APUNTS D'ÀLGEBRA COMPUTACIONAL (CAPÍTOL 2):

BASES DE GRÖBNER

A. MONTES

Date: 4 d'abril de 2001.

1. Problemes a resoldre

A partir d'aquest moment ens interessem bàsicament en l'anell $K[\overline{x}] = K[x_1, \ldots, x_n]$ de polinomis de n variables sobre un cos K. Sabem, pel capítol anterior que és un UFD Noetherià.

La teoria exposada fins aquí dona pocs recursos de càlcul a l'hora de resoldre tot un seguit de problemes. Citem-ne alguns:

1. Descripció d'un ideal, comparació d'ideals.
2. Pertinença d'un polinomi $f \in K[\overline{x}]$ a un ideal $\mathcal{I} \subseteq K[\overline{x}]$.
3. Determinació del gcd i el lcm.
4. Solució d'un sistema d'equacions polinòmiques.
5. Varietats irreductibles i ideals primers. Descomposició minimal d'una varietat en irreductibles.
6. Determinació de la varietat definida per una parametrització polinòmica o racional.
7. Trobar la clausura de Zariski d'un conjunt de K^n.
8. Determinació de l'ideal d'una varietat.
9. Determinació de la intersecció d'ideals.
10. Determinació de l'ideal de varietat d'un ideal.

Tots aquests problemes són fàcils de resoldre a $K[x]$, amb una sola variable. La raó és que $K[x]$ és un domini euclidià on existex la divisió, i per tant és també un PID. En alguns problemes cal distingir si el cos és algebraicament tancat (ex: $\mathbb{C}$, la clausura algebraica de $\mathbb{Q}$) o no (ex: $\mathbb{Q}$ o $\mathbb{R}$). Recordem com es resolen aquests problemes a $K[x]$ (quan calgui diferenciarem entre els dos casos esmentats).

1. Per ser $K[x]$ un PID, tot ideal $\mathcal{I} \subseteq K[x]$ està generat per un únic polinomi generador, que és ademés el gcd de tots els polinomis de $\mathcal{I}$. Es verifica que $\langle f \rangle \subseteq \langle g \rangle$ ssi $g \mid f$.
2. Si $\mathcal{I} = \langle g \rangle$, llavors $f \in \mathcal{I}$ ssi el residu de dividir f per g és 0.
3. El $\gcd(f, g)$ es calcula per l'algorisme d'Euclides, i existeixen identitats de Bézout, etc.
4. Tot conjunt d'equacions polinòmiques és equivalent a una única equació. En un cos algebraicament tancat tot polinomi de grau n descomposa com a producte de n arrels, que poden ser múltiples. L'exemple emblemàtic és $\mathbb{C}[x]$ (teorema fonamental de l'àlgebra). En canvi a $\mathbb{Q}[x]$ podem tenir polinomis de grau arbitrari que corresponen a la varietat buida.
5. Els ideals primers són els generats per un polinomi irreductible. A $\mathbb{C}[x]$, els únics polinomis irreductibles són lineals, i per tant, els ideals primers són de la forma $\langle x - a \rangle$. A $\mathbb{Q}[x]$ hi ha ademés polinomis irreductibles de grau qualsevol. Els corresponents ideals generats són primers, i la varietat associada és buida. Les úniques varietats irreductibles no buides, en ambdos casos, estan formades per un únic punt. Les varietats són

ϕ, K i conjunts finits de punts. La descomposició d'una varietat en irreductibles és trivial.
6. Com sabem, les varietats parametritzables són irreductibles i per tant les úniques varietats de $K[x]$ parametritzables són de la forma $x = a$.
7. Si K és infinit i el conjunt S té infinits punts, la clausura de Zariski de S és tot K.
8. Si $V = \{a_1, a_2, \ldots, a_s\}$, llavors $\mathbb{I}(V) = \langle (x-a_1)(x-a_2)\ldots(x-a_s)\rangle$.
9. La intersecció dels ideals $\langle f\rangle$ i $\langle g\rangle$ és $\langle \mathrm{lcm}(f,g)\rangle$.
10. A $\mathbb{C}[\overline{x}]$, si $\mathcal{I} = \langle f\rangle$, llavors $\mathbb{I}\mathbb{V}(\mathcal{I}) = \langle g\rangle$ on g és el polinomi lliure de quadrats que s'obté com a producte sense multiplicitat de les arrels de f.

    A $\mathbb{Q}[x]$ el polinomi lliure de quadrats pot tenir factors sense arrels i per tant no figuren en el generador de l'ideal de la varietat de l'ideal.

A $K[\overline{x}]$ les coses són més complicades. La teoria de les bases de Gröbner donarà eines per abordar alguns d'aquests problemes. Per entrar en matèria, intentem resoldre el següent exemple.

Exemple 1.1. Donats els polinomis de $\mathbb{Q}[x,y]$

$$f = x^2\,y - 3\,x\,y + x, \qquad \text{i} \qquad g = x\,y + y$$

1. És cert que $\langle f, g\rangle = \left\langle x + 4\,y, 4\,y^2 - y\right\rangle$?
2. És cert que $x - 4\,x\,y \in \langle f, g\rangle$?
3. Determinem $\mathbb{V}(\mathcal{I})$.
4. La varietat determinada no es pot parametritzar. Per què?
5. Quin és l'ideal de la varietat $\mathbb{V}(\mathcal{I})$?

1. $\mathbb{Q}[x,y]$ no és un PID i per tant no és euclidià. No podem esperar trobar una divisió euclidiana. Tenim

$$\begin{aligned} f_1 &= x\,g - f = 4\,x\,y - x \\ f_2 &= 4\,g - f_1 = x + 4\,y \\ f_3 &= y\,f_2 - g = 4\,y^2 - y \end{aligned}$$

   d'on resulta

$$\begin{aligned} f_2 &= 4\,g - f_1 = 4\,g - (x\,g - f) = f + (4-x)\,g \\ f_3 &= y\,f_2 - g = y\,(x\,f + (4-x)\,g) - g \\ &= y\,f + (-x\,y + 4\,y - 1)\,g \\ g &= y\,f_2 - f_3 \\ f &= x\,g - f_1 = x\,g - (4\,g - f_2) = (x-4)\,g + f_2 \\ &= (x-4)(y\,f_2 - f_3) + f_2 = (x\,y - 4\,y + 1)f_2 + (4-x)f_3 \end{aligned}$$

   i en conseqüència $\langle f, g\rangle = \langle f_2, f_3\rangle$.
2. $x - 4\,x\,y = f - x\,g \in \langle f, g\rangle$.
3. $V = \mathbb{V}(\mathcal{I}) = \mathbb{V}(f_2, f_3) = \{(0,0), (-1, 1/4)\}$
4. V no es pot parametritzar perquè no és irreductible.

5. Més difícil és demostrar que en aquest exemple $\mathbb{I}\mathbb{V}(\mathcal{I}) = \mathcal{I}$.

Comprovem que no disposem de mètode general per respondre en aquestes preguntes. Cal una teoria més elaborada.

2. Polinomis, notacions.

Precisem les notacions que fem servir per a polinomis.

Definició 2.1 (Anell de polinomis de n variables sobre un cos (o UFD) K)**.** El denotem $K[x_1, \dots, x_n] = K[\overline{x}]$.

Multigrau: (multideg)	$\alpha = (\alpha_1, \alpha_2 \dots, \alpha_n)$, on $\alpha \in \mathbb{Z}^n_{\geq 0}$
Producte de potències:	$x^\alpha = x_1^{\alpha_1}\, x_2^{\alpha_2} \dots x_n^{\alpha_n}$
Monomi:	$a\, x^\alpha$, on $a \in K$ és el coeficient
Grau total d'un producte de potències x^α:	$\lvert\, \alpha \,\rvert = \alpha_1 + \alpha_2 + \cdots + \alpha_n$
Polinomi:	$f = \sum_\alpha a_\alpha\, x^\alpha$, on $a_\alpha \in K$
Grau total d'un polinomi$f$:	$\deg(f) = \max\{\lvert\, \alpha \,\rvert : f = \sum a_\alpha\, x^\alpha, a_\alpha \neq 0\}$

3. Ordres monomials

Per avançar en la resolució dels problemes esmentats en la secció 1 cal introduir algún algorisme de divisió que donats un polinomi $f \in K[\overline{x}]$ i un ideal $\langle g_1, \dots, g_s \rangle$ expressi f en una forma del tipus $f = \sum_i h_i\, g_i + r$, on $h_i \in K[\overline{x}]$ amb certes bones propietats del residu i quocients. L'algorisme de la divisió funciona a $K[x]$ perquè existeix un ordre natural dels monomis $a\, x^i$, i resulta obvi determinar el monomi principal. A fi d'introduir una divisió cal doncs definir ordres monomials a $K[\overline{x}]$.

Definició 3.1 (Ordre monomial)**.** A $K[\overline{x}]$ un **ordre monomial** és una relació $\succ$ sobre $\mathbb{Z}^n_{\geq 0}$, o de manera equivalent entre productes de potències $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$, o encara entre monomis $a\, x^\alpha$, que verifica

(i) $\succ$ és un ordre total sobre $\mathbb{Z}^n_{\geq 0}$.
(ii) Si $\alpha \succ \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$, llavors $\alpha + \gamma \succ \beta + \gamma$.
(iii) $\succ$ és una bona ordenació de $\mathbb{Z}^n_{\geq 0}$. Això vol dir que tot subconjunt no buit de $\mathbb{Z}^n_{\geq 0}$ té un element mínim.

Lema 3.2. *Una relació d'ordre $\succ$ a $\mathbb{Z}^n_{\geq 0}$ és una bona ordenació ssi tota seqüència de $\mathbb{Z}^n_{\geq 0}$ estrictament decreixent, $\alpha(1) \succ \alpha(2) \succ \alpha(3) \dots$ estaciona.*

Demostració. Ho provarem per reducció a l'absurd.

$\Rightarrow$: Suposem que $\succ$ és un bon ordre i que en canvi a $\mathbb{Z}^n_{\geq 0}$ existeix una seqüència infinita estrictament decreixent: $\alpha_1 \succ \alpha_2 \succ \dots$. Llavors el conjunt $S = \{\alpha_1, \alpha_2, \dots\} \subset \mathbb{Z}^n_{\geq 0}$, no tindria mínim i per tant $\succ$ no seria un bon ordre.

$\Leftarrow$ Suposem ara que tota successió estrictament decreixent estabilitza i que en canvi $\succ$ no és un bon ordre. Si $\succ$ no és una bona ordenació, existeix un subconjunt $S \subset \mathbb{Z}^n_{\geq 0}$ que no té element mínim. Triem $\alpha(1) \in S$. Com que no és l'element més petit, podem trobar $\alpha(1) \succ \alpha(2)$ i així successivament. Obtindrem una seqüència infinita estrictament decreixent $\alpha(1) \succ \alpha(2) \succ \dots$, que no estabilitza.

□

Definició 3.3. Ordre lexicogràfic (lex). Donats $\alpha = (\alpha_1, \dots, \alpha_n)$ i $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, direm que $\alpha \succ_{\text{lex}} \beta$ si en el vector $\alpha - \beta \in \mathbb{Z}^n$, la primera component per l'esquerra no nul.la és positiva. Si $\alpha \succ_{\text{lex}} \beta$ escriurem $x^\alpha \succ_{\text{lex}} x^\beta$.

Amb l'ordre donat, les variables estan en l'ordre habitual:

$$x_1 \succ_{\text{lex}} x_2 \succ_{\text{lex}} \dots \succ_{\text{lex}} x_n$$

ja que

$$(1, 0, \dots, 0) \succ_{\text{lex}} (0, 1, \dots, 0) \succ_{\text{lex}} \dots \succ_{\text{lex}} (0, 0, \dots, 1)$$

Per donar completament un ordre lex, cal precisar en quin ordre considerem les variables (és a dir quina component correspon a cada variable).

Per tant, existeixen $n!$ ordres lex diferents, un per cada permutació dels indexos.

Definició 3.4. Ordre total + invers lexicogràfic (grevlex). Donats $\alpha = (\alpha_1, \dots, \alpha_n)$ i $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, direm que $\alpha \succ_{\text{grevlex}} \beta$ si

$$|\alpha| = \sum_{i=1}^n \alpha_i \;>\; |\beta| = \sum_{i=1}^n \beta_i,$$

o be $|\alpha| = |\beta|$ i en el vector $\alpha - \beta \in \mathbb{Z}^n$, la primera component per la dreta no nul.la és negativa.

Definició 3.5. Ordre total +lexicogràfic (grlex). Donats $\alpha = (\alpha_1, \dots, \alpha_n)$ i $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, direm que $\alpha \succ_{\text{grlex}} \beta$ si

$$|\alpha| = \sum_{i=1}^n \alpha_i \;>\; |\beta| = \sum_{i=1}^n \beta_i,$$

o be $|\alpha| = |\beta|$ i $\alpha \succ_{\text{lex}} \beta$.

Proposició 3.6. *Els ordres* lex, grevlex *i* grlex *a* $\mathbb{Z}^n_{\geq 0}$ *són ordres monomials.*

Exercici 3.7. Demostreu la proposició anterior.

Exercici 3.8. Comproveu que ordenant els monomis del polinomi $f = x^3\,y\,z^2 + x^2\,z^5 + x^2\,y^3\,z$ en ordre monomial decreixent amb $x \succ y \succ z$ tenim

$$\begin{array}{rcll} f &=& x^3\,y\,z^2 + x^2\,y^3\,z + x^2\,z^5 & \text{en ordre } \succ_{\text{lex}} . \\ f &=& x^2\,z^5 + x^2\,y^3\,z + x^3\,y\,z^2 & \text{en ordre } \succ_{\text{grevlex}} . \\ f &=& x^2\,z^5 + x^3\,y\,z^2 + x^2\,y^3\,z & \text{en ordre } \succ_{\text{grlex}} . \end{array}$$

Exercici 3.9.

1. Quants productes de potències diferents de grau total m amb n variables hi ha?
2. Proveu que pels ordres grevlex i grlex tot producte de potències x^α té un anterior $A(x^\alpha) = x^{\alpha'}$ tal que $x^\alpha \succ x^{\alpha'}$ i no hi ha cap altre entre ambdos. Escriviu 10 multigraus en ordre grevlex descendent a partir de $(2,1,3,4)$.
3. Quina és la distància grevlex entre $(2,1,3,4)$ i $(6,2,1,3)$?
4. És certa la qüestió 2 per l'ordre lex? Quin seria el multigrau anterior a $(3,2,0,5)$ en odre lex? I l'anterior a $(3,2,0,0)$?
5. Té sentit la pregunta de la distància per l'ordre lex?

Definició 3.10. Sigui $f = \sum_\alpha a_\alpha\, x^\alpha$ un polinomi no nul de $K[\overline{x}]$ i sigui $\succ$ un ordre monomial. Definim:

(i) **Multigrau (multideg)** de f
$$\text{multideg}(f) = \max_\succ(\alpha \in \mathbb{Z}^n_{\geq 0} \ : \ a_\alpha \neq 0).$$

(ii) **Coeficient principal, (leading coefficient)** de f
$$\text{lc}(f) = a_{\text{multideg}(f)} \in K.$$

(iii) **Producte de potències principal (leading power product)** de f
$$\text{lp}(f) = x^{\text{multideg}(f)}.$$

(iv) **Monomi principal (leading monomial)** de f
$$\text{lm}(f) = \text{lc}(f)\ \text{lp}(f)$$

Lema 3.11. *Siguin $f, g \in K[\overline{x}]$ polinomis no nuls. Tenim:*

(i) $\text{multideg}(f\,g) = \text{multideg}(f) + \text{multideg}(g)$.
(ii) *Si $f+g \neq 0$, llavors* $\text{multideg}(f+g) \preceq \max(\text{multideg}(f), \text{multideg}(g))$. *Si a més a més,* $\text{multideg}(f) \neq \text{multideg}(g)$, *llavors hi ha igualtat.*

Exercici 3.12. Proveu el lema anterior.

4. Algorisme de divisió a $K[\overline{x}]$

Havent defint ordres monomials, estem en disposició de donar un algorisme de divisió amb certes propietats encara que no tan bones com a $K[x]$, però que ens permetran fonamentar la teoria de les bases de Gröbner.

Algorisme de divisió a $K[\overline{x}]$

Input: $f \in K[\overline{x}]$ i $F = [f_1, \dots, f_s] \subset K[\overline{x}]$,
$\succ$: un $\overline{x}$-ordre monomial.
Output: $r \in K[\overline{x}]$ i $Q = \{q_1, \dots, q_s\} \subset K[\overline{x}]$ tals que $f = \sum_{i=1}^{s} q_i\, f_i + r$

```
q_1 := 0; ... q_s := 0;  r := 0
p := f
MENTRE p ≠ 0 FER
    i := 1
    dividit:=fals
    MENTRE i ≤ s I dividit=fals FER
        SI lm(f_i) divideix lm(p) LLAVORS
            q_i := q_i + lm(p)/ lm(f_i)
            p := p − (lm(p)/ lm(f_i)) f_i
            dividit:=cert
        ALTRAMENT
            i := i + 1
    SI dividit=fals LLAVORS
        r := r + lm(p)
        p := p − lm(p)
```

Exemple 4.1. Fem la divisió de $f = x^2\, y + x\, y^2 + y^2$ entre $f_1 = x\, y - 1$ i $f_2 = y^2 - 1$ en ordre lex amb $x \succ y$.

Ho disposem en la forma següent:

$$\begin{array}{l} f_1 = x\, y - 1 : \\ f_2 = y^2 - 1 : \\ \\ \sqrt{x^2\, y + x\, y^2 + y^2} \end{array}$$

i anem fent quocients i separant els residus que no caben. El resultat serà:

$$\begin{array}{l} f_1 = x\,y - 1 : x + y \\ f_2 = y^2 - 1 \ : 1 \end{array}$$

$$\begin{array}{lcr}
\sqrt{x^2\,y + x\,y^2 + y^2} & & \\
-x^2\,y + x & & \\
\hline
\ \ x\,y^2 + x + y^2 & & \\
-x\,y^2 + y & & \\
\hline
\ \ x + y^2 + y & & \\
-x & & x \\
\hline
\ \ y^2 + y & & \\
-y^2 + 1 & & \\
\hline
\ \ y + 1 & & \\
-y - 1 & & y + 1 \\
\hline
\quad 0 & & x + y + 1
\end{array}$$

On hem anat col.locant, per ordre, els quocients parcials x per f_1, y per f_1; després el proper terme principal x no és divisible i passa al residu; a continuació el quocient parcial és 1 per f_2. Finalment passen al residu, ja que no són divisibles y i 1. El residu de la divisió és en total $x + y + 1$, i resultat de la divisió és:

$$f = x^2\,y + x\,y^2 + y^2 = (x + y) \cdot f_1 + 1 \cdot f_2 + (x + y + 1)$$

Exercici 4.2. Comproveu que fent la divisió anterior amb els divisors en l'ordre f_2, f_1. el residu de la divisió és $2\,x + 1$, i resutat de la divisió és:

$$f = x^2\,y + x\,y^2 + y^2 = (x + 1) \cdot f_2 + x \cdot f_1 + (2\,x + 1)$$

Observem, doncs, que la divisió no dona un residu idèntic segons l'ordre en que s'agafen els divisors. Obviament, si al dividir f entre $f_1, \dots, f_s$ el residu val zero, estem segurs que $f \in \langle f_1, \dots, f_s \rangle$ però no podem esperar, sense més, que el recíproc sigui cert. El teorema que caracteritza la divisió que hem descrit és el següent:

Teorema 4.3. *Donat un ordre monomial $\succ$ a $\mathbb{Z}^n_{\geq 0}$ i una s-tupla de polinomis $F = [f_1, \dots, f_s] \subset K[\overline{x}]$,*

(i) *tot $f \in K[\overline{x}]$ pot expressar-se en la forma*

$$f = \sum_{i=1}^{s} q_i\,f_i + r$$

on $q_i, r \in K[\overline{x}]$, i

(ii) *o be $r = 0$ o be r és una K combinació lineal de productes de potències, tals que cap d'elles és divisible per cap* $\mathrm{lm}(f_i)$ *per* $1 \le i \le s$. *Direm que r és un* **residu** *de la divisió de f per F.*

(iii) *Es cumpleix que, si $q_i\, f_i \neq 0$, llavors*

$$\mathrm{multideg}(f) \succeq \mathrm{multideg}(q_i\, f_i)$$

(iv) *L'algorisme de divisió donat produeix els resultats* (i), (ii), (iii).

Demostració. En l'algorisme de la divisió, la variable p representa el residu parcial a cada pas de divisió. Els q_i's i r són els respectius quocients i residu parcials. La variable "dividit" indica si en el bucle corresponent hi ha hagut divisió parcial o no. En cas que no hi hagi, el corresponent terme principal de p passa al residu.

(i) A cada nou bucle es cumpleix que

$$f = \sum_{i=1}^{s} q_i\, f_i + p + r.$$

És cert inicialment. A cada bucle, part del contingut de p passa a r o a la suma, de manera que l'equació es conserva. Si provem que l'algorisme acaba, com que finalment $p = 0$ quedarà provat que es verifica (i).

Per veure que l'algorisme acaba només cal veure que a cada bucle redefinim p de tal manera que el seu monomi principal és eliminat. Per tant, $\mathrm{multideg}(p)$ decreix estrictament. Per ser $\succ$ una bona ordenació, l'algorisme acaba.

(ii) Cada monomi que ha passat a r durant l'algorisme no és divisible per cap $\mathrm{lm}(f_i)$ per $1 \le i \le s$. Per tant, quan l'algorisme acabi es seguirà cumplint (ii).

(iii) Cada terme de q_i és de la forma $\mathrm{lm}(p)/\,\mathrm{lm}(f_i)$ per algun p intermig. L'algorisme comença amb $p = f$ i a (ii) hem vist que $\mathrm{multideg}(p)$ decreix. Utilitzant el lema 3.11 resulta immediatament la condició (iii).

□

5. Ideals de monomis i lema de Dickson

Definició 5.1 (Ideal de monomis)**.** Direm que $\mathcal{I} \subset K[\overline{x}]$ és un ideal de monomis si existeix un conjunt A (finit o infinit) de productes de potències que el genera:

$$\mathcal{I} = \langle x^\alpha \;:\; \alpha \in A \rangle = \left\{ \sum_\alpha h_\alpha\, x^\alpha \;:\; h_\alpha \in K[\overline{x}],\ \alpha \in A \right\}$$

Observis que fora equivalent parlar de conjunt de monomis, ja que K és un cos, i si $c \neq 0$, dir que $c\, x^\alpha$ és un generador és equivalent a dir que ho és x^α.

Exemple 5.2. $\mathcal{I} = \left\langle x^3\, y^2\, z, x\, y^5\, z^3, y^3\, z^2 \right\rangle \subset K[x, y, z]$.

Lema 5.3. *Sigui* $\mathcal{I} = \langle x^\alpha \ : \ \alpha \in A\rangle$ *un ideal de monomis. Llavors un producte de potències* $x^\beta \in \mathcal{I}$ *ssi* x^β *és divisible per algún producte de potències* $x^\alpha, \quad \alpha \in A$.

Demostració. $\Rightarrow$: Obviament si x^β és múltiple d'algún x^α per algún $\alpha \in A$, llavors $x^\beta \in \mathcal{I}$.

$\Leftarrow$: Si $x^\beta \in \mathcal{I}$, llavors $x^\beta = \sum_{i=1}^{s} h_i\, x^{\alpha(i)}$, per certs $h_i \in K[\overline{x}]$ i $\alpha(i) \in A$. Expandint el producte tindrem

$$x^\beta = \sum_{i=1}^{s} h_i\, x^{\alpha(i)} = \sum_{i=1}^{s} \sum_{j=1}^{t_i} c_{ij} x^{\gamma_{ij} + \alpha(i)}$$

on $c_{ij} \in K$. Un cop expandit el producte, únicament no es cancel.len els productes de potències amb exponent β. Per cada un dels productes de potències restants és $\gamma_{ij} + \alpha(i) = \beta$. Per tant x^β és divisible per cada un dels productes de potències $x^{\alpha(i)}$ que no s'hagin cancel.lat. $\square$

Els productes de potències x^β que són divisibles per x^α corresponen a

$$\alpha + \mathbb{Z}^n_{\geq 0} = \left\{\alpha + \gamma \ : \ \gamma \in \mathbb{Z}^n_{\geq 0}\right\}$$

Així, els productes de potències de l'ideal de l'exemple anterior seran:

$$\left((3, 2, 1) + \mathbb{Z}^3_{\geq 0}\right) \cup \left((1, 5, 3) + \mathbb{Z}^3_{\geq 0}\right) \cup \left((0, 3, 2) + \mathbb{Z}^3_{\geq 0}\right)$$

Exemple 5.4. Podem representar gràficament els monomis d'un ideal de monomis. Per exemple, per l'ideal $\mathcal{I} = \left\langle x\, y^3, x^3\, y^2, x^4\, y \right\rangle \subset K[x, y]$, els monomis de $\mathcal{I}$ venen representats en el gràfic següent:

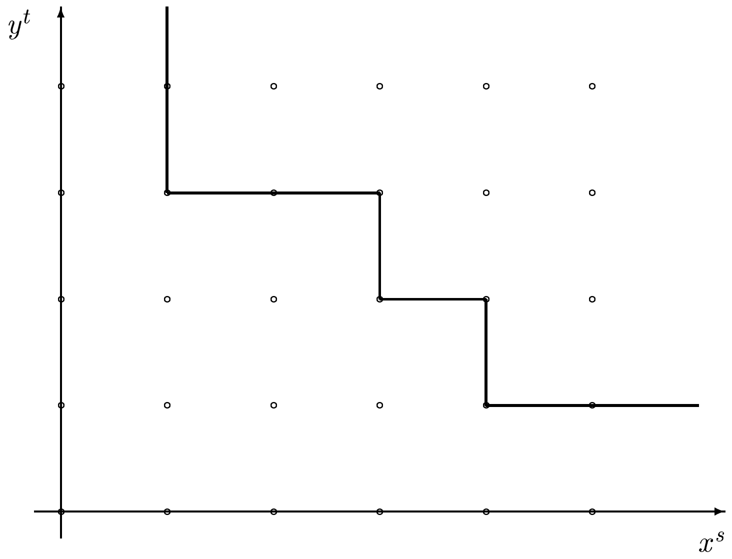

Fig. 1: Monomis de l'ideal $\mathcal{I} = \left\langle x\, y^3, x^3\, y^2, x^4\, y \right\rangle$

Lema 5.5. *Sigui $\mathcal{I}$ un ideal de monomis i $f \in K[\overline{x}]$. Són equivalents les afirmacions següents:*

(i) $f \in \mathcal{I}$.
(ii) *Cada monomi de f pertany a $\mathcal{I}$.*
(iii) *f és una K-combinació lineal de productes de potències de $\mathcal{I}$.*

Demostració. Obviament (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). Només cal provar que (i) implica (iii). La demostració és anàloga a la del lema anterior. Sigui $f \in \mathcal{I}$. Llavors, existeixen certs $h_i \in K[\overline{x}]$ i $\alpha(i) \in A$, tals que

$$f = \sum_{i=1}^{s} h_i\, x^{\alpha(i)} = \sum_{i=1}^{s} \sum_{j=1}^{t_i} c_{ij}\, x^{\gamma_{ij}+\alpha(i)}$$

on $c_{ij} \in K$. Per tant, cada monomi de f és divisible per algún $x^{\alpha(i)}$ i per tant, pel lema 5.3, pertany a $\mathcal{I}$. $\square$

Corol·lari 5.6. *Dos ideals de monomis són iguals ssi tenen els mateixos productes de potències.*

Teorema 5.7 (Lema de Dickson). *Si $\mathcal{I} \subset K[\overline{x}]$ és un ideal de monomis $\mathcal{I} = \langle x^\alpha \ :\ \alpha \in A\rangle$, llavors podem extreure $B = \{\alpha(1), \ldots, \alpha(s)\} \subset A$, subconjunt finit de A, tal que*

$$\mathcal{I} = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle .$$

Demostració. Havent demostrat el teorema de la base d'Hilbert al capítol 1, ara el lema de Dickson és un corol·lari.

Per la proposició demostrada al capítol 1 que segueix al teorema de la base d'Hilbert, de tota base d'un ideal podem extreure una base finita. Per tant, donat $\mathcal{I} = \langle x^\alpha \ :\ \alpha \in A\rangle$ podem extreure una base finita $\{\alpha(1), \ldots, \alpha(s)\} \subset A$. $\square$

Corol·lari 5.8. *Sigui $\succ$ una relació a $\mathbb{Z}^n_{\geq 0}$ que verifica*

(i) *$\succ$ és una relació d'ordre total a $\mathbb{Z}^n_{\geq 0}$.*
(ii) *Si $\alpha \succ \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$, llavors $\alpha + \gamma \succ \beta + \gamma$.*

Llavors $\succ$ és un bon ordre ssi $\alpha \succeq 0$ per tot $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Demostració. $\Leftarrow$: Si existeix $\alpha_0 \prec 0$ diferent de 0, afegint repetidament α_0 a cada banda, emprant (ii), tindriem una succesió

$$\alpha_0 \prec 2\,\alpha_0 \prec \ldots n\,\alpha_0 \prec \ldots$$

estrictament decreixent que no estacionaria, i per tant $\succ$ no seria un bon ordre.

$\Rightarrow$: Suposem ara que tot $\alpha \in \mathbb{Z}^n_{\geq 0}$ és $\alpha \succeq 0$. Llavors si $A \subset \mathbb{Z}^n_{\geq 0}$ qualsevol demostrem que té un element mínim. En efecte, sigui $\mathcal{I} = \langle x^{\overline{\alpha}} \ :\ \alpha \in A\rangle$. Pel lema de Dickson existeixen elements tals que $\mathcal{I} = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$. Sigui, reordenant si cal, $\alpha(1) \preceq \alpha(i)$. Anem a veure que $\alpha(1)$ és el mínim dels elements de A. En efecte, si $\beta \in A$, llavors $x^\beta \in \mathcal{I}$, i pel lema 5.3 és divisible per algún $x^{\alpha(i)}$. Això implica $\beta = \gamma + \alpha(i)$. Per (ii) tindrem

$$\beta = \gamma + \alpha(i) \succeq \alpha(i) \succeq \alpha(1)$$

tal com voliem demostrar. □

6. Teorema de les bases de Gröbner

Les bases de Gröbner van ser introduïdes a mitjans dels anys 60 per H. Hironaka (que les anomenà bases estandard). Paral·lelament i independent, les va trobar B. Buchberger en la seva tesi doctoral al 1965, i les va anomenar així en honor al seu director de tesi W. Gröbner.

Definició 6.1. Donat un ideal $\mathcal{I} \subset K[\overline{x}]$ diferent de $\{0\}$ i un ordre monomial $\succ$, denotem

(i) $\mathrm{lm}(\mathcal{I})$ al conjunt dels monomis principals de tots els elements de $\mathcal{I}$:

$$\mathrm{lm}(\mathcal{I}) = \{c\, x^\alpha \ : \ c\, x^\alpha = \mathrm{lm}(f),\ f \in \mathcal{I}\}$$

(ii) $\langle \mathrm{lm}(\mathcal{I})\rangle$ a l'ideal generat pels elements de $\mathrm{lm}(\mathcal{I})$.

Proposició 6.2. *Si $\mathcal{I} \subset K[\overline{x}]$ és un ideal, llavors $\langle \mathrm{lm}(\mathcal{I})\rangle$ és un ideal de monomis.*

Demostració. Exercici □

Teorema 6.3 (Base de Gröbner). *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal diferent de $\{0\}$. Llavors*

(i) *Donat un ordre monomial $\succ$, existeix un conjunt finit $G = \{g_1, \dots, g_s\} \subset \mathcal{I}$, tal que*

$$\langle \mathrm{lm}(\mathcal{I})\rangle = \langle \mathrm{lm}(g_1), \dots, \mathrm{lm}(g_s)\rangle \tag{6.1}$$

(ii) *Tot subconjunt $G \subset \mathcal{I}$ que verifiqui la relació (6.1) és una base de $\mathcal{I}$. És a dir,*

$$\mathcal{I} = \langle g_1, \dots, g_s\rangle\,.$$

Direm que és una **base de Gröbner** *de $\mathcal{I}$.*

Demostració. (i) Per la proposició 6.2 $\langle \mathrm{lm}(I)\rangle$ és un ideal de monomis. Pel lema de Dickson, existeix un subconjunt finit d'elements que el genera. Però els elements de $\mathrm{lm}(I)$ són de la forma $\mathrm{lm}(f)$, on $f \in \mathcal{I}$. Per tant, existeix $G = \{g_1, \dots, g_s\} \subset \mathcal{I}$ tal que $\langle \mathrm{lm}(\mathcal{I})\rangle = \langle \mathrm{lm}(g_1), \dots, \mathrm{lm}(g_s)\rangle$.

(ii) Demostrem que el conjunt G de (i) verifica també $\mathcal{I} = \langle g_1, \dots, g_s\rangle$. És evident que $\langle g_1, \dots, g_s\rangle \subseteq \mathcal{I}$, ja que cada $g_i \in \mathcal{I}$. Recíprocament, si $f \in \mathcal{I}$ l'algorisme de la divisió expressa f en la forma

$$f = a_1\, g_1 + \dots, a_s\, g_s + r$$

on $a_1, \ldots, a_s, r \in K[\overline{x}]$ i cap terme de r és divisible per cap dels $\mathrm{lm}(g_i)$, $1 \leq i \leq s$. Demostrarem que $r = 0$. En efecte, de l'expressió anterior en deduim que

$$r = f - a_1\, g_1 - \ldots, a_s\, g_s \in \mathcal{I}.$$

Per tant

$$\mathrm{lm}(r) \in \langle \mathrm{lm}(\mathcal{I}) \rangle = \langle \mathrm{lm}(g_1, \ldots, \mathrm{lm}(g_s)) \rangle \,.$$

Pel lema 5.3, si $r \neq 0$, llavors $\mathrm{lm}(r)$ ha de ser divisible per algún $\mathrm{lm}(g_i)$. Això contradiu el fet que r sigui el residu de la divisió. En conseqüència r ha de ser 0 i $f \in \langle g_1, \ldots, g_s \rangle$, el que prova que $\mathcal{I} \subseteq \langle g_1, \ldots, g_s \rangle$. En conseqüència $\mathcal{I} = \langle g_1, \ldots, g_s \rangle$ i tot conjunt que verifiqui (6.1) és una base de Gröbner de $\mathcal{I}$. □

Recordem, doncs,

Definició 6.4 (**Base de Gröbner).** Donat un ideal $\mathcal{I} \subset K[\overline{x}]$ i fixat un ordre monomial $\succ$, direm que un subconjunt $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ és una **base de Gröbner** o una **base estandard** si cumpleix la condició (6.1).

De manera equivalent, encara que més informal, un conjunt $\{g_1, \ldots, g_s\} \subset \mathcal{I}$ és una base de Gröbner de $\mathcal{I}$ ssi el terme principal de qualsevol element de $\mathcal{I}$ és divisible per algún dels $\mathrm{lm}(g_i)$.

7. Propietats de les bases de Gröbner

Proposició 7.1. *Sigui $f \in K[\overline{x}]$, i $G = \langle g_1, \ldots, g_s \rangle \subset K[\overline{x}]$ una base de Gröbner d'un ideal $\mathcal{I}$. Llavors el residu $r \in K[\overline{x}]$ de la divisió de f entre G té les quatre propietats següents:*

(i) *Cap terme de r és divisible per cap* $\mathrm{lm}(g_i)$, $1 \leq i \leq s$.
(ii) *Existeix $g \in \mathcal{I}$ tal que $f = g + r$.*
(iii) *r és únic. És a dir, no existeix cap altre r' amb les propietats* (i) *i* (ii). *En particular, el residu és independent de l'ordre en que considerem els elements de G.*
(iv) *El residu r és zero ssi $f \in \mathcal{I}$.*

Demostració. (i) L'algorisme de la divisió de f entre G dona

$$f = q_1\, g_1 + \cdots + q_s\, g_s + r$$

i ens mostra l'existència d'un r que verifica (i).

(ii) Tenim $g = q_1\, g_1 + \cdots + q_s\, g_s$ que verifica (ii).

(iii) Suposem que existisin dos parells (r, g) i (r', g') que cumplissin (i) i (ii). Tindriem $f = g + r = g' + r'$. Per tant, $r' - r = g - g' \in \mathcal{I}$. Per tant,

$$\mathrm{lm}(r' - r) \in \langle \mathrm{lm}(\mathcal{I}) \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle \,.$$

Pel lema 5.3, $\mathrm{lm}(r' - r)$ hauria de ser divisible per algún $\mathrm{lm}(g_i)$, $1 \leq i \leq s$. Però això és impossible ja que cap terme de r ni de r' ho és. Per tant $r' - r = 0$.

(iv) És conseqüència immediata de (i), (ii) i (iii).

□

De vegades s'utilitza la caracterització que dona la proposició 7.1 per definir les bases de Gröbner. La definició 6.4 referida a la condició (6.1) és equivalent a que per tot $f \in \mathcal{I}$ el residu de dividir f per G és zero.

La proposició 7.1 resol el problema de la pertineça a un ideal: f pertany a $\mathcal{I}$ ssi el residu de dividir f per una base de Gröbner de $\mathcal{I}$ és zero.

Lema 7.2. *Sigui G una base de Gröbner de l'ideal $\mathcal{I} \subset K[\overline{x}]$. Sigui $p \in G$ tal que $\operatorname{lm}(p) \in \langle \operatorname{lm}(G - \{p\}) \rangle$. Llavors $G - \{p\}$ també és una base de Gröbner de $\mathcal{I}$.*

Demostració. Sabem que $\langle \operatorname{lm}(\mathcal{I}) \rangle = \langle \operatorname{lm}(G) \rangle$. Si $\operatorname{lm}(p) \in \langle \operatorname{lm}(G - \{p\}) \rangle$, llavors $\langle \operatorname{lm}(G - \{p\}) \rangle = \langle \operatorname{lm}(G) \rangle$. Per tant, $G - \{p\}$ també és una base de Gröbner de $\mathcal{I}$. □

Eliminant tots els polinomis que cumpleixen el lema anterior un radera de l'altre i normalitzant després, arribem a una base de Gröbner minimal.

Definició 7.3 (Base de Gröbner minimal)**.** Direm que G és una base de Gröbner minimal de $\mathcal{I} \subset K[\overline{x}]$, si és una base de Gröbner tal que

(i) Per cada $p \in G$, $\operatorname{lm}(p) \notin \langle \operatorname{lm}(G - \{p\}) \rangle$.
(ii) Per cada $p \in G$, $\operatorname{lc}(p) = 1$.

Proposició 7.4. *Donades dues bases minimals G i G' del mateix ideal $\mathcal{I} \subset K[\overline{x}]$, aquestes tenen el mateix nombre de polinomis i estan en correspondència bijectiva. Els associats en la correspondència tenen el mateix terme principal.*

Demostració. Exercici. □

Però un ideal admet encara moltes bases de Gröbner minimals. En l'exemple 7.9, enlloc del polinomi x^2 podem posar $x^2 + a\,x\,y$, ja que aquest darrer té el mateix terme principal que l'anterior i també pertany a F. A fi d'obtenir una base única introduim el concepte de base de Gröbner reduida.

Definició 7.5 (Base de Gröbner reduida)**.** Direm que G és una base de Gröbner reduida de $\mathcal{I} \subset K[\overline{x}]$, si és una base de Gröbner tal que

(i) Per cada $p \in G$, cap monomi de p pertany a $\langle \operatorname{lm}(G - \{p\}) \rangle$.
(ii) Per cada $p \in G$, $\operatorname{lc}(p) = 1$.

Observis que de les possibles bases minimals de l'exemple anterior donades, únicament la que correspon a $a = 0$ cumpleix la condició donada. En general, tenim la següent proposició:

Proposició 7.6. *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal no nul. Llavors, fixat un ordre monomial $\succ$, $\mathcal{I}$ admet una i una sola base de Gröbner reduida.*

Demostració. Ho provarem de forma constructiva.

Sigui G una base minimal. Per cada $g \in G$ determinem $g' = \overline{g}^{G-\{g\}}$. i posem $G' = (G - \{g\}) \cup \{g'\}$. És immediat comprovar que G' segueix sent una base minimal, ja que el terme principal no ha canviat. Però g' cumpleix la condició (i). Fent el mateix per tots els polinomis de G, anem reduint cada polinomi de la G inicial. Observis que en fer-ho, els polinomis que ja hem reduit prèviament, continuen estant reduits, ja que per això únicament compten els termes principals, i aquests no canvien en el procés. El resultat és una base de Gröbner reduida.

No més cal provar que aquesta és única. Si existissin dues G i G', ambdues serien minimals. No més cal provar que els polinomis $g \in G$ i $g' \in G'$ que es corresponen per tenir el mateix terme principal són iguals. En efecte, $r = g - g' \in \mathcal{I}$ i per tant, el residu de dividir-lo per G és zero. Però cap terme de g ni de g' és divisible per cap terme principal de G, i per tant passen directament al residu. Com que aquest és nul, això implica que $g - g' = \overline{g - g'}^G = 0$. ☐

Corol·lari 7.7 (Igualtat d'ideals). *Dos ideals són iguals ssi tenen la mateixa base de Gröbner reduida per un ordre monomial $\succ$.*

L'ideal $\mathcal{I}_1$ està contingut en $\mathcal{I}_2$, $\mathcal{I}_1 \subset \mathcal{I}_2$, si tots els generadors d'una base del segon redueixen a zero al ser dividits per una base de Gröbner del primer.

L'existència d'una base de Gröbner reduïda única per cada ordre monomial resol el problema de la descripció dels ideals.

El problema és ara saber detectar quan un conjunt de generadors d'un ideal $\mathcal{I}$ és una base de Gröbner i saber construïr-ne una a partir d'un conjunt donat de generadors. Això serà l'objecte de secció següent. Veiem, però un exemple.

Exemple 7.8. Donada la base $F = \{f_1, \ldots, f_m\}$ d'un ideal formada per polinomis lineals: $f_i = \sum_{j=1}^{n} a_{ij}x_j + a_i$, per eliminació gaussiana podem formar una nova base $G = \{g_1, \ldots, g_s\}$ amb $s \leq m$ i

$$g_i = x_{k_i} + l_i + b_i \quad \text{on} \quad l_i = \sum_{j=k_i+1}^{n} b_{ij}x_j$$

Els vectors dels coeficients

$$\begin{array}{cccccccccc|c}
(1 & b_{1,2} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & & b_1 \,) \\
(0 & \ldots & 1 & b_{2,k_2+1} & \ldots & \ldots & \ldots & \ldots & \ldots & & b_2 \,) \\
(0 & \ldots & 0 & \ldots & 1 & b_{3,k_3+1} & \ldots & \ldots & \ldots & & b_3 \,) \\
\vdots & & & & & & & & & & \vdots \\
(0 & \ldots & 0 & \ldots & 0 & \ldots & 1 & b_{s,k_s+1} & \ldots & & b_s \,)
\end{array}$$

són linealment independents. Veurem més endavant que G és una base de Gröbner de F per un ordre de les variables $x_1 \succ x_2 \succ \cdots \succ x_n$ (lex o grlex o grevlex). Obviament l'ideal generat pels monomis principals de $\langle \mathrm{lm}(G) \rangle = \langle x_1, x_{k_2}, \ldots, x_{k_s} \rangle$ és més gran que $\langle \mathrm{lm}(F) \rangle = \langle x_1 \rangle$.

Ara és fàcil veure que és minimal. Com pot obtenir-se una base reduïda?

Exemple 7.9. Donat $F = \langle f_1, f_2 \rangle$, on $f_1 = x^3 - 2\,x\,y$, i $f_2 = x^2\,y - 2\,y^2 + x$ aplicant l'algorisme de Buchberger que veurem a la secció 9, calculem una base de Gröbner de F en ordre grlex amb $y \succ x$. Obtenim

$$G = \{f_1, f_2, f_3, f_4, f_5\}$$

on

$$f_3 = -x^2 \quad f_4 = -2\,x\,y \quad f_5 = -2\,y^2 + x$$

Observem que $\mathrm{lm}(f_3) \mid \mathrm{lm}(f_1)$, i per tant f_1 pot eleminar-se de la base. També podem eliminar f_2, ja que $\mathrm{lm}(f_4) \mid \mathrm{lm}(f_2)$. Finalment, normalitzant, obtenim una base de Gröbner minimal:

$$G_M = [x^2, x\,y, y^2 - (1/2)\,x]$$

8. Determinació de les bases de Gröbner

Demostrada l'existència de bases de Gröbner, ara ens cal saber reconèixer si una base donada ho és i saber completar una base donada d'un ideal fins a obtenir una base de Gröbner.

En tot el que segueix, suposarem fixat un ordre monomial $\succ$, i tots els càlculs seran relatius a l'ordre donat.

Definició 8.1. Denotem $\overline{f}^F$ el residu de la divisió de f per la s-tupla $F = [f_1, \ldots, f_s]$.

Si F és una base de Gröbner de $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$, llavors l'ordre en els f_i no importa, i a més a més, $\overline{f}^F$ és el representant únic de $K[\overline{x}]/\mathcal{I}$ equivalent a f tal que cap monomi és divisible per cap $\mathrm{lm}(g_i)$, per $1 \leq i \leq s$.

A fi de determinar una base de Gröbner, ens interessa generalitzar el mètode d'eliminació de Gauss. El S-polinomi, que introdïm a continuació, juga aquest paper:

Definició 8.2 (S-polinomi)**.** Siguin $f, g \in K[\overline{x}]$, no nuls. Siguin

$$\alpha = \mathrm{multideg}(f), \quad \beta = \mathrm{multideg}(g), \quad i \quad x^\gamma = \mathrm{lcm}(x^\alpha, x^\beta)$$

Definim el S-polinomi de f i g per

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

Els S-polinomis produeixen cancel·lació de monomis principals. En conseqüència, és evident que

$$\mathrm{multideg}(S) \prec \gamma$$

A fi de provar el teorema de reconeixement d'una base de Gröbner, necessitem un lema tècnic:

Lema 8.3. *Sigui una suma de la forma* $\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i$, *on*

(i) $\mathrm{lm}(g_i) = d_i\, x^{\beta(i)}$
(ii) $c_i \in K$ *per* $1 \leq i \leq t$,
(iii) $\alpha(i) + \beta(i) = \delta \in \mathbb{Z}^n_{\geq 0}$ *si* $c_i \neq 0$.

Si $\mathrm{multideg}\left(\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i\right) \prec \delta$, *és a dir, si hi ha cancel·lació de monomis principals, llavors existeixen constants* $c_{jk} \in K$ *tals que*

$$\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i = \sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}}\, S(g_j, g_k),$$

on

$$x^{\gamma_{jk}} = \mathrm{lcm}(\mathrm{lp}(g_j), \mathrm{lp}(g_k)) \tag{8.1}$$

A més a més, cada sumand $c_{jk}\, x^{\delta-\gamma_{jk}}\, S(g_j, g_k)$ *té multigrau estrictament inferior a* δ.

Observació 8.4. La importància del lema radica en que a la fórmula del lema, cada sumand del primer membre té el mateix monomi principal x^δ, i es produeix la cancel·lació de terme principal un cop efectuada tota la suma. En canvi, en el segon membre, cada terme ja te un monomi principal de multigrau menor que δ, i ell mateix conté cancel·lació.

Demostració. Amb la notació de l'enunciat, el coeficient principal de $c_i\, x^{\alpha(i)}\, g_i$ serà $c_i\, d_i$. Tenint en compte que cada un d'aquests sumands té el mateix multigrau δ i que la suma té multigrau estrictament inferior, resulta que $\sum_{i=1}^{t} c_i\, d_i = 0$.

Posem $p_i = x^{\alpha(i)}\, g_i/d_i$. Observem que el coeficient principal de p_i és 1. Ara considerarem un desenvolupament telescòpic de la suma. Però abans hem de comentar, que hi poden haver termes i que no hi figurin en la suma, de manera, que al considerar el desenvolupament telescòpic, cal entendre que parlem dels indexos correlatius presents en la suma, que no són necessàriament tots els i. Amb aquesta observació, considerem el desenvolupament telescòpic següent

$$\begin{aligned}\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i &= \sum_{i=1}^{t} c_i\, d_i\, p_i = c_1\, d_1\,(p_1 - p_2) + (c_1\, d_1 + c_2\, d_2)(p_2 - p_3) + \dots \\ &\quad +(c_1\, d_1 + \dots + c_{t-1}\, d_{t-1})(p_{t-1} - p_t) + p_i \sum_{i=1}^{t} c_i\, d_i\end{aligned}$$

Per hipòtesi $\alpha(i) + \beta(i) = \delta$. Per tant $\mathrm{lp}(g_i) \mid x^\delta$ per $1 \leq i \leq t$. En conseqüència $x^{\gamma_{jk}} \mid x^\delta$, i per tant, $x^{\delta-\gamma_{jk}} \in \mathbb{Z}^n_{\geq 0}$. Anàlogament $x^{\gamma_{jk}-\beta(i)} \in$

$\mathbb{Z}^n_{\geq 0}$. Per tant,

$$\begin{aligned} x^{\delta-\gamma_{jk}} S(g_j, g_k) &= x^{\delta-\gamma_{jk}} \left(\frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_j)} g_j - \frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_k)} g_k \right) \\ &= \frac{x^{\delta}}{d_j\, x^{\beta(j)}} g_j - \frac{x^{\delta}}{d_k\, x^{\beta(k)}} g_k \\ &= \frac{x^{\alpha(j)}}{d_j} g_j - \frac{x^{\alpha(k)}}{d_k} g_k = p_j - p_k. \end{aligned}$$

Substituint a la suma anterior, i tenint en compte que el darrer sumand es cancel·la, resulta

$$\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i = \sum_{j,k} c_{jk}\, x^{\delta-\gamma_{j,k}}\, S(g_j, g_k).$$

Cal recordar, segons el comentari fet més amunt, que a la suma, únicament figuren els indexos j, k de la forma i_k, i_{k+1}, on $i_1 < \cdots < i_t$ és el conjunt de indexos pels que figuraven g_{i_k}, en la suma del primer membre del lema. En conseqüencia, no podem considerar únicament els $S(g_j, g_k)$ d'indexos correlatius.

Pel que fa a l'observació de l'enunciat del lema, només cal tenir en compte que multideg$(S(g_j, g_k)) \prec \gamma_{jk}$. □

Teorema 8.5 (Reconeixement d'una base de Gröbner). *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal. Llavors $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ és una base de Gröbner de $\mathcal{I}$ per un ordre monomial $\succ$ donat, ssi per cada parell $i \neq j$, el residu de dividir $S(g_i, g_j)$ per G, (amb la s-tupla en un ordre fixat) és zero.*

Demostració. $\Rightarrow$: Obviament, Si G és una base de Gröbner com que cada S-polinomi pertany a $\langle G\rangle$, la proposició 7.1 assegura que el residu és zero.

$\Leftarrow$: Hem de provar que si $f \in \mathcal{I}$, i tots els S-polinomis tenen residu zero, llavors $\mathrm{lm}(f) \in \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\rangle$. Abans de provar-ho, anem a donar l'estratègia de la prova.

Donat $f \in \langle g_1, \ldots, g_s\rangle$ existeixen polinomis $h_i \in K[\overline{x}]$ tals que

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

Posem

$$m(i) = \mathrm{multideg}(h_i\, g_i), \quad \text{i} \quad \delta = \max_i \{m(1), \ldots, m(s)\}.$$

Pel lema 3.11 es verifica multideg$(f) \preceq \delta$. Si no hi ha igualtat, és que es produeix alguna cancel·lació de monomis principals al segon membre. Entre les expressions de f en termes dels g_i n'hi poden haver moltes. Com que $\succ$ és un bon ordre, existeix alguna expressió que correspón a una δ mínima.

L'estratègia consistirà en provar que un cop triada una expressió amb δ mínima, si tots els residus dels S-polinomis són nuls, llavors multideg$(f) = \delta$, i per tant existeix algún i amb $m(i) = \delta = \text{multideg}(f)$. Això implica que $\text{lp}(g_i) \mid \text{lp}(f)$, i per tant que $f \in \langle \text{lm}(g_1), \dots, \text{lm}(g_s) \rangle$, tal com volem provar.

Queda per provar, que si tots els $\overline{S(g_i, g_j)}^G = 0$, llavors $\text{multideg}(f) = \delta$. Ho provarem per reducció a l'absurd. Suposarem que δ és mínima i que en canvi $\text{multideg}(f) \prec \delta$. Utilitzant la condició sobre els S-polinomis i el lema anterior 8.3 aconseguirem una nova expressió de f en termes dels g_i amb un $\delta' \prec \delta$, arribant a una contradicció. Veiem els detalls.

L'expressió de f amb δ mínima pot posar-se en la forma següent:

$$\begin{aligned} f &= \sum_{i=1}^{s} h_i\, g_i = \sum_{m(i)=\delta} h_i\, g_i + \sum_{m(i)\prec\delta} h_i\, g_i \\ &= \sum_{m(i)=\delta} \text{lm}(h_i)\, g_i + \sum_{m(i)=\delta} (h_i - \text{lm}(h_i)) g_i + \sum_{m(i)\prec\delta} h_i\, g_i \end{aligned}$$

Únicament els productes de potències de la primera suma de la segona linea tenen multigrau igual a δ.

Posem $\text{lm}(h_i) = c_i\, x^{\alpha(i)}$. Llavors la suma esmentada

$$S_\delta = \sum_{m(i)=\delta} \text{lm}(h_i)\, g_i = \sum_{m(i)=\delta} c_i\, x^{\alpha(i)}\, g_i$$

té exactament la forma i les condicions del primer membre de l'equació del lema 8.3, ja que hem suposat que $\text{multideg}(f) \prec \delta$. L'esmentat lema permet, llavors expressar aquesta suma així:

$$S_\delta = \sum_{j,k} c_{jk}\, x^{\delta - \gamma_{jk}}\, S(g_i, g_j),$$

on $c_{jk} \in K$, i $x^{\gamma_{jk}}$ donat per la fórmula (8.1).

Ara utilitzem la hipòtesi $\overline{S(g_i, g_j)}^G = 0$, per $1 \le i < j \le s$. Per l'algorisme de la divisió, aquesta hipòtesi implica que existeix una expressió de cada S-polinomi de la forma

$$S(g_i, g_j) = \sum_{i=1}^{t} a_{ijk}\, g_i$$

on $a_{ijk} \in K[\overline{x}]$ i

$$\text{multideg}(a_{ijk}\, g_i) \preceq \text{multideg}(S(g_j, g_k)) \prec \gamma_{jk}$$

per cada i, j, k. Aquest resultat el podem interpretar dient que la hipòtesi sobre els S-polinomis ens permet expressar cada S-polinomi en termes dels g_i's sense que hi hagi cancel·lació.

El resultat obtingut ens permet reescriure ara la suma S_δ així:

$$S_\delta = \sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}} \left(\sum_i a_{ijk}\, g_i \right) = \sum_i \left(\sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}}\, a_{ijk} \right) g_i$$

on, per cada i, $1 \leq i \leq s$ és

$$\operatorname{multideg}\left((\sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}}\, a_{ijk})\, g_i \right) \prec \delta$$

Substituint ara aquesta expressió de S_δ en l'expressió completa de f, arribem a una expressió de la forma $f = \sum_i \tilde{h}_i\, g_i$ que correspondria a una δ inferior a la mínima precedent. Tