DEPARTAMENTO DE CIENCIAS
SECCIÓN MATEMÁTICAS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

REPORTE DE INVESTIGACIÓN

N° 31

Serie: B

ALGUNAS APLICACIONES DE LAS BASES DE GRÖBNER

Maynard Kong W., Ricardo Bances H., Nélida Medina G., Mariano González U., Maritza Luna V. y Roy Sánchez G.

Lima, mayo de 2014

DEPARTAMENTO
DE CIENCIAS
SECCIÓN MATEMÁTICAS

REPORTE DE INVESTIGACIÓN

N° 31

Serie: B

ALGUNAS APLICACIONES DE LAS BASES DE GRÖBNER

Maynard Kong W., Ricardo Bances H., Nélida Medina G.,
Mariano González U., Maritza Luna V. y Roy Sánchez G.

Lima, mayo de 2014

Sección Matemáticas
Departamento de Ciencias
Pontificia Universidad Católica del Perú
Apartado 1761
Lima-Perú

Algunas Aplicaciones de las Bases de Gröbner

Maynard Kong W., Ricardo Bances H., Nélida Medina G.,
Mariano González U., Maritza Luna V. y Roy Sánchez G.

Revisado por:

El Director y la Comisión de Publicaciones del Departamento Académico de Ciencias

Teléfono: 626 2000
E-mail: publicacionesdac@pucp.edu.pe
http://www.pucp.edu.pe

Primera edición: Mayo de 2014
100 ejemplares

ISBN: **978-612-46647-1-7**
Hecho el Depósito Legal en la Biblioteca Nacional del Perú: **2014-07067**

Diagramación de Interiores: Carlos E. Iman Ancajima
Impreso en Editorial Moshera S.R.L.
Jr. Tacna 2969, San Martín de Porres
Telefax: 567-9299
editorialmoshera@hotmail.com

Índice general

Introducción

El objetivo de esta publicación es presentar una introducción a las Bases de Gröbner y desarrollar algunas de sus aplicaciones. En primer lugar se expone diferentes maneras de ordenar los monomios en el anillo de polinomios $k[x_1, x_2, \cdots, x_n]$, donde k es un campo; y una generalización del algoritmo de la división. Luego, se define una base de Gröbner de un ideal $I \subset k[x_1, x_2, \cdots, x_n]$ y se construye una de ellas, utilizando el algoritmo de Buchberger.

Como aplicaciones de las Bases de Gröbner se presentan: solución de sistemas de ecuaciones polinomiales en varias variables, relación de las variedades algebraicas con los ideales de polinomios, solución del problema de los tres colores, solución de problemas de optimización con restricciones polinomiales en varias variables y solución de problemas de programación entera. En todas estas aplicaciones, para realizar los cálculos, hemos usado el software *Mathematica* V.8.0.4.0.

Capítulo 1

Anillo de polinomios $k[x_1, \cdots, x_n]$

En esta sección presentamos las definiciones y resultados necesarios para la construcción de una base de Gröbner de un ideal $I \subset k[x_1, \cdots, x_n]$.

1.1. Monomios. Órdenes monomiales

Definición 1.1.1. *Se denomina **monomio** a un producto de una colección de variables $x_1, x_2, \cdots, x_n$ de la forma*

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

donde $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.
En particular, si $\alpha = (0, \ldots, 0), x^\alpha = x^0 = 1$.
*El **grado total** de un monomio x^α se define por*

$$|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n.$$

Definición 1.1.2. *Sea k un campo. Un **polinomio** f en las variables $x_1, x_2, \cdots, x_n$ es una combinación lineal de un número finito de monomios con coeficientes en k y se representa mediante*

$$f = \sum_\alpha c_\alpha x^\alpha, \quad c_\alpha \in k. \tag{1.1.1}$$

El conjunto de polinomios con coeficientes en k es un anillo conmutativo con elemento identidad y se denota por $k[x_1, \cdots, x_n]$.

Definición 1.1.3. *Un **orden monomial** sobre* $k[x_1, x_2, \cdots, x_n]$ *es una relación* $\succ$ *en el conjunto de los monomios* x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, *o equivalentemente una relación* $\succ$ *en* $\mathbb{Z}^n_{\geq 0}$ *que satisface:*

1. $\succ$ *es un orden total sobre* $\mathbb{Z}^n_{\geq 0}$.

2. *Si* $\alpha \succ \beta$ *y* $\gamma \in \mathbb{Z}^n_{\geq 0}$ *, entonces* $\alpha + \gamma \succ \beta + \gamma$.

3. $\succ$ *es un buen orden en* $\mathbb{Z}^n_{\geq 0}$. *Esto significa que cada subconjunto no vacío de* $\mathbb{Z}^n_{\geq 0}$ *tiene un elemento minimal bajo el orden* $\succ$.

Sean x^α y x^β donde $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$,

$$\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n), \quad \beta = (\beta_1, \beta_2, \cdots, \beta_n)$$

y considerando $x_1 > x_2 > \cdots > x_n$, usaremos los siguientes órdenes monomiales:

a) **Orden Lexicográfico (lex)**. Decimos que $x^\alpha \succ_{lex} x^\beta$, si en la diferencia $(\alpha_1, \cdots, \alpha_n) - (\beta_1, \cdots, \beta_n)$ la primera coordenada no nula, de izquierda a derecha, es positiva.

b) **Orden Lexicográfico Graduado (grlex)**.

$$x^\alpha \succ_{grlex} x^\beta \Leftrightarrow \begin{cases} |\alpha| > |\beta| \\ \text{ó} \\ |\alpha| = |\beta| \text{ y } x^\alpha \succ_{lex} x^\beta, \end{cases}$$

esto es, los monomios se ordenan por grado total, y en caso de igualdad de grados, se usa el orden lexicográfico.

c) **Orden Lexicográfico Graduado Inverso (grevlex)**.

$$x^\alpha \succ_{grevlex} x^\beta \Leftrightarrow \begin{cases} |\alpha| > |\beta| \\ \text{ó} \\ |\alpha| = |\beta| \quad \text{y en } (\alpha_1, \cdots, \alpha_n) - (\beta_1, \cdots, \beta_n) \\ \qquad\qquad\quad \text{la primera coordenada no nula, de derecha} \\ \qquad\qquad\quad \text{a izquierda, es negativa.} \end{cases}$$

Ejemplo 1.1.4. *Los monomios $x^2y^2z^2$, x^3, xy^4z, x^2y^3z en $k[x, y, z]$ con $x > y > z$ se ordenan:*
según el orden lexicográfico

$$x^3 \succ_{lex} x^2y^3z \succ_{lex} x^2y^2z^2 \succ_{lex} xy^4z,$$

según el orden lexicográfico graduado

$$x^2y^3z \succ_{grlex} x^2y^2z^2 \succ_{grlex} xy^4z \succ_{grlex} x^3,$$

según el orden lexicográfico graduado inverso

$$x^2y^3z \succ_{grevlex} xy^4z \succ_{grevlex} x^2y^2z^2 \succ_{grevlex} x^3.$$

Definición 1.1.5. *Sea $f = \sum_\alpha c_\alpha x^\alpha$ un polinomio no nulo, $\alpha = (\alpha_1, \cdots, \alpha_n)$ en $\mathbb{Z}^n_{\geq 0}$. Fijado un orden monomial en $k[x_1, x_2, \cdots, x_n]$, definimos:*

- *Multigrado de f: $M(f) = \max\{\alpha \in \mathbb{Z}^n_{\geq 0},\ c_\alpha \neq 0\}$.*
- *Coeficiente líder de f: $LC(f) = c_{M(f)} \in k$.*
- *Monomio líder de f: $LM(f) = x^{M(f)}$.*
- *Término líder de f: $LT(f) = LC(f)LM(f)$.*

1.2. Algoritmo de la división

Teorema 1.2.1 (Algoritmo de la división)**.** *Fijado un orden monomial $\succ$ sobre $k[x_1, x_2, \cdots, x_n]$, considere $F = (f_1, f_2, \cdots, f_s)$ una s-upla ordenada de polinomios en $k[x_1, x_2, \cdots, x_n]$. Entonces cada $f \in k[x_1, x_2, \cdots, x_n]$ puede ser escrito en la forma:*

$$f = a_1 f_1 + a_2\, f_2 + \cdots + a_s f_s + r$$

donde para cada i: $a_i,\ r \in k[x_1, x_2, \cdots, x_n]$, $a_i\, f_i = 0$ o $LT(f) \succ LT(a_i\, f_i)$ y $r = 0$ o r es una combinación lineal de monomios, de manera que ninguno de ellos es divisible por alguno de los $LT(f_1),\ LT(f_2), \cdots, LT(f_s)$.

