Bases de Gröbner y aplicaciones

Jornadas Invernales de Álgebra

Matías Valdés

IMERL, Ingeniería
CENUR Noreste, Tacuarembó

07/07/25

Objetivos de la charla

- Introducir el concepto de base de Gröbner.

Objetivos de la charla

- Introducir el concepto de base de Gröbner.
- Dar ejemplos de sus aplicaciones en Álgebra Computacional.

Objetivos de la charla

- Introducir el concepto de base de Gröbner.
- Dar ejemplos de sus aplicaciones en Álgebra Computacional.
- Describir un algoritmo para calcular Bases de Gröbner.

Objetivos de la charla

- Introducir el concepto de base de Gröbner.
- Dar ejemplos de sus aplicaciones en Álgebra Computacional.
- Describir un algoritmo para calcular Bases de Gröbner.
- Hablar sobre la complejidad del cálculo de bases de Gröbner.

Objetivos de la charla

- Introducir el concepto de base de Gröbner.
- Dar ejemplos de sus aplicaciones en Álgebra Computacional.
- Describir un algoritmo para calcular Bases de Gröbner.
- Hablar sobre la complejidad del cálculo de bases de Gröbner.
- Mostrar software que permite calcularlas de forma eficiente.

Problema motivacional

Consideremos el siguiente sistema de ecuaciones polinomiales:

$$\begin{cases} x+y+z=3 \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z)\in\mathbb{C}^3.$$

Problema motivacional

Consideremos el siguiente sistema de ecuaciones polinomiales:

$$\begin{cases} x+y+z=3 \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z)\in\mathbb{C}^3.$$

1. El sistema admite alguna solución?

Problema motivacional

Consideremos el siguiente sistema de ecuaciones polinomiales:

$$\begin{cases} x+y+z=3 \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z)\in\mathbb{C}^3.$$

1. El sistema admite alguna solución?
2. Cuántas soluciones tiene el sistema?

Problema motivacional

Consideremos el siguiente sistema de ecuaciones polinomiales:

$$\begin{cases} x+y+z=3 \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z)\in\mathbb{C}^3.$$

1. El sistema admite alguna solución?
2. Cuántas soluciones tiene el sistema?
3. Es cierto que toda solución cumple: $x^4+y^4+z^4=9$?

Problema motivacional

Consideremos el siguiente sistema de ecuaciones polinomiales:

$$\begin{cases} x+y+z=3 \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z)\in\mathbb{C}^3.$$

1. El sistema admite alguna solución?
2. Cuántas soluciones tiene el sistema?
3. Es cierto que toda solución cumple: $x^4+y^4+z^4=9$?

Si tenemos una "base de Gröbner del sistema", podemos responder a todas estas preguntas de forma sencilla.

Es cierto que toda solución cumple: $x^4 + y^4 + z^4 = 9$?

Es cierto que toda solución cumple: $x^4 + y^4 + z^4 = 9$?

Supongamos que existen $h_1, h_2, h_3 \in \mathbb{Q}[x, y, z]$ (polinomios de 3 variables y coeficientes racionales), tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1(X)+(x^2+y^2+z^2-5)h_2(X)+$$

$$(x^3+y^3+z^3-7)h_3(X)+0.$$

Es cierto que toda solución cumple: $x^4 + y^4 + z^4 = 9$?

Supongamos que existen $h_1, h_2, h_3 \in \mathbb{Q}[x, y, z]$ (polinomios de 3 variables y coeficientes racionales), tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1(X)+(x^2+y^2+z^2-5)h_2(X)+$$

$$(x^3 + y^3 + z^3 - 7)h_3(X) + 0.$$

Evaluando en una solución del sistema $(x, y, z) \in \mathbb{C}^3$, se cumple:

$$x^4 + y^4 + z^4 - 9 = 0h_1(X) + 0h_2(X) + 0h_3(X) = 0 \quad \checkmark$$

Es cierto que toda solución cumple: $x^4 + y^4 + z^4 = 9$?

Supongamos que existen $h_1, h_2, h_3 \in \mathbb{Q}[x, y, z]$ (polinomios de 3 variables y coeficientes racionales), tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1(X)+(x^2+y^2+z^2-5)h_2(X)+$$

$$(x^3 + y^3 + z^3 - 7)h_3(X) + 0.$$

Evaluando en una solución del sistema $(x, y, z) \in \mathbb{C}^3$, se cumple:

$$x^4 + y^4 + z^4 - 9 = 0h_1(X) + 0h_2(X) + 0h_3(X) = 0 \quad \checkmark$$

Esto prueba que toda solución cumple: $x^4 + y^4 + z^4 = 9$.

Es cierto que toda solución cumple: $x^4 + y^4 + z^4 = 9$?

Supongamos que existen $h_1, h_2, h_3 \in \mathbb{Q}[x, y, z]$ (polinomios de 3 variables y coeficientes racionales), tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1(X)+(x^2+y^2+z^2-5)h_2(X)+$$

$$(x^3+y^3+z^3-7)h_3(X)+0.$$

Evaluando en una solución del sistema $(x, y, z) \in \mathbb{C}^3$, se cumple:

$$x^4 + y^4 + z^4 - 9 = 0h_1(X) + 0h_2(X) + 0h_3(X) = 0 \quad \checkmark$$

Esto prueba que toda solución cumple: $x^4 + y^4 + z^4 = 9$.

- Cómo podemos determinar si existen los polinomios h_i?

Es cierto que toda solución cumple: $x^4 + y^4 + z^4 = 9$?

Supongamos que existen $h_1, h_2, h_3 \in \mathbb{Q}[x, y, z]$ (polinomios de 3 variables y coeficientes racionales), tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1(X)+(x^2+y^2+z^2-5)h_2(X)+$$

$$(x^3+y^3+z^3-7)h_3(X)+0.$$

Evaluando en una solución del sistema $(x, y, z) \in \mathbb{C}^3$, se cumple:

$$x^4 + y^4 + z^4 - 9 = 0h_1(X) + 0h_2(X) + 0h_3(X) = 0 \quad \checkmark$$

Esto prueba que toda solución cumple: $x^4 + y^4 + z^4 = 9$.

- Cómo podemos determinar si existen los polinomios h_i?
- Idea: dividir $x^4 + y^4 + z^4 - 9$ entre los polinomios del sistema, y ver si el "resto" es nulo.

Es cierto que toda solución cumple: $x^4 + y^4 + z^4 = 9$?

Supongamos que existen $h_1, h_2, h_3 \in \mathbb{Q}[x, y, z]$ (polinomios de 3 variables y coeficientes racionales), tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1(X)+(x^2+y^2+z^2-5)h_2(X)+$$

$$(x^3+y^3+z^3-7)h_3(X)+0.$$

Evaluando en una solución del sistema $(x, y, z) \in \mathbb{C}^3$, se cumple:

$$x^4 + y^4 + z^4 - 9 = 0h_1(X) + 0h_2(X) + 0h_3(X) = 0 \quad \checkmark$$

Esto prueba que toda solución cumple: $x^4 + y^4 + z^4 = 9$.

- Cómo podemos determinar si existen los polinomios h_i?
- Idea: dividir $x^4 + y^4 + z^4 - 9$ entre los polinomios del sistema, y ver si el "resto" es nulo.
- Precisamos un algoritmo de división para polinomios de varias variables. Para esto vamos a necesitar bases de Gröbner.

Ideal asociado a un sistema de polinomios

Ideal asociado a un sistema de polinomios

Definition (Ideal asociado)

Consideremos el sistema polinomial: $f_1 = 0, \ldots, f_k = 0$. El ideal asociado a estos polinomios, es:

$$I := \{f_1 h_1 + \ldots + f_k h_k \ / \ h_i \in k[x_1, \ldots, x_n]\}.$$

Se denota: $I = (f_1, \ldots, f_k)$ (ideal generado por los f_i).

Ideal asociado a un sistema de polinomios

Definition (Ideal asociado)

Consideremos el sistema polinomial: $f_1 = 0, \ldots, f_k = 0$. El ideal asociado a estos polinomios, es:

$$I := \{f_1 h_1 + \ldots + f_k h_k \ / \ h_i \in k[x_1, \ldots, x_n]\}.$$

Se denota: $I = (f_1, \ldots, f_k)$ (ideal generado por los f_i).

Contiene todas las combinaciones lineales de los polinomios f_i del sistema, con coeficientes polinomiales h_i.

