4.3, deducimos que $\sigma_a(G) \in \text{GRÖB}_{\leq_x}(\sigma_a(I))$. □

Sin embargo, esta proposición no nos dice nada de cómo obtener una base de Gröbner de $\sigma_a(I)$ cuando $a \in W$, más allá de calcularla directamente en cada caso. Idealmente nos gustaría tener una forma de corregir de algún modo los problemas que causan que G deje de ser base de Gröbner al especializar en W.

Esta idea llevó al desarrollo de las bases y sistemas comprensivos de Gröbner por parte de Weispfenning, que serían refinados por Montes y Wibmer con la definición del recubrimiento canónico de Gröbner.

2.8 Bases y Sistemas Comprensibles de Gröbner

En esta sección introduciremos las nociones de base y sistema comprensivo de Gröbner, así como una demostración de su existencia, siguiendo su presentación original por Weispfenning en [10].

Definición 2.8.1. Con la notación de secciones anteriores, sea $I \subseteq R := \mathbb{K}[\mathbf{t}][\mathbf{x}]$ un ideal, y $G = \langle g_1, ..., g_n \rangle \in \text{GRÖB}_{\preccurlyeq}(I)$ para algún orden monomial $\preccurlyeq := \preccurlyeq_x \cdot \preccurlyeq_t$, donde $\preccurlyeq_x$ y $\preccurlyeq_t$ son órdenes monomiales sobre $\mathbb{K}[\mathbf{x}]$ y $\mathbb{K}[\mathbf{t}]$ respectivamente.

Decimos que G es una **base de Gröbner comprensiva** con respecto a $\preccurlyeq$ si para toda extensión de cuerpos $\mathbb{K} \hookrightarrow \mathbb{K}'$ y toda especialización $\sigma : \mathbb{K}[\mathbf{t}] \longrightarrow \mathbb{K}'$ de R, $\sigma(G)$ es una base de Gröbner en $\mathbb{K}'[\mathbf{x}]$ de $\sigma(I)$.

Denotaremos el conjunto de las bases de Gröbner comprensivas de I con respecto a $\preccurlyeq$ por $\textsc{CompGröb}_{\preccurlyeq}(I)$, donde, como es habitual, omitiremos el orden monomial cuando no sea relevante.

En general, cuando no hay una especialización de por medio, la propiedad de bases de Gröbner se conserva por extensiones de cuerpo, como consecuencia directa de su caracterización por S-polinomios 2.4.5.

Lema 2.8.1 (Estabilidad de bases de Gröbner por extensiones de cuerpos)**.** *Sea $\mathbb{K}'$ una extensión de un cuerpo $\mathbb{K}$, $R = \mathbb{K}[\mathbf{x}]$, $R' = \mathbb{K}'[\mathbf{x}]$ y $G \in \textsc{Gröb}_{\preccurlyeq}(I)$ para algún ideal I y un orden monomial $\preccurlyeq$ de R. Entonces G también es base de Gröbner respecto a $\preccurlyeq$ en R'.*

Demostración. Sean f y g dos polinomios distintos de G, por definición de G, su S-polinomio verifica que $S(f,g) \text{ rem } G = 0$ en R, y, como, tanto en R como en R', el algoritmo de la división se realiza sobre $\mathbb{K}$, el resto es el mismo en R', y concluimos por el Teorema 2.4.5. □

Esto motiva que solo nos interese estudiar las especializaciones que *generan* completamente la extensión de cuerpos que tienen como imagen, que reciben el nombre de *epi*-especializaciones.

Definición 2.8.2. Decimos que una especialización $\sigma : \mathbb{K}[\mathbf{t}] \longrightarrow \mathbb{K}' \supseteq \mathbb{K}$ es **epi**-especialización, si $\mathbb{K}' = CF(\sigma(\mathbb{K}[\mathbf{t}]))$, donde denotamos por $CF(R)$ el cuerpo de fracciones de un anillo R [10, p. 5].

Si σ es una epi-especialización, entonces $\mathbb{K}'$ es $\mathbb{K}$-isomorfo a $CF(\mathbb{K}[\mathbf{t}]/\ker(\sigma))$. Por otro lado, si $\pi \in \text{Spec}(\mathbb{K}[\mathbf{t}])$, el conjunto de ideales primos de $\mathbb{K}[\mathbf{t}]$, tenemos una epi-especialización $\sigma_\pi : \mathbb{K}[\mathbf{t}] \longrightarrow CF(\mathbb{K}[\mathbf{t}]/\ker(\sigma))$, por lo que hay una correspondencia entre las epi-especializaciones y $\text{Spec}(\mathbb{K}[\mathbf{t}])$.

Corolario 2.8.1.1. *Sea G un subconjunto finito de $R := \mathbb{K}[\mathbf{t},\mathbf{x}]$, $G \in \textsc{CompGröb}_{\preccurlyeq}(I)$ para algún ideal I, si y solo si para toda epi-especialización $\sigma : \mathbb{K}[\mathbf{t}] \longrightarrow \mathbb{K}'$, $\sigma(G)$ es una base de Gröbner en $\mathbb{K}'[\mathbf{x}]$ con respecto a $\preccurlyeq$.*

Con el objetivo de estudiar los términos principales de polinomios en $\sigma(G)$, extendemos nuestras definiciones de términos principales, considerando solo los términos cuyos coeficientes no pertenecen a un ideal concreto.

Definición 2.8.3. Sea $I \subseteq \mathbb{K}[\mathbf{t}]$ un ideal, $f \in \mathbb{K}[\mathbf{t}][\mathbf{x}]$, y $\preccurlyeq$ un orden monomial, denotamos por $\text{LT}_{(I)}(f)$ el mayor término de f respecto a $\preccurlyeq_x$ cuyo coeficiente, un polinomio de $\mathbb{K}[\mathbf{t}]$, no pertenece a I, o 0 si no existe.

Análogamente, definimos $\text{LC}_{(I)}(f)$ y $\text{LM}_{(I)}(f)$ como su coeficiente y monomio respectivamente.

Estas definiciones nos permiten caracterizar las imágenes de conjuntos por epi-especializaciones como bases de Gröbner, a partir de la observación de que si σ_π es una epi-especialización con $\ker(\sigma_\pi) = \pi$, $\text{LT}_{(\pi)} = \text{LT} \circ \sigma_\pi$.

Lema 2.8.2. *Sea $I = \langle G \rangle = \langle g_1, ..., g_n \rangle$ un ideal de $R := \mathbb{K}[\mathbf{t},\mathbf{x}]$, $\sigma_\pi : \mathbb{K}[\mathbf{t}] \longrightarrow \mathbb{K}'$ una epi-especialización de R con $\ker(\sigma) = \pi \in \text{Spec}(\mathbb{K}[\mathbf{t}])$.*

Entonces, $\sigma_\pi(G)$ es una base de Gröbner de $\langle \sigma_\pi(I) \rangle$ en $\mathbb{K}'[\mathbf{x}]$ si y solo si para todo $f \in I$ para el que $\text{LT}_{(\pi)}(f) \neq 0$, existe $g \in G$ tal que $\text{LT}_{(\pi)}(g) \mid \text{LT}_{(\pi)}(f)$.

Demostración. Si $\sigma_\pi(G) \in \textsc{Gröb}_{\preccurlyeq}(\langle \sigma_\pi(I) \rangle)$, y $f \neq 0$, dado que $\sigma_\pi(f) \in \langle \sigma_\pi(G) \rangle$, necesariamente existe $g \in G$ con $\text{LT}_{(\pi)}(g) = \text{LT}(\sigma_\pi(g)) \mid \text{LT}(\sigma_\pi(f)) = \text{LT}_{(\pi)}(f)$.

Para probar el recíproco, si $0 \neq f \in \langle \sigma_\pi(I) \rangle$, entonces existe algún $c \in \mathbb{K}[\mathbf{t}] \setminus \pi$ y un $h \in I$, tal que $\sigma_\pi(h) = \sigma_\pi(c)f$. Por hipótesis existe $g \in G$ tal que $\text{LT}_{(\pi)}(g) \mid \text{LT}_{(\pi)}(h) = \text{LT}(\sigma_\pi(h)) = c \cdot \text{LT}(f)$, por lo que $\text{LT}(f) \in \langle \text{LT}(\sigma_\pi(G)) \rangle$, y $\sigma_\pi(G) \in \textsc{Gröb}_{\preccurlyeq}(\langle \sigma_\pi(I) \rangle)$. □

Por tanto, podemos caracterizar una base de Gröbner comprensiva a partir del espectro de $\mathbb{K}[\mathbf{t}]$.

Teorema 2.8.3. *Sea $G = \{g_1, ..., g_n\} \subseteq I \subseteq \mathbb{K}[\mathbf{t}][\mathbf{x}]$, con I un ideal, y sea $\preccurlyeq$ un orden monomial, entonces $G \in \text{CompGröb}_{\preccurlyeq}(I)$ si y solo si para todo $\pi \in \text{Spec}(\mathbb{K}[\mathbf{t}])$ y todo $t \in \text{LT}_{(\pi)}(I)$, existe $g \in G$ con $\text{LT}_{(\pi)}(g) \mid t$.*

Nótese que en este momento no sabemos si existe un G en las condiciones del Teorema 2.8.3, puesto que $\text{Spec}(\mathbb{K}[\mathbf{t}])$ es infinito, y, aún si existe, el Teorema no nos dice como calcularlo.

Por este motivo, sea $I \subseteq \mathbb{K}[\mathbf{t}, \mathbf{x}]$ un ideal, consideramos la relación de equivalencia en $\text{Spec}(\mathbb{K}[\mathbf{t}])$, inducida por los términos principales de I bajo epi-especializaciones.

Definición 2.8.4. En las condiciones anteriores, definimos la relación de equivalencia $\sim_I$, dada por

$$\pi_1 \sim_I \pi_2 \iff \text{LT}_{(\pi_1)}(I) = \text{LT}_{(\pi_2)}(I).$$

Teorema 2.8.4. *Sea $I = \langle F \rangle \subseteq \mathbb{K}[\mathbf{t}][\mathbf{x}]$ un ideal finitamente generado por $F := \{f_1, ..., f_n\}$, y $\preccurlyeq$ un orden monomial, se tiene que:*

i) La relación de equivalencia $\sim_I$ tiene un número finito de clases de equivalencia.

ii) Existe $G \in \text{CompGröb}_{\preccurlyeq}(I)$.

Demostración. i) Damos la idea de la demostración que da Weispfenning en su demostración original [11, 412 - Teorema 5]. Si G es la base de Gröbner reducida para el orden $\preccurlyeq$, entonces, dado un ideal $\pi \in \text{Spec}(\mathbb{K}[\mathbf{t}])$, el conjunto de términos principales de I respecto a π, $\text{LT}_{(\pi)}(I)$, está determinado por los términos de los elementos de G que se anulan o no por σ_π. Esto nos particiona el espacio en un conjunto finito de conjuntos constructibles, en cada cual, los términos principales de la base de Gröbner no dependen de la especialización concreta.

Por tanto, como el número de términos de los elementos de G es finito, también lo es el número de clases de equivalencia de $\sim_I$.

ii) Sean $\pi_1, ..., \pi_m$ un conjunto de representantes para las clases de equivalencia de $\sim_I$, y sean $H_i = \text{LT}_{(\pi_i)}(I)$ para todo $i \in \{1, \dots, m\}$, sus conjuntos de términos principales asociados.

Dado que los H_i son ideales monomiales, por el Lema de Dickson (2.3.1), cada H_i tiene una base finita B_i. Para cada $t \in B_i$, elegimos $f_t \in I \cap \text{LT}^{-1}_{(\pi_i)}(t)$, de manera que $G_i := \{f_t : t \in B_i\} \subseteq I$ es tal que $\text{LT}_{(\pi_i)}(G_i) = B_i$.

Entonces, la unión $G = \bigcup_{i=1}^{r} G_i \in \text{CompGröb}_{\preccurlyeq}(I)$, ya que $G \subseteq I$ y, para todo $\pi \in \text{Spec}(\mathbb{K}[\mathbf{t}])$ y todo $t \in \text{LT}_{(\pi)}(I)$, existe $i \in \{1, \dots, m\}$ con $\pi \sim_I \pi_i$, y, por tanto, existe $g \in G_i$ tal que $\text{LT}_{(\pi)}(g) = \text{LT}_{(\pi_i)}(g) \mid t \in \text{LT}_{(\pi_i)}(I)$, que por el Teorema 2.8.3 caracteriza a G como una base de Gröbner comprensiva. □

Las clases de equivalencia por $\sim_I$ y las bases B_i de esta demostración son los elementos que definen un sistema comprensivo de Gröbner.

