Sistemas polinomiales
(Elementos básicos)

ALBERTO VIGNERON TENORIO
Dpto. de Matemáticas

Universidad de Cádiz

Índice general

1. Introducción **2**

2. Generalidades sobre polinomios **5**

2.1. Orden monomial 6

2.2. Algoritmo de división 7

2.3. $S-$polinomios 9

2.4. Bases de Gröbner 9

3. Generalizando Gauss a sistemas polinomiales **11**

4. Ejemplo **12**

Capítulo 1

Introducción

Los sistemas polinomiales son una pieza importante dentro de la modelización de problemas reales. El estudio y cálculo de sus soluciones exactas constituyen todo un campo de trabajo con aplicaciones directas en la economía, la ingeniería, informática, telecomunicaciones, etc. Estos problemas se estudian dentro de diversas ramas de las Matemáticas. La aproximación que vamos a realizar la abordaremos desde el punto de vista del *Álgebra Computacional*.

Las preguntas a las que vamos tratar de dar respuesta son:

- ¿Cuándo tiene solución un sistema polinomial?
- ¿Cuándo tiene una cantidad finita de soluciones un sistema polinomial?
- ¿Cómo podemos calcular dichas soluciones?

Si nos encontramos frente a un sistema de ecuaciones lineales, aplicamos el método de eliminación de Gauss. Por ejemplo, dado el sistema de ecuaciones (p_i es la ecuación i)

$$\left\{\begin{array}{lrrrrrrl} p_1 \equiv & x & +2y & -z & +t & +u & & = 0 \\ p_2 \equiv & +3x & -y & & +t & -u & -6 & = 0 \\ p_3 \equiv & 6x & +y & & +t & +u & -1 & = 0 \\ p_4 \equiv & x & -2y & +2z & -2t & & +5 & = 0 \end{array}\right. \tag{1.1}$$

el primer paso sería fijar un elemento sobre el que pivotar, en este ejemplo escogemos el monomio en x de la primera ecuación, el segundo reducir las ecuaciones pivotando sobre el elemento elegido,

$$\left\{\begin{array}{ccc} p_2-3p_1 & \rightarrow & p_2 \\ p_3-6p_1 & \rightarrow & p_3 \\ p_4-p_1 & \rightarrow & p_4 \end{array}\right. \Rightarrow \left\{\begin{array}{rrrrrrr} x & +2y & -z & +t & +u & & =0 \\ & -7y & +3z & -2t & -4u & -6 & =0 \\ & -11y & +6z & -5t & -5u & -1 & =0 \\ & -4y & +3z & -3t & -u & +5 & =0 \end{array}\right. \tag{1.2}$$

Esta reducción tiene como consecuencia que en todas las ecuaciones, salvo la primera, hemos eliminado la variable x. Además, sus soluciones son las mismas que las del sistema (1.1).

La anterior operación $p_2-3p_1 \rightarrow p_2$ es equivalente a sustituir p_2 por una combinación de p_1 y p_2 obtenidas a partir del mínimo común múltiplo de los coeficientes de x, dividido por el coeficiente de cada ecuación. Las otras dos se obtienen a partir del mínimo común múltiplo de los coeficientes de x de la primera ecuación, y la tercera y cuarta respectivamente.

Análogamente, si pivotamos ahora sobre $-7y$ en la segunda ecuación para continuar con la reducción,

$$\left\{\begin{array}{ccc} 7p_3-11p_2 & \rightarrow & p_3 \\ & & \\ 7p_4-4p_2 & \rightarrow & p_4 \end{array}\right. \Rightarrow \left\{\begin{array}{rrrrrrr} x & +2y & -z & +t & +u & & =0 \\ & -7y & +3z & -2t & -4u & -6 & =0 \\ & & 9z & -13t & +9u & +59 & =0 \\ & & 9z & -13t & +9u & +59 & =0 \end{array}\right.$$