Ideal asociado a un sistema de polinomios

Definition (Ideal asociado)

Consideremos el sistema polinomial: $f_1 = 0, \ldots, f_k = 0$. El ideal asociado a estos polinomios, es:

$$I := \{f_1 h_1 + \ldots + f_k h_k \ / \ h_i \in k[x_1, \ldots, x_n]\}.$$

Se denota: $I = (f_1, \ldots, f_k)$ (ideal generado por los f_i).

Contiene todas las combinaciones lineales de los polinomios f_i del sistema, con coeficientes polinomiales h_i.

Preguntarse por la existencia de polinomios h_1, h_2, h_3, tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1+(x^2+y^2+z^2-5)h_2+(x^3+y^3+z^3-7)h_3,$$

Ideal asociado a un sistema de polinomios

Definition (Ideal asociado)

Consideremos el sistema polinomial: $f_1 = 0, \ldots, f_k = 0$. El ideal asociado a estos polinomios, es:

$$I := \{f_1 h_1 + \ldots + f_k h_k \ / \ h_i \in k[x_1, \ldots, x_n]\}.$$

Se denota: $I = (f_1, \ldots, f_k)$ (ideal generado por los f_i).

Contiene todas las combinaciones lineales de los polinomios f_i del sistema, con coeficientes polinomiales h_i.

Preguntarse por la existencia de polinomios h_1, h_2, h_3, tales que:

$$x^4+y^4+z^4-9 = (x+y+z-3)h_1+(x^2+y^2+z^2-5)h_2+(x^3+y^3+z^3-7)h_3,$$

equivale a preguntarse si

$$x^4+y^4+z^4-9 \in I := \left(x+y+z-3, x^2+y^2+z^2-5, x^3+y^3+z^3-7\right).$$

División de polinomios de una variable

División de polinomios de una variable

En 1 variable tenemos un algoritmo que funciona bien: resto único.

División de polinomios de una variable

En 1 variable tenemos un algoritmo que funciona bien: resto único.

Example

Dividir $f = 2x^3 - 4x + 1$ entre $g = x^2 + 3x + 2$

División de polinomios de una variable

En 1 variable tenemos un algoritmo que funciona bien: resto único.

Example

Dividir $f = 2x^3 - 4x + 1$ entre $g = x^2 + 3x + 2$

Notación: Término de mayor grado = Término Líder = LT.

División de polinomios de una variable

En 1 variable tenemos un algoritmo que funciona bien: resto único.

Example

Dividir $f = 2x^3 - 4x + 1$ entre $g = x^2 + 3x + 2$

Notación: Término de mayor grado = Término Líder = LT.

1. Eliminamos el $LT(f) = 2x^3$, usando el $LT(g) = x^2$:

$$f(x) - \left(\frac{2x^3}{x^2}\right) g(x) = (2x^3 - 4x + 1) - 2x(x^2 + 3x + 2) = -6x^2 - 8x + 1.$$

División de polinomios de una variable

En 1 variable tenemos un algoritmo que funciona bien: resto único.

Example

Dividir $f = 2x^3 - 4x + 1$ entre $g = x^2 + 3x + 2$

Notación: Término de mayor grado = Término Líder = LT.

1. Eliminamos el $LT(f) = 2x^3$, usando el $LT(g) = x^2$:

$$f(x) - \left(\frac{2x^3}{x^2}\right) g(x) = (2x^3 - 4x + 1) - 2x(x^2 + 3x + 2) = -6x^2 - 8x + 1.$$

2. Eliminamos el $LT(r_1) = -6x^2$, usando el $LT(g) = x^2$:

$$r_1(x) - \left(\frac{-6x^2}{x^2}\right) g(x) = (-6x^2 - 8x + 1) + 6(x^2 + 3x + 2) = 10x + 13.$$

División de polinomios de una variable

En 1 variable tenemos un algoritmo que funciona bien: resto único.

Example

Dividir $f = 2x^3 - 4x + 1$ entre $g = x^2 + 3x + 2$

Notación: Término de mayor grado = Término Líder = LT.

1. Eliminamos el $LT(f) = 2x^3$, usando el $LT(g) = x^2$:

$$f(x) - \left(\frac{2x^3}{x^2}\right) g(x) = (2x^3 - 4x + 1) - 2x(x^2 + 3x + 2) = -6x^2 - 8x + 1.$$

2. Eliminamos el $LT(r_1) = -6x^2$, usando el $LT(g) = x^2$:

$$r_1(x) - \left(\frac{-6x^2}{x^2}\right) g(x) = (-6x^2 - 8x + 1) + 6(x^2 + 3x + 2) = 10x + 13.$$

3. Paramos porque $r_2(x) := 10x + 13$ no es divisible entre $LT(g)$.

División con dos o más variables...

División con dos o más variables...

- El algoritmo de división utiliza el concepto de Término Líder.

División con dos o más variables...

- El algoritmo de división utiliza el concepto de Término Líder.
- En una variable, el Término Líder de un polinomio es el sumando de mayor grado: $LT(-2x^3 + 6x - 1) = -2x^3$.

División con dos o más variables...

- El algoritmo de división utiliza el concepto de Término Líder.
- En una variable, el Término Líder de un polinomio es el sumando de mayor grado: $LT(-2x^3 + 6x - 1) = -2x^3$.
- Los monomios quedan ordenados por su grado:

$$1 < x < x^2 < \dots.$$

División con dos o más variables...

- El algoritmo de división utiliza el concepto de Término Líder.
- En una variable, el Término Líder de un polinomio es el sumando de mayor grado: $LT(-2x^3 + 6x - 1) = -2x^3$.
- Los monomios quedan ordenados por su grado:

$$1 < x < x^2 < \ldots.$$

En dos variables:

- Consideremos $p(x, y) = -5x^2y + 2x^2 + y^3$.

División con dos o más variables...

- El algoritmo de división utiliza el concepto de Término Líder.
- En una variable, el Término Líder de un polinomio es el sumando de mayor grado: $LT(-2x^3 + 6x - 1) = -2x^3$.
- Los monomios quedan ordenados por su grado:

$$1 < x < x^2 < \dots.$$

En dos variables:

- Consideremos $p(x, y) = -5x^2y + 2x^2 + y^3$.
- Sus monomios son: $x^2y,\ x^2,\ y^3$. Cómo podemos ordenarlos?

División con dos o más variables...

- El algoritmo de división utiliza el concepto de Término Líder.
- En una variable, el Término Líder de un polinomio es el sumando de mayor grado: $LT(-2x^3 + 6x - 1) = -2x^3$.
- Los monomios quedan ordenados por su grado:

$$1 < x < x^2 < \dots.$$

En dos variables:

- Consideremos $p(x, y) = -5x^2y + 2x^2 + y^3$.
- Sus monomios son: $x^2y,\ x^2,\ y^3$. Cómo podemos ordenarlos?
- El grado (total) no es suficiente: $x^2y^1 > y^3$ o $x^2y^1 < y^3$?

División con dos o más variables...

- El algoritmo de división utiliza el concepto de Término Líder.
- En una variable, el Término Líder de un polinomio es el sumando de mayor grado: $LT(-2x^3 + 6x - 1) = -2x^3$.
- Los monomios quedan ordenados por su grado:

$$1 < x < x^2 < \dots.$$

En dos variables:

- Consideremos $p(x, y) = -5x^2y + 2x^2 + y^3$.
- Sus monomios son: $x^2y,\ x^2,\ y^3$. Cómo podemos ordenarlos?
- El grado (total) no es suficiente: $x^2y^1 > y^3$ o $x^2y^1 < y^3$?
- Para definir el Término Líder, y generalizar el algoritmo de división, necesitamos un orden monomial en varias variables.

Orden monomial Lexicográfico (Lex)

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

- Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

- Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:
  - $x^2y > x^2 = x^2y^0$, pues $2 = 2$ y $1 > 0$.

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

- Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:
  - $x^2y > x^2 = x^2y^0$, pues $2 = 2$ y $1 > 0$.
  - $x^2y > y^3 = x^0y^3$, pues $2 > 0$.

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

- Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:
  - $x^2y > x^2 = x^2y^0$, pues $2 = 2$ y $1 > 0$.
  - $x^2y > y^3 = x^0y^3$, pues $2 > 0$.
  - $x^2y^0 > x^0y^3$, pues $2 > 0$.

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

- Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:
  - $x^2y > x^2 = x^2y^0$, pues $2 = 2$ y $1 > 0$.
  - $x^2y > y^3 = x^0y^3$, pues $2 > 0$.
  - $x^2y^0 > x^0y^3$, pues $2 > 0$.
- En particular: un monomio que contenga x es mayor a uno que no contenga x: $x^3 > y^{100} = x^0y^{100}$ pues $3 > 0$.

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

- Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:
  - $x^2y > x^2 = x^2y^0$, pues $2 = 2$ y $1 > 0$.
  - $x^2y > y^3 = x^0y^3$, pues $2 > 0$.
  - $x^2y^0 > x^0y^3$, pues $2 > 0$.
- En particular: un monomio que contenga x es mayor a uno que no contenga x: $x^3 > y^{100} = x^0y^{100}$ pues $3 > 0$.
- Asumimos:
  1. $x > y$ (podemos definir un Lex con $y > x$), y

Orden monomial Lexicográfico (Lex)

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$, sii $\alpha_1 > \alpha_2$, o $\alpha_1 = \alpha_2$ y $\beta_1 > \beta_2$.

- Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:
  - $x^2y > x^2 = x^2y^0$, pues $2 = 2$ y $1 > 0$.
  - $x^2y > y^3 = x^0y^3$, pues $2 > 0$.
  - $x^2y^0 > x^0y^3$, pues $2 > 0$.
- En particular: un monomio que contenga x es mayor a uno que no contenga x: $x^3 > y^{100} = x^0y^{100}$ pues $3 > 0$.
- Asumimos:
  1. $x > y$ (podemos definir un Lex con $y > x$), y
  2. $1 = x^0y^0$ menor a cualquier otro monomio (buen orden)

Orden monomial Graduado Lexicográfico Inverso (DRL)

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1} y^{\beta_1} > x^{\alpha_2} y^{\beta_2}$ sii

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1} y^{\beta_1} > x^{\alpha_2} y^{\beta_2}$ sii

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$ "Graded", o

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$ sii

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$ "Graded", o
- $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$, y "Reverse Lexicographic":
  1. $\beta_1 < \beta_2$, o
  2. $\beta_1 = \beta_2$, y $\alpha_1 < \alpha_2$.

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$ sii

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$ "Graded", o
- $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$, y "Reverse Lexicographic":
  1. $\beta_1 < \beta_2$, o
  2. $\beta_1 = \beta_2$, y $\alpha_1 < \alpha_2$.

Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$ sii

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$ "Graded", o
- $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$, y "Reverse Lexicographic":
  1. $\beta_1 < \beta_2$, o
  2. $\beta_1 = \beta_2$, y $\alpha_1 < \alpha_2$.

Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:

- $x^2y > x^2$, pues $2 + 1 > 2$.

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$ sii

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$ "Graded", o
- $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$, y "Reverse Lexicographic":
  1. $\beta_1 < \beta_2$, o
  2. $\beta_1 = \beta_2$, y $\alpha_1 < \alpha_2$.

Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:

- $x^2y > x^2$, pues $2 + 1 > 2$.
- $x^2y^1 > y^3 = x^0y^3$, pues $3 = 3$ y $1 < 3$.

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$ sii

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$ "Graded", o
- $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$, y "Reverse Lexicographic":
  1. $\beta_1 < \beta_2$, o
  2. $\beta_1 = \beta_2$, y $\alpha_1 < \alpha_2$.

Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:

- $x^2y > x^2$, pues $2 + 1 > 2$.
- $x^2y^1 > y^3 = x^0y^3$, pues $3 = 3$ y $1 < 3$.
- $x^2y^0 < x^0y^3$, pues $2 + 0 < 3 + 0$.

Orden monomial Graduado Lexicográfico Inverso (DRL)

Poco intuitivo, pero muy utilizado.

Definition (En dos variables)

$x^{\alpha_1}y^{\beta_1} > x^{\alpha_2}y^{\beta_2}$ sii

- $\alpha_1 + \beta_1 > \alpha_2 + \beta_2$ "Graded", o
- $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$, y "Reverse Lexicographic":
  1. $\beta_1 < \beta_2$, o
  2. $\beta_1 = \beta_2$, y $\alpha_1 < \alpha_2$.

Aplicado a los monomios de $p(x, y) = -5x^2y + 2x^2 + y^3$:

- $x^2y > x^2$, pues $2 + 1 > 2$.
- $x^2y^1 > y^3 = x^0y^3$, pues $3 = 3$ y $1 < 3$.
- $x^2y^0 < x^0y^3$, pues $2 + 0 < 3 + 0$.

Asumimos: $x > y$, y 1 menor a cualquier otro monomio.

Término líder de un polinomio

Término líder de un polinomio

Una vez que elegimos un orden monomial (Lex, DRL, etc.), queda bien definido el "Término Líder" de un polinomio.

Término líder de un polinomio

Una vez que elegimos un orden monomial (Lex, DRL, etc.), queda bien definido el "Término Líder" de un polinomio.

Example

Con el orden Lex, $p(x, y) = -5x^2y + 2x^2 + y^3$ tiene:

Término líder de un polinomio

Una vez que elegimos un orden monomial (Lex, DRL, etc.), queda bien definido el "Término Líder" de un polinomio.

Example

Con el orden Lex, $p(x, y) = -5x^2y + 2x^2 + y^3$ tiene:

- Término líder: $LT(p) = -5x^2y$.

Término líder de un polinomio

Una vez que elegimos un orden monomial (Lex, DRL, etc.), queda bien definido el "Término Líder" de un polinomio.

Example

Con el orden Lex, $p(x, y) = -5x^2y + 2x^2 + y^3$ tiene:

- Término líder: $LT(p) = -5x^2y$.
- Monomio líder: $LM(p) = x^2y$.

Término líder de un polinomio

Una vez que elegimos un orden monomial (Lex, DRL, etc.), queda bien definido el "Término Líder" de un polinomio.

Example

Con el orden Lex, $p(x, y) = -5x^2y + 2x^2 + y^3$ tiene:

- Término líder: $LT(p) = -5x^2y$.
- Monomio líder: $LM(p) = x^2y$.
- Coeficiente líder: $LC(p) = -5$.

Término líder de un polinomio

Una vez que elegimos un orden monomial (Lex, DRL, etc.), queda bien definido el "Término Líder" de un polinomio.

Example

Con el orden Lex, $p(x, y) = -5x^2y + 2x^2 + y^3$ tiene:

- Término líder: $LT(p) = -5x^2y$.
- Monomio líder: $LM(p) = x^2y$.
- Coeficiente líder: $LC(p) = -5$.

Ahora podemos generalizar el algoritmo de división a polinomios de varias variables.

División en varias variables...

División en varias variables...

Example

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

División en varias variables...

Example

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

1. $LT(f_1) = xy$, $LT(f_2) = y^2$. Ambos dividen a $LT(f) = xy^2$.

División en varias variables...

Example

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

1. $LT(f_1) = xy$, $LT(f_2) = y^2$. Ambos dividen a $LT(f) = xy^2$.
2. Eliminamos el $LT(f) = xy^2$ usando el $LT(f_1) = xy$:

$$f - \left(\frac{xy^2}{xy}\right) f_1 = (xy^2 - x) - y(xy - 1) = -x + y.$$

División en varias variables...

Example

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

1. $LT(f_1) = xy$, $LT(f_2) = y^2$. Ambos dividen a $LT(f) = xy^2$.
2. Eliminamos el $LT(f) = xy^2$ usando el $LT(f_1) = xy$:

$$f - \left(\frac{xy^2}{xy}\right) f_1 = (xy^2 - x) - y(xy - 1) = -x + y.$$

3. Paramos porque $-x + y$ no es divisible por $LT(f_1)$ ni $LT(f_2)$.

División en varias variables...

Example

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

1. $LT(f_1) = xy$, $LT(f_2) = y^2$. Ambos dividen a $LT(f) = xy^2$.
2. Eliminamos el $LT(f) = xy^2$ usando el $LT(f_1) = xy$:

$$f - \left(\frac{xy^2}{xy}\right) f_1 = (xy^2 - x) - y(xy - 1) = -x + y.$$

3. Paramos porque $-x + y$ no es divisible por $LT(f_1)$ ni $LT(f_2)$.

Obtuvimos resto no nulo:

$$f := xy^2 - x = y(xy - 1) + 0(y^2 - 1) + (-x + y).$$

División en varias variables... puede fallar

División en varias variables... puede fallar

Example (Mismo ejemplo de antes)

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

División en varias variables... puede fallar

Example (Mismo ejemplo de antes)

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

1. Eliminamos el $LT(f) = xy^2$ usando primero el $LT(f_2) = y^2$:

$$f - \left(\frac{xy^2}{y^2}\right) f_2 = (xy^2 - x) - x(y^2 - 1) = -x + x = 0.$$

División en varias variables... puede fallar

Example (Mismo ejemplo de antes)

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

1. Eliminamos el $LT(f) = xy^2$ usando primero el $LT(f_2) = y^2$:

$$f - \left(\frac{xy^2}{y^2}\right) f_2 = (xy^2 - x) - x(y^2 - 1) = -x + x = 0.$$

Obtuvimos resto nulo:

$$f := xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0.$$

División en varias variables... puede fallar

Example (Mismo ejemplo de antes)

Dividir $f(x,y) = xy^2 - x$ entre $f_1(x,y) = xy - 1$ y $f_2(x,y) = y^2 - 1$. Usando orden monomial Lex.

1. Eliminamos el $LT(f) = xy^2$ usando primero el $LT(f_2) = y^2$:

$$f - \left(\frac{xy^2}{y^2}\right) f_2 = (xy^2 - x) - x(y^2 - 1) = -x + x = 0.$$

Obtuvimos resto nulo:

$$f := xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0.$$

El resto no es único, y depende del orden en que se utilizan los f_i.

División en varias variables... qué pasó?

División en varias variables... qué pasó?

Obtuvimos dos igualdades:

$$f := xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0,$$

$$f := xy^2 - x = y(xy - 1) + 0(y^2 - 1) + (-x + y).$$

División en varias variables... qué pasó?

Obtuvimos dos igualdades:

$$f := xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0,$$

$$f := xy^2 - x = y(xy - 1) + 0(y^2 - 1) + (-x + y).$$

Restando:

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

División en varias variables... qué pasó?

Obtuvimos dos igualdades:

$$f := xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0,$$

$$f := xy^2 - x = y(xy - 1) + 0(y^2 - 1) + (-x + y).$$

Restando:

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

Agregar $-x + y$ al sistema no altera el conjunto solución:

$$\begin{cases} y^2 - 1 = 0, \\ xy - 1 = 0 \end{cases} \Leftrightarrow \begin{cases} y^2 - 1 = 0, \\ xy - 1 = 0, \\ -x + y = 0 \end{cases}.$$

División en varias variables... qué pasó?

Obtuvimos dos igualdades:

$$f := xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0,$$

$$f := xy^2 - x = y(xy - 1) + 0(y^2 - 1) + (-x + y).$$

Restando:

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

Agregar $-x + y$ al sistema no altera el conjunto solución:

$$\begin{cases} y^2 - 1 = 0, \\ xy - 1 = 0 \end{cases} \Leftrightarrow \begin{cases} y^2 - 1 = 0, \\ xy - 1 = 0, \\ -x + y = 0 \end{cases}.$$

Aumenta el conjunto de divisores disponibles, y brinda nuevos LT para el correcto funcionamiento del algoritmo de división.

División en varias variables... qué pasó?

Obtuvimos dos igualdades:

$$f := xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0,$$

$$f := xy^2 - x = y(xy - 1) + 0(y^2 - 1) + (-x + y).$$

Restando:

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

Agregar $-x + y$ al sistema no altera el conjunto solución:

$$\begin{cases} y^2 - 1 = 0, \\ xy - 1 = 0 \end{cases} \Leftrightarrow \begin{cases} y^2 - 1 = 0, \\ xy - 1 = 0, \\ -x + y = 0 \end{cases}.$$

Aumenta el conjunto de divisores disponibles, y brinda nuevos LT para el correcto funcionamiento del algoritmo de división.
La división se trancó en un resto no nulo, por no conocer suficientes LT de polinomios asociados a nuestro sistema.

Definición de base de Gröbner

Definición de base de Gröbner

Es un sistema con las mismas soluciones que el original, cuyos polinomios tienen todos los términos líder necesarios para que la división funcione correctamente: resto único.

Definición de base de Gröbner

Es un sistema con las mismas soluciones que el original, cuyos polinomios tienen todos los términos líder necesarios para que la división funcione correctamente: resto único.

Definition (Base de Gröbner)

Una base de Gröbner de un ideal I, es un conjunto de polinomios $G = \{g_1, \ldots, g_k\} \subset I$, que cumple: $LT(f) \in (LT(G))$, $\forall\ f \in I$.

Definición de base de Gröbner

Es un sistema con las mismas soluciones que el original, cuyos polinomios tienen todos los términos líder necesarios para que la división funcione correctamente: resto único.

Definition (Base de Gröbner)

Una base de Gröbner de un ideal I, es un conjunto de polinomios $G = \{g_1, \ldots, g_k\} \subset I$, que cumple: $LT(f) \in (LT(G))$, $\forall\ f \in I$.

En forma equivalente:

$$\text{si } f \in I,\ \exists\ g \in G\ /\ LT(g) \text{ divide a } LT(f).$$

Definición de base de Gröbner

Es un sistema con las mismas soluciones que el original, cuyos polinomios tienen todos los términos líder necesarios para que la división funcione correctamente: resto único.

Definition (Base de Gröbner)

Una base de Gröbner de un ideal I, es un conjunto de polinomios $G = \{g_1, \ldots, g_k\} \subset I$, que cumple: $LT(f) \in (LT(G))$, $\forall\ f \in I$.

En forma equivalente:

$$\text{si } f \in I,\ \exists\ g \in G\ /\ LT(g) \text{ divide a } LT(f).$$

En particular: al dividir entre G, nunca vamos a obtener un resto $r \in I$ (como en el ejemplo que falló), porque podríamos eliminar $LT(r)$ con algún LT de G.

Volviendo al ejemplo motivacional...

$$\begin{cases} x+y+z=3, \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z) \in \mathbb{C}^3.$$

Volviendo al ejemplo motivacional...

$$\begin{cases} x+y+z=3, \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z) \in \mathbb{C}^3.$$

Una base de Gröbner (usando orden monomial **DRL**), es:

```
R = QQ[x,y,z, MonomialOrder => GRevLex];
I = ideal(x+y+z-3, x^2+y^2+z^2-5, x^3+y^3+z^3-7);
G = gens gb I;
```

Volviendo al ejemplo motivacional...

$$\begin{cases} x+y+z=3, \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z) \in \mathbb{C}^3.$$

Una base de Gröbner (usando orden monomial **DRL**), es:

```
R = QQ[x,y,z, MonomialOrder => GRevLex];
I = ideal(x+y+z-3, x^2+y^2+z^2-5, x^3+y^3+z^3-7);
G = gens gb I;
```

$$G = \{x+y+z-3, y^2+yz+z^2-3y-3z+2, 3z^3-9z^2+6z+2\}.$$

Volviendo al ejemplo motivacional...

$$\begin{cases} x+y+z=3, \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z) \in \mathbb{C}^3.$$

Una base de Gröbner (usando orden monomial **DRL**), es:

```
R = QQ[x,y,z, MonomialOrder => GRevLex];
I = ideal(x+y+z-3, x^2+y^2+z^2-5, x^3+y^3+z^3-7);
G = gens gb I;
```

$$G = \{x+y+z-3, y^2+yz+z^2-3y-3z+2, 3z^3-9z^2+6z+2\}.$$

- Los LT de G son: $LT(g_1) = x$, $LT(g_2) = y^2$, $LT(g_3) = 3z^3$.

Volviendo al ejemplo motivacional...

$$\begin{cases} x+y+z=3, \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z) \in \mathbb{C}^3.$$

Una base de Gröbner (usando orden monomial **DRL**), es:

```
R = QQ[x,y,z, MonomialOrder => GRevLex];
I = ideal(x+y+z-3, x^2+y^2+z^2-5, x^3+y^3+z^3-7);
G = gens gb I;
```

$$G = \{x+y+z-3, y^2+yz+z^2-3y-3z+2, 3z^3-9z^2+6z+2\}.$$

- Los LT de G son: $LT(g_1)=x,\ LT(g_2)=y^2,\ LT(g_3)=3z^3$.
- Los LT del sistema original son:

$$LT(f_1)=x,\ LT(f_2)=x^2=xLT(f_1),\ LT(f_3)=x^3=x^2LT(f_1).$$

Volviendo al ejemplo motivacional...

$$\begin{cases} x+y+z=3, \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=7 \end{cases}, \quad (x,y,z)\in\mathbb{C}^3.$$

Una base de Gröbner (usando orden monomial **DRL**), es:

```
R = QQ[x,y,z, MonomialOrder => GRevLex];
I = ideal(x+y+z-3, x^2+y^2+z^2-5, x^3+y^3+z^3-7);
G = gens gb I;
```

$$G=\{x+y+z-3,\ y^2+yz+z^2-3y-3z+2,\ 3z^3-9z^2+6z+2\}.$$

- Los LT de G son: $LT(g_1)=x,\ LT(g_2)=y^2,\ LT(g_3)=3z^3$.
- Los LT del sistema original son:

$$LT(f_1)=x,\ LT(f_2)=x^2=xLT(f_1),\ LT(f_3)=x^3=x^2LT(f_1).$$

- La base de Gröbner agrega dos LT al conjunto de divisores.