Definición 2.8.5. Sea $I \subseteq \mathbb{K}[\mathbf{t}][\mathbf{x}] := \mathbb{K}[t_1, ..., t_m][x_1, ..., x_n]$ un ideal, definimos un **sistema comprensivo de Gröbner** de I como un conjunto de pares $\{(S_1, G_1), ..., (S_s, G_s)\}$, tal que,

1. Los $S_i \subseteq \mathbb{K}^m$ son subconjuntos constructibles del espacio de parámetros, que llamamos segmentos.

2. Los G_i son subconjuntos de $(\mathbb{K}[\mathbf{t}][\mathbf{x}])$ que especializan para cada punto $p \in S_i$ en una base de Gröbner de $\sigma_p(I)$.

3. La unión de los subconjuntos S_i abarca todo el espacio de parámetros, i.e., $\bigcup_{i=1}^{s} S_i = \mathbb{K}^m$.

Esta noción fue introducida inicialmente por Weispfenning como una representación intermedia de las bases comprensivas de Gröbner, como se aprecia en la demostración del Teorema 2.8.4. Existe una correspondencia entre los sistemas comprensivos de Gröbner y las bases comprensivas.

Los algoritmos que construyen bases comprensivas de Gröbner lo hacen construyendo sistemas comprensivos primero. En el mismo artículo en que los introdujo, Weispfenning dio un algoritmo para construir estos sistemas [10, §3].

Una serie de algoritmos fueron desarrollados posteriormente por Montes y Manubens, así como por Suzuki, Sato en 2006 y Nabeshima en 2007, y, finalmente, por Kapur, Sun y Wang en 2010, cuyo algoritmo supera al de Suzuki-Sato. Estas mejoras tienen el objetivo de reducir el número de segmentos obtenidos y hacerlos disjuntos, así como obtener un mejor rendimiento [5, §3.1].

Una refinación de los sistemas comprensivos de Gröbner son los **recubrimientos de Gröbner**, que son esencialmente sistemas comprensivos en los que los segmentos vienen dados por conjuntos paramétricos, que no definiremos.

Entre ellos, es posible definir un **recubrimiento canónico de Gröbner**, con un número mínimo de segmentos. En el caso de ideales homogéneos, los segmentos provienen de la partición de espacio de parámetros dada por las clase de equivalencia inducidas por el conjunto de términos principales del ideal bajo especialización, i.e., dos puntos a y b del espacio de parámetros están en el mismo segmento si y solo si $\operatorname{LT}(\sigma_a(I)) = \operatorname{LT}(\sigma_b(I))$.

Para ideales no homogéneos, el recubrimiento canónico de Gröbner se define a partir del de su homogeneización, introduciendo una nueva variable subordinada a todas las demás por el orden monomial.

El recubrimiento canónico se suele denominar simplemente como el recubrimiento de Gröbner de un ideal (GC por sus siglas en inglés), y tiene multitud de aplicaciones, por la información que contiene sobre la dependencia del ideal sobre los parámetros, algunas de las cuales serán exploradas en el Capítulo 3.

En el caso del recubrimiento de Gröbner, el Teorema de Wibmer asegura que los segmentos son conjuntos localmente cerrados, i.e., que pueden ser expresados como la intersección de un conjunto abierto y uno cerrado. Para la topología de Zariski, esto es equivalente a que se correspondan con la diferencia de dos conjuntos algebraicos, lo que proporciona una forma de operar algorítmicamente con estos conjuntos.

La definición rigurosa del recubrimiento de Gröbner, así como de los algoritmos que lo construyen, tratados en [5, §5], requieren definir adecuadamente el tipo de conjuntos que intervienen en su definición, así como la forma de operar con ellos algorítmicamente, que escapan al alcance de este trabajo.

Capítulo 3

Aplicaciones de las Bases de Gröbner

En este capítulo exploraremos algunas de las muchas aplicaciones de las bases de Gröbner en distintos ámbitos, incluyendo una aplicación teórica a la implicitación de conjuntos algebraicos, otra más práctica a la resolución de un problema mecánico, y finalmente una aplicación del recubrimiento de Gröbner a la deducción automática de teoremas geométricos.

3.1 Teoría de la Eliminación

La Teoría de la Eliminación estudia la eliminación de variables de sistemas de ecuaciones. En el caso de sistemas de ecuaciones polinomiales, las bases de Gröbner permiten realizar este tipo de eliminaciones.

Para ilustrar este proceso, presentamos el siguiente ejemplo.

Ejemplo 3.1.1. *Consideramos el siguiente sistema de ecuaciones:*

$$\begin{cases} x^2 + yz = 1 \\ y^2 + xz = 1 \\ z^2 + xy = 1 \end{cases} \tag{3.1}$$

Las soluciones de este sistema se corresponden con el conjunto algebraico del ideal generado por sus ecuaciones,

$$I := \langle x^2 + yz - 1, y^2 + xz - 1, z^2 + xy - 1 \rangle,$$

Si buscamos una base de Gröbner de I con respecto al orden lexicográfico $x \succ y \succ z$, observamos que en algunos de los generadores no aparece la variable x. Además, en el último solo interviene la variable z:

$$G = \{g_1, g_2, g_3, g_4\}$$

$$
\begin{aligned}
g_1 &= x + 2yz^2 - y - z \\
g_2 &= y^2 - yz - 2z^4 + 3z^2 - 1 && \in \mathbb{K}[y,z] \\
g_3 &= yz^3 - yz - z^4 + z^2 && \in \mathbb{K}[y,z] \\
g_4 &= z^5 - \frac{3}{2}z^3 + \frac{1}{2}z && \in \mathbb{K}[z],
\end{aligned}
$$

En este caso, observamos que $g_4 = \left(\frac{1}{2}z(z-1)(z+1)(2z^2-1)\right) \in \mathbb{K}[z]$*, por lo que todas las soluciones del sistema, deben tener valores de* z *que sean soluciones de* g_4*:*

$$z \in \{0, 1, -1, \sqrt{2}/2, -\sqrt{2}/2\}.$$

Una primera observación es que esta idea nos podría permitir acotar posibles valores para cada variable si obtuviéramos una base de Gröbner respecto a distintos ordenes lexicográficos.

Sin embargo, en la práctica, esta idea no es eficiente. En lugar de obtener una base para un orden distinto, podemos intentar reconstruir soluciones completas del sistema a partir de sus valores de z*.*

Dado que en los polinomios g_2 *y* g_3 *solo aparecen las variables* $\{y, z\}$*, podemos intentar determinar valores de* y *a para cada posible valor de* z*.*

Si sustituimos los valores de z*, por ejemplo,* 0*, en* g_2 *y* g_3*, obtenemos las ecuaciones*

$$
\begin{aligned}
g_2(y, 0) &= y^2 - 1 \\
g_3(y, 0) &= 0
\end{aligned}
$$

En este caso, la ecuación de g_3 *es redundante, y deducimos que* $(y, z) = (\pm 1, 0)$ *son* ***soluciones parciales*** *del sistema. Sustituyendo* $(y, z) = (1, 0)$ *en* g_1*, obtenemos que*

$$g_1(x, 1, 0) = x - 1 = 0,$$

y por tanto, $(1, 1, 0)$ *es una solución del sistema.*

Este proceso por el que hemos obtenido una solución completa del sistema a partir de una solución parcial, se denomina extensión*.*

Aplicando el mismo proceso para el resto de valores de z *y de* y*, se pueden obtener fácilmente todas las soluciones del sistema, que han sido representadas en la Figura 3.1,*

$$
\begin{gathered}
(1, 1, 0), (1, 0, 1), (0, 1, 1), (-1, -1, 0), (-1, 0, -1), (0, -1, -1) \\
(\sqrt{2}/2, \sqrt{2}/2, \sqrt{2}/2), (-\sqrt{2}/2, -\sqrt{2}/2, -\sqrt{2}/2).
\end{gathered}
$$

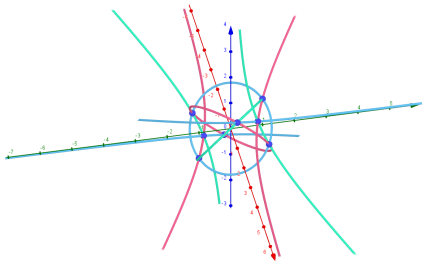


Figure 3.1: Representación gráfica de las soluciones del sistema, como cruce de los sistemas indeterminados que resultan de omitir cada una de las 3 ecuaciones

Este proceso de extensión de soluciones parece sencillo. Sin embargo, presenta algunas dificultades. Si intentamos extender la solución parcial $z = \sqrt{2}/2$, al sustituir en las ecuaciones g_2 y g_3,

$$g_2(y, \sqrt{2}/2) = y(y - \sqrt{2}/2)$$
$$g_3(y, \sqrt{2}/2) = -\sqrt{2}/4 y + 1/4$$

resulta que las ecuaciones se intercambian los papeles, pues $g_2(y, \sqrt{2}/2) = -4/\sqrt{2}y \cdot g_3(y, \sqrt{2}/2)$. Es decir, la ecuación que resulta redundante en el paso de extensión puede depender de la solución parcial.

Otro problema más importante es, que puede aparecer es que no siempre son todas las soluciones parciales extensibles a una solución completa cuando el sistema es indeterminado. Si por ejemplo consideramos el sistema dado por las ecuaciones

$$xz = 1$$
$$y^2 = z^2$$

que describen de por sí una base de Gröbner respecto a $\preceq_{lex}$, $\{xz - 1, y^2 - z^2\}$, a partir de la segunda ecuación, en la que no aparece x, se deduce que $(y, z) = (a, a)$ donde $a \in \mathbb{K}$ es una solución parcial.

Sin embargo, cuando $a = 0$, no existe ningún valor de x que satisfaga la primera ecuación, ya que se anulan todos los coeficientes.

Desde el punto de vista algebraico, este problema es esencialmente que la extensión de anillos $\mathbb{K}[y,z]/(y^2 - z^2) \subseteq \mathbb{K}[x, y, z]$ no es una extensión entera. El lema de normalización de Noether, afirma que existe un cambio de coordenadas para el cuál la extensión es entera y aplicando el Teorema del ascenso, toda solución parcial se puede extender. Si tratamos da calcular una familia normalizante de un ideal I, necesitamos calcular polinomios en $I \cap \mathbb{K}[y, z]$.

Como aparece en el Capítulo 3 de [2], el ejemplo anterior puede generalizarse como la aplicación de dos pasos, el paso de eliminación, en el que obtenemos soluciones parciales a partir de una base de Gröbner respecto a un orden lexicográfico, y el paso de extensión, en el que obtenemos soluciones completas sustituyendo las soluciones parciales en las ecuaciones del sistema. En las siguientes subsecciones expondremos los resultados teóricos que nos permiten aplicar este método.

3.1.1 Paso de Eliminación

De estos dos pasos, el paso de eliminación es el más sencillo, pues no presenta ninguna de las complicaciones que hemos visto. La idea de este paso es encontrar un ideal que sea la proyección del ideal original, eliminando una de las variables.

Definición 3.1.1. Sea $I = \langle f_1, ..., f_s \rangle \subseteq \mathbb{K}[x_1, ..., x_n]$ un ideal, el **m-ésimo ideal de eliminación**, es el ideal $I_m := I \cap \mathbb{K}[x_m, ..., x_n] \subseteq \mathbb{K}[x_m, ..., x_n]$.

Esta intersección es un ideal de $\mathbb{K}[x_m, ..., x_n]$ como consecuencia directa de la estructura de $\mathbb{K}[x_m, ..., x_n]$ como subanillo de $\mathbb{K}[x_1, ..., x_n]$. Vemos ahora como calcular ideales de eliminación.

Teorema 3.1.1 (de Eliminación)**.** *Sea $I \subseteq \mathbb{K}[x_1, ..., x_n]$ un ideal, $m \in \mathbb{N}$, y $G \in \text{GRÖB}_{\preccurlyeq}(I)$ con $\preccurlyeq$ un orden monomial que puede descomponerse como $\preccurlyeq = \preccurlyeq_1 \cdot \preccurlyeq_2$, siendo $\preccurlyeq_1$ y $\preccurlyeq_2$ órdenes monomiales sobre $\mathbb{K}[x_1, ..., x_{m-1}]$ y $\mathbb{K}[x_m, ..., x_n]$ respectivamente.*

Entonces, $G_m := G \cap \mathbb{K}[x_m, ..., x_n] \in \text{GRÖB}_{\preccurlyeq}(I_m)$, donde $\preccurlyeq$ es el orden heredado de $\mathbb{K}[x_m, ..., x_n]$.

