ECUACIONES POLINOMIALES Y ALGORITMOS

Primer Cuatrimestre 2006– Práctica 4

Bases de Gröbner y primeras aplicaciones

(**1**) Justificar (sin hacer cuentas) por qué los polinomios dados en los ejercicios 8, 9 y 10 de la Práctica 3 no son una base de Gröbner del ideal que generan para los órdenes considerados, mientras que los del ejercicio 11 sí lo son para el orden lexicográfico $X < Y < Z$. ¿ Y para un orden diagonal ?

(**2**) Sea $I \subset K[\mathbf{X}]$ un ideal y G una base de Gröbner de I para $<$, y sean $f, g \in K[\mathbf{X}]$.
- Probar que $r_G(f) = r_G(g) \iff f - g \in I$.
- Deducir que $r_G(f + g) = r_G(f) + r_G(g)$ y que $r_G(fg) = r_G(r_G(f)r_G(g))$.

(**3**) Sean G y G' dos bases de Gröbner de un ideal $I \subset K[\mathbf{X}]$ para un orden monomial fijado. Mostrar que si $f \in K[\mathbf{X}]$, entonces $r_G(f) = r_{G'}(f)$ (donde $r_G(f)$ nota el resto de dividir a f por la base de Gröbner G). Es decir, una vez fijado el orden monomial, el resto es independiente de la base de Gröbner considerada.

(**4**) Mostrar que un conjunto finito de generadores de un ideal monomial es siempre una base de Gröbner del ideal.

(**5**) Sean $f_1, \ldots, f_s \in K[X]$ (una variable). Determinar una base de Gröbner de $\langle f_1, \ldots, f_s \rangle$.

(**6**) Sea $I \subset K[\mathbf{X}]$ un ideal principal (i.e $I = \langle f \rangle$ para algún polinomio f). Mostrar que cualquier subconjunto finito de I que contenga un generador de I es una base de Gröbner de I.

(**7**) Sea $A \in \mathbb{R}^{4\times 7}$ la siguiente matriz :

$$A = \begin{bmatrix} 1 & 2 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- Sea $I \subset \mathbb{R}[X_1, X_2, \ldots, X_7]$ el ideal generado por las formas lineales $\{f_1, f_2, f_3, f_4\}$ que se deducen de las filas de A (es decir, $f_i = a_{i1}X_1 + \cdots + a_{i7}X_7$ $(1 \le i \le 7)$ si $A = (a_{ij})$). Probar que $\{f_1, f_2, f_3, f_4\}$ es una base de Gröbner de I para algún orden monomial.
- Generalizar a matrices $A \in \mathbb{R}^{n\times m}$ en forma triangulada.
- ¿ Cuál es el proceso de triangulación que corresponde a producir una base de Gröbner reducida (para el orden lexicográfico puro $X_1 > \cdots > X_n$) del ideal de $K[\mathbf{X}]$ genrado por los polinomios lineales determinados por las filas de A ?

(**8**) ¿ Es $G = \{X^4Y^2 - Z^5, X^3Y^3 - 1, X^2Y^4 - 2Z\}$ una base de Gröbner del ideal que genera con respecto al orden diagonal con $X > Y > Z$?

(**9**) ¿ Depende $S(f, g)$ del orden monomial que se considera ? Ejemplificar.

(10) Sean $f, g \in K[\mathbf{X}]$ mónicos por simplicidad, X^α, X^β monomios, y $<$ fijado. Determinar para qué monomio X^γ se tiene $S(X^\alpha f, X^\beta g) = X^\gamma S(f, g)$.

(11) Hallar bases de Gröbner y bases de Gröbner reducidas para los órdenes lexicográfico puro $X > Y$ y diagonal con $X > Y$ de los siguientes ideales de $K[X, Y]$:

$$I = \langle X^2Y - 1, XY^2 - X\rangle \quad \text{y} \quad J = \langle X^2 + Y, X^4 + 2X^2Y + Y^3 + 3\rangle$$

y deducir si se puede alguna característica del conjunto de ceros de I y de J en K^2.

(12) Sean $f, g \in K[X]$ (una variable). Determinar la base de Gröbner reducida de $\langle f, g\rangle$.

(13) Determinar si $XY^3 - Z^2 + Y^5 - Z^3 \in \langle -X^3 + Y, X^2Y - Z\rangle$
y si $X^3Z - 2Y^2 \in \langle XZ - Y, XY + 2Z^2, Y - Z\rangle$.

(14) Usando órdenes lexicográficos puros, determinar exactamente los ceros comunes en $\mathbb{C}^3$ de los polinomios $X^2 + Y^2 + Z^2 - 1$, $X^2 + Y^2 + Z^2 - 2X$ y $2X - 3Y - Z$ y de los polinomios $X^2Y - Z^3$, $2XY - 4Z - 1$, $Z - Y^2$ y $X^3 - 4YZ$.

(15) Sea $I = \langle X^{n+1} - YZ^{n+1}W, XY^{n-1} - Z^n, X^nZ - Y^nW\rangle \subset \mathbb{C}[X, Y, Z, W]$ y el orden monomial "grevlex" (orden graduado lexicográfico reverso) con $X > Y > Z > W$. El matemático italiano T. Mora mostró alrededor de 1980 que la base de Gröbner reducida de I contiene al polinomio $Z^{n^2+1} - Y^{n^2}W$. Mostrar que es cierto para $n = 3, 4$ y 5

(16) Calcular con Maple por ejemplo, para los ordenes lexicográfico puro y "grevlex" con $X > Y > Z$, bases de Gröbner de los ideales $\langle X^5 + Y^4 + Z^3 - 1, X^3 + Y^2 + Z^2 - 1\rangle$ y $\langle X^5 + Y^4 + Z^3 - 1, X^3 + Y^3 + Z^2 - 1\rangle$, y comparar los tamaños.
¿ Qué se observa ? ¿ Pudo la máquina terminar todas los cómputos para "lex" ?

(17) Comprobar que para el ideal del ejercicio 15 con $n = 3$, se obtiene la misma base de Gröbner usando el orden lexicográfico puro y el "grevlex".
(La experiencia muestra que si bien el orden "grevlex" no siempre funciona mejor que el "lex", en general es una buena idea usar el primero cuando sirve para lo que uno quiere.)

(18) Calcular la base de Gröbner reducida de los ideales $\langle X^3, Y^3 - X, Z^3 - Y, 1 - ZW^2\rangle$
y $\langle X^3, Y^3 - X, Z^3 - Y, W^3 - Z, 1 - WT^2\rangle$ para algún orden. ¿ Se tarda mucho ?

(19) Sea $I = \langle X^2 + 2Y^2 - 3, X^2 + XY + Y^2 - 3\rangle \subset \mathbb{C}[X, Y]$.
- Caracterizar los ideales $I \cap \mathbb{C}[X]$ e $I \cap \mathbb{C}[Y]$.
- Determinar $\mathbf{V}(I) := \{(x, y) \in \mathbb{C}^2 : f(x, y) = 0 \ \forall f \in I\}$. ¿ Cuáles de estas soluciones pertenecen a $\mathbb{Q}^2$?

(20) Sea $I = \langle X^2 + Y^2 + Z^2 - 4, X^2 + 2Y^2 - 5, XZ - 1\rangle \subset \mathbb{C}[X, Y, Z]$.
- Caracterizar $I \cap \mathbb{C}[Y, Z]$ e $I \cap \mathbb{C}[Z]$.
- ¿ Cuántas soluciones racionales hay en $\mathbf{V}(I) := \{(x, y, z) \in \mathbb{C}^3 : f(x, y, z) = 0 \ \forall f \in I\}$?

(21) Sea $I = \langle T^2 + X^2 + Y^2 + Z^2, T^2 + 2X^2 - XY - Z^2, T + Y^3 - Z^3\rangle \subset \mathbb{C}[X, Y, Z, T]$.

- Determinar un sistema de generadores de $I \cap \mathbb{C}[X, Y, Z]$.
- Calcular una Base de Gröbner del sistema de generadores hallado, con respecto al orden "grevlex".
- Calcular ahora una base de Gröbner de I con respecto al orden producto siguiente :

$$T^{\alpha} X^{\beta} Y^{\gamma} Z^{\delta} < T^{\alpha'} X^{\beta'} Y^{\gamma'} Z^{\delta'} \iff \alpha < \alpha' \text{ o } (\alpha = \alpha' \text{ y } X^{\beta} Y^{\gamma} Z^{\delta} <_{\text{grevlex}} X^{\beta'} Y^{\gamma'} Z^{\delta'})$$

  Comparar las dos bases de Gröbner y explicar el resultado.
- Tratar de enunciar condiciones sobre un orden para que valga el teorema de eliminación.

(**22**) Sean $I = \langle (X+Y)^4 (X^2+Y)^2 (X-5Y) \rangle$ y $J = \langle (X+Y)(X^2+Y)^3 (X+3Y) \rangle$. Calcular $I+J$, $I\,J$ e $I \cap J$.

(**23**) Sean f, $g \in K[\mathbf{X}]$.
- Probar que $\langle f \rangle \cap \langle g \rangle$ es un ideal principal. ¿ Quién es h?
- Probar que $\langle f \rangle \cdot \langle g \rangle = \langle f \rangle \cap \langle g \rangle \iff \operatorname{mcd}(f; g) = 1$
- Suponiendo que no se conocen las factorizaciones de f y g, ¿ cómo se hace para calcular h?
- Deducir un algoritmo para calcular $\operatorname{mcd}(f; g)$ sin conocer las factorizaciones de f y g.

(**24**) Sean $f = X^4 + X^3Y + X^3Z^2 - X^2Y^2 + X^2YZ^2 - XY^3 - XY^2Z^2 - Y^3Z^2$ y $g = X^4 + 2X^3Z^2 - X^2Y^2 + X^2Z^4 - 2XY^2Z^2 - Y^2Z^4$.
- Calcular $\langle f \rangle \cap \langle g \rangle$ y $\operatorname{mcd}(f; g)$
- Calcular $\langle f, g \rangle \cap \langle X^2 + XY + XZ + YZ, X^2 - XY - XZ + YZ \rangle$.