Pertenencia a un ideal

Pertenencia a un ideal

$\bar{f}^G$ denota el resto de dividir f entre un conjunto finito G.

Pertenencia a un ideal

$\bar{f}^G$ denota el resto de dividir f entre un conjunto finito G.

Theorem (División funciona bien al dividir entre G Gröbner)

Sea G base de Gröbner de $I := (f_1, \ldots, f_m)$. Se cumple:

$$f = h_1 f_1 + \ldots + h_m f_m \Leftrightarrow \bar{f}^G = 0 \quad (f \in I \Leftrightarrow \bar{f}^G = 0).$$

Pertenencia a un ideal

$\bar{f}^G$ denota el resto de dividir f entre un conjunto finito G.

Theorem (División funciona bien al dividir entre G Gröbner)

Sea G base de Gröbner de $I := (f_1, \ldots, f_m)$. Se cumple:

$$f = h_1 f_1 + \ldots + h_m f_m \Leftrightarrow \bar{f}^G = 0 \quad (f \in I \Leftrightarrow \bar{f}^G = 0).$$

En el ejemplo motivacional: $x^4 + y^4 + z^4 - 9 \in I$?

Pertenencia a un ideal

$\bar{f}^G$ denota el resto de dividir f entre un conjunto finito G.

Theorem (División funciona bien al dividir entre G Gröbner)

Sea G base de Gröbner de $I := (f_1, \ldots, f_m)$. Se cumple:

$$f = h_1 f_1 + \ldots + h_m f_m \Leftrightarrow \bar{f}^G = 0 \quad (f \in I \Leftrightarrow \bar{f}^G = 0).$$

En el ejemplo motivacional: $x^4 + y^4 + z^4 - 9 \in I$?

```
R = QQ[x,y,z, MonomialOrder => Lex];
I = ideal(x+y+z-3, x^2+y^2+z^2-5, x^3+y^3+z^3-7);
G = gens gb I;

f = x^4 + y^4 + z^4 - 9;
r = f % G; -- se obtiene r=0
H = f // G; -- coeficientes h_i (certificado)
```

El sistema admite alguna solución?

El sistema admite alguna solución?

Theorem (Hilbert Nullstellensatz (1893))

Sea el sistema $f_1 = 0, \ldots, f_k = 0$, *con* $f_i \in \mathbb{Q}[x_1, \ldots, x_n]$ *(polinomio de n variables y coeficientes racionales).* $\exists$ *solución en* $\mathbb{C}^n$, *sii:*

$$1 \neq f_1(x)h_1(x) + \ldots + f_k(x)h_k(x), \ \forall \ h_i \in \mathbb{C}[x_1, \ldots, x_n].$$

El sistema admite alguna solución?

Theorem (Hilbert Nullstellensatz (1893))

Sea el sistema $f_1 = 0, \ldots, f_k = 0$, *con* $f_i \in \mathbb{Q}[x_1, \ldots, x_n]$ *(polinomio de n variables y coeficientes racionales).* $\exists$ *solución en* $\mathbb{C}^n$, *sii:*

$$1 \neq f_1(x)h_1(x) + \ldots + f_k(x)h_k(x), \ \forall \ h_i \in \mathbb{C}[x_1, \ldots, x_n].$$

Es decir: tiene solución, sii 1 **no** es combinación lineal de los polinomios del sistema (con coeficientes polinomiales h_i).

El sistema admite alguna solución?

Theorem (Hilbert Nullstellensatz (1893))

Sea el sistema $f_1 = 0, \ldots, f_k = 0$, *con* $f_i \in \mathbb{Q}[x_1, \ldots, x_n]$ *(polinomio de n variables y coeficientes racionales).* $\exists$ *solución en* $\mathbb{C}^n$, *sii:*

$$1 \neq f_1(x)h_1(x) + \ldots + f_k(x)h_k(x), \ \forall \ h_i \in \mathbb{C}[x_1, \ldots, x_n].$$

Es decir: tiene solución, sii 1 **no** es combinación lineal de los polinomios del sistema (con coeficientes polinomiales h_i).

Si tenemos una base de Gröbner G del sistema: existe solución sii el resto de dividir 1 entre G es no nulo: $1 \notin I := (f_1, \ldots, f_k)$.

El sistema admite alguna solución?

Theorem (Hilbert Nullstellensatz (1893))

Sea el sistema $f_1 = 0, \ldots, f_k = 0$, *con* $f_i \in \mathbb{Q}[x_1, \ldots, x_n]$ *(polinomio de n variables y coeficientes racionales).* $\exists$ *solución en* $\mathbb{C}^n$, *sii:*

$$1 \neq f_1(x)h_1(x) + \ldots + f_k(x)h_k(x), \ \forall \ h_i \in \mathbb{C}[x_1, \ldots, x_n].$$

Es decir: tiene solución, sii 1 **no** es combinación lineal de los polinomios del sistema (con coeficientes polinomiales h_i).

Si tenemos una base de Gröbner G del sistema: existe solución sii el resto de dividir 1 entre G es no nulo: $1 \notin I := (f_1, \ldots, f_k)$.

El sistema del ejemplo motivacional admite solución:

```
f = 1_R; -- polinomio 1 del anillo R
G = gens gb I; -- base Grobner
r = f % G; -- se obtiene r = 1 != 0
```

¿El conjunto de soluciones es finito?

¿El conjunto de soluciones es finito?

Theorem

*Sea G base de Gröbner de $I = (f_1, \ldots, f_k)$ con un "***degree order***" (DRL por ejemplo). El sistema $f_1 = 0, \ldots, f_k = 0$ tiene una cantidad finita de soluciones, sii: G tiene elementos con LT de la forma $c_i x_i^{n_i}$, para cada variable x_i del anillo $(n_i > 0,\ c_i \neq 0)$.*

¿El conjunto de soluciones es finito?

Theorem

*Sea G base de Gröbner de $I = (f_1, \ldots, f_k)$ con un "**degree order**" (DRL por ejemplo). El sistema $f_1 = 0, \ldots, f_k = 0$ tiene una cantidad finita de soluciones, sii: G tiene elementos con LT de la forma $c_i x_i^{n_i}$, para cada variable x_i del anillo $(n_i > 0,\ c_i \neq 0)$.*

En nuestro ejemplo, una base de Gröbner con orden **DRL**, es:

$$G = \{x + y + z - 3, y^2 + yz + z^2 - 3y - 3z + 2, 3z^3 - 9z^2 + 6z + 2\}.$$

¿El conjunto de soluciones es finito?

Theorem

*Sea G base de Gröbner de $I = (f_1, \ldots, f_k)$ con un "**degree order**" (DRL por ejemplo). El sistema $f_1 = 0, \ldots, f_k = 0$ tiene una cantidad finita de soluciones, sii: G tiene elementos con LT de la forma $c_i x_i^{n_i}$, para cada variable x_i del anillo $(n_i > 0,\ c_i \neq 0)$.*

En nuestro ejemplo, una base de Gröbner con orden **DRL**, es:

$$G = \{x + y + z - 3, y^2 + yz + z^2 - 3y - 3z + 2, 3z^3 - 9z^2 + 6z + 2\}.$$

Cada una de las tres variables aparece **sola** en al menos un LT. Por lo tanto, el sistema tiene finitas soluciones.

Si son finitas, ¿cuántas son exactamente?

Si son finitas, ¿cuántas son exactamente?

Theorem

Supongamos que $f_1 = 0, \ldots, f_k = 0$ tiene finitas soluciones. Sea G base de Gröbner del sistema. La cantidad de soluciones (en $\mathbb{C}^n$ y contando multiplicidad), es la cantidad de monomios que no son múltiplo de los LT de G.

Si son finitas, ¿cuántas son exactamente?

Theorem

Supongamos que $f_1 = 0, \ldots, f_k = 0$ tiene finitas soluciones. Sea G base de Gröbner del sistema. La cantidad de soluciones (en $\mathbb{C}^n$ y contando multiplicidad), es la cantidad de monomios que no son múltiplo de los LT de G.

En nuestro ejemplo, una base de Gröbner, es:

$$G = \{x + y + z - 3, y^2 + yz + z^2 - 3y - 3z + 2, 3z^3 - 9z^2 + 6z + 2\}.$$

Si son finitas, ¿cuántas son exactamente?

Theorem

Supongamos que $f_1 = 0, \ldots, f_k = 0$ tiene finitas soluciones. Sea G base de Gröbner del sistema. La cantidad de soluciones (en $\mathbb{C}^n$ y contando multiplicidad), es la cantidad de monomios que no son múltiplo de los LT de G.

En nuestro ejemplo, una base de Gröbner, es:

$$G = \{x + y + z - 3, y^2 + yz + z^2 - 3y - 3z + 2, 3z^3 - 9z^2 + 6z + 2\}.$$

Los monomios que no son múltiplo de los LT de G, son:

$$C := \{1, y, z, z^2, yz, yz^2\}.$$

Si son finitas, ¿cuántas son exactamente?

Theorem

Supongamos que $f_1 = 0, \ldots, f_k = 0$ tiene finitas soluciones. Sea G base de Gröbner del sistema. La cantidad de soluciones (en $\mathbb{C}^n$ y contando multiplicidad), es la cantidad de monomios que no son múltiplo de los LT de G.

En nuestro ejemplo, una base de Gröbner, es:

$$G = \{x + y + z - 3, y^2 + yz + z^2 - 3y - 3z + 2, 3z^3 - 9z^2 + 6z + 2\}.$$

Los monomios que no son múltiplo de los LT de G, son:

$$C := \{1, y, z, z^2, yz, yz^2\}.$$

Entonces, el sistema tiene exactamente $\#C = 6$ soluciones en $\mathbb{C}^3$, contando multiplicidad.

Si son finitas, ¿cuántas son exactamente?

Theorem

Supongamos que $f_1 = 0, \ldots, f_k = 0$ tiene finitas soluciones. Sea G base de Gröbner del sistema. La cantidad de soluciones (en $\mathbb{C}^n$ y contando multiplicidad), es la cantidad de monomios que no son múltiplo de los LT de G.

En nuestro ejemplo, una base de Gröbner, es:

$$G = \{x + y + z - 3, y^2 + yz + z^2 - 3y - 3z + 2, 3z^3 - 9z^2 + 6z + 2\}.$$

Los monomios que no son múltiplo de los LT de G, son:

$$C := \{1, y, z, z^2, yz, yz^2\}.$$

Entonces, el sistema tiene exactamente $\#C = 6$ soluciones en $\mathbb{C}^3$, contando multiplicidad.

Observación

Además, C es base del espacio vectorial R módulo I: R/I.

Eliminar variables

Eliminar variables

Definition (Ideal de eliminación)

Sea $I \subset k[x, y, z]$ un ideal. El ideal de eliminación de x, denotado $I \cap k[y, z]$, es el conjunto formado por todos los polinomios de variables (y, z) solamente, obtenidos combinando polinomios de I.

Eliminar variables

Definition (Ideal de eliminación)

Sea $I \subset k[x, y, z]$ un ideal. El ideal de eliminación de x, denotado $I \cap k[y, z]$, es el conjunto formado por todos los polinomios de variables (y, z) solamente, obtenidos combinando polinomios de I.

Example

$I = (x^2 + 2yz, 3xy - 5yz^2)$. Entonces:

$$9y(x^2 + 2yz) - (3x + 5z^2)(3xy - 5yz^2) =$$

$$= 18y^2z + 25yz^4 \in I \cap k[y, z].$$

Eliminar variables

Definition (Ideal de eliminación)

Sea $I \subset k[x, y, z]$ un ideal. El ideal de eliminación de x, denotado $I \cap k[y, z]$, es el conjunto formado por todos los polinomios de variables (y, z) solamente, obtenidos combinando polinomios de I.

Example

$I = (x^2 + 2yz, 3xy - 5yz^2)$. Entonces:

$$9y(x^2 + 2yz) - (3x + 5z^2)(3xy - 5yz^2) =$$

$$= 18y^2z + 25yz^4 \in I \cap k[y, z].$$

Gröbner permite calcular elementos de los ideales de eliminación.

Eliminar variables (escalerizar un sistema polinomial)

Eliminar variables (escalerizar un sistema polinomial)

Theorem (Eliminación ($n = 3$ variables))

Sea G base de **Gröbner** *de un ideal $I \subset k[x, y, z]$, con el orden monomial* **Lexicográfico**, *y asumiendo: $x > y > z$.*

Eliminar variables (escalerizar un sistema polinomial)

Theorem (Eliminación ($n = 3$ variables))

Sea G base de **Gröbner** *de un ideal $I \subset k[x, y, z]$, con el orden monomial* **Lexicográfico**, *y asumiendo: $x > y > z$.*

1. *Si $I \cap k[y, z] \neq \{0\}$, G tiene polinomios que no dependen de x. Estos forman una base de Gröbner de $I \cap k[y, z]$.*

Eliminar variables (escalerizar un sistema polinomial)

Theorem (Eliminación ($n = 3$ variables))

Sea G base de **Gröbner** *de un ideal $I \subset k[x, y, z]$, con el orden monomial* **Lexicográfico**, *y asumiendo: $x > y > z$.*

1. *Si $I \cap k[y, z] \neq \{0\}$, G tiene polinomios que no dependen de x. Estos forman una base de Gröbner de $I \cap k[y, z]$.*
2. *Si $I \cap k[z] \neq \{0\}$, G tiene polinomios que no dependen de x ni de y. Estos forman una base de Gröbner de $I \cap k[z]$.*

Eliminar variables (escalerizar un sistema polinomial)

Theorem (Eliminación ($n = 3$ variables))

Sea G base de **Gröbner** *de un ideal $I \subset k[x, y, z]$, con el orden monomial* **Lexicográfico**, *y asumiendo: $x > y > z$.*

1. *Si $I \cap k[y, z] \neq \{0\}$, G tiene polinomios que no dependen de x. Estos forman una base de Gröbner de $I \cap k[y, z]$.*
2. *Si $I \cap k[z] \neq \{0\}$, G tiene polinomios que no dependen de x ni de y. Estos forman una base de Gröbner de $I \cap k[z]$.*

Example (En el ejemplo motivacional)

Una base de Gröbner con el orden monomial **Lex**, es:

$$G = \begin{cases} x + y + z - 3, & \\ y^2 + yz - 3y + z^2 - 3z + 2, & \in I \cap \mathbb{Q}[y, z] \\ 3z^3 - 9z^2 + 6z + 2 & \in I \cap \mathbb{Q}[z] \end{cases} .$$

Implicitación

Implicitación

Consideremos un sistema de ecuaciones de parámetro t:

$$\begin{cases} x = 2t - 4t^3 \\ y = t^2 - 3t^4 \end{cases}.$$

Implicitación

Consideremos un sistema de ecuaciones de parámetro t:

$$\begin{cases} x = 2t - 4t^3 \\ y = t^2 - 3t^4 \end{cases}.$$

Objetivo: obtener una relación implícita entre x e y solamente:

Implicitación

Consideremos un sistema de ecuaciones de parámetro t:

$$\begin{cases} x = 2t - 4t^3 \\ y = t^2 - 3t^4 \end{cases}.$$

Objetivo: obtener una relación implícita entre x e y solamente:

$$h(x, y) := 27x^4 - 144x^2y - 4x^2 + 256y^3 + 128y^2 + 16y = 0.$$

Implicitación

Consideremos un sistema de ecuaciones de parámetro t:

$$\begin{cases} x = 2t - 4t^3 \\ y = t^2 - 3t^4 \end{cases}.$$

Objetivo: obtener una relación implícita entre x e y solamente:

$$h(x, y) := 27x^4 - 144x^2y - 4x^2 + 256y^3 + 128y^2 + 16y = 0.$$

Procedimiento: Gröbner con un orden monomial que elimine t:

Implicitación

Consideremos un sistema de ecuaciones de parámetro t:

$$\begin{cases} x = 2t - 4t^3 \\ y = t^2 - 3t^4 \end{cases}.$$

Objetivo: obtener una relación implícita entre x e y solamente:

$$h(x, y) := 27x^4 - 144x^2y - 4x^2 + 256y^3 + 128y^2 + 16y = 0.$$

Procedimiento: Gröbner con un orden monomial que elimine t:

```
R = QQ[t,x,y, MonomialOrder => Lex]; -- anillo orden Lex

I = ideal(x-2*t-4*t^3, y-t^2-3*t^4); -- ideal ecuaciones
G = gens gb I; -- generadores base de Grobner de I
```

Implicitación

Consideremos un sistema de ecuaciones de parámetro t:

$$\begin{cases} x = 2t - 4t^3 \\ y = t^2 - 3t^4 \end{cases}.$$

Objetivo: obtener una relación implícita entre x e y solamente:

$$h(x, y) := 27x^4 - 144x^2y - 4x^2 + 256y^3 + 128y^2 + 16y = 0.$$

Procedimiento: Gröbner con un orden monomial que elimine t:

```
R = QQ[t,x,y, MonomialOrder => Lex]; -- anillo orden Lex

I = ideal(x-2*t-4*t^3, y-t^2-3*t^4); -- ideal ecuaciones
G = gens gb I; -- generadores base de Grobner de I
```

El primer polinomio de G es $h(x, y)$, que sólo depende de x e y.

Otras aplicaciones: usan bases de Gröbner más de una vez

Otras aplicaciones: usan bases de Gröbner más de una vez

- Calcular el radical de un ideal:

$$\sqrt{I} := \{f \ / \ f^k \in I\} = I + (h_1, \ldots, h_n), \quad h_i \in I \cap k[x_i];$$

Cada h_i calculando base de Gröbner con orden de eliminación.

Otras aplicaciones: usan bases de Gröbner más de una vez

- Calcular el radical de un ideal:

$$\sqrt{I} := \{f \ / \ f^k \in I\} = I + (h_1, \ldots, h_n), \quad h_i \in I \cap k[x_i];$$

  Cada h_i calculando base de Gröbner con orden de eliminación.
- Factorizar un ideal en ideales primos:

$$I = I_1 \cap I_2 \cap \ldots \cap I_l, \quad I_i \text{ ideal primo.}$$

  Descompone el conjunto de soluciones $V(I)$ en irreducibles:

$$V(I) = V(I_1) \cup V(I_2) \cup \ldots \cup V(I_l), \quad V(I_i) \text{ irreducible.}$$

Otras aplicaciones: usan bases de Gröbner más de una vez

- Calcular el radical de un ideal:

$$\sqrt{I} := \{f \ / \ f^k \in I\} = I + (h_1, \ldots, h_n), \quad h_i \in I \cap k[x_i];$$

  Cada h_i calculando base de Gröbner con orden de eliminación.

- Factorizar un ideal en ideales primos:

$$I = I_1 \cap I_2 \cap \ldots \cap I_l, \quad I_i \text{ ideal primo.}$$

  Descompone el conjunto de soluciones $V(I)$ en irreducibles:

$$V(I) = V(I_1) \cup V(I_2) \cup \ldots \cup V(I_l), \quad V(I_i) \text{ irreducible.}$$

- Saturar respecto a un polinomio f:

$$I : (f)^\infty := \{h \ / \ f^k h \in I, \text{para un } k \geq 0\}.$$

  Permite eliminar los puntos donde f se anula:

$$V(I : (f)^\infty) = \overline{V(I) \backslash V(f)} \quad \text{(clausura Zariski)}.$$

Muy lindo pero... ¿cómo calcular una base de Gröbner?

Muy lindo pero... ¿cómo calcular una base de Gröbner?

- En 1899, Gordan introduce el concepto de base de Gröbner, pero no da un algoritmo para calcularlas.

Muy lindo pero... ¿cómo calcular una base de Gröbner?

- En 1899, Gordan introduce el concepto de base de Gröbner, pero no da un algoritmo para calcularlas.
- El primer algoritmo lo da Bruno Buchberger, en su tesis de doctorado de 1965 (algoritmo de Buchberger). Su director de tesis era Gröbner.

Muy lindo pero... ¿cómo calcular una base de Gröbner?

- En 1899, Gordan introduce el concepto de base de Gröbner, pero no da un algoritmo para calcularlas.
- El primer algoritmo lo da Bruno Buchberger, en su tesis de doctorado de 1965 (algoritmo de Buchberger). Su director de tesis era Gröbner.
- El algoritmo de Buchberger se basa en el "criterio de Buchberger": $G = (f_1, \ldots, f_k)$ es base de Gröbner sii:

$$S(f_i, f_j) := LCM(LT(f), LT(g)) \left(\frac{f}{LM(f)} - \frac{g}{LM(g)} \right)$$

tiene resto nulo al dividirlo entre G, para todo par $\{f_i, f_j\} \subset G$.

Muy lindo pero... ¿cómo calcular una base de Gröbner?

- En 1899, Gordan introduce el concepto de base de Gröbner, pero no da un algoritmo para calcularlas.
- El primer algoritmo lo da Bruno Buchberger, en su tesis de doctorado de 1965 (algoritmo de Buchberger). Su director de tesis era Gröbner.
- El algoritmo de Buchberger se basa en el "criterio de Buchberger": $G = (f_1, \ldots, f_k)$ es base de Gröbner sii:

$$S(f_i, f_j) := LCM(LT(f), LT(g)) \left(\frac{f}{LM(f)} - \frac{g}{LM(g)} \right)$$

  tiene resto nulo al dividirlo entre G, para todo par $\{f_i, f_j\} \subset G$.
- El polinomio $S(f_i, f_j)$ se conoce como S-par o S-polynomial.

Algoritmo de Buchberger (en base a su criterio)

Algorithm Algoritmo de Buchberger

Entrada: Un conjunto finito de polinomios B.
Salida: Un conjunto finito G, base de Gröbner del ideal (B).
$G := B$
$C := G \times G$ {conjunto de pares}
while $C \neq \emptyset$ **do**
    Elegir un par (f, g) del conjunto C
    $C := C \backslash \{(f, g)\}$
    $h = RED(S(f, g), G)$ {reduce el S-par de (f, g)}
    if $h \neq 0$ **then**
        $C := C \cup (G \times \{h\})$ {lo incluye en los pares restantes}
        $G := G \cup \{h\}$ {lo agrega a la base en construcción}
    end if
end while
return G

Algoritmo F4 (basado en el de Buchberger)

Algoritmo F4 (basado en el de Buchberger)

- Introducido por Jean-Charles Faugère en 1999.

Algoritmo F4 (basado en el de Buchberger)

- Introducido por Jean-Charles Faugère en 1999.
- Utiliza el criterio de Buchberger (reducir S-pares).

Algoritmo F4 (basado en el de Buchberger)

- Introducido por Jean-Charles Faugère en 1999.
- Utiliza el criterio de Buchberger (reducir S-pares).
- Reduce muchos S-pares a la vez, usando álgebra lineal.

Algoritmo F4 (basado en el de Buchberger)

- Introducido por Jean-Charles Faugère en 1999.
- Utiliza el criterio de Buchberger (reducir S-pares).
- Reduce muchos S-pares a la vez, usando álgebra lineal.
- Para esto, codifica el conjunto de S-pares en una matriz, y luego la escaleriza.

Algoritmo F4 (basado en el de Buchberger)

- Introducido por Jean-Charles Faugère en 1999.
- Utiliza el criterio de Buchberger (reducir S-pares).
- Reduce muchos S-pares a la vez, usando álgebra lineal.
- Para esto, codifica el conjunto de S-pares en una matriz, y luego la escaleriza.
- La humanidad dispone de algoritmos muy eficientes para escalerizar.

Algoritmo F4 (basado en el de Buchberger)

- Introducido por Jean-Charles Faugère en 1999.
- Utiliza el criterio de Buchberger (reducir S-pares).
- Reduce muchos S-pares a la vez, usando álgebra lineal.
- Para esto, codifica el conjunto de S-pares en una matriz, y luego la escaleriza.
- La humanidad dispone de algoritmos muy eficientes para escalerizar.

Figure: Buchberger (2005) y Faugère

¿Qué tan costoso es calcular una base de Gröbner?

¿Qué tan costoso es calcular una base de Gröbner?

Proposición (Dube, 1990)

Polinomios de n variables y B conjunto finito de polinomios con grado total $\leq d$. Sea G base de Gröbner del ideal (B). Entonces:

$$\text{grado polinomios en } G \leq 2\left(\frac{d^2}{2}+d\right)^{2^{n-1}}.$$

¿Qué tan costoso es calcular una base de Gröbner?

Proposición (Dube, 1990)

Polinomios de n variables y B conjunto finito de polinomios con grado total $\leq d$. Sea G base de Gröbner del ideal (B). Entonces:

$$\text{grado polinomios en } G \leq 2\left(\frac{d^2}{2}+d\right)^{2^{n-1}}.$$

- Doblemente exponencial en la cantidad de variables n.

¿Qué tan costoso es calcular una base de Gröbner?

Proposición (Dube, 1990)

Polinomios de n variables y B conjunto finito de polinomios con grado total $\leq d$. Sea G base de Gröbner del ideal (B). Entonces:

$$\text{grado polinomios en } G \leq 2\left(\frac{d^2}{2}+d\right)^{2^{n-1}}.$$

- Doblemente exponencial en la cantidad de variables n.
- Esta cota es "justa": existen ejemplos donde se alcanza.

¿Qué tan costoso es calcular una base de Gröbner?

Proposición (Dube, 1990)

Polinomios de n variables y B conjunto finito de polinomios con grado total $\leq d$. Sea G base de Gröbner del ideal (B). Entonces:

$$\text{grado polinomios en } G \leq 2\left(\frac{d^2}{2}+d\right)^{2^{n-1}}.$$

- Doblemente exponencial en la cantidad de variables n.
- Esta cota es "justa": existen ejemplos donde se alcanza.
- Implica altos costos en tiempo de ejecución y uso de memoria.

¿Qué tan costoso es calcular una base de Gröbner?

Proposición (Dube, 1990)

Polinomios de n variables y B conjunto finito de polinomios con grado total $\leq d$. Sea G base de Gröbner del ideal (B). Entonces:

$$\text{grado polinomios en } G \leq 2\left(\frac{d^2}{2}+d\right)^{2^{n-1}}.$$

- Doblemente exponencial en la cantidad de variables n.
- Esta cota es "justa": existen ejemplos donde se alcanza.
- Implica altos costos en tiempo de ejecución y uso de memoria.
- Sin embargo, es una cota de **peor caso**, por lo que podría no alcanzarse en algunos problemas de interés.

Impacto del orden monomial

Impacto del orden monomial

- Degree Reverse Lexicographic (DRL) suele ser el orden monomial más conveniente para calcular una base de Gröbner: menor tiempo de ejecución y uso de memoria.

Impacto del orden monomial

- Degree Reverse Lexicographic (DRL) suele ser el orden monomial más conveniente para calcular una base de Gröbner: menor tiempo de ejecución y uso de memoria.
- Sin embargo, DRL no es un orden de eliminación, y algunas aplicaciones requieren un orden de eliminación (como Lex).

Impacto del orden monomial

- Degree Reverse Lexicographic (DRL) suele ser el orden monomial más conveniente para calcular una base de Gröbner: menor tiempo de ejecución y uso de memoria.
- Sin embargo, DRL no es un orden de eliminación, y algunas aplicaciones requieren un orden de eliminación (como Lex).
- Lo que se suele hacer en estos casos, es:

Impacto del orden monomial

- Degree Reverse Lexicographic (DRL) suele ser el orden monomial más conveniente para calcular una base de Gröbner: menor tiempo de ejecución y uso de memoria.
- Sin embargo, DRL no es un orden de eliminación, y algunas aplicaciones requieren un orden de eliminación (como Lex).
- Lo que se suele hacer en estos casos, es:
  1. Calcular una base con orden DRL.

Impacto del orden monomial

- Degree Reverse Lexicographic (DRL) suele ser el orden monomial más conveniente para calcular una base de Gröbner: menor tiempo de ejecución y uso de memoria.
- Sin embargo, DRL no es un orden de eliminación, y algunas aplicaciones requieren un orden de eliminación (como Lex).
- Lo que se suele hacer en estos casos, es:
  1. Calcular una base con orden DRL.
  2. Aplicar un algoritmo para cambiar el orden monomial de la base: FGLM (Faugere, 1993) o Gröbner Walk (Collart, 1997).

Software

Software

- Macaulay2: de propósito general (en Álgebra Computacional).

Software

- Macaulay2: de propósito general (en Álgebra Computacional).
- Msolve: implementación eficiente del algoritmo F4 (calcular bases de Gröbner con ejecución en paralelo).

Software

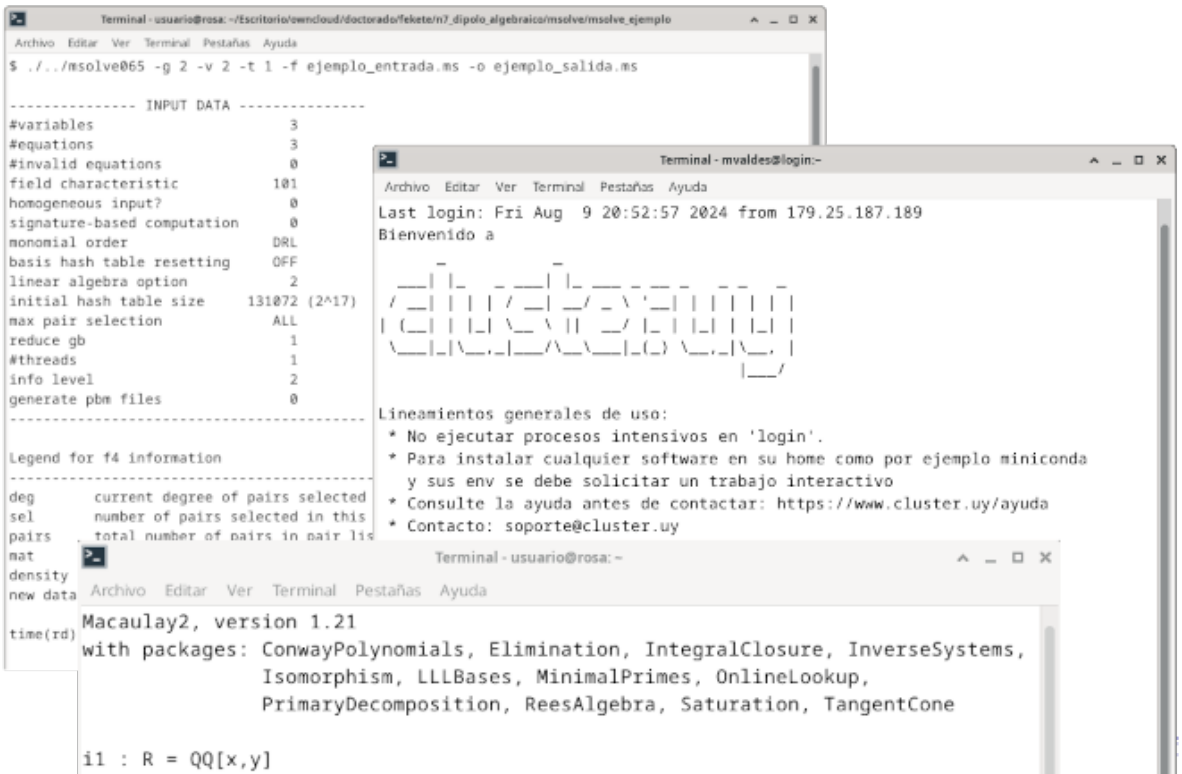
- Macaulay2: de propósito general (en Álgebra Computacional).
- Msolve: implementación eficiente del algoritmo F4 (calcular bases de Gröbner con ejecución en paralelo).
- Ambos son Software libre, desarrollado por investigadores.

Software

- Macaulay2: de propósito general (en Álgebra Computacional).
- Msolve: implementación eficiente del algoritmo F4 (calcular bases de Gröbner con ejecución en paralelo).
- Ambos son Software libre, desarrollado por investigadores.
- ClusterUy: hardware con muchas CPU y memoria RAM (para ejecutar msolve y Macaulay2).

Software

- Macaulay2: de propósito general (en Álgebra Computacional).
- Msolve: implementación eficiente del algoritmo F4 (calcular bases de Gröbner con ejecución en paralelo).
- Ambos son Software libre, desarrollado por investigadores.
- ClusterUy: hardware con muchas CPU y memoria RAM (para ejecutar msolve y Macaulay2).



FIN

Gracias.

Referencias

1. Gordan. Neuer Beweis des Hilbertschen Satzes über homogene Funktionen. Göttinger Nachrichten, pp. 240-284, 1899.
2. Buchberger. An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal. PhD thesis, Universität Innsbruck, 1965.
3. Dube. The Structure of Polynomial Ideals and Gröbner Bases. SIAM Journal of Computing, 19(4):750–773, 1990.
4. Faugere, Gianni, Lazard, Mora. Efficient computation of zero dimensional Gröbner bases by change of ordering. Journal of Symbolic Computation, 16(4):329–344, 1993.
5. Collart, Kalkbrenner, Mall. Converting bases with the Gröbner walk. Journal of Symbolic Computation, 24(3/4):465–469, 1997.
6. Faugere. A new efficient algorithm for computing Gröbner bases (F4). Journal of pure and applied algebra, 139(1-3), 61-88, 1999.
7. Cox, Little, O'Shea (2015). Ideals, Varieties, and Algorithms.