De nuevo, la operación $7p_3-11p_2 \rightarrow p_3$ se obtiene a partir del mínimo común múltiplo de los coeficientes de y en la segunda y tercera ecuación, divididos por los correspondientes coeficientes de y en cada una de las ecuaciones:

$$7p_3-11p_2=\frac{mcm(7,11)}{11}p_3-\frac{mcm(7,11)}{7}p_2,$$

y $7p_4-4p_2 \rightarrow p_4$ de

$$7p_4-4p_2=\frac{mcm(7,4)}{4}p_3-\frac{mcm(7,4)}{7}p_2.$$

La última operación de la reducción, $p_4-p_3 \rightarrow p_4$, la obtendremos de

$$p_4-p_3=\frac{mcm(9,9)}{9}p_4-\frac{mcm(9,9)}{9}p_3,$$

quedando el sistema:

$$\left\{\begin{array}{cccccccc} x & +2y & -z & +t & +u & & =0 \\ & -7y & +3z & -2t & -4u & -6 & =0 \\ & & 9z & -13t & +9u & +59 & =0 \\ & & & & & 0 & =0 \end{array}\right.$$

Al final de este proceso, hemos re-escrito el sistema inicial en una *expresión agradable*. Las nuevas ecuaciones tienen las mismas soluciones que en el sistema inicial (1.1). Mediante este procedimiento obtenemos, para ecuaciones lineales, respuestas a las preguntas anteriores:

- ¿Cuándo tiene solución un sistema lineal? El sistema es compatible porque no hemos obtenido ninguna ecuación incompatible, es decir, del tipo $1 = 0$.
- ¿Cuándo tiene una cantidad finita de soluciones un sistema lineal? El sistema tiene infinitas soluciones porque, por ejemplo, la variable u puede tomar cualquier valor.
- ¿Cómo podemos calcular dichas soluciones? Podemos calcular todas las soluciones despejando z en función de t y u de la última ecuación (no nula), después y en función de z, t y u de la penúltima, y x en función del resto de la primera ecuación.

¿Podemos encontrar un proceso equivalente cuando tratamos con sistemas de ecuaciones polinómicas? ¿Podemos encontrar esa *expresión agradable* con un sistema polinomial? Las respuestas a estas preguntas son afirmativas, y se basan, al igual que la reducción de Gauss en:

- encontrar elementos sobre los que pivotar,
- reducir las ecuaciones obteniendo nuevos sistemas (con una *expresión agradable*) que tengan las mismas soluciones que los de partida.

Para ello vamos a utilizar las llamadas bases de Gröbner, dando un procedimiento de reducción de polinomios en varias variables similar al que hemos aplicado sobre el ejemplo anterior.

Capítulo 2

Generalidades sobre polinomios

Consideremos ahora un conjunto de polinomios, $F = \{f_1, \ldots, f_t\}$, en las variables $x_1, \ldots, x_n$. En general, vamos a denotar por $\mathbb{C}[x_1, \ldots, x_n]$ al conjunto de todos los polinomios en las variables $x_1, \ldots, x_n$, con coeficientes en $\mathbb{C}$ (conocido como anillo de polinomios). Dado un monomio $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, llamaremos *exponente* de $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ al vector $(a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$. Nótese que cada monomio tiene asociado un único exponente y viceversa.

Definición 1. *Dado un conjunto de polinomios $I \subset \mathbb{C}[x_1, \ldots, x_n]$, diremos que I es un ideal si verifica:*

- $0 \in I$.
- *Si $f, g \in I$, entonces $f + g \in I$.*
- *Si $f \in I$ y $h \in \mathbb{C}[x_1, \ldots, x_n]$, entonces $hf \in I$.*

Lema 1. *Dados los polinomios iniciales $F = \{f_1, \ldots, f_t\}$, el conjunto*

$$\{h_1 f_1 + \cdots + h_t f_t \,|\, h_1, \ldots, h_t \in \mathbb{C}[x_1, \ldots, x_n]\}$$

es un ideal de $\mathbb{C}[x_1, \ldots, x_n]$, al que llamaremos ideal generado por F, y denotaremos por

$$< f_1, \ldots, f_t > .$$

Nótese que las soluciones del sistema polinomial $f_1 = 0, \ldots, f_t = 0$, que nos ocupa, son las mismas que las de cualquier sistema de generadores del ideal $< f_1, \ldots, f_t >$. Por lo tanto, encontrar esa *expresión agradable* a la que nos referimos en la introducción pasa por encontrar sistemas de generadores *especiales* del ideal. En lo que sigue, vamos a plantear los elementos necesarios para ello.

2.1. Orden monomial

La elección del pivote en una generalización de la reducción de Gauss, va a suponer, en primer lugar, escoger una ecuación y un monomio en ella. Para ello se utilizan los llamados órdenes monomiales. Dado que hemos relacionado de manera única un monomio con su exponente,

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \leftrightsquigarrow (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n,$$

podemos ordenar los monomios mediante esos exponentes. En particular, y para el problema que nos ocupa, vamos a considerar el conocido como orden lexicográfico, aunque, como es comprensible, existen gran cantidad de órdenes con distintas utilidades.

Definición 2. *Diremos que* $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$ *es menor (respecto al orden lexicográfico) que* $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{N}^n$*, y lo denotaremos por* $\mathbf{a} <_{lex} \mathbf{b}$*, si existe* $i \in \{1, \ldots, n-1\}$ *tal que* $a_j = b_j$*, si* $1 \leq j \leq i$*, y* $a_i < b_i$*, o equivalentemente, si en la diferencia* $\mathbf{b} - \mathbf{a}$ *la primera coordenada distinta de cero de izquierda a derecha es positiva.*

La definición anterior traslada el orden en $\mathbb{N}^n$ a los monomios. Por ejemplo,

$$x_1 x_2 x_3^2 x_4^5 <_{lex} x_1 x_2 x_3^3 x_4^2$$

porque $(1, 1, 2, 5) <_{lex} (1, 1, 3, 2)$.

Es al orden inducido en los monomios, por un orden sobre $\mathbb{N}^n$, a lo que se denomina *orden monomial.*

Fijado un orden monomial, podemos escribir los polinomios ordenando sus monomios mediante ese orden. Dado un polinomio $f \in \mathbb{C}[x_1, \ldots, x_n]$, lo escribiremos como

$$f = c_{\mathbf{a}}X^{\mathbf{a}} + \hat{f},$$

donde $c_{\mathbf{a}}X^{\mathbf{a}}$ es el monomio de mayor exponente de f, y $\hat{f} = f - c_{\mathbf{a}}X^{\mathbf{a}}$. Todos los monomios de $\hat{f}$ tienen exponente menor que $\mathbf{a}$. Al monomio con mayor exponente dentro de un polinomio lo denominaremos *monomio líder.*

Por ejemplo, fijado el orden lexicográfico, el polinomio

$$f = yz^2 - 2 + x^3yz - 34z^5 - x^3,$$

tiene por monomio líder a x^3yz, y $\hat{f} = yz^2 - 2 - 34z^5 - x^3$.

2.2. Algoritmo de división

Al contrario de lo que ocurre con polinomios en una variable, dado un polinomio $x^2y + 3z$ podemos dividirlo entre otro, $xy + z$, de varias formas:

- Si dividimos $x^2y + 3z$ entre $xy + z$ empezando la división por xy, $x^2y + 3z = x(xy + z) - xz + 3z$, donde $-xz + 3z$ es el resto de la división.

- Si dividimos $x^2y + 3z$ entre $xy + z$ empezando la división por z, $x^2y + 3z = 3(xy + z) - 3xy + x^2y$, donde $-3xy + x^2y$ es el resto de la división.

Como se puede apreciar, no existe un resto único en la división ya que existen varias posibilidades a la hora de realizarla. Esta disparidad de caminos se elimina fijando un orden sobre los monomios.

Por ejemplo, fijado el orden lexicográfico, la división que hubiéramos realizado es la primera, dividiendo el monomio líder del primer polinomio por el líder del segundo:

$$\begin{array}{llll|l} x^2y & & +3z & & xy + z \\ \hline -x^2y & -xz & & & x \\ & -xz & +3z & & \end{array}$$

Como el monomio líder de $-xz + 3z$ no es divisible por el líder de $xy + z$, xy, ya hemos terminado la división.

Esta idea nos permite dar un algoritmo de división dentro del conjunto de polinomios basado en,

Teorema 1. *Sea $F = \{f_1, \ldots, f_t\}$ un conjunto de polinomios ordenados no nulos en las variables $x_1, \ldots, x_n$, y f otro polinomio. Entonces existen unos únicos polinomios $q_1, \ldots, q_t$ y r tales que:*

1. $f = \sum_{i=1}^{t} q_i f_i + r$

2. $r = 0$, *ó, si* $r \neq 0$, *ningún monomio de r es divisible por los líderes de cada f_i.*

3. *el monomio líder de cada producto $q_i f_i$, es menor o igual que el líder de f.*

Al polinomio r lo llamaremos resto de la división.

Ejemplo 1. *A modo de ejemplo, vamos a dividir $f = 2x_1^2x_2 + 4x_1x_2^2 + x_1$ entre $F = \{f_1 = x_1^2 + x_2 + 1, f_2 = x_2^2 + 1\}$ considerando de nuevo el orden lexicográfico:*

1. *Para comenzar, dividiremos f entre f_1 (el monomio líder de f_1, x_1^2, es mayor que el de f_2, $2x_1x_2$):*

$$\begin{array}{lcc|c} 2x_1^2x_2 + 4x_1x_2^2 + x_1 & & & x_1^2 + x_2 + 1 \\ \hline -2x_1^2x_2 & -2x_2^2 - 2x_2 & & 2x_2 \\ & 4x_1x_2^2 + x_1 - 2x_2^2 - 2x_2 & & \end{array}$$

   Por lo tanto $f = 2x_2f_1 + 4x_1x_2^2 + x_1 - 2x_2^2 - 2x_2$, donde $r_1 = 4x_1x_2^2 + x_1 - 2x_2^2 - 2x_2$ es el resto de la división anterior.

2. *Ahora, dado que el monomio líder de r_1 es divisible por el de f_2, procedemos a hacer la división r_1 entre f_2 :*

$$\begin{array}{lc|c} 4x_1x_2^2 + x_1 - 2x_2^2 - 2x_2 & & x_2^2 + 1 \\ \hline -4x_1x_2^2 - 4x_1 & & 4x_1 \\ & -5x_1 - 2x_2^2 - 2x_2 & \end{array}$$

   Por lo tanto $r_1 = 4x_1f_2 - 5x_1 - 2x_2^2 - 2x_2$, donde $r_2 = -5x_1 - 2x_2^2 - 2x_2$ es el resto de la división anterior.

Al final tenemos que $f = 2x_2f_1 + 4x_1f_2 - 5x_1 - 2x_2^2 - 2x_2$.

2.3. $S-$polinomios

Generalizar la reducción realizada durante la aplicación del método de Gauss pasa por definir alguna acción sobre los polinomios equivalente a lo que hicimos, por ejemplo, en (1.2). Esa operación se realiza a través del conocido como $S-$polinomio. Recordamos que tenemos fijado un orden monomial.

Definición 3. *Sean f, g dos polinomios en las variables $x_1, \ldots, x_n$,*

$$f = c_{\mathbf{a}} X^{\mathbf{a}} + \hat{f},\ g = c_{\mathbf{b}} X^{\mathbf{b}} + \hat{g},$$

y $cX^{\mathbf{m}}$ el mínimo común múltiplo de $c_{\mathbf{a}} X^{\mathbf{a}}$ y $c_{\mathbf{b}} X^{\mathbf{b}}$.

Llamaremos S-polinomio de f, g al polinomio:

$$S(f,g) = \frac{cX^{\mathbf{m}}}{c_{\mathbf{a}} X^{\mathbf{a}}} \cdot f - \frac{cX^{\mathbf{m}}}{c_{\mathbf{b}} X^{\mathbf{b}}} \cdot g$$

Ejemplo 2. *El $S-$polinomio de los polinomios $2x_1^2x_2 + 4x_1x_2^2 + x_1$ y $x_2^2 + 1$ es:*

$$S(2x_1^2x_2 + 4x_1x_2^2 + x_1, x_2^2 + 1) = \frac{2x_1^2x_2^2}{2x_1^2x_2}(2x_1^2x_2 + 4x_1x_2^2 + x_1) - \frac{2x_1^2x_2^2}{x_2^2}(x_2^2 + 1) =$$

$$= x_2(2x_1^2x_2 + 4x_1x_2^2 + x_1) - 2x_1^2(x_2^2 + 1) = 4x_1x_2^3 + x_1x_2 - 2x_1^2.$$

2.4. Bases de Gröbner

Ya estamos en condiciones de definir un conjunto especial de polinomios: las bases de Gröbner. A partir de las bases de Gröbner construiremos la *expresión agradable* de un sistema polinomial a la que nos hemos referido en la introducción. Vamos a realizar la definición de base de Gröbner de forma algorítmica para ajustarla al problema que nos ocupa: encontrar la citada *expresión agradable* del sistema.

Consideremos de nuevo un conjunto de polinomios, $F = \{f_1, \ldots, f_t\} \in \mathbb{C}[x_1, \ldots, x_n]$, que nos determina un sistema polinomial $f_1 = 0, \ldots, f_t = 0$. Denotaremos por I al ideal generado por el conjunto F.

Definición 4. *El conjunto F es una base de Gröbner de I (respecto a un orden monomial fijado) si y sólo si para cualquier par $i \neq j$, el resto de la división de $S(f_i, f_j)$ por F es cero.*

La forma de construir una base de Gröbner la recogemos en el siguiente algoritmo:

Algoritmo 1. *Cálculo de una base de Gröbner*
DATOS DE ENTRADA: $F = \{f_1, \ldots, f_m\}$.
DATOS DE SALIDA: *Una base de Gröbner del ideal generado por F.*

CUERPO DEL ALGORITMO:

- $F' = F$.
- *Para cada par* $f, g \in F$, *con* $f \neq g$, *haz, hasta que todos los restos sean nulos:*
  1. $S = S(f, g)$.
  2. *Calcula el resto de dividir (fijando un orden monomial)* S *por el conjunto* F'. *Al resto de la división lo denotaremos* r.
  3. *Si* $r \neq 0$, *considera* $F = F \cup \{r\}$.
- *La base de Gröbner es F.*

Existe un tipo especial de bases de Gröbner que es la base de Gröbner reducida. Esta base, fijado un orden monomial, es única para cada ideal y tiene un tamaño (número de polinomios) más reducido.

Por último, más adelante nos interesará poder calcular los polinomios de un ideal que contienen sólo una variable, es decir $I \cap \mathbb{C}[x_i]$. Ello lo haremos basándonos en el siguiente teorema.

Teorema 2. *Dado un ideal* $I \subset \mathbb{C}[x_1, \ldots, x_n]$, *existe un polinomio en* I *sólo con la variable* x_i *si y sólo si hay uno de ese tipo en la base de Gröbner de* I *respecto de un orden donde* x_i *sea la menor variable.*

Capítulo 3

Generalizando Gauss a sistemas polinomiales

Ya estamos en condiciones de responder a las preguntas planteadas en la introducción:

- ¿Cuándo tiene solución un sistema polinomial?

  Teorema 3. $f_1 = 0, \ldots, f_t = 0$ *no tiene solución si y sólo si cualquier base de Gröbner (reducida) del ideal* $< f_1, \ldots, f_t >$ *es* 1. *Esto equivale a que no hay ecuaciones incongruentes del tipo* ”$1 = 0$” *en el sistema.*

- ¿Cuándo tiene una cantidad finita de soluciones un sistema polinomial?

  Teorema 4. $f_1 = 0, \ldots, f_t = 0$ *tiene una cantidad finita de soluciones si y sólo si para cada variable, existe un polinomio, sólo en esa variable, en el ideal* $< f_1, \ldots, f_t >$. *Esto lo podemos detectar calculando los polinomios en* $< f_1, \ldots, f_t > \cap \mathbb{C}[x_i]$ *mediante bases de Gröbner (teorema 2).*

- ¿Cómo podemos calcular dichas soluciones?

  Teorema 5. *Dado el sistema polinomial* $f_1 = 0, \ldots, f_t = 0$, *la* expresión agradable *que buscamos viene dada por una base de Gröbner (reducida) del ideal* $< f_1, \ldots, f_t >$ *respecto del orden lexicográfico.*

Capítulo 4

Ejemplo

Consideremos el sistema polinomial

$$\left\{ \begin{array}{rcccl} f & = & \underline{xy^2} - 2\,x - y^2 + 2 & = & 0 \\ g & = & \underline{x^2y} - x^2 + y - 1 & = & 0 \end{array} \right. \tag{4.1}$$

donde hemos subrayado los monomios líderes de cada polinomio. Para hallar la *expresión agradable* del sistema, aplicamos el algoritmo 1 considerando fijado el orden lexicográfico con $x > y$.

En primer lugar calculamos el $S-$polinomio de f y g :

$$S(f,g) = x^2y - 2\,x^2 - xy^2 + 2\,x - y^2 + y,$$

y lo dividimos por el conjunto $F = \{f, g\}$,

$$S(f,g) = -f + g + (-x^2 - 2\,y^2 + 3).$$

Como el resto es no nulo, añadimos dicho resto, que denotaremos por r_1, al conjunto F.

Ahora realizamos el $S-$polinomio de f y r_1 :

$$S(f, r_1) = 2\,x^2 + xy^2 - 2\,x + 2\,y^4 - 3\,y^2,$$

y lo dividimos por el conjunto $F = \{f, g, r_1\}$,

$$S(f, r_1) = -f - 2r_1 + (2\,y^4 - 6\,y^2 + 4).$$

Como el resto es no nulo, añadimos dicho resto, que denotaremos por r_2, al conjunto F.

Continuando ese procedimiento, llegamos a que una base de Gröbner de $F = \{f, g\}$ respecto del orden lexicográfico es:

$$\{f, g, x^2 + 2\,y^2 - 3, y^4 - 3\,y^2 + 2, y^3 - y^2 - 2\,y + 2\},$$

por lo tanto, el sistema tiene solución porque dicha base no es $\{1\}$. El sistema inicial (4.1) tiene una *expresión agradable*

$$\begin{cases} xy^2 - 2\,x - y^2 + 2 &= 0 \\ x^2y - x^2 + y - 1 &= 0 \\ x^2 + 2\,y^2 - 3 &= 0 \\ y^4 - 3\,y^2 + 2 &= 0 \\ y^3 - y^2 - 2\,y + 2 &= 0 \end{cases}$$

De las dos últimas ecuaciones, obtenemos que los posibles valores de y son $\pm\sqrt{2}$ y 1.

Fijados estos valores, calculamos los de x :

- Para $y = 1$, $x = 1$.
- Para $y = \sqrt{2}$, $x = \pm\sqrt{-1} = \pm i$.
- Para $y = -\sqrt{2}$, $x = \pm\sqrt{-1} = \pm i$.

Al final, hemos calculado las 4 soluciones del sistema, aunque sólo una de ellas, el par $(1, 1)$, es real.

De haber calculado una base de Gröbner de $F = \{f, g\}$ respecto al orden lexicográfico $y > x$, habríamos obtenido que el polinomio $x^3 - 1 - x^2 + x$ estaría en ella. Como en la base que hemos calculado antes considerando $x > y$ tenemos polinomios sólo en la variable y, concluiríamos, aplicando el teorema 4, que el sistema tenía una cantidad finita de soluciones. En cualquier caso, en este ejemplo hemos calculado primero las soluciones y hemos visto que hay una cantidad finita de ellas.

Bibliografía

[1] D. COX, J. LITTLE, D. O'SHEA. Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra. Springer (2007).