Demostración. Dado que $G_m \subseteq I_m$, lo único que necesitamos probar es que $\text{LT}(I_m) \subseteq \langle \text{LT}(G_m) \rangle$. Sea $f \in I_m$, dado que $f \in I$, por hipótesis existe $g \in G$, tal que $\text{LT}(g) \mid \text{LT}(f)$. Dado que $f \in I_m$, sabemos que $\text{LT}(g) \in \mathbb{K}[x_m, ..., x_n]$.

Queremos ver que, de hecho, $g \in \mathbb{K}[x_m, ..., x_n]$, y aquí es donde interviene el orden. Como $\preccurlyeq = \preccurlyeq_1 \cdot \preccurlyeq_2$, y $\preccurlyeq_1$ es un orden monomial sobre $\mathbb{K}[x_1, ..., x_{m-1}]$, cualquier monomio en el que intervengan las variables $x_1, ..., x_{m-1}$ es mayor por $\preccurlyeq$ que $\text{LT}(g)$. Por tanto, todos los términos de g deben pertenecer a $\mathbb{K}[x_m, ..., x_n]$, $g \in G_m$, y $\text{LT}(f) \in \langle \text{LT}(G_m) \rangle$. □

3.1.2 Paso de Extensión

Recordamos que en el paso de extensión, solo considerábamos las ecuaciones que involucraban exactamente una variable más que en el paso anterior. Por este motivo, y dado que la demostración va a ser por inducción, estudiamos el caso del primer ideal de eliminación.

Teorema 3.1.2 (de Extensión)**.** *Sea $I \subseteq \mathbb{K}[x_1, ..., x_n]$ un ideal, con $\mathbb{K}$ un cuerpo algebraicamente cerrado, I_1 el primer ideal de eliminación de I, con $I = \langle f_1, ..., f_r \rangle$ y para todo $i \in \{1, ..., r\}$:*

$$f_i = c_i(x_2, ..., x_n)x_1^{N_i} + o(x_1^{N_i}),$$

donde $c_i \in \mathbb{K}[x_2, ..., x_n]$, y $N_i \geq 0$.

Sea $(a_2, ..., a_n) \in \mathcal{V}(I_1)$ una solución parcial. Entonces, si $(a_2, ..., a_n) \notin \mathcal{V}(c_1, ..., c_n)$, existe $a_1 \in \mathbb{K}$, tal que $(a_1, a_2, ..., a_n) \in \mathcal{V}(I)$ es una solución completa del sistema.

Este teorema no nos dice como encontrar los valores de a_1 que nos permitan extender las soluciones parciales. En el primer ejemplo de eliminación, habíamos observado como al extender una solución parcial, una de las ecuaciones se hacía redundante. En el siguiente lema veremos que esto ocurre en general. En cada paso de extensión todas las ecuaciones se pueden reducir a una.

Lema 3.1.3. *Sea $G = \{g_1, ..., g_s\} \in \text{GRÖB}_{\preccurlyeq}(I)$, con $\preccurlyeq := \preccurlyeq_{x_1} \cdot \preccurlyeq_{x_2,...,x_n}$, un producto de ordenes monomiales que permite eliminar x_1, y $a = (a_2, ..., a_n) \in \mathcal{V}(I_1)$ una solución parcial para la que no se anulan simultáneamente todos los términos principales de G respecto de x_1, i.e. tal que $a \notin \mathcal{V}(\text{LC}_{x_1}(g_1), ..., \text{LC}_{x_1}(g_s))$. Entonces, existe un generador $g_a \in G$, tal que $\pi_a(I) := \{f(x_1, a) : f \in I\} = \langle g_a(x_1, a) \rangle$, y además $\deg(g_a(x_1, a)) > 0$.*

Demostración. Dado que la evaluación parcial en a, $\pi_a : \mathbb{K}[\mathbf{x}] \longrightarrow \mathbb{K}[x_1]$ es un homomorfismo sobreyectivo, la imagen de I, $\{\pi_a(f) := f(x_1, a) : f \in I\}$, es ideal de $\mathbb{K}[x_1]$, y, además, está generado por las evaluaciones parciales de los elementos de G, $\{g_i(x_1, a) : g_i \in G\}$.

Elegimos g_a como el generador de menor grado respecto de x_1 de entre los que no se anulan por π_a, y razonamos por inducción sobre el grado en x_1 de los generadores.

Denotamos por $d_a = \deg_{x_1}(g_a)$, y consideramos $g_j \in G$. El caso base de la inducción, cuando $\deg_{x_1}(g_j) < d_a$ es trivial por elección de g_a.

Por otro lado, si $\deg_{x_1}(g_j) = d \geq d_a$, consideramos su S-polinomio con g_a, respecto a x_1:

$$S = S_{x_1}(g_j, g_a) = c_a g_j - c_j x_1^{d-d_a} g_a.$$

Dado que $\deg_{x_1}(S) < d$, $S \in I$, y el orden $\preccurlyeq$ elimina x_1, podemos expresar S como combinación de elementos $g_1, ..., g_\ell \in G$ con grado en x_1 menor que d, i.e.,

$$c_a g_j - c_j x_1^{d-d_a} g_a = \sum_{k=1}^{\ell} h_k g_k,$$

con $h_k \in \mathbb{K}[\mathbf{x}]$ y $\deg_{x_1}(g_k) < d$ para todo $k \in \{1, \dots, \ell\}$.

Entonces, por hipótesis de inducción, la imagen de estos generadores por π_a está en $\langle g_a(x_1, a)\rangle$, y, dado que $c_a \neq 0$,

$$\pi_a(g_j) = \frac{1}{c_a}\left(c_j x_1^{d-d_a}\pi_a(g_a) + \sum_{k=1}^{\ell}\pi_a(h_k)\pi_a(g_k)\right) \in \langle \pi_a(g_a)\rangle.$$

Por otro lado, suponemos por reducción al absurdo que $\deg(g_a(x_1, a)) = 0$, i.e., que $g_a(x_1, a) = c \in \mathbb{K}$. Sea h uno de los g_i tal que $\pi_a(\mathrm{LC}_{x_1}(h)) \neq 0$, es decir,

$$h = h_p(x)x_1^{N_h} + o(x_1),$$

con $h_p(a) \neq 0$, entonces $\deg_{x_1}(h) = \deg_{x_1}(\sigma(h))$, y consideramos la especialización de la resultante de h con g_a que elimina x_1, mediante los resultados conocidos de especialización de resultantes,

$$\pi_a(Res_{x_1}(h, g_a)) = h_p(a)^{N_g} Res_{x_1}(h(x_1, a), c) = h_p(a)^{N_g} c^{N_h} \neq 0,$$

lo que contradice que a sea solución parcial. □

Utilizando este lema, la demostración del Teorema de Extensión se reduce a probar que si uno de los generadores preserva el multigrado al especializar en la solución parcial, tenemos una base de Gröbner que nos permite extender la solución.

Demostración del Teorema de Extensión. Sea $G = \{g_1, ..., g_t\} \in \mathrm{GRÖB}_{\preccurlyeq}(I)$, y $a = (a_2, ..., a_n)$ una solución parcial, tal que $a \notin \mathcal{V}(\mathrm{LC}_{x_1}(G))$. Por hipótesis del Teorema de Extensión, existe un $i \in \{1, \dots, r\}$ tal que $c_i = \mathrm{LC}_{x_1}(f_i) \neq 0$.

El generador f_i se puede expresar como combinación de los generadores de G,

$$f_i = \sum_{j=1}^{s} h_j g_j,$$

luego necesariamente existe un $j \in \{1, \dots, s\}$ tal que $\mathrm{LC}_{x_1}(h_j) \neq 0$, y estamos en condiciones de aplicar el Lema 3.1.3.

Por tanto, existe un generador $g_a \in G$ tal que $\{f(x_1, a) : f \in I\} = \langle g_a(x_1, a)\rangle$. Esto implica que $\deg(g_a(x_1, a)) > 0$, y, al ser $\mathbb{K}$ algebraicamente cerrado, existe $a_1 \in \mathbb{K}$ con $g_a(a_1, a) = 0$, de manera que $(a_1, ..., a_n) \in \mathcal{V}(I)$ es solución completa del sistema. □

3.2 Implicitación

Una aplicación de la teoría de eliminación que hemos visto en la sección anterior es la implicitación de variedades algebraicas dadas en forma paramétrica. Los resultados que se exponen en esta sección están tomados de [2, §3.3].

Con el objetivo de fijar notación introducimos la siguiente definición.

Definición 3.2.1. Sean $f_1, ..., f_n \in \mathbb{K}[t_1, ..., t_m]$, consideramos la aplicación $F : \mathbb{K}^m \longrightarrow \mathbb{K}^n$ que definen:

$$F(t_1, ..., t_m) = (f_1(t_1, ..., t_m), ..., f_n(t_1, ..., t_m)),$$

y denotamos por $P_x(F)$ a la variedad de $\mathbb{K}^n$ parametrizada por $x_i = f_i(t_1, ..., t_m)$ para todo $i \in \{1, \dots, n\}$, i.e., la variedad más pequeña de $\mathbb{K}^n$ que contiene a $F(\mathbb{K}^m)$.

A una variedad descrita de esta forma la denominamos **variedad paramétrica**.

Esta relación es consecuencia de la siguiente observación.

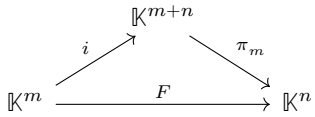
Observación 2. Sea $P = P_x(F) \subseteq \mathbb{K}[\mathbf{x}]$ una variedad paramétrica, las ecuaciones que la definen describen una variedad en $\mathbb{K}[\mathbf{t}, \mathbf{x}] := \mathbb{K}[t_1, ..., t_m, x_1, ..., x_n] \approx \mathbb{K}^{m+n}$, dada por

$$V = \mathcal{V}(x_1 - f_1, ..., x_n - f_n),$$

cuya proyección sobre $\mathbb{K}[\mathbf{x}]$, $\pi_m(V)$, es P, pues los puntos de V son de la forma

$$(t_1, ..., t_m, f_1(t_1, ..., t_m), ..., f_n(t_1, ..., t_m)).$$

Por tanto, el resultado de eliminar las primeras m variables (los parámetros) en V es una variedad en $\mathbb{K}[\mathbf{x}]$ que contiene a P, pues contiene todos los puntos para los que se puede encontrar parámetros por el Teorema de Extensión.



(3.2)

Veremos que, de hecho, la variedad resultante de eliminar los parámetros es P.

Teorema 3.2.1 (de Implicitación Polinómica)**.** *Sea $\mathbb{K}$ un cuerpo no finito, $F : \mathbb{K}^m \longrightarrow \mathbb{K}^n$ una parametrización polinómica, $I = \langle x_1 - f_1, ..., x_n - f_n \rangle \subseteq \mathbb{K}[t_1, ..., t_m, x_1, ..., x_n]$ el ideal que describe el grafo de F, e $I_m = I \cap \mathbb{K}[\mathbf{x}]$, el m-ésimo ideal de eliminación de I, entonces $\mathcal{V}(I_m)$ es la variedad más pequeña de $\mathbb{K}^n$ que contiene a $F(\mathbb{K}^m)$.*

Demostración. Para probar que $\mathcal{V}(I_m)$ es la variedad más pequeña que contiene a $F(\mathbb{K}[\mathbf{t}])$, consideramos $h \in \mathbb{K}[\mathbf{x}]$ tal que se anula en $F(\mathbb{K}^m)$, y queremos ver que $h \in I_m$. Observamos que, en $\mathbb{K}[\mathbf{t}, \mathbf{x}]$, podemos dividir h por $x_1 - f_1, ..., x_n - f_n$ utilizando algún orden monomial, obteniendo la igualdad

$$h(x_1, ..., x_n) = q_1 \cdot (x_1 - f_1) + \cdots + q_n \cdot (x_n - f_n) + r(t_1, ..., t_m).$$

Si elegimos un orden monomial $\preccurlyeq := \preccurlyeq_x \cdot \preccurlyeq_t$ tal que $\preccurlyeq_x$ y $\preccurlyeq_t$ son órdenes de $\mathbb{K}[\mathbf{x}]$ y $\mathbb{K}[\mathbf{t}]$ respectivamente, entonces, para todo $i \in \{1, \dots, n\}$ $\text{LT}(x_i - f_i) = x_i$, de manera que, dado un conjunto de parámetros $b = (b_1, ..., b_m) \in \mathbb{K}^m$, substituyendo t_i por b_i y x_i por $f_i(b)$ se deduce que

$$h(f_1(b), ..., f_n(b)) = 0 + \cdots + 0 + r(b).$$

Como h se anula en $F(\mathbb{K}^m)$, se tiene que $r(b) = 0$, para todo $b \in \mathbb{K}^m$. Al ser $\mathbb{K}$ no finito, podemos concluir que $r(t_1, ..., t_m) = 0$, por lo que

$$h(x_1, ..., x_n) = q_1 \cdot (x_1 - f_1) + \cdots + q_n \cdot (x_n - f_n) \in I \cap \mathbb{K}[\mathbf{x}] = I_m.$$

Finalmente, si $\mathcal{V}(h_1, ..., h_s)$ es una variedad de $\mathbb{K}^n$ que contiene a $F(\mathbb{K}^m)$, cada generador h_i se anula en $F(\mathbb{K}^m)$, y, por tanto, está en I_m, por lo que

$$\mathcal{V}(I_m) \subseteq \mathcal{V}(h_1, ..., h_s),$$

y concluimos que $\mathcal{V}(I_m)$ es la variedad más pequeña de $\mathbb{K}^n$ que contiene a $F(\mathbb{K}^m)$. □

Este resultado nos permite garantizar la corrección del siguiente algoritmo cuando $\mathbb{K}$ es un cuerpo no finito.

Algoritmo 3 Implicitación Polinómica

Entrada: $F : \mathbb{K}^m \longrightarrow \mathbb{K}^n$, una parametrización polinómica dada por $f_1, ..., f_n \in \mathbb{K}[\mathbf{t}]$, y $\preccurlyeq$, un orden monomial de $\mathbb{K}[\mathbf{x}]$

Salida: $G \in \text{GRÖB}_{\preccurlyeq}(V)$, una base de Gröbner de V respecto a $\preccurlyeq$, donde V es la menor variedad de $\mathbb{K}[\mathbf{x}]$ que contiene a $F(\mathbb{K}[\mathbf{t}])$

1: $I \leftarrow \langle x_1 - f_1, ..., x_n - f_n \rangle$
2: $\preccurlyeq_i \leftarrow \preccurlyeq \cdot \preccurlyeq_{lex(t_1,...,t_m)}$
3: $G_i \leftarrow B \in \text{GRÖB}_{\preccurlyeq_i}(I)$
4: $G \leftarrow G_i \cap \mathbb{K}[\mathbf{x}]$

Nótese que aquí no hemos probado que $F(\mathbb{K}^m)$ sea un conjunto algebraico, y, en particular, que $F : \mathbb{K}^m \longrightarrow \mathcal{V}(I_m)$ sea sobreyectiva.

3.3 Problema Cinemático Inverso

Otra de las aplicaciones de las bases de Gröbner estudiadas es en la resolución algebraica del problema cinemático inverso, un problema procedente del campo de la robótica, que también ha adquirido relevancia en la animación digital, y sirve como introducción a la siguiente aplicación que veremos, la deducción automática de teoremas geométricos.

En nuestro estudio nos limitaremos al análisis de este problema en brazos robóticos como los de la Figura 3.2, es decir, compuestos por una cadena de r articulaciones que unen la **base** del robot con su **mano** por medio de una serie de **piezas** rígidas, cuya posición relativa depende del estado de las articulaciones.

En este caso, el problema cinemático inverso consiste en determinar el estado que necesitan tener las articulaciones del brazo para que la mano se encuentre en una posición concreta.

Figure 3.2: Brazos robóticos en $\mathbb{R}^2$ con 4 y 7 articulaciones.

Una forma de modelar este problema es considerando un sistema de coordenadas reales afín, $(o_i; x_i, y_i, ...)$ en cada articulación, donde o_i denota la posición de la articulación, y $x_i, y_i, ...$ son vectores unitarios, de manera que la primera coordenada, x_i, siempre la tomamos en la dirección de la pieza conectada a dicha articulación. También denotamos por $(0; x_0, y_0, ...)$ el sistema de coordenadas respecto a la base del robot. La figura 3.3 muestra estos sistemas de referencia en el caso de un robot con 3 articulaciones en $\mathbb{R}^2$.

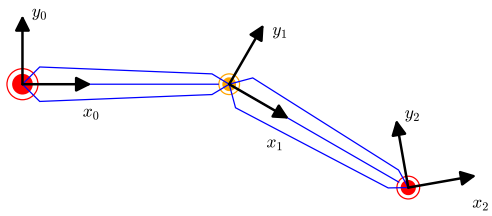


Figure 3.3: Bases afines asociadas a articulaciones de un brazo robótico.

Entonces, podemos definir por cada articulación una aplicación afín en $\mathbb{R}^n$ parametrizada por un conjunto P_i, i.e., $f_i : P_i \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$, que realice el cambio afín de coordenadas entre su sistema de coordenadas y el anterior, es decir, funciones, por ahora continuas, $f_1, ..., f_r$ donde para todo $p \in P_i$, la restricción $f_{i_p} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$, dada por $f_{i_p}(x) = f_i(p, x)$ es una aplicación afín.

Definición 3.3.1. Llamamos **espacio de articulación** del robot al producto de los espacios de parámetros de sus articulaciones, y lo denotamos por $\mathcal{A} := P_1 \times \cdots \times P_n$.

Por otro lado, denotamos por $\mathcal{O} \subseteq \mathbb{R}^n$ al **espacio operacional** del robot, el conjunto de posibles posiciones de la mano del robot [2, p. 294].

De este modo, el problema se reduce a estudiar la función $f : \mathcal{A} \longrightarrow \mathcal{O}$, que asigna a cada configuración de las articulaciones la posición de la mano. Este problema se denomina inverso porque la respuesta a la pregunta en sentido contrario es la más natural y tiene respuesta única, el resultado de evaluar f.

Con las definiciones anteriores, la evaluación de f solo requiere, interpretando la mano del robot como la última articulación, componer las transformaciones afines, $f := f_1 \circ \cdots \circ f_r$, y evaluar f en el origen, i.e., la posición de la mano respecto a su propio sistema de referencia, para obtener la posición de la mano en el sistema de coordenadas de la base del robot.

El problema inverso, sin embargo, requiere resolver un sistema de ecuaciones, que en general podría no ser polinomial, ya que no hemos impuesto aún condiciones sobre las transformaciones f_i. Para estudiar que tipo de condiciones podemos pedir a las articulaciones, planteamos un ejemplo.

Ejemplo 3.3.1. *Una de las articulaciones más sencillas de imaginar es, en $\mathbb{R}^2$, un eje de rotación en el que un parámetro $\theta \in S_1(-\pi, \pi]$ controla la rotación relativa de la articulación siguiente.*

La transformación afín que determina la posición de la siguiente articulación también depende de la forma de la pieza sobre la que se encuentra la articulación. Si asumimos que esta pieza es un segmento de longitud fija, l_1, podemos escribir la transformación f_1 como composición de un giro y una traslación, que en forma matricial resulta en

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ l_1 & \cos\theta_1 & -\operatorname{sen}\theta_1 \\ 0 & \operatorname{sen}\theta_1 & \cos\theta_1 \end{pmatrix}.$$

De manera que, si la posición de la mano en el sistema de referencia de la siguiente articulación es (x_2, y_2), su posición en el de esta articulación, que se corresponde con el de la base en caso de ser la primera, viene dada por

$$\begin{pmatrix} 1 \\ x_1 \\ y_1 \end{pmatrix} = A_1 \begin{pmatrix} 1 \\ x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 \\ \cos(\theta_1)\, x_2 - \operatorname{sen}(\theta_1)\, y_2 + l_1 \\ \operatorname{sen}(\theta_1)\, x_2 + \cos(\theta_1)\, y_2 \end{pmatrix}.$$

Otro tipo de articulación sencilla es una longitudinal, que permite controlar la longitud del segmento descrito anteriormente. Para considerar este caso, basta con tomar l_1 como un parámetro más, i.e., tomando $l_1 \in [l_1^-, l_1^+] \subseteq \mathbb{R}_+$, y $S_1 = (-\pi, \pi] \times [l_1^-, l_1^+]$.

Si denotamos por A_i la matriz de transformación de la aplicación i-ésima, f_i, como en el Ejemplo 3.3.1, la expresión de f, i.e., la respuesta al problema cinemático directo es

$$\begin{pmatrix} 1 \\ \mathbf{x}_0 \end{pmatrix} = A_n \cdots A_1 \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix},$$

donde $\mathbf{x}_0$ son las coordenadas de la mano en el sistema de referencia de la base, y $\mathbf{0}$ es el vector 0.

Si consideramos un robot con una única articulación como la del Ejemplo 3.3.1, además de la mano, que solo realiza una traslación afín de longitud l_2 en el eje x_2, el problema inverso requiere resolver un sistema trigonométrico,

$$\begin{cases} l_1 + \cos(\theta_1)\, l_2 - m_1 = 0 \\ \operatorname{sen}(\theta_1)\, l_2 - m_2 = 0 \end{cases},$$

donde m_1, m_2 son las coordenadas de la mano que queremos alcanzar.

Una forma de evitar este problema es sustituyendo $\operatorname{sen}(\theta_1)$ y $\cos(\theta_1)$ por nuevas variables, s_1 y c_1, y tomando como espacio de parámetros $S_1 = \mathbb{S}^1 \subseteq \mathbb{R}^2$.

A pesar de que esto parece complicar la búsqueda de parámetros, dado que S_1 es un conjunto algebraico, ahora el problema ha pasado de resolver una ecuación trigonométrica a resolver un sistema de ecuaciones polinomiales, si bien involucrando más ecuaciones,

$$\begin{cases} l_1 + c_1 l_2 - m_1 = 0 \\ s_1 l_2 - m_2 = 0 \\ c_1^2 + s_1^2 - 1 = 0 \end{cases}$$

La ventaja de este cambio, es que ahora podemos aplicar resultados vistos en el Capítulo 3.1, y resolver el sistema calculando una base de Gröbner del ideal generado por las ecuaciones.

Por este motivo, reformulamos nuestro problema, definiendo las transformaciones $f_1, ..., f_r$ como vectores de un $\mathbb{K}[\mathbf{t}_i][\mathbf{x}]$-módulo libre de dimensión n, asociados a una serie de conjuntos algebraicos $V_1, ..., V_r$, con $V_i = \mathcal{V}(I_i)$ e $I_i \subseteq \mathbb{K}[\mathbf{t}_i]$, que restringen los posibles valores de los parámetros $\mathbf{t}_i$. Si queremos preservar la propiedad de que las transformaciones sean afines, podemos limitar el multigrado de los polinomios sobre $\mathbf{x}$ a grados con valor absoluto 1 en $\mathbb{N}^n$.

Ejemplo 3.3.2. *En estas condiciones, una articulación que permita realizar una rotación libre en $\mathbb{R}^3$, denominada como* rótula esférica*, se podría expresar sencillamente como*

$$f_i = \begin{pmatrix} t_{11}x_1 + t_{12}x_2 + (t_{21}t_{32} - t_{22}t_{31})x_3 + l \\ t_{21}x_1 + t_{22}x_2 + (t_{31}t_{12} - t_{32}t_{11})x_3 \\ t_{31}x_1 + t_{32}x_2 + (t_{11}t_{22} - t_{12}t_{21})x_3 \end{pmatrix}, \qquad V_i = \begin{cases} t_{11}^2 + t_{21}^2 + t_{31}^2 - 1 = 0 \\ t_{12}^2 + t_{22}^2 + t_{32}^2 - 1 = 0 \\ t_{11}t_{12} + t_{21}t_{22} + t_{31}t_{32} = 0 \end{cases}$$

donde hemos asumido de nuevo que la pieza sobre la que se encuentra la articulación es un segmento de longitud l en el eje x_1 del sistema de referencia de la articulación anterior. Las ecuaciones de V_i describen las condiciones para que la aplicación lineal asociada sea una isometría directa arbitraria, es decir, preserve la ortogonalidad, norma y orientación de la base.

Dado que el ideal que describe el sistema involucra a la posición de la mano como parámetro, si queremos poder resolver el problema calculando una única base de Gröbner, es necesario determinar una base de Gröbner comprensiva respecto de los parámetros que describen la posición de la mano (a y b en ejemplos anteriores).

Esta forma de resolver el problema tiene la ventaja de que, una vez calculada la base comprensiva asociada al robot, podemos determinar todas las posibles configuraciones de las articulaciones aplicando el proceso de eliminación y extensión de soluciones.

De hecho, este enfoque también nos permite resolver el problema no solo para una posición concreta de la mano, sino también para una curva que describa su trayectoria, siempre y cuando esta pueda darse por una curva algebraica, es decir, un conjunto algebraico de dimensión 1.

El problema más general de planificar estas trayectorias, potencialmente evitando colisiones, es considerablemente más complejo, particularmente en su formulación algebraica, por lo que en la práctica no es de mucha utilidad resolverlo de esta manera.

3.4 Deducción Automática de Teoremas Geométricos

Una aplicación más reciente de las bases de Gröbner es a la Deducción Automática de Teoremas Geométricos (ADGT por sus siglas en inglés), tratada por Montes en [5], donde se discuten en mayor profundidad los aspectos algorítmicos que la hacen efectivamente automática.

La idea detrás de esta técnica es en ciertos aspectos similar a la resolución del problema cinemático inverso que hemos estudiado en la sección anterior. En perspectiva, un robot no es más que una construcción geométrica muy concreta, y la resolución del problema cinemático inverso constituye en cierto modo una forma de demostrar que el robot es capaz de satisfacer una propiedad geométrica.

Si, en lugar de trabajar con robots articulados, consideramos construcciones geométricas arbitrarias que dependan de una serie de parámetros libres, la búsqueda de una base de Gröbner comprensiva nos puede dar información sobre la satisfactibilidad de tesis geométricas sobre la construcción.

No obstante, en este caso nos interesa analizar directamente el sistema comprensivo de Gröbner que define la base (Definición 2.8.5), ya que nos proporciona una partición del espacio de parámetros en segmentos en los que la base de Gröbner, y, por tanto, el tipo de soluciones del sistema es uniforme.

En particular, el recubrimiento de Gröbner, por su minimalidad en el número de segmentos, es la herramienta más útil en esta situación, ya que nos permite reducir el estudio al menor número posible de casos distintos en el comportamiento de la construcción.

Esta aplicación del recubrimiento de Gröbner a la Deducción Automática de Teoremas Geométricos fue introducida por A. Montes y T. Recio en [6], donde demuestran la generalización del Teorema de Steiner-Lehmus, que proporciona condiciones necesarias y suficientes para que dos bisectrices de un triángulo tengan la misma longitud.

3.4.1 Deducción Automática del Teorema del Arco Capaz

En esta sección no vamos a dar definiciones generales ni resultados teóricos, sino que ilustraremos esta técnica con un ejemplo original, dando una demostración algebraica del Teorema del Arco Capaz, que enunciamos a continuación.

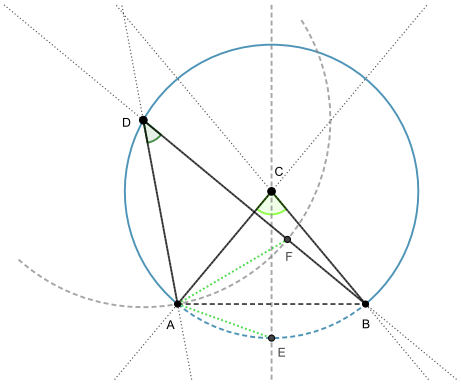


Figure 3.4: Construcción del Teorema 3.4.1

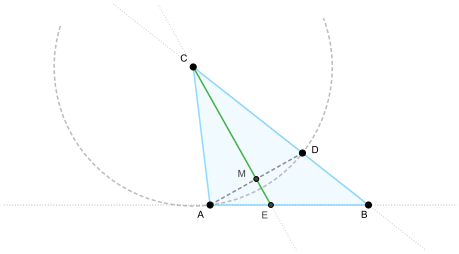


Figure 3.5: Construcción de la Sección 3.5.1

Teorema 3.4.1. *Todo ángulo inscrito en una circunferencia es igual a la mitad del ángulo central que comprende el mismo arco, i.e., si $\overline{AB}$ es un arco de una circunferencia c con centro en C, y $D \in c$ es un punto arbitrario de c que no esté en el arco comprendido entre A y B, $\widehat{ACB}$, entonces $\angle ACB = 2\angle ADB$.*

Para demostrar este teorema algebraicamente, debemos enunciarlo en tales términos, usando la construcción de la Figura 3.4 Sin pérdida de generalidad, podemos suponer que $A = (-1, 0)$ y $B = (1, 0)$, y que $C = (0, c_y)$, para algún $c_y \in \mathbb{R}$, ya que el centro de la circunferencia debe estar sobre la mediatriz m del segmento $\overline{AB}$.

El único objeto que falta por introducir es D. Al igual que ocurría en la formulación del problema cinemático inverso, dado que las funciones trigonométricas no son algebraicas, nos vemos obligados a introducir dos nuevas variables, d_x y d_y, y definir D como (d_x, d_y), un punto a priori arbitrario.

La hipótesis $D \in c$ del teorema, puede formularse entonces como la ecuación

$$(d_x - 0)^2 + (d_y - c_y)^2 - (0 - 1)^2 - (c_y - 0)^2 = 0.$$

Por otro lado, para expresar la tesis, $\angle ACB = 2\angle ADB$, existen varias posibilidades:

i) Expresar la relación entre los ángulos a partir de sus senos y cosenos, utilizando las igualdades trigonométricas

$$\begin{aligned} \operatorname{sen}(\angle ACB) &= 2\operatorname{sen}(\angle ADB)\cos(\angle ADB) \\ \cos(\angle ACB) &= \cos(\angle ADB)^2 - \operatorname{sen}(\angle ADB)^2 \end{aligned}$$

ii) Definir la bisectriz de $\angle ACB$, y probar que la mitad del ángulo $\angle ACB$ es igual al ángulo $\angle ADB$.

La primera opción es más general, en el sentido de que permite expresar cualquier relación entre ángulos dada por igualdades trigonométricas, pero la segunda requiere introducir menos variables, por lo que será la que utilizaremos. Para ello, introducimos un punto $E = (0, e_y)$, tal que $E \in c$ y $E \in m$. La condición $E \in m$ se cumple al fijar E sobre el eje y, mientras que la condición $E \in c$ es

$$(0 - 0)^2 + (e_y - c_y)^2 - (0 - 1)^2 - (c_y - 0)^2 = 0.$$

Observamos que esta condición no es suficiente para determinar E de forma única, la bisectriz no distingue entre el ángulo $\angle ACB$ y el ángulo $\angle BCA$.

Por otro lado, para comparar los ángulos $\angle ACE$ y $\angle ADB$, la opción más sencilla es comparar la razón entre la cuerda que describe cada ángulo en una circunferencia y el radio de dicha circunferencia, ya que en el caso de $\angle ACE$, conocemos tanto la cuerda como el radio, y en el caso de $\angle ADB$, podemos tomar una circunferencia d, con centro en D y radio $\|\overline{AD}\|$, que solo nos requiere introducir una nueva variable.

Introducimos un punto $F \in BD \cap d$, que podemos definir con una única variable, f, aprovechando que $F \in BD$,

$$F = (1 + f(d_x - 1), 0 + f(d_y - 0)),$$

de modo que la hipótesis $F \in d$ se traduce en la ecuación

$$(1 + f(d_x - 1) - d_x)^2 + (0 + f(d_y - 0) - d_y)^2 - (d_x + 1)^2 - (d_y - 0)^2 = 0.$$

Al igual que en el caso de D, estas condiciones no determinan F de forma única, ya que la intersección $BD \cap d$ contiene dos puntos.

En estas condiciones, la tesis de nuestro teorema se traduce en la ecuación $\frac{\|\overline{AE}\|}{\|\overline{CA}\|} = \frac{\|\overline{AF}\|}{\|\overline{DA}\|}$, que, en términos de las variables introducidas, podemos escribir como

$$(1^2 + e_y^2)((d_x + 1)^2 + d_y^2) - ((1 + f(d_x - 1) + 1)^2 + (fd_y)^2)(1^2 + c_y^2) = 0$$

Llegados a este punto, tenemos un sistema de ecuaciones H, que describe nuestras hipótesis, y otro sistema T que describe la tesis:

$$H : \begin{cases} d_x^2 + (d_y - c_y)^2 - 1 - c_y^2 = 0 \\ (e_y - c_y)^2 - 1 - c_y^2 = 0 \\ (1 + f(d_x - 1) - d_x)^2 + (fd_y - d_y)^2 - (d_x + 1)^2 - d_y^2 = 0 \end{cases},$$
$$T : (1^2 + e_y^2)((d_x + 1)^2 + d_y^2) - ((1 + f(d_x - 1) + 1)^2 + (fd_y)^2)(1^2 + c_y^2) = 0$$

Queremos ver entonces, qué condiciones sobre c_y, d_x y d_y, los parámetros de los que depende toda la construcción, son necesarias para que $H \Rightarrow T$.

Para ello, consideramos el conjunto de ecuaciones total, $H + T$, y el ideal que generan sobre $\mathbb{R}[c_y, d_x, d_y][e_y, f]$, si bien en la práctica los cálculos requieren trabajar sobre $\mathbb{C}$ y restringir nuestro estudio posterior al caso en el que $c_x, d_x, d_y \in \mathbb{R}$.

Podemos determinar el recubrimiento de Gröbner de este ideal utilizando los algoritmos proporcionados por `grobcov.lib` [7] en el sistema algebraico computacional Singular [3].

Esta implementación permite restringir los segmentos del espacio de parámetros a una variedad o a su complementario utilizando las opciones `"null"` y `"nonnull"` respectivamente.

Esto permite en muchos casos reducir el número de segmentos, descartando aquellos en los que la construcción no es relevante o es degenerada. Por ejemplo, en el caso de nuestro teorema, no nos interesan los casos en los que $D \in AB$, pues la construcción se vuelve degenerada. Es decir, podemos considerar que tenemos una hipótesis negativa $d_y \neq 0$, e ignorar la intersección de nuestros segmentos con la variedad $\mathcal{V}(d_y)$. Aunque, si no lo hiciéramos el recubrimiento de Gröbner nos permitiría detectar que es un caso especial.

```
LIB "grobcov.lib";
ring R = (0, c_y, d_x, d_y), (e_y, f), lp;
ideal IArcoCapaz =
    (d_x - 0)^2 + (d_y - c_y)^2 - (1 - 0)^2 - (c_y - 0)^2,
    (0 - 0)^2 + (e_y - c_y)^2 - (1 - 0)^2 - (c_y - 0)^2,
    (1 + f*(d_x - 1) - d_x)^2 + (f*d_y - d_y)^2
      - (d_x + 1)^2 - (d_y - 0)^2,
    ((0 + 1)^2 + (e_y - 0)^2)*((d_x + 1)^2 + (d_y - 0)^2)
      - ((1 + f*(d_x - 1) + 1)^2 + (f*d_y - 0)^2)
        * ((0 + 1)^2 + (c_y - 0)^2);
grobcov(IArcoCapaz, "nonnull", d_y, "ext", 1);
```

El GC resultante contiene 6 segmentos, en cuya definición aparecen 12 conjuntos algebraicos, cuya interpretación real se muestra en la Tabla 3.1.

Variedad	Interpretación real
$V_1 = \mathcal{V}(2c_y d_y - d_x^2 - d_y^2 + 1)$	$D \in c$
$V_2 = \mathcal{V}(d_y)$	$d_y = 0$
$V_3 = \mathcal{V}(d_x + 1, d_y)$	$D = (-1, 0)$
$V_4 = \mathcal{V}(d_x - 1, d_y)$	$D = (1, 0)$
$V_5 = \mathcal{V}((d_x - 1)^2 + d_y^2,$ $c_y d_y - d_x + 1,$ $c_y d_x - c_y + d_y,$ $c_y^2 + 1)$	$D = (1, 0)$ $C \notin \mathbb{R}^2$
$V_6 = \mathcal{V}((d_x + 1)^2 + d_y^2,$ $c_y d_y + d_x + 1,$ $c_y d_x + c_y - d_y,$ $c_y^2 + 1)$	$D = (-1, 0)$ $C \notin \mathbb{R}^2$
$V_7 = \mathcal{V}(d_x^2 + d_y^2 - 1, c_y)$	$D \in \mathbb{S}^1$ $C = (0, 0)$
$V_8 = \mathcal{V}(d_x - 1, d_y, c_y^2 + 1)$	$D = (1, 0)$ $C \notin \mathbb{R}^2$
$V_9 = \mathcal{V}(d_x, d_y^2 + 1, c_y - d_y)$	$C = D \notin \mathbb{R}^2$
$V_{10} = \mathcal{V}(d_x + 1, d_y, c_y^2 + 1)$	$D = (-1, 0)$ $C \notin \mathbb{R}^2$
$V_{11} = \mathcal{V}(d_x - 1, d_y, c_y)$	$D = (1, 0)$ $C = (0, 0)$
$V_{12} = \mathcal{V}(d_x + 1, d_y, c_y)$	$D = (-1, 0)$ $C = (0, 0)$

Table 3.1: Variedades que aparecen en el recubrimiento de Gröbner del Teorema del Arco Capaz

De estos 5 segmentos, solo 3 se corresponden con configuraciones reales. Presentamos estos segmentos en la Tabla 3.2.

Índice	Segmento	Interpretación real	LM (G_i)
1	$\mathbb{R}^2 \setminus (V_1 \cup V_2)$	$D \notin c \vee D \in \overline{AB}$	$\{1\}$
2	$V_1 \setminus (V_3 \cup V_4 \cup V_5 \cup V_6 \cup V_7)$	$D \in c$ $D \neq A$, $D \neq B$, $C \neq (0,0)$	$\{f^2, e_y\}$
3	$V_5 \setminus (V_8 \cup V_9)$	Sin interpretación real	$\{1\}$
4	V_9	Sin interpretación real	$\{e_y^2\}$
5	$(V_7 \setminus (V_{11} \cup V_{12})) \cup (V_6 \setminus (V_{10} \cup V_9))$	$C = (0,0)$, $D \in c$ $D \neq A$, $D \neq B$	$\{f^2, e_y^2\}$

Table 3.2: Segmentos del recubrimiento de Gröbner del Teorema del Arco Capaz

Como vemos, el único segmento con interpretación real en el que el conjunto algebraico asociado al ideal formado por la hipótesis y la tesis es vacío, es el primero, en el que el ideal es $\langle 1 \rangle$. Diremos que este segmento no es compatible con la tesis del teorema. Además, este segmento se corresponde con los casos en los que fallan nuestras hipótesis, ya sea porque $D \notin c$ o porque $d_y = 0$.

Los otros dos segmentos reales, 2 y 5, se corresponden respectivamente con el caso en el que $C \neq (0,0)$ y $C = (0,0)$.

Interpretación Geométrica

En la construcción algebraica que hemos utilizado, no hemos distinguido entre los ángulos $\angle ABC$ y $\angle BCA$, ni entre el ángulo $\angle ADB$ y su suplementario.

Esto permite que existan varias interpretaciones de la construcción geométrica en cada segmento del recubrimiento. Por continuidad, el tipo de soluciones dentro de cada componente arco-conexa de cada conjunto algebraico será constante, por lo que, para estudiar el tipo de las soluciones en cada región, solo es necesario hacerlo para uno de sus puntos.

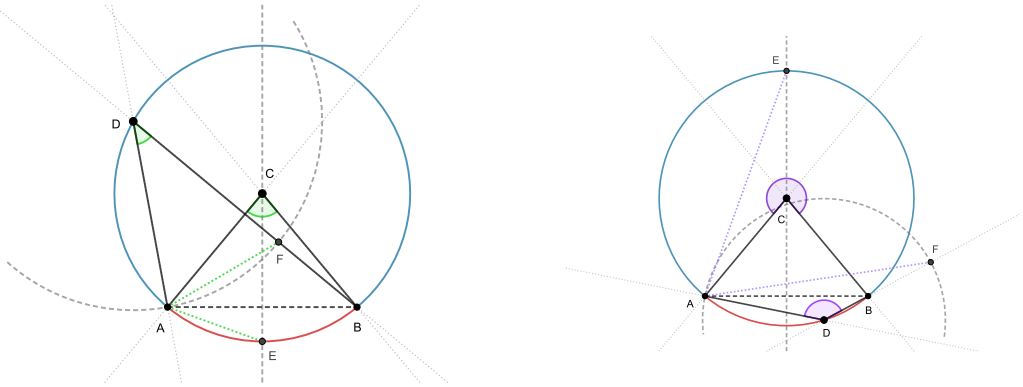


Figure 3.6: Regiones de la variedad V_1 con el mismo tipo de soluciones cuando $c_y > 0$.

En la Figura 3.6 se muestran las dos regiones de la variedad V_1 con interpretaciones distintas cuando $c_y > 0$. Cuando D está en el mismo semiplano generado por el arco que C, se tiene la

igualdad $\angle ACB = 2\angle ADB$, mientras que cuando D se encuentra en el semiplano opuesto, la igualdad es $\angle BCA = 2\angle BDA$, tomando el ángulo exterior al arco en C.

Los casos con $c_y < 0$ se corresponden a la construcción simétrica, y tienen las mismas interpretaciones. Por otro lado, el caso en que $c_y = 0$ (segmento 6) se corresponde con el Teorema de Tales, como se muestra en la Figura 3.7.

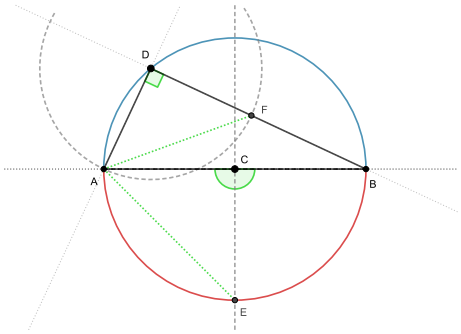


Figure 3.7: Caso degenerado del teorema, cuando $C = (0, 0)$

En general, cualquier construcción geométrica que solo involucre conjuntos algebraicos, entre las que se incluyen todas las construcciones de regla y compás, puede formularse como un ideal de la forma que hemos visto.

Si una propiedad sobre dicha construcción también puede expresarse como un ideal, por ejemplo, si es una igualdad de distancias, calculando el recubrimiento de Gröbner del ideal asociado al conjunto completo de hipótesis y tesis podemos comprobar que todos los segmentos no compatibles con la tesis, no intersecan al conjunto descrito por las hipótesis sobre los parámetros.

Algorítmicamente, estos segmentos son aquellos cuya base de Gröbner en el recubrimiento es $\{1\}$, por lo que es fácil identificarlos. Sin embargo, al igual que con el algoritmo para determinar el recubrimiento de Gröbner de un ideal, la comprobación algorítmica de que estos segmentos no intersecan al conjunto descrito por las hipótesis requiere definir una forma apropiada de representar y operar con los conjuntos involucrados, denominados conjuntos constructibles, como se describe en el Capítulo 2 de [5], y por tanto no entraremos en detalles sobre la formulación algorítmica completa del método.

Observación 3. El hecho de que el segmento 1 de la Tabla 3.2 sea el único en el que la construcción no admite solución verificando la tesis no constituye una demostración de la implicación recíproca, es decir, que $\angle ACB = 2\angle ADB$ implique $D \in c$, ya que el ideal del que hemos calculado el recubrimiento de Gröbner ya está contenido en V_1.

Dicho de otro modo, este método no distingue realmente entre hipótesis y tesis. Pueden existir otras especializaciones de los parámetros que verifiquen la tesis pero fallen en alguna de las hipótesis. En este contexto, la diferencia entre tesis e hipótesis es una cuestión puramente relativa a la interpretación del teorema.

Si quisiéramos probar el recíproco, tendríamos que eliminar la ecuación asociada a la hipótesis $D \in c$ del ideal, y comprobar que ningún segmento no contenido en V_1 es compatible con la tesis, y, al hacerlo observaríamos que, de hecho, existe otro conjunto de puntos que verifican la tesis, los correspondientes a la reflexión de c respecto del eje x, como se muestra en la Figura 3.8.

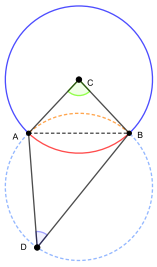


Figure 3.8

Esta idea de eliminar hipótesis para comprobar si son necesarias se puede formular de manera más general.

3.5 Descubrimiento de Hipótesis Adicionales

Como hemos visto, estamos interesados en estudiar implicaciones geométricas de la forma

$$H \Rightarrow T$$

donde H son las ecuaciones que describen una figura que depende de una serie de parámetros, y T es una propiedad que queremos demostrar sobre dicha figura.

En el ejemplo anterior, las hipótesis eran suficientes para demostrar la tesis. No obstante, vimos como al eliminar la hipótesis $D \in c$ del ideal, permitiendo que D pueda ser un punto arbitrario, el recubrimiento de Gröbner nos permitía encontrar el conjunto de todos los puntos D que satisfacían el problema.

En general, dada una construcción geométrica y una tesis, aún si las hipótesis no son suficientes para demostrar la tesis, el recubrimiento de Gröbner nos permite determinar algorítmicamente un conjunto de hipótesis adicionales sobre los parámetros, que sí sean suficientes, y sean necesarias respecto a las hipótesis que fijamos.

Una vez obtenido el recubrimiento de Gröbner, G, solo es necesario tomar la unión de los segmentos con bases de Gröbner no triviales, i.e., $S := \bigcup \{S_i : \text{LM}(G_i) \neq \{1\}\}$.

3.5.1 Búsqueda de Hipótesis para un Resultado Geométrico

En esta sección, vamos a ilustrar esta forma de descubrir hipótesis adicionales con un ejemplo concreto. Queremos encontrar condiciones necesarias y suficientes para que una de las bisectrices de un triángulo tenga la misma longitud que su lado opuesto.

En este caso, la construcción geométrica está formada por un triángulo, ABC, y su bisectriz, que aparecen representados en la Figura 3.5. Sin pérdida de generalidad podemos tomar $A = (-1, 0)$, $B = (1, 0)$ y $C = (c_x, c_y)$.

Dado que podemos elegir cualquiera de los lados, tomamos el lado AB, cuya longitud es fija, y su bisectriz. Para construir esta bisectriz, consideramos una circunferencia, c, de centro C y su intersección con los segmentos $\overline{AC}$ y $\overline{BC}$.

Dado que el radio de la circunferencia es libre, podemos tomarlo como $\|\overline{AC}\|$, eliminando la necesidad de introducir variables adicionales.

Consideramos entonces $D = (d_x, d_y) \in c \cap BC$, y el punto medio de A y D, $M = \left(\frac{d_x-1}{2}, \frac{d_y}{2}\right)$, así como el punto de corte de la bisectriz, CM, con AB, $E = (e_x, 0)$.

Las condiciones sobre D y E forman entonces un sistema de ecuaciones en $\mathbb{R}[c_x, c_y][d_x, d_y, e_x]$,

$$H : \begin{cases} (d_x - c_x)^2 + (d_y - c_y)^2 - (-1 - c_x)^2 - (0 - c_y)^2 = 0 \\ (d_x - 1)(c_y - 0) - (d_y - 0)(c_x - 1) = 0 \\ (e_x - c_x)\left(\frac{d_y}{2} - c_y\right) - (0 - c_y)\left(\frac{d_x - 1}{2} - c_x\right) = 0 \end{cases},$$

y, la tesis es $T : (c_x - e_x)^2 + (c_y - 0)^2 - 2^2 = 0$.

En este caso, el recubrimiento de Gröbner del ideal resulta en 4 segmentos, en cuya definición intervienen los siguientes conjuntos algebraicos:

Variedad	Interpretación real
$V_1 = \mathcal{V}(c_x^4 c_y^2 - 4c_x^4 + 2c_x^2 c_y^4 - 10c_x^2 c_y^2 + 24c_x^2 + c_y^6 - 2c_y^4 - 7c_y^2 - 4)$	Séxtica (irreducible sobre $\mathbb{Q}$)
$V_2 = \mathcal{V}(c_y)$	$C \in AB$
$V_3 = \mathcal{V}((c_x - 1)^2 - 2, c_y)$	$C = (\pm\sqrt{2} + 1, 0)$
$V_4 = \mathcal{V}((c_x + 1)^2 - 2, c_y)$	$C = (\pm\sqrt{2} - 1, 0)$
$V_5 = \mathcal{V}(c_x^2 - 3, c_y^2 - 2)$	$C = (\pm\sqrt{3}, \pm\sqrt{2}) \vee C = (\pm\sqrt{3}, \mp\sqrt{2})$
$V_6 = \mathcal{V}(c_x, c_y^2 + 1)$	$C \notin \mathbb{R}^2$

Table 3.3: Conjuntos algebraicos de la construcción geométrica

En este caso, no hay ningún segmento vacío en $\mathbb{R}$.

Índice	Segmento	Interpretación real	$\text{LM}(G_i)$
1	$\mathbb{R}^2 \setminus (V_1 \cup V_2)$	$C \notin V_1 \vee C \notin AB$	$\{1\}$
2	$V_1 \setminus (V_3 \cup V_4 \cup V_5 \cup V_6)$	$C \in V_1$ $C \neq (\pm\sqrt{2} + 1, 0)$, $C \neq (\pm\sqrt{2} - 1, 0)$ $C \neq (\pm\sqrt{3}, \pm\sqrt{2})$, $C \neq (\pm\sqrt{3}, \mp\sqrt{2})$	$\{e_x, d_y, d_x\}$
3	V_2	$C \in AB$	$\{e_x^2, d_y, d_x^2\}$
4	$V_5 \cup V_6$	$C = (\pm\sqrt{3}, \pm\sqrt{2}) \vee C = (\pm\sqrt{3}, \mp\sqrt{2})$	$\{e_x^2, d_y, d_x\}$

Table 3.4: Segmentos del recubrimiento de Gröbner de la construcción

El único segmento con $\text{LM}(G_i) = \{1\}$ es el primero. No obstante, observamos que el tercer segmento se corresponde con el caso degenerado, $C \in AB$, en el que la bisectriz no está definida, y que tampoco nos interesa.

Por tanto, las condiciones necesarias y suficientes para que la bisectriz de $\angle ABC$ tenga la misma longitud que el segmento $\overline{AB}$, son:

$$\begin{cases} C \in V_1 \\ C \notin AB \end{cases}.$$

Además, observamos que la curva V_1 tiene cuatro puntos especiales, $(\pm\sqrt{3}, \pm\sqrt{2})$ y $(\pm\sqrt{3}, \mp\sqrt{2})$, en los que la longitud de ambas bisectrices coincide con la longitud del segmento $\overline{AB}$. Estos 4 puntos dividen la curva en 10 regiones, en las que las soluciones tienen carácter constante por continuidad.

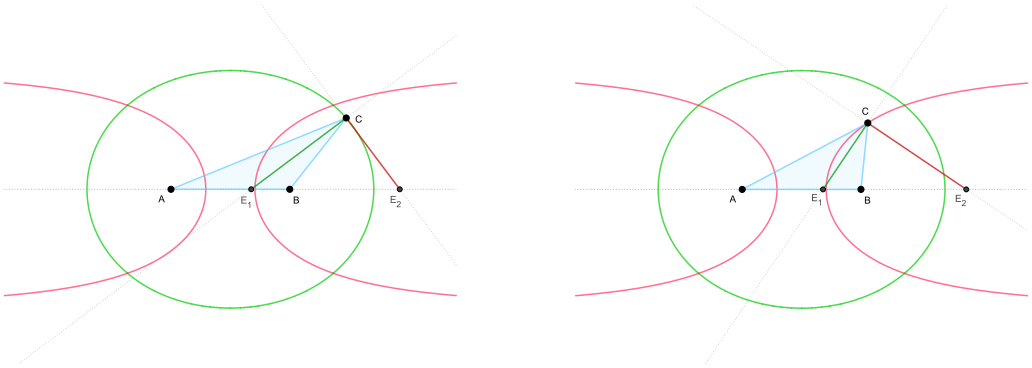


Figure 3.9: Regiones de la variedad V_1 con el mismo tipo de soluciones.

En la Figura 3.9, se han representado en verde las regiones de la curva que se corresponden a construcciones en las que la bisectriz interior coincide con el lado, y en rojo en las que es la bisectriz exterior la que coincide.

Las variedades V_3 y V_4 son las intersecciones de V_1 con AB, en las que la bisectriz coincide con el lado, y el teorema carece por tanto de interpretación.

Teorema 3.5.1. *Los únicos triángulos tales que uno de sus lados es igual a una de las bisectrices de su vértice opuesto son semejantes a un triángulo ABC con $A = (-1, 0)$, $B = (1, 0)$ y $C \in V_1 \setminus AB$, donde V_1 es la séxtica dada por*

$$V_1 = \mathcal{V}(x^4y^2 - 4x^4 + 2x^2y^4 - 10x^2y^2 + 24x^2 + y^6 - 2y^4 - 7y^2 - 4).$$

Si bien la expresión de la séxtica resultante es bastante compleja, el caso particular de V_5 nos permite enunciar un resultado algo más elegante, con unicidad salvo semejanzas.

Corolario 3.5.1.1. *El único triángulo salvo semejanzas tal que uno de sus lados es igual a las dos bisectrices de su vértice opuesto tiene lados con longitudes 2 y $\sqrt{\left(\sqrt{3} \pm 1\right)^2 + 2}$. (Figura 3.10)*

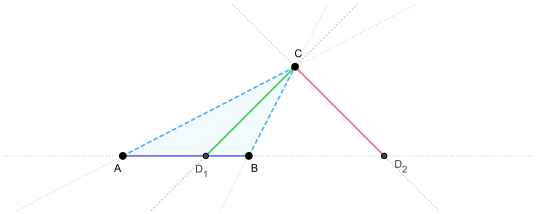


Figure 3.10: Triángulo descrito por el Corolario 3.5.1.1

Algorítmicamente, esta búsqueda de hipótesis adicionales se reduce a determinar la unión de los segmentos compatibles con la tesis, es decir, cuya base de Gröbner sea distinta de $\{1\}$.

Esta búsqueda de hipótesis puede tener como resultado hipótesis negativas, que eliminan un conjunto algebraico de los segmentos compatibles con la tesis, por lo que en general, el tipo de resultados que estamos estudiando tienen la forma más general $(H_p \wedge \neg H_n) \Rightarrow T$. Este estudio se puede extender fácilmente a tesis también negativas de la forma

$$(H_p \wedge \neg H_n) \Rightarrow (T_p \wedge \neg T_n)$$

buscando hipótesis adicionales $(H_p^* \wedge \neg H_n^*)$ para la implicación $H_p \Rightarrow T_n$ a partir del recubrimiento de Gröbner de su ideal asociado, y añadiendo el complementario de estas hipótesis a la implicación original,

$$((H_p \cup H_n^*) \wedge \neg(H_n \cup H_p^*)) \Rightarrow T_p.$$

El problema de búsqueda de hipótesis geométricas que verifiquen una propiedad forma parte de una familia más general de problemas, la búsqueda de lugares geométricos.

Capítulo 4

Complejidad Computacional

El principal problema que afecta a las bases de Gröbner, y por tanto, a todas sus potenciales aplicaciones, es su complejidad computacional intratable.

Este problema no es solo propio de las bases de Gröbner, sino del problema al que dan respuesta, la pertenencia a un ideal.

El problema de pertenencia a un ideal es un problema muy flexible, en el sentido de que existen muchos problemas que se pueden reducir a él. Es fácil expresar muchos problemas distintos en el lenguaje del Álgebra en términos de ideales.

Esta flexibilidad tiene la ventaja de que nos permite encontrar multitud de aplicaciones. Por contraparte, esto implica que puede ser tan difícil de resolver como algunos de estos problemas.

Por ejemplo, si dada una máquina de Turing M sobre un alfabeto Σ y una entrada $a \in \Sigma^*$, consideramos el ideal $I_M = \langle x, f_1, ..., f_k, ... \rangle \subseteq \mathbb{K}[x, y]$, donde $f_i = x$ si M no ha parado en menos de i pasos e y en caso contrario, el problema de pertenencia de y al ideal I_M es equivalente al problema de parada de M, y, por tanto, indecidible.

En este ejemplo, la causa de la indecidibilidad proviene del conjunto de generadores del ideal, algo que no hemos considerado hasta ahora en el documento, ya que siempre hemos supuesto que conocemos los generadores de los ideales con los que trabajamos. También hemos asumido implícitamente que el anillo sobre el que trabajamos es computable, i.e., podemos decidir algorítmicamente la igualdad de dos coeficientes, algo que no es cierto en general.

No obstante, incluso si los generadores del ideal son conocidos, y, por tanto, podemos determinar algorítmicamente una base de Gröbner del mismo, la complejidad del problema de pertenencia sigue siendo intratable.

El primer resultado sobre la complejidad de este problema se atribuye a Mayr y Meyer [4], que demostraron que el problema de la palabra en semigrupos conmutativos (CSG) es ExpSpace-completo, y puede reducirse al problema de pertenencia a un ideal, por lo que este es ExpSpace-duro.

La clase de complejidad ExpSpace engloba los problemas de decisión cuya resolución se puede decidir en espacio $2^{O(n)}$. En general, decimos que un problema es duro para una clase de complejidad si cualquier otro problema de la clase se puede reducir a él en tiempo polinomial, y que es completo si es duro y pertenece a la clase.

Definición 4.0.1. Sea $\Sigma := \{\sigma_1, ..., \sigma_r\}$ un alfabeto finito, y $R := \{\{a_1, b_1\},\{a_2, b_2\},\{a_3, b_3\},...\}$ un conjunto de reglas de reescritura de la forma $\{a, b\}$ donde a, b son palabras de Σ^*, el semigrupo generado por Σ para la composición de palabras, $\cdot : \Sigma^* \times \Sigma^* \longrightarrow \Sigma$, dada por $a \cdot b \mapsto ab$.

Además, asumimos que para todos $i, j \in \{1, ... , r\}$, $(\sigma_i\sigma_j, \sigma_j\sigma_i) \in R$, de manera que el semigrupo cociente $S = {}^{\Sigma^*}/_{\sim}$, donde $\sim$ es la relación de equivalencia generada por R, que identifica las palabras que pueden reescribirse de acuerdo a las reglas de R es un semigrupo conmutativo.

El **problema de la palabra en semigrupos conmutativos** (CSG por sus siglas en inglés), consiste en determinar si dos palabras, $w_1, w_2 \in S$, son iguales.

Dado que S es conmutativo, este problema se puede simplificar asumiendo sin pérdida de generalidad que las palabras $w \in S$ siempre vienen dadas en orden, i.e., $w = \sigma_1^{e_1}, ..., \sigma_r^{e_r}$, y que la concatenación en S respeta esta condición, reordenando el resultado para preservar el orden.

Para formalizar esta reducción, resulta de utilidad la siguiente definición.

Definición 4.0.2. Sea $f \in \mathbb{K}[\mathbf{x}]$ un polinomio, diremos que f es un **binomio de reescritura** si $f = 0$, o puede escribirse como la diferencia de dos monomios, i.e., $f = \mathbf{x}^\alpha - \mathbf{x}^\beta$, con $\alpha, \beta \in \mathbb{N}^n$.

También diremos que un ideal generado por binomios de reescritura es un **ideal de reescritura**.

Teorema 4.0.1. *El problema (CSG) se puede reducir al problema de pertenencia a un ideal.*

La demostración original que daremos de este teorema utilizando bases de Gröbner es algo más detallada que la original dada por Mayr y Meyer, pero permite ilustrar mejor la complejidad que aparece al utilizar bases de Gröbner para resolver el problema de pertenencia a un ideal. Para ello, introducimos primero dos resultados intermedios.

Lema 4.0.2. *El resto de un binomio de reescritura por binomios de reescritura es un binomio de reescritura.*

Demostración. Si tanto el dividendo como los divisores son binomios de reescritura, en cada paso de la división multivariada, la eliminación del monomio principal del dividendo solo puede resultar en la cancelación del otro monomio, o la adición de un monomio con el mismo signo que el eliminado. En consecuencia, todos los restos parciales y, por tanto, el resto son binomios de reescritura. □

Lema 4.0.3. *La base de Gröbner de un ideal de reescritura está formada únicamente por binomios de reescritura, independientemente del orden monomial elegido.*

Demostración. Gracias al lema anterior, solo necesitamos demostrar que el S-polinomio de dos binomios de reescritura es también un binomio de reescritura.

Sin embargo, un S-polinomio de este tipo es la diferencia de dos sumas de dos monomios en la que al menos 2 de ellos se cancelan, y, por tanto, es también un binomio de reescritura. □

Demostración del Teorema 4.0.1. Con la notación anterior, consideramos el anillo $P := \mathbb{Q}[x_1, ..., x_r]$, el homomorfismo natural entre semigrupos multiplicativos, $\varphi : S \longrightarrow P$ determinado por $\sigma_i \mapsto x_i$, y el ideal de reescritura $I := \langle\{\varphi(b) - \varphi(a) : (a, b) \in R\}\rangle$.

Queremos ver que el problema CSG, consiste en decidir la igualdad de w_1 y w_2 en S, es equivalente a decidir la pertenencia de $\varphi(w_1) - \varphi(w_2)$ en I.

Necesitamos probar que $\varphi(w_1) - \varphi(w_2) \in I$ si y solo si existe una derivación entre w_1 y w_2 en S.

Dada una derivación en S, $w_1 = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n = w_2$ en S, donde cada paso $\gamma_{i-1} \to \gamma_i$ describe la aplicación de una regla de reescritura $\{a_i, b_i\} \in R$, de modo que $\gamma_{i-1} = u_i a_i$ y $\gamma_i = u_i b_i$, queremos probar que $\varphi(w_1) - \varphi(w_2) \in I$.

Para ello, observamos que la aplicación de reglas de reescritura en S es equivalente a la suma de sus binomios asociados en I. Si partimos del binomio $f_n = \varphi(w_2) - \varphi(w_2) = 0 \in I$, al ser φ homomorfismo, sabemos que $\varphi(w_2) = \varphi(w_n) \cdot \varphi(b_n)$, luego consideramos $g_n = \varphi(u_n)(\varphi(a_n) - \varphi(b_n)) = \varphi(\gamma_n) - \varphi(\gamma_{n-1})$ y $f_{n-1} = f_n + g_n$. Dado que el primer monomio de f_n y el segundo de g_n se cancelan en f_{n-1}, tanto g_n como f_{n-1} son binomios de reescritura de I.

Continuando este proceso para las $n-1$ reglas de reescritura restantes, deducimos que $f_0 = \varphi(w_1) - \varphi(w_2) = \sum_{i=1}^{n} g_i \in I$, como queríamos.

Para ver la equivalencia en el otro sentido, consideramos $f = \varphi(w_1) - \varphi(w_2) \in I$ y una base de Gröbner G de I, que por el lema anterior, está formada únicamente por binomios de reescritura. Además, en este caso los S-polinomios que aparecen en G representan atajos en el conjunto de reglas de reescritura.

Es decir, si asumimos sin pérdida de generalidad que $\varphi(a_1) \succ \varphi(b_1)$ y $\varphi(a_2) \succ \varphi(b_2)$, entonces el S-polinomio de las reglas de reescritura $\{b_1, a_1\}$ y $\{a_2, b_2\}$ es

$$S(\varphi(a_1) - \varphi(b_1), \varphi(a_2) - \varphi(b_2)) = \varphi(c_2)\varphi(b_2) - \varphi(c_1)\varphi(b_1),$$

donde c_1 y c_2 dependen de $\varphi(a_1)$ y $\varphi(a_2)$, que representa la regla de reescritura $\{c_1 b_1, c_2 b_2\}$, equivalente a aplicar sucesivamente estas reglas.

En el contexto de una base de Gröbner, estas reglas podrían venir a su vez de otros S-polinomios, en cuyo caso representarían la aplicación sucesiva de más de 2 reglas de R.

A partir de esta observación, dado que f rem $G = 0$, la división multivariada de f por G nos permite recuperar una derivación entre w_1 y w_2 en S, de la forma $w_1 \to \gamma_1 \to \cdots \to \gamma_n \to w_2$.

Empezando con una derivación incompleta, $w_1 \to \cdots \to w_2$, en cada paso de la división, se dan dos casos. Si el divisor elegido proviene de una regla de reescritura, añadimos esta a la derivación directamente, y, si proviene de un S-polinomio, en su lugar añadimos a la derivación la sucesión de reglas de R a las que es equivalente.

El lugar donde añadimos estas reglas depende del término principal del resto parcial en cada paso. Cada vez que el término principal del resto parcial cambia de signo podemos considerar que estamos resolviendo el problema en la dirección contraria. Por este motivo, añadimos reglas a la izquierda de los puntos $\cdots$ cuando el signo del término principal es positivo y a la derecha cuando es negativo.

En cada paso, las derivaciones parciales a cada lado de los puntos $\cdots$ son correctas, y, en el último paso de la división, el resto es $\varphi(\gamma_*) - \varphi(\gamma_*) = 0$ para algún $\gamma_* \in S$, luego podemos unir ambos lados de la derivación que hemos construido, deduciendo que $w_1 = w_2$ como queríamos. □

En términos de complejidad computacional, esta reducción es de hecho lineal, pues solo requiere aplicar φ a las palabras de cada regla de reescritura de R, y a w_1 y w_2.

Observación 4. Nótese que esta forma de replantear el problema requiere que S sea conmutativo, ya que $\mathbb{K}[x_1, ..., x_r]$ es conmutativo. Las reglas de reescritura de la forma $(\sigma_i\sigma_j, \sigma_j, \sigma_i)$ de hecho pertenecen al núcleo de φ.

Observación 5. En la demostración del Teorema 4.0.1 podemos observar directamente como se traduce la complejidad exponencial en espacio del problema de pertenencia a un ideal al cálculo de bases de Gröbner.

Una vez determinada una base de Gröbner para un orden apropiado, como $\preceq_{grlex}$, la respuesta al problema de pertenencia a un ideal se reduce al cálculo de una división multivariada, cuyo número de pasos es lineal respecto al grado del polinomio.

Sin embargo, esta reducción de la complejidad temporal para la respuesta a polinomios concretos, requiere que la base de Gröbner contenga todos los *atajos* necesarios para dar respuesta a todos los posibles polinomios en dicho tiempo, que, como se deduce de los resultados de Mayr y Meyer puede ser exponencial respecto al tamaño del ideal (en términos de número de generadores y sus grados).

En general, esto no quiere decir que todos los problemas de pertenencia a ideales sean EXP-SPACE-completos, ya que, en algunos casos, la complejidad puede ser menor. Por ejemplo, si nos restringimos a ideales monomiales f.g., el problema tiene complejidad en $O(nks)$, siendo n el número de variables, k el número de términos del polinomio y s el número de generadores del ideal.

Alternativamente, si nos restringimos a ideales lineales, el problema se reduce a la resolución de un sistema de ecuaciones lineales, cuya complejidad es también polinomial.

Como ejemplo de la flexibilidad del problema de pertenencia a un ideal, planteamos un ejemplo.

Ejemplo 4.0.1. *El problema de satisfactibilidad booleana restringido a cláusulas con* 3 *literales,* 3*-SAT, se puede reducir a un problema de pertenencia a un ideal.*

Dado un conjunto de variables, $\mathbf{x} := \{x_1, ..., x_n\}$*, el* 3*-SAT consiste en decidir si una fórmula booleana en forma normal conjuntiva con cláusulas de tamaño* 3*, es decir, una fórmula*

$$\Phi = (l_{1,1} \vee l_{1,2} \vee l_{1,3}) \wedge \cdots \wedge (l_{r,1} \vee l_{r,2} \vee l_{r,3}),$$

donde los $l_{i,j}$ *pueden ser una variable* $x_k \in \mathbf{x}$*, o su negación,* $\neg x_k$*.*

Para reducir este problema al de pertenencia a un ideal, basta observar que podemos expresar esta fórmula como un sistema de polinomios en el anillo $\mathbb{F}_2[\mathbf{x}]$*,*

$$S : \begin{cases} s_{1,1} \cdot s_{1,2} \cdot s_{1,3} = 0 \\ \quad \vdots \\ s_{r,1} \cdot s_{r,2} \cdot s_{r,3} = 0 \end{cases}$$

donde $\mathbb{F}_2$ *es el cuerpo de dos elementos, y* $s_{i,j}$ *es* x_k *si* $l_{i,j} = \neg x_k$ *y* $(1 - x_k)$ *si* $l_{i,j} = x_k$*.*

Para evitar soluciones en la clausura algebraica de $\mathbb{F}_2$*, podemos añadir los* n *polinomios*

$$\{x_i^2 - x_i : i \in \{1, ..., n\}\}.$$

De este modo, Φ *es satisfactible si y solo si existe una solución de* S*, i.e., si y solo si* $1 \notin I$*.*

Las bases de Gröbner proporcionan una manera *efectiva*, en el sentido de que, una vez calculada una base de un ideal concreto, es posible responder a distintos problemas de pertenencia sobre el ideal realizando una única división multivariada, de manera similar a como, en la resolución de sistemas de ecuaciones lineales, el cálculo de la matriz inversa o una descomposición adecuada de la matriz del sistema permite responder directamente a problemas con distintos términos independientes.

En la práctica, la principal causa de complejidades intratables suele ser el elevado número de variables necesarias para describir el problema, ya que este puede crecer con facilidad, y conlleva en muchos casos la necesidad de añadir una cantidad exponencial de S-polinomios involucrando todas las posibles combinaciones de variables a la base de Gröbner.

Por ejemplo, si intentáramos aplicar la técnica de Deducción Automática de Teoremas Geométricos vista en el Capítulo 3 a un teorema que involucre más variables, como el Teorema del Trisector de Morley, que, a pesar de su sencilla formulación geométrica, involucra un mínimo de 20 variables, de las cuales solo 2 son parámetros, tanto el tiempo como la memoria necesarios para calcular el recubrimiento de Gröbner pueden ser prohibitivos.

En un intento de resolver este problema, un ordenador con 32GiB de memoria RAM se quedó sin memoria tras casi 4 horas de ejecución.

Teorema 4.0.4 (del Trisector de Morley)**.** *Las tres intersecciones de los trisectores de los ángulos de un triángulo más cercanas a los lados forman un triángulo equilátero [8, p. 738].*

4.1 Mejoras del algoritmo de Buchberger

Dado el interés práctico motivado por la multitud de aplicaciones de las bases de Gröbner, existe una gran cantidad de algoritmos que intentan mejorar el rendimiento del algoritmo de Buchberger.

Es debido a estos algoritmos que el cálculo de bases de Gröbner es de utilidad en algunas aplicaciones prácticas, por lo que destacamos algunos de los más relevantes, como se discuten en el Capítulo 10 de [2].

Estas mejoras se obtienen, en general, introduciendo criterios que permitan ahorrar comprobaciones o reducciones innecesarias.

Dos algoritmos, o familias de algoritmos, particularmente relevantes son los algoritmos F_4 y F_5, introducidos por Faugère en 1999 y 2002 respectivamente, así como sus muchas variantes.

Los algoritmos de la familia F_4 utilizan una representación matricial de los polinomios de la base para realizar múltiples reducciones simultáneamente, y son particularmente eficientes en el caso de ideales homogéneos y órdenes graduados.

Por otro lado, los algoritmos de la familia F_5, utilizan técnicas para llevar la cuenta de los pasos seguidos hasta introducir cada polinomio en la base, con la intención de aprovechar dicha información para evitar realizar reducciones innecesarias. La demostración de la corrección y terminación de los algoritmos de esta familia no fue obtenida hasta 2012.

No obstante, a pesar de la falta de una demostración de corrección, estos algoritmos fueron los primeros en resolver una serie de problemas previamente considerados intratables, particularmente en el campo de la criptografía, despertando un gran interés que llevó a la creación de tantas variaciones como tiene.

Algunos algoritmos son particularmente útiles en casos concretos, como, por ejemplo, pasar de una base de Gröbner sobre un orden monomial a otro, ya que en la práctica, es frecuente que calcular una base respecto a un orden graduado lexicográfico y convertirla a una base respecto a un orden lexicográfico sea más rápido que calcular directamente la base respecto al orden lexicográfico.

Bibliografía

[1] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner bases: A computational approach to commutative algebra*. Springer-Verlag, 1998.

[2] David A. Cox, John B. Little, and Donal O'Shea. *Ideals, varieties, and Algorithms: An introduction to computational algebraic geometry and commutative algebra*. Springer, 2018.

[3] Wolfram Decker et al. SINGULAR *4-2-1 — A computer algebra system for polynomial computations*. http://www.singular.uni-kl.de. 2021.

[4] Ernst W Mayr and Albert R Meyer. "The complexity of the word problems for commutative semigroups and polynomial ideals". In: *Advances in Mathematics* 46.3 (1982), pp. 305–329. ISSN: 0001-8708. DOI: https://doi.org/10.1016/0001-8708(82)90048-2. URL: https://www.sciencedirect.com/science/article/pii/0001870882900482.

[5] Antonio Montes. *The Gröbner cover*. Springer, 2018.

[6] Antonio Montes and Tomas Recio. "Generalizing the Steiner–Lehmus theorem using the Gröbner cover". In: *Mathematics and Computers in Simulation* 104 (Oct. 2014), pp. 67–81. DOI: 10.1016/j.matcom.2013.06.006.

[7] Antonio Montes and Hans Schoenemann. GROBCOV.LIB *4-2-1 — A* SINGULAR *4-2-1 library for computing the canonical Gröbner Cover of a parametric ideal*. https://www.singular.uni-kl.de/Manual/4-0-2/sing_956.htm. 2021.

[8] Cletus O. Oakley and Justine C. Baker. "The Morley Trisector theorem". In: *The American Mathematical Monthly* 85.9 (1978), p. 737. DOI: 10.2307/2321680.

[9] J. L. Rabinowitsch. "Zum Hilbertschen Nullstellensatz". In: *Mathematische Annalen* 102.1 (1930), pp. 520–520. DOI: 10.1007/bf01782361.

[10] Volker Weispfenning. "Comprehensive Gröbner bases". In: *Journal of Symbolic Computation* 14.1 (1992), pp. 1–29. ISSN: 0747-7171. DOI: https://doi.org/10.1016/0747-7171(92)90023-W. URL: https://www.sciencedirect.com/science/article/pii/074771719290023W.

[11] Volker Weispfenning. "Constructing universal Gröbner bases". In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Ed. by Llorenç Huguet and Alain Poli. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 408–417. ISBN: 978-3-540-46150-0.

[12] Gathen Joachim von zur and Gerhard Jürgen. *Modern Computer algebra*. Cambridge University Press, 2013.