El polinomio r se denomina residuo de la división de f por F y se denota mediante $\overline{f}^F$.

Ejemplo 1.2.2. *Dividir f por $F = (f_1, f_2)$ donde*

$$f = \frac{3}{4}x^2yz + xy^2z + xyz^2, \quad f_1 = xy - z, \quad f_2 = xz - z$$

son polinomios en $\mathbb{Q}[x, y, z]$ provisto del orden lexicográfico con $x > y > z$.

Solución.

$$\begin{array}{rr}
 & \frac{3}{4}xz + yz + z^2 \ , \ \frac{3}{4}z \\ \cline{2-2}
xy - z \ , \ xz - z \ \big) & \frac{3}{4}x^2yz + xy^2z + xyz^2 \\
 & -\frac{3}{4}x^2yz + \frac{3}{4}xz^2 \\ \cline{2-2}
 & xy^2z + xyz^2 + \frac{3}{4}xz^4 \\
 & - xy^2z + yz^2 \\ \cline{2-2}
 & xyz^2 + \frac{3}{4}xz^2 + yz^2 \\
 & - xyz^2 + z^3
\end{array} \qquad ([1])$$

[1] $\begin{array}{r|l} & \text{cociente} \\ \cline{2-2} \text{divisores} & \text{dividendo} \end{array}$

$$\begin{array}{r} \frac{3}{4}xz^2 + yz^2 + z^3 \\ -\frac{3}{4}xz^2 + \frac{3}{4}z^2 \\ \hline yz^2 + z^3 + \frac{3}{4}z^2 \end{array}$$

En *Mathematica* se usa la función

```
PolynomialReduce[f,{f1,f2},{x,y,z}]
```

que origina

$$\left\{\left\{\frac{1}{4}\left(3xz+4yz+4z^2\right),\frac{3z}{4}\right\},\frac{1}{4}\left(4yz^2+4z^3+3z^2\right)\right\}$$

es decir

$$f = \left(\frac{3}{4}xz + yz + z^2\right) f_1 + \left(\frac{3}{4}z\right) f_2 + \left(\frac{3}{4}z^2 + yz^2 + z^3\right)$$

1.3. Teorema de la base de Hilbert

Sean $A \subset \mathbb{Z}^n_{\geq 0}$ y $S = \{f_\alpha \ : \ \alpha \in A\} \subset k[x_1, x_2, \cdots, x_n]$. El conjunto

$$I = \left\{\sum_{\alpha \in A} h_\alpha f_\alpha \ : \ h_\alpha \in k[x_1, x_2, \cdots, x_n]\right\}$$

es un ideal de $k[x_1, x_2, \cdots, x_n]$. El ideal I se denomina *ideal generado* por S y se denota $I = \langle S \rangle$; S se denomina conjunto de generadores de I. En particular, si $S = \{f_1, f_2, \cdots, f_n\}$, se dice que $I = \langle f_1, f_2, \cdots, f_n \rangle$ es *finitamente generado*.

Definición 1.3.1. *Un ideal $I \subset k[x_1, x_2, \cdots, x_n]$ es un ideal **monomial** si se puede expresar en la forma*

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

Un ideal es monomial si es generado por monomios.

Por ejemplo, el ideal $I = \langle\ x^3 + xy^4, y^2\rangle$ es un ideal monomial porque $I = \langle\ x^3, y^2\rangle$.

Lema 1.3.2 (Dickson). *Si $I = \langle x^\alpha : \alpha \in A\rangle \subset k[x_1, x_2, \cdots, x_n]$ es un ideal monomial, entonces I se puede escribir como $I = \langle x^{\alpha(1)}, \cdots, x^{\alpha(s)}\rangle$ donde $\alpha(1), \cdots, \alpha(s) \in A$, es decir I es finitamente generado.*

Teorema 1.3.3 (Teorema de la Base de Hilbert). *Cada ideal $I \subset k[x_1, x_2, \ldots, x_n]$ tiene un conjunto finito de generadores. Es decir, existen $f_1, f_2, \ldots, f_s \in I$ tal que*

$$I = \langle f_1, f_2, \ldots, f_s\rangle.$$

1.4. Bases de Gröbner

1.4.1. Definición y propiedades

Las bases de Gröbner constituyen los mejores conjuntos generadores de un ideal $I \subset k[x_1, x_2, \cdots, x_n]$.

Sea $I \subset k[x_1, x_2, \cdots, x_n]$ un ideal, $I \neq \{0\}$. Denotemos con

$$LT(I) = \{cx^\alpha : \exists f \in I; LT(f) = cx^\alpha\},$$

al conjunto de los términos líderes de I.

Proposición 1.4.1. *Sea $I \subset k[x_1, x_2, \cdots, x_n]$ un ideal, $I \neq \{0\}$. Entonces*

1. *$\langle LT(I)\rangle$ es un ideal monomial.*

2. *Existen $g_1, \cdots, g_t \in I$ de tal manera que*

$$\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle.$$

Definición 1.4.2. *Fijado un orden monomial en* $k[x_1, x_2, \cdots, x_n]$*, un conjunto finito* $G = \{g_1, \ldots, g_t\}$ *de un ideal* $I \subset k[x_1, x_2, \cdots, x_n]$ *es una Base de Gröbner para* I *si*

$$\langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle.$$

Proposición 1.4.3. *Sea* $I \subset k[x_1, x_2, \cdots, x_n]$ *un ideal,* $I \neq \{0\}$ *y* $G = \{g_1, \ldots, g_t\} \subset I$*,* $g_i \neq 0$*. Las siguientes afirmaciones son equivalentes:*

i) G *es una base de Gröbner para* I*.*

ii) $f \in I$ *si y solo si el residuo de la división de* f *por* G *es cero (* $\overline{f}^{G} = 0$ *).*

iii) Para todo $f \in I$*,* $f \neq 0$*, existe un* $i \in \{1, 2, \cdots, n\}$ *tal que* $LM(g_i)$ *divide a* $LM(f)$*.*

Las bases de Gröbner tienen la propiedad: el residuo de la división de un polinomio $f \in k[x_1, x_2, ..., x_n]$ por los elementos de G es único aunque se permuten los elementos de G.

1.4.2. Algoritmo de Buchberger

Definición 1.4.4. *Sean $f, g \in k[x_1, x_2, ..., x_n]$ polinomios no nulos con multigrados $\alpha = (\alpha_1, \cdots, \alpha_n)$ y $\beta = (\beta_1, \cdots, \beta_n)$, respectivamente. El S-polinomio de f y g denotado por S(f,g), se define mediante*

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

*donde $\gamma = (\gamma_1, \cdots, \gamma_n)$, $\gamma_i = \text{máx}\{\alpha_i, \beta_i\}$, $i = 1, 2, \cdots, n$. x^γ se denomina el **mínimo común múltiplo** de $LM(f)$ y $LM(g)$, $x^\gamma = MCM\{LM(f), LM(g)\}$.*

Fijado un orden monomial en $k[x_1, x_2, ..., x_n]$, sea $I = \langle f_1, \cdots, f_s \rangle \neq \{0\}$ un ideal polinomial. Una base de Gröbner para I puede ser construida en un número finito de pasos como lo muestra el algoritmo de Buchberger:

Algoritmo de Buchberger

```
Input: F = (f1, ..., fs)
Ouput: una base de Gröbner G = (g1, .., gt) para I, con F ⊂ G
G := F
REPEAT
        G':=G
        FOR cada par (p, q), p ≠ q en G' DO
            S:= residuo de la división de S(p, q) por G'
            IF S ≠ 0 THEN G := G ∪ {S}
UNTIL G=G'
```

El conjunto que origina el algoritmo de Buchberger, generalmente, contiene elementos redundantes. La depuración de estos elementos se logra construyendo una base de Gröbner reducida.

Definición 1.4.5. *Una base de Gröbner reducida para un ideal polinomial I es una base de Gröbner G para I tal que:*

1. $LC(g) = 1$ *para todo* $g \in G$.

2. *Para todo* $p \in G$, *ningún monomio de* p *pertenece a* $\langle LT(G \setminus \{p\}) \rangle$.

Proposición 1.4.6. *Sea* $I \neq \{0\}$ *un ideal polinomial. Para un orden mononial fijado,* I *tiene una única base de Gröbner reducida.*

Ejemplo 1.4.7. *Dado* $I = \langle x^2 - 2x + z, x - yz, y^2 - 7yz \rangle \subset \mathbb{Q}[x, y, z]$, *con el orden lexicográfico. ¿Pertenece el polinomio* $f = x^2y + 2y^2 - z^2$ *al ideal* I*?*

Solución.
Hagamos $f1 = x^2 - 2x + z$, $f2 = x - yz$, $f3 = y^2 - 7yz$ y $f = x^2y + 2y^2 - z^2$.
Usando el algoritmo de Buchberger calculamos la base de Gröbner del ideal I, la cual es

$$G = \{z - 14z^2 + 49z^4, yz - 7z^2, y^2 - 49z^2, x - 7z^2\}.$$

Finalmente dividimos f por G obteniendo

$$f = yf1 + 2yf2 + (2z + 2)f3 + 13yz - z^2 + 14yz^2.$$

Como el residuo $r = 13yz - z^2 + 14yz^2$ es diferente de cero, entonces $f \notin I$.

Capítulo 2

Aplicaciones de las Bases de Gröbner

Existen muchas aplicaciones de las bases de Gröbner en distintas áreas, en esta publicación mostramos algunas de ellas en: geometría algebraica, teoría de grafos, sistemas de ecuaciones polinomiales, optimización con restricciones polinomiales y programación entera.

2.1. Variedades afines y sistemas de ecuaciones polinomiales.

2.1.1. Variedades afines.

El *espacio afín de dimensión* n sobre el campo k es el conjunto

$$k^n = \{(a_1, \ldots, a_n);\ a_1, \ldots, a_n \in k\}.$$

Los elementos de k^n se denominan *puntos*. k^1 es la *recta afín*, k^2 es el *plano afín*.

Si S es un subconjunto del anillo de polinomios $k[x_1, x_2, ..., x_n]$, el conjunto de los ceros comunes de los polinomios de S,

$$\nu(S) = \{P = (a_1, ..., a_n) \in k^n;\ f(P) = 0, \forall f \in S\}$$

se denomina *conjunto algebraico afín* o simplemente *conjunto algebraico o conjunto afín*.

Si I es el ideal generado por S, $I = \langle S \rangle$, entonces los ceros de I son los ceros de S, es decir $\nu(I) = \nu(S)$.

Por ejemplo: $\nu(\{0\}) = k^n$ y $\nu(\{1\}) = \phi$. Luego k^n y ϕ son conjuntos algebraicos afines.

Por el Teorema de la base de Hilbert, todos los ideales de $k[x_1, x_2, ..., x_n]$ son finitamente generados. Entonces, existe un conjunto finito de polinomios $\{f_1, \ldots, f_s\}$ tal que $I = \langle f_1, ..., f_s \rangle$. Es decir, $\nu(I)$ es el conjunto de soluciones simultáneas $(a_1, ..., a_n) \in k^n$ del sistema de ecuaciones polinomiales

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_s(x_1, \ldots, x_n) &= 0. \end{aligned}$$

Un conjunto algebraico $V \subset k^n$ es *irreducible* si en toda expresión de V como una unión de otros conjuntos algebraicos $V = V_1 \cup V_2$, se tiene $V = V_1$ o $V = V_2$. Un conjunto algebraico afín irreducible en k^n se denomina *variedad afín*.

Dado un subconjunto X de k^n, el subconjunto de polinomios que se anulan en X forman un ideal de $k[x_1, x_2, ..., x_n]$ llamado el *ideal del conjunto de puntos* X,

$$\mathcal{I}(X) = \{f \in k[x_1, x_2, ..., x_n]; f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in X\}$$

Por ejemplo, $\mathcal{I}(k^n) = \{0\}$ cuando k es infinito.

Definición 2.1.1. *Si A es un anillo conmutativo con identidad e $I \subseteq A$ es un ideal, el radical de I es el conjunto $\sqrt{I} = \{a \in A; a^n \in I,$ para algún $n \in \mathbb{N}\}$.*

$\sqrt{I}$ es un ideal. Un ideal I es un *ideal radical* si $\sqrt{I} = I$.

Teorema 2.1.2 (Teorema de los ceros de Hilbert. Versión débil)**.** *Sea I un ideal de $\mathbb{C}[x_1, \ldots, x_n]$. I es un ideal propio si y solo si $\nu(I) \neq \phi$.*

Del teorema se deduce que $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$ si y solo $\nu(I) = \phi$. Una demostración de este teorema usa bases de Gröbner.

Teorema 2.1.3 (Teorema de los ceros de Hilbert. Versión fuerte)**.** *Si I es un ideal de $\mathbb{C}[x_1, \ldots, x_n]$, entonces $\mathcal{I}(\nu(I)) = \sqrt{I}$. Es decir, todo ideal de $\mathbb{C}[x_1, \ldots, x_n]$ es un ideal radical.*

Aplicando el Teorema 2.1.3, se concluye que las aplicaciones $\mathcal{I}$, ν

$$\{\text{subconjuntos algebraicos de } \mathbb{C}^n\} \rightleftarrows \{\text{ideales radicales de } \mathbb{C}[x_1, ..., x_n]\}$$

son inversas una de la otra.

Esta correspondencia “traduce” propiedades geométricas de conjuntos algebraicos afines en $\mathbb{C}^n$ a propiedades algebraicas de los ideales radicales en el anillo $\mathbb{C}[x_1, \ldots, x_n]$.

Ejemplo 2.1.4. *Grafique los conjuntos algebraicos :*

1. $\nu(x^2 + y^2 + (z-1)^2 - 4, x^2 + z^2 - 1)$ en $\mathbb{R}^3$ es el conjunto de ceros de

$$\begin{aligned} x^2 + y^2 + (z-1)^2 - 4 &= 0 \\ x^2 + z^2 - 1 &= 0. \end{aligned}$$

   Es la curva de intersección de las variedades afines: la esfera de centro $(0, 0, 1)$ y radio 2 y el cilindro circular de radio 1 con eje el eje Y (figura 2.1).

   Usamos *Mathematica* para hallar la base de Gröbner del ideal generado por los polinomios dados:

   `GroebnerBasis`$[x^2 + y^2 + (z-1)^2 - 4, x^2 + z^2 - 1, x, y, z]$.

   Obtenemos: $G = \{-2 + y^2 - 2z, -1 + x^2 + z^2\}$.

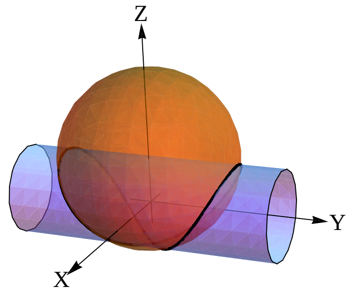

Figura 2.1: $\nu(x^2 + y^2 + (z-1)^2 - 4, x^2 + z^2 - 1)$ en $\mathbb{R}^3$.

Ahora, $\nu(-2+y^2-2z, -1+x^2+z^2)$ es la intersección de los cilindros $y^2-2z-2=0$ y $x^2+z^2-1=0$ (figura 2.2).

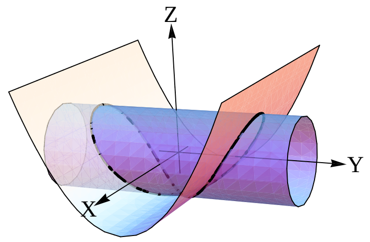

Figura 2.2: $\nu(-2 + y^2 - 2z, -1 + x^2 + z^2)$ en $\mathbb{R}^3$.

2. $\nu((x^2 + y^2 - z)(z + 2))$ en $\mathbb{R}^3$.

   Tenemos: $x^2+y^2-z=0$ o $z+2=0$. Este conjunto algebraico no es irreducible y por tanto no es una variedad afín (figura 2.3).

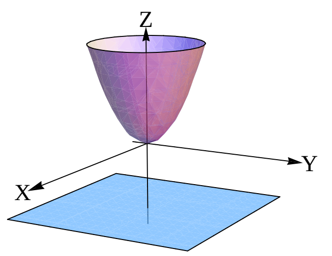

Figura 2.3: $\nu((x^2 + y^2 - z)(z + 2))$ en $\mathbb{R}^3$.

2.1.2. Sistemas de ecuaciones polinomiales

En la resolución de sistemas polinomiales por eliminación usaremos los Teoremas de Eliminación y Extensión.
Si $I \subset \mathbb{C}[x_1, \ldots, x_n]$ es un ideal, entonces

$$I_i = I \cap \mathbb{C}[x_{i+1}, \ldots, x_n]$$

es un ideal llamado *ideal de la i-ésima eliminación*

Teorema 2.1.5. *(Teorema de Eliminación) Si G es una base de Gröbner para I, entonces*

$$G_i = G \cap \mathbb{C}[x_{i+1}, \ldots, x_n]$$

es una base de Gröbner para el ideal I_i,

Un punto $(a_{i+1}, \ldots, a_n) \in \nu(I_i) \subset \mathbb{C}^{n-i}$ se denomina una *solución parcial* de $\nu(I)$.

Teorema 2.1.6. *(Teorema de Extensión) Si el coeficiente líder de los polinomios de una base de Gröbner para I_{i-1} respecto al orden lexicográfico, no se anula, entonces una solución parcial $(a_{i+1}, \ldots, a_n)$ en $\nu(I_i)$ se extiende a una solución $(a_i, a_{i+1}, \ldots, a_n)$ en $\nu(I_{i-1})$.*

Ejemplo 2.1.7. *Resolvemos el sistema de ecuaciones:*

$$\begin{aligned} x^2 + y^2 + z^2 - 3 &= 0 \\ x^2 + z^2 - 2 &= 0 \\ x - y + 2z &= 0. \end{aligned}$$

Obtenemos la base de Gröbner del ideal

$$I = \langle x^2 + y^2 + z^2 - 3,\ x^2 + z^2 - 2,\ x - y + 2z \rangle,$$

`GroebnerBasis`$[\{x^2 + y^2 + z^2 - 3, x^2 + z^2 - 2, x - y + 2z\}, \{x, y, z\}]$.

$G = \{1 - 26z^2 + 25z^4, 4y + 21z - 25z^3, 4x + 29z - 25z^3\}$.

Aplicamos el teorema de eliminación y obtenemos la solución parcial del sistema,

$G \cap \mathbb{C}[y, z] = \{1 - 26z^2 + 25z^4, 4y + 21z - 25z^3\}$

$\texttt{Solve}[\{1 - 26z^2 + 25z^4 == 0, 4y + 21z - 25z^3 == 0\}, \{y, z\}]$

$y = -1, z = -1;$
$y = -1, z = \frac{1}{5};$
$y = 1, z = -\frac{1}{5};$
$y = 1, z = 1.$

Como el coeficiente lider de $4x + 29z - 25z^3$ es diferente de cero, aplicamos el teorema de extensión. La solución del sistema de ecuaciones es:

$x = -\frac{7}{5}, y = -1, z = \frac{1}{5};$
$x = 1, y = -1, z = -1;$
$x = -1, y = 1, z = 1;$
$x = \frac{7}{5}, y = 1, z = -\frac{1}{5}.$

2.2. Problema de los tres colores.

Sea $\mathcal{G}$ un grafo de n vértices con a lo más una arista entre cualquier par de vértices. Deseamos colorear todos los vértices de tal manera que sólo se usen 3 colores y ningún par de vértices adyacentes tengan el mismo color. Si $\mathcal{G}$ puede ser coloreado de esta manera, entonces $\mathcal{G}$ es llamado 3-coloreable. Esta aplicación se basa en el trabajo realizado por Bayer [2].

A continuación presentamos el procedimiento a seguir para resolver este problema.

i) Cada color será representado por una de las raíces cúbicas complejas de la unidad: $1, \xi, \xi^2$, donde $\xi = e^{\frac{2\pi i}{3}}$.

ii) Denotaremos cada vértice con p, donde $p = 1, 2, \cdots, n$ y con x_p el color asignado al correspondiente vértice p, es decir se tiene

$$x_p^3 = 1, \quad 1 \leq p \leq n. \tag{2.2.1}$$

iii) Sea (p, q) un par de vértices adyacentes. Se cumple

$$0 = x_p^3 - x_q^3 = (x_p - x_q)(x_p^2 + x_p x_q + x_q^2).$$

Como deseamos que $x_p \neq x_q$, entonces

$$x_p^2 + x_p x_q + x_q^2 = 0 \tag{2.2.2}$$

iv) Construimos el ideal I generado por todos los polinomios $x_p^3 - 1, x_p^2 + x_p x_q + x_q^2$ obtenidos de las ecuaciones (2.2.1) y (2.2.2), respectivamente.
Para determinar si el grafo $\mathcal{G}$ es coloreable o no, basta averiguar si la variedad algebraica $\nu(I) \subset \mathbb{C}^n$ es diferente del vacío o no.

v) Hallamos una base reducida de Gröbner G de I y por el teorema 2.1.2 bastará observar si 1 pertenece o no a G.

Si 1 no pertenece a G, entonces $\mathcal{G}$ es 3-coloreable. En caso contrario no lo es.

Ejemplo 2.2.1. *Consideremos el grafo $\mathcal{G}$ con 8 vértices y 14 aristas mostrado en la figura 2.4:*

Construimos el ideal I generado por los polinomios
$x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_5^3 - 1, x_6^3 - 1, x_7^3 - 1, x_8^3 - 1,$

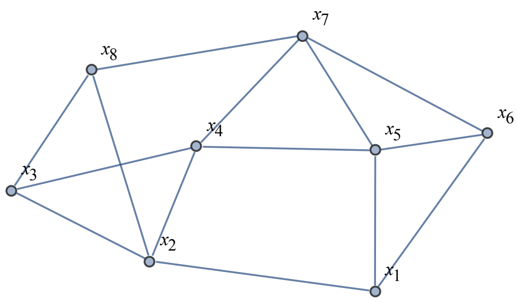

Figura 2.4: Grafo $\mathcal{G}$ antes de ser coloreado.

$$x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_5 + x_5^2, x_1^2 + x_1x_6 + x_6^2,$$
$$x_2^2 + x_2x_3 + x_3^2, x_2^2 + x_2x_4 + x_4^2, x_2^2 + x_2x_8 + x_8^2, x_3^2 + x_3x_4 + x_4^2,$$
$$x_3^2 + x_3x_8 + x_8^2, x_4^2 + x_4x_5 + x_5^2, x_4^2 + x_4x_7 + x_7^2,$$
$$x_5^2 + x_5x_6 + x_6^2, x_5^2 + x_5x_7 + x_7^2, x_6^2 + x_6x_7 + x_7^2, x_7^2 + x_7x_8 + x_8^2.$$

Usando la función `GroebnerBasis` de Mathematica obtenemos la base de Gröbner de I:

$$G = \{-1 + x_8^3, x_7^2 + x_7x_8 + x_8^2, x_6 - x_8, x_5 + x_7 + x_8, x_4 - x_8, x_3 - x_7,$$
$$x_2 + x_7 + x_8, x_1 - x_7\}.$$

Como $1 \notin G$ el problema tiene solución. Una de ellas se muestra en la figura 2.5.

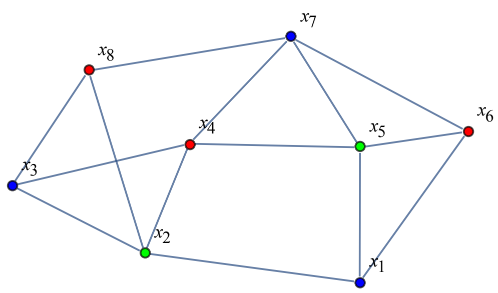

Figura 2.5: Grafo $\mathcal{G}$ coloreado.

El problema de los tres colores es equivalente al problema de pintar todos las regiones de un mapa con 3 colores donde los vértices son las regiones y los vértices adyacentes son las regiones limítrofes. Mostramos algunos ejemplos que ilustran esta equivalencia.

Ejemplo 2.2.2. *Consideremos el mapa de América del Sur. Veamos si el conjunto de paises enumerados del 1 al 8 es 3 - coloreable.*

Figura 2.6: Mapa de América del Sur.

`GroebnerBasis` $[\{x_1^3-1, x_2^3-1, x_3^3-1, x_4^3-1, x_5^3-1, x_6^3-1, x_7^3-1, x_8^3-1,$ $x_1^2+x_1x_2+x_2^2, x_1^2+x_1x_3+x_3^2, x_1^2+x_1x_7+x_7^2, x_1^2+x_1x_8+x_8^2, x_2^2+x_2x_8+x_8^2, x_3^2+$ $x_3x_5+x_5^2, x_3^2+x_3x_6+x_6^2, x_3^2+x_3x_7+x_7^2, x_4^2+x_4x_5+x_5^2, x_5^2+x_5x_6+x_6^2, x_5^2+x_5x_7+$ $x_7^2,\}, \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}]$

G=$\{-1+x_8^3, -1+x_7^3, x_6-x_7, x_5x_7+x_7^2-x_5x_8-x_8^2, x_5^2+x_5x_8+x_8^2, x_4^2+x_4x_5-$ $x_5x_8-x_8^2, x_3+x_5+x_7, x_2+x_5+x_8, x_1-x_5\}$.

Nuevamente $1 \notin G$. Una solución se muestra en la figura 2.7:

Para hallar otra solución sugerida por la base de Gröbner podemos factorizar algunos de los polinomios.

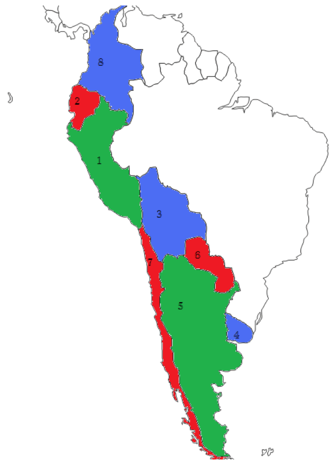

Figura 2.7: Primera Solución.

$G = \{-1 + x_8^3, -1 + x_7^3, x_6 - x_7, (x_7 - x_8)(x_5 + x_7 + x_8), x_5^2 + x_5x_8 + x_8^2, (x_4 - x_8)(x_4 + x_5 + x_8), x_3 + x_5 + x_7, x_2 + x_5 + x_8, x_1 - x_5\}$.

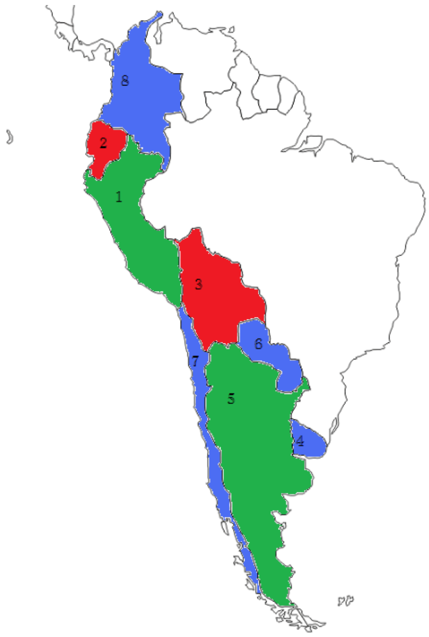

Figura 2.8: Segunda Solución.

Ejemplo 2.2.3. *¿Qué ocurre si en el problema 2.2.2 agregamos a Brasil como país número 9 ?*

Por el número de países que limitan con Brasil, figura 2.8, se puede intuir que el problema no tiene solución.

Veamos que nos dice la base de Gröbner en este caso.

`GroebnerBasis` $[\{x_1{}^3-1, x_2{}^3-1, x_3{}^3-1, x_4{}^3-1, x_5{}^3-1, x_6{}^3-1, x_7{}^3-1, x_8{}^3-1, x_9{}^3-1, x_1{}^2+x_1x_2+x_2{}^2, x_1{}^2+x_1x_3+x_3{}^2, x_1{}^2+x_1x_7+x_7{}^2, x_1{}^2+x_1x_8+x_8{}^2, x_1{}^2+x_1x_9+x_9{}^2, x_2{}^2+x_2x_8+x_8{}^2, x_3{}^2+x_3x_5+x_5{}^2, x_3{}^2+x_3x_6+x_6{}^2, x_3{}^2+x_3x_7+x_7{}^2, x_3{}^2+x_3x_9+x_9{}^2, x_4{}^2+x_4x_5+x_5{}^2, x_4{}^2+x_4x_9+x_9{}^2, x_5{}^2+x_5x_6+x_6{}^2, x_5{}^2+x_5x_7+x_7{}^2, x_5{}^2+x_5x_9+x_9{}^2, x_6{}^2+x_6x_9+x_9{}^2, x_8{}^2+x_8x_9+x_9{}^2\}, \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\}]$

G=$\{1\}$

Esto confirma que el problema no tiene solución.

Ejemplo 2.2.4. *Finalmente veamos en el ejemplo 2.2.3 lo que ocurriría si agregamos un cuarto color.*

Figura 2.9: Problema con 4 colores.

`GroebnerBasis` $[\{{x_1}^4-1, {x_2}^4-1, {x_3}^4-1, {x_4}^4-1, {x_5}^4-1, {x_6}^4-1, {x_7}^4-1, {x_8}^4-1, {x_9}^4-1, {x_1}^3+x_1{x_2}^2+{x_1}^2x_2+{x_2}^3, {x_1}^3+x_1{x_3}^2+{x_1}^2x_3+{x_3}^3, {x_1}^3+x_1{x_7}^2+{x_1}^2x_7+{x_7}^3, {x_2}^3+x_2{x_8}^2+{x_2}^2x_8+{x_3}^3, {x_3}^3+x_3{x_5}^2+{x_3}^2x_5+{x_5}^3, {x_3}^3+x_3{x_6}^2+{x_3}^2x_6+{x_6}^3, {x_3}^3+x_3{x_7}^2+{x_3}^2x_7+{x_7}^3, {x_3}^3+x_3{x_9}^2+{x_3}^2x_9+{x_9}^3, {x_4}^3+x_4{x_5}^2+{x_4}^2x_5+{x_5}^3, {x_4}^3+x_4{x_9}^2+{x_4}^2x_9+{x_9}^3, {x_5}^3+x_5{x_6}^2+{x_5}^2x_6+{x_6}^3, {x_5}^3+x_5{x_7}^2+{x_5}^2x_7+{x_7}^3, {x_6}^3+x_6{x_9}^2+{x_6}^2x_9+{x_9}^3\}, \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\}]$

$G=\{-1+x_9^4, x_8^3+x_8^2x_9+x_8x_9^2+x_9^3, x_7^3+x_7^2x_8+x_7x_8^2-x_8^2x_9-x_8x_9^2-x_9^3, x_6^2+x_6x_8+x_8^2+x_6x_9+x_8x_9+x_9^2, x_5x_7^2+x_6x_7^2+x_5x_7x_8+x_6x_7x_8+x_7^2x_8+x_5x_8^2+x_6x_8^2+x_7x_8^2+x_5x_7x_9+x_6x_7x_9+x_7^2x_9+x_5x_8x_9+x_6x_8x_9+2x_7x_8x_9+x_8^2x_9+x_5x_9^2+x_6x_9^2+x_7x_9^2+x_8x_9^2, x_5x_6-x_5x_7-x_7^2-x_7x_8-x_8^2-x_6x_9-x_8x_9-x_9^2, x_5^2+x_5x_7+x_7^2+x_5x_8+x_7x_8+x_8^2, x_4^2x_7^2-x_4x_6x_7^2+x_4^2x_7x_8-x_4x_6x_7x_8-x_4x_7^2x_8+x_6x_7^2x_8+x_4^2x_8^2-x_4x_6x_8^2-x_4x_7x_8^2+x_6x_7x_8^2+x_4^2x_7x_9-x_4x_6x_7x_9+x_4^2x_8x_9-x_4x_6x_8x_9-x_4x_7x_8x_9+x_6x_7x_8x_9+x_4^2x_9^2-x_4x_6x_9^2+x_4x_9^3-x_6x_9^3, x_4^2x_5-x_4x_5x_7-x_4x_7^2-x_4x_5x_8-x_4x_7x_8+x_5x_7x_8+x_7^2x_8-x_4x_8^2+x_7x_8^2-x_4^2x_9-x_4x_9^2-x_9^3, x_4^3+x_4^2x_9+x_4x_9^2+x_9^3, x_3-x_8, x_2^3+x_2^2x_8+x_2x_8^2-x_8^2x_9-x_8x_9^2-x_9^3, x_1x_2+x_2^2-x_1x_7-x_7^2+x_2x_8-x_7x_8, x_1^2+x_1x_7+x_7^2+x_1x_8+x_7x_8+x_8^2\}.$

Antes de dar una solución podemos factorizar los polinomios de G que tienen más de dos términos.

F1=$(x_8+x_9)\left(x_8^2+x_9^2\right)$
F2=$(x_7-x_9)\left(x_7^2+x_7x_8+x_8^2+x_7x_9+x_8x_9+x_9^2\right)$
F3=$x_6^2+x_6x_8+x_8^2+x_6x_9+x_8x_9+x_9^2$
F4=$x_5x_7^2+x_6x_7^2+x_5x_7x_8+x_6x_7x_8+x_7^2x_8+x_5x_8^2+x_6x_8^2+x_7x_8^2+x_5x_7x_9+x_6x_7x_9+x_7^2x_9+x_5x_8x_9+x_6x_8x_9+2x_7x_8x_9x_8^2x_9+x_5x_9^2+x_6x_9^2+x_7x_9^2+x_8x_9^2$
F5=$x_5x_6-x_5x_7-x_7^2-x_7x_8-x_8^2-x_6x_9-x_8x_9-x_9^2$
F6=$x_5^2+x_5x_7+x_7^2+x_5x_8+x_7x_8+x_8^2$
F7=$(x_4-x_6)(x_4x_7^2+x_4x_7x_8-x_7^2x_8+x_4x_8^2-x_7x_8^2+x_4x_7x_9+x_4x_8x_9-x_7x_8x_9+x_4x_9^2+x_9^3)$
F8=$x_4^2x_5-x_4x_5x_7-x_4x_7^2-x_4x_5x_8-x_4x_7x_8+x_5x_7x_8+x_7^2x_8-x_4x_8^2+x_7x_8^2-x_4^2x_9-$

$x_4x_9^2 - x_9^3$

F9=$(x_4 + x_9)\,(x_4^2 + x_9^2)$

F10=$(x_2 - x_9)\,(x_2^2 + x_2x_8 + x_8^2 + x_2x_9 + x_8x_9 + x_9^2)$

F11=$(x_2 - x_7)\,(x_1 + x_2 + x_7 + x_8)$

F12=$x_1^2 + x_1x_7 + x_7^2 + x_1x_8 + x_7x_8 + x_8^2$.

Los siguientes polinomios son los únicos que no han sido factorizados:
$-1 + x_9^4, x_3 - x_8$.

Una solución del problema, a la luz de estos resultados, se muestra en la figura 2.10:

Figura 2.10: Solución con 4 colores.

2.3. Optimización restringida a un sistema polinomial

En esta aplicación se muestra el uso de las bases de Gröbner en la solución de problemas de optimización, cuyas restricciones son funciones polinomiales, mediante el método de los Multiplicadores de Lagrange. Se presenta ejemplos cuya solución se obtiene usando el software *Mathematica*.

Consideremos el siguiente problema: Dada una función polinomial $f : U \to \mathbb{R}$ y funciones polinomiales $\varphi_1, \ldots, \varphi_k : U \to \mathbb{R}$ definidas en un conjunto abierto $U \subset \mathbb{R}^n$, $k < n$.

Sea M el conjunto cero de

$$\varphi = (\varphi_1, \ldots, \varphi_k) : U \to \mathbb{R}^k,$$

es decir

$$M = \{x \in U | \varphi(x) = 0\}.$$

Estamos interesados en encontrar extremos locales de f en una vecindad $V(x_0) \subset U$, es decir

$$f(x) \leq f(x_0),\ \ \forall x \in M \cap V(x_0), \quad \text{o} \quad f(x) \geq f(x_0),\ \ \forall x \in M \cap V(x_0).$$

El teorema de Lagrange establece una condición necesaria para la existencia de extremos de f en M, cuando M es una variedad algebraica.

Teorema 2.3.1 (Lagrange). *Sean $f : U \to \mathbb{R}$ una función polinomial diferenciable y $\varphi = (\varphi_1, \ldots, \varphi_k) : U \to \mathbb{R}^k$ continuamente diferenciable en un abierto $U \subset \mathbb{R}^n$. Además la matriz Jacobiana de φ tiene rango k en cualquier punto x del conjunto cero M de φ, es decir*

$$rank(J(\varphi)(x)) = k, \forall x \in M = \{x \in U | \varphi(x) = 0\}.$$

Entonces se tiene: Si $x_0 \in M$ y $f(x_0)$ es un extremo de f, entonces $\bigtriangledown f(x_0)$ es una combinación lineal de $\bigtriangledown \varphi_1(x_0), \ldots, \bigtriangledown \varphi_k(x_0)$, es decir, existen $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ satisfaciendo

$$\bigtriangledown f(x_0) + \sum_{i=1}^{k} \lambda_i \bigtriangledown \varphi_i(x_0) = 0.$$

Además, si

$$F(x, \lambda) := f(x) + \sum_{i=1}^{k} \lambda_i \varphi_i(x)$$

con $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ *y* $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbb{R}^k$*; y* $p \in M$ *es un punto donde la función alcanza un extremo local de* $f|_M$*, entonces existe*

$$\overline{\lambda} = (\overline{\lambda_1}, \ldots, \overline{\lambda_k}) \in \mathbb{R}^k$$

tal que el sistema de ecuaciones polinomiales

$$\nabla F(x, \lambda) = 0$$

tiene solución $(p, \overline{\lambda}) \in M \times \mathbb{R}^k$.

La función f se denomina función objetivo, la función F se denomina *función de Lagrange* y los números $\lambda_1, \ldots \lambda_k$ se denominan ***Multiplicadores de Lagrange***.

Ejemplo 2.3.2. *Halle los valores extremos de la función* $f(x,y) = \frac{x^2y}{6} - \frac{(x-y^2)}{4} + 4$ *sujeta a la restricción* $\frac{x^2}{9} + \frac{y^2}{4} - 1 = 0$.

Solución. La función objetivo

$$f(x,y) = \frac{x^2y}{6} - \frac{(x-y^2)}{4} + 4 \in \mathbb{Q}[x,y]$$

y la restricción

$$\varphi(x,y) = \frac{x^2}{9} + \frac{y^2}{4} - 1 \in \mathbb{Q}[x,y].$$

En la figura 2.11 se muestra la gráfica de la función f y la restricción donde calcular sus valores extremos.

La función de Lagrange está dada por

$$\mathbf{F}[\mathbf{x}, \mathbf{y}, \lambda]\mathbf{:=}f(x,y) + \lambda\varphi(x,y).$$

A continuación hallamos las derivadas parciales de F

$$\mathrm{D}[\mathrm{F}[\mathbf{x}, \mathbf{y}, \lambda], \{\mathbf{x}, \mathbf{1}\}], \quad \mathrm{D}[\mathrm{F}[\mathbf{x}, \mathbf{y}, \lambda], \{\mathbf{y}, \mathbf{1}\}], \quad \mathrm{D}[\mathrm{F}[\mathbf{x}, \mathbf{y}, \lambda], \{\lambda, \mathbf{1}\}]$$

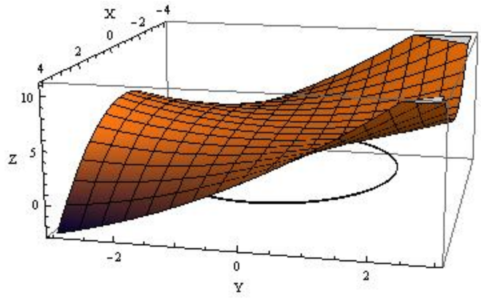

Figura 2.11: Función a optimizar sujeta a una restricción.

con las cuales construimos el sistema de ecuaciones polinomiales

$$\begin{cases} -\frac{1}{4} + \frac{xy}{3} + \frac{2x\lambda}{9} = 0 \\ \frac{x^2}{6} + \frac{y}{2} + \frac{y\lambda}{2} = 0 \\ -1 + \frac{x^2}{9} + \frac{y^2}{4} = 0. \end{cases} \tag{2.3.1}$$

Para hallar la solución del sistema (2.3.1) hacemos uso de las bases de Gröbner. Con esta finalidad consideremos los polinomios

$$\mathrm{f1} = -\frac{1}{4} + \frac{xy}{3} + \frac{2x\lambda}{9}; \qquad \mathrm{f2} = \frac{x^2}{6} + \frac{y}{2} + \frac{y\lambda}{2}; \qquad \mathrm{f3} = -1 + \frac{x^2}{9} + \frac{y^2}{4}.$$

Hallamos la base de Gröbner del ideal $I = \langle f1, f2, f3 \rangle$ en el anillo de polinomios $\mathbb{Q}[x, y, \lambda]$ con el orden lexicográfico y $x > y > \lambda$

G=$\texttt{GroebnerBasis}[\{\mathrm{f1}, \mathrm{f2}, \mathrm{f3}\}, \{x, y, \lambda\}]$

$\{\ 1254951. + 1852416\lambda - 860672\lambda^2 - 2100736\lambda^3 - 299264\lambda^4 + 491520\lambda^5 + 147456\lambda^6,\ 46692878940 + 633606651y + 23035250268\lambda - 54269954816\lambda^2 - 24083257088\lambda^3 + 12797018112\lambda^4 + 5491261440\lambda^5,\ 343508976 + 23466913x + 181494448\lambda - 354277120\lambda^2 - 150707872\lambda^3 + 73646080\lambda^4 + 29386752\lambda^5\ \}$

luego resolvemos el sistema de ecuaciones conformado por la base de Gröbner

$\texttt{SolSist} = \texttt{NSolve}[\mathrm{G} == 0, \{x, y, \lambda\}, 4]$

cuyas soluciones son:

$$\begin{array}{lll} x = -2{,}566 & y = -1{,}037 & \lambda = 1{,}116 \\ x = 1{,}869 & y = 1{,}564 & \lambda = -1{,}745 \\ x = 2{,}693 & y = -0{,}8818 & \lambda = 1{,}741 \\ x = -0{,}283 & y = -1{,}991 & \lambda = -0{,}986 \\ x = -2{,}312 & y = 1{,}274 & \lambda = -2{,}398 \\ x = 0{,}5988 & y = 1{,}960 & \lambda = -1{,}061, \end{array}$$

Finalmente evaluando la función objetivo en los puntos (x, y) de la matriz anterior se tiene

`Table[`f[SolSist[[i]][[1]][[2]],SolSist[[i]][[2]][[2]]],{i,1,6}]

$\{5{,}797;\ 5{,}119;\ 2{,}730;\ 5{,}250;\ 4{,}002;\ 5{,}202\}$

de donde se tiene que $5{,}797$ y $2{,}730$ son los valores extremos de la función f bajo la restricción $\varphi(x, y)$, valores que se alcanzan en los puntos $(-2{,}566; -1{,}037)$ y $(2{,}693; -0{,}8818)$, respectivamente.

2.4. Programación entera

En esta sección desarrollamos el método propuesto por Conti y Traverso [5] para obtener una solución de un problema de optimización lineal entera haciendo uso de bases de Gröbner. Este método transforma las ecuaciones lineales en ecuaciones polinomiales y el problema se reduce a calcular el residuo del monomio de “recursos” respecto de una base de Gröbner.

Un problema de programación entera (IP) consiste en encontrar una solución, $(x_1, x_2, \cdots, x_m)$

en $\mathbb{N}^m$, del sistema de ecuaciones

$$\left\{ \begin{array}{c} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m = b_2 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = b_n \end{array} \right. \tag{2.4.1}$$

que minimice la función de "costo"

$$c(x_1, x_2, \cdots, x_m) = \sum_{j=1}^{m} c_j x_j \tag{2.4.2}$$

donde $a_{ij}, b_i \in \mathbb{Z}$, y $c_j \in \mathbb{R}$, $i = 1, 2, \cdots, n$, $j = 1, 2, \cdots, m$.
Sea $A = (a_{ij})$ y $B = (b_i)$. Consideremos el conjunto

$$\mathbb{P} = \{X = (x_1, x_2, \cdots, x_m) \in \mathbb{N}^n / AX = B\},$$

es decir el conjunto de todas las soluciones del sistema $A\,X = B$, (2.4.1), que se denomina **conjunto factible** con los **recursos** B.

Ahora podemos dividir el problema IP en dos partes:

1. Hallar el conjunto factible $\mathbb{P}$.

2. Evaluar la función de costo en el conjunto $\mathbb{P}$

Inicialmente, nuestro objetivo consiste en hallar un $\overline{X} \in \mathbb{P}$, solución del sistema (2.4.1).

Para hallar $\overline{X} \in \mathbb{P}$, si existe, se considera tres etapas:

a) Transformar el problema (2.4.1) en un problema polinomial asociado.

b) Resolver el problema polinomial usando Bases de Gröbner.

c) Obtener, de la solución del problema polinomial, una solución del sistema (2.4.1), es decir un elemento de $\mathbb{P}$.

Para transformar el sistema (2.4.1) en un problema polinomial asumiremos que los elementos de la matriz $A = (a_{ij})$ son no negativos.

Consideremos variables $z_1, z_2, \cdots, z_n$, una para cada ecuación del sistema (2.4.1) y construimos el sistema

$$\begin{cases} z_1^{a_{11}x_1+a_{12}x_2+\cdots+a_{1m}x_m} = z_1^{b_1} \\ z_2^{a_{21}x_1+a_{22}x_2+\cdots+a_{2m}x_m} = z_2^{b_2} \\ \vdots \\ z_n^{a_{n1}x_1+a_{n2}x_2+\cdots+a_{nm}x_m} = z_n^{b_n} \end{cases} \tag{2.4.3}$$

multiplicando miembro a miembro todas las ecuaciones de (2.4.3) y agrupando convenientemente se obtiene

$$\prod_{j=1}^{m}\left(\prod_{i=1}^{n} z_i^{a_{ij}}\right)^{x_j} = \prod_{i=1}^{n} z_i^{b_i} \tag{2.4.4}$$

Para cada $j = 1, 2, \cdots, m$ llamemos

$$y_j = \prod_{i=1}^{n} z_i^{a_{ij}}$$

con lo cual se tiene el sistema polinomial asociado a (2.4.1)

$$f_j = \prod_{i=1}^{n} z_i^{a_{ij}} - y_j; \quad j = 1, 2, \cdots, m$$

en las variables $z_1, z_2, \cdots, z_n, y_1, y_2, \cdots, y_m$, es decir que $f_j \in k[z_1, z_2, \cdots, z_n, y_1, y_2, \cdots, y_m]$ para cada $j = 1, 2, \cdots, m$.

Proposición 2.4.1. *Sea k un campo y definamos la aplicación*

$$\phi \ : \ k[y_1, y_2, \cdots, y_m] \ \rightarrow \ k[z_1, z_2, \cdots, z_n]$$
$$\phi(y_j) = \prod_{i=1}^{n} z_i^{a_{ij}}$$

para cada $j = 1, 2, \cdots, m$ y $\phi(g(y_1, y_2, \cdots, y_m)) = g(\phi(y_1), \phi(y_2), \cdots, \phi(y_m))$ para $g \in k[y_1, y_2, \cdots, y_m]$. Entonces $(x_1, x_2, \cdots, x_m) \in \mathbb{P}$ si y solo si ϕ aplica el monomio $y_1^{x_1} y_2^{x_2} \cdots y_m^{x_m}$ en el monomio $z_1^{b_1} z_2^{b_2} \cdots z_n^{b_n}$.

Definición 2.4.2. *Un orden monomial en* $k[z_1, z_2, \cdots, z_n, y_1, y_2, \cdots, y_n]$ *tiene la* **propiedad de eliminación** *si cualquier monomio que contiene alguna variable* z_i *es mayor que cualquier monomio que contiene solamente las variables* y_j.

Proposición 2.4.3. *Fijado un orden en* $k[z_1, z_2, \cdots, z_n, y_1, y_2, \cdots, y_m]$ *con la pro- piedad de eliminación, sean* $f_1, f_2, \cdots, f_m \in k[z_1, z_2, \cdots, z_n]$. *Sea* G *una base de Gröbner del ideal*

$$I = \langle f_1 - y_1, f_2 - y_2, \cdots, f_m - y_m \rangle \subset k[z_1, z_2, \cdots, z_n, y_1, y_2, \cdots, y_m]$$

y para cada $f \in k[z_1, z_2, \cdots, z_n]$, *sea* $\overline{f}^G$ *el residuo de la división de* f *por G. Entonces*

a) Un polinomio $f \in k[f_1, f_2, \cdots, f_m]$ *si y solo si* $\overline{f}^G \in k[y_1, y_2, \cdots, y_m]$

b) Si $f \in k[f_1, f_2, \cdots, f_m]$ *y* $g = \overline{f}^G \in k[y_1, y_2, \cdots, y_m]$, *entonces* $f = g(f_1, f_2, \cdots, f_m)$, *es decir que* f *es una expresión polinomial en los* f_j.

c) Si cada f_j *y* f *son monomios y* $f \in k[f_1, f_2, \cdots, f_m]$, *entonces* g *también es un monomio.*

Con la finalidad de mostrar el procedimiento descrito, desarrollamos 2 ejemplos.

Ejemplo 2.4.4. *Resuelva el siguiente sistema de ecuaciones*

$$\begin{aligned} 3x_1 + 2x_2 + x_3 = 10 \\ 4x_1 + 3x_2 + x_3 = 12 \end{aligned}$$

con $x_1, x_2, x_3 \in \mathbb{Z}_{\geq 0}$

Solución. Consideremos las variables z_1 y z_2, una por cada ecuación, con lo cual se tiene el sistema

$$\begin{aligned} {z_1}^{3x_1+2x_2+x_3} &= {z_1}^{10} \\ {z_2}^{4x_1+3x_2+x_3} &= {z_2}^{12} \end{aligned}$$

multiplicando las dos ecuaciones miembro a miembro resulta

$$z_1^{3x_1+2x_2+x_3} z_2^{4x_1+3x_2+x_3} = z_1^{10} z_2^{12}$$

ó

$$(z_1^3 z_2^4)^{x_1} (z_1^2 z_2^3)^{x_2} (z_1 z_2)^{x_3} = z_1^{10} z_2^{12}.$$

Definamos los polinomios

$$\begin{cases} f_1 = z_1^3 z_2^4 - y_1 \\ f_2 = z_1^2 z_2^3 - y_2 \\ f_3 = z_1 z_2 - y_3 \\ q = z_1^{10} z_2^{12} \end{cases}$$

luego se halla la base de Gröbner para el ideal $I = \langle f_1, f_2, f_3 \rangle$ respecto de las variables $z_1 > z_2 > y_1 > y_2 > y_3$

G=`GroebnerBasis`[$\{f_1, f_2, f_3\}, \{z_1, z_2, y_1, y_2, y_3\}$]

$\{y_1 - y_2 y_3, -y_2 + y_3^2 z_2, -y_3^3 + y_2 z_1, -y_3 + z_1 z_2\}$,

el residuo de dividir el monomio de recursos q por G es

r =`PolynomialReduce`[q,G,$\{z_1, z_2, y_1, y_2, y_3\}$][[2]]

$y_2^2 y_3^6$.

Como el residuo $r = y_2^2 y_3^6$ no depende de las variables $z_i, i = 1, 2$, los exponentes de las variables $y_i, i = 1, 2, 3$ que conforman r, constituyen una solución del sistema de ecuaciones inicial, es decir

Solución=`Table[Exponent`[r,u],{u ,{y1,y2,y3}}]

{0,2,6}

es una solución del sistema inicial.

Ejemplo 2.4.5. *Consideremos el sistema de ecuaciones lineales*

$$4x_1 + 5x_2 + x_3 = 37$$
$$2x_1 + 3x_2 + x_4 = 20$$

e introducimos las variables z_1, z_2, una para cada ecuación, en la forma

$$z_1^{4x_1+5x_2+x_3} = z_1^{37}$$
$$z_2^{2x_1+3x_2+x_4} = z_2^{20}$$

luego, multiplicando ambas ecuaciones, el sistema se expresa mediante

$$(z_1^4 z_2^2)^{x_1}(z_1^5 z_2^3)^{x_2}(z_1)^{x_3}(z_2)^{x_4} = z_1^{37} z_2^{20}$$

Sean

$$f_1 = z_1^4 z_2^2 - y_1, \qquad f_2 = z_1^5 z_2^3 - y_2, \qquad f_3 = z_1 - y_3, \qquad f_4 = z_2 - y_4,$$

entonces se tiene el sistema polinomial asociado

$$\begin{cases} f_1 = z_1^4 z_2^2 - y_1 \\ f_2 = z_1^5 z_2^3 - y_2 \\ f_3 = z_1 - y_3 \\ f_4 = z_2 - y_4 \end{cases}$$

en el anillo de polinomos $\mathbb{Q}[z_1, z_2, y_1, y_2, y_3, y_4]$ (con las variables adicionales $y_j, j = 1, 2, 3, 4$). Sea $I = \langle f_1, f_2, f_3, f_4 \rangle$. Ahora, calculamos el residuo, r, de la división del monomio $g = z_1^{37} z_2^{20}$ (que representa los recursos) por una base de Gröbner de I.

a) Respecto del orden lexicográfico con

$$z_1 > z_2 > y_1 > y_2 > y_3 > y_4$$

el residuo es $r = y_3^{37} y_4^{20}$, de donde se tiene una solución del problema original: $x_1 = 0, x_2 = 0, x_3 = 37, x_4 = 20$.

b) Respecto al orden

$$z_1 > z_2 > y_4 > y_3 > y_2 > y_1,$$

el residuo es $r = y_1^8 y_2 y_4$, de donde $x_1 = 8, x_2 = 1, x_3 = 0, x_4 = 1$, que también constituye una solcuión del sistema de ecuaciones.

La función `ContiTraverso` definida en el programa 1, escrito en *Mathematica*, permite encontrar una solución de un sistema de ecuaciones del tipo 2.4.1, usando bases de Gröbner. Sus parámetros son la matriz de coeficientes A y la matriz de recursos B.

Programa 1

```
ContiTraverso[Coef_, Recursos_] :=
  Module[{A = Coef, B = Recursos, m, n, j, k, X, Y, Z, TA, FZ, F, BZ,
      VarZY, Gb, Coeficientes, PreSol}, {m, n} = Dimensions[A];
    X = Table[{x_k}, {k, n}]; Y = Table[y_k, {k, n}]; Z = Table[z_k, {k, m}];
    TA = Transpose[A];
    FZ = Table[Z^TA[[k]], {k, n}];
    F = Table[Product[FZ[[k]][[j]], {j, 1, m}], {k, 1, n}];
    BZ = Product[Z^B[[k]], {k, 1, m}];
    VarZY = Join[Z, Y];
    Gb = GroebnerBasis[F - Y, VarZY];
    {Coeficientes, r} = PolynomialReduce[BZ, Gb, VarZY];
    PreSol = Table[Exponent[r, u], {u , VarZY}];
    {PreSol, r}
  ]
```

La función `ContiTraverso` devuelve el residuo y los exponentes de las variables que lo conforman.

Por ejemplo, para hallar una solución del sistema

$$3x_1 + 2x_2 + x_3 = 10$$
$$4x_1 + 3x_2 + x_3 = 12$$

ingrese

```
ContiTraverso[{{3, 2, 1}, {4, 3, 1}}, {10, 12}]
```

obtendrá

$$\{\{0, 0, 0, 2, 6\}, y_2^2 y_3^6\}$$

de donde se tiene que $\{0, 2, 6\}$ es una solución del sistema, como ya se vió en el ejemplo 2.4.4.

Bibliografía

[1] ADAMS, W.; LOUSTAUNAU, P., *An Introduction to Gröbner Bases*. AMS, providence RI, 1994.

[2] BAYER, D., *The division algoritm and the Hilbert Scheme* Ph.D. Thesis, Harvard University, Cabridge, Massachusetts, 1982.

[3] COX, David; LITTLE, Jhon; O'SHEA, Donald, *Ideal, Varieties, and Algorithms*. An Introduction to Computational Algebraic Geometry and Commutative Algebra Editorial Springer. Segunda Edición, 2005.

[4] COX, David; LITTLE, Jhon; O'SHEA, Donald, *Using Algebraic Geometry*. Editorial Springer. Segunda Edición, 2005.

[5] CONTI, Pascualina; TRAVERSO Carlo, *Buchberger Algotihm and Integer Programming*. Instituto di Matematica Applicata. Universitá di Pisa, 1999.

[6] WELLIN, Paul; GAYLORD, Richard; KAMIN Samuel, *Mathematica*. Editorial Cambridge Univerity Press. 2005.

[7] WOLFRAM. *Mathematica 8*. V.8.0.4.1 (2011).

REPORTE DE INVESTIGACIÓN

Los reportes de investigación son una publicación del Departamento de Ciencias, de la Pontificia Universidad Católica del Perú, cuya finalidad es presentar a la comunidad científica los resultados de los últimos trabajos realizados por los profesores de la Sección Matemáticas y sus estudiantes. Las series de esta colección reúnen tesis de maestría o doctorado, artículos que contienen los resultados de investigaciones recientes, conferencias magistrales o seminarios.

Serie A : Matemáticas Puras
Serie B : Matemáticas Aplicadas
Serie C : Probabilidad y Estadística
Serie D : Didáctica de las Matemáticas

ISBN: 978-612-46647-1-7

9 786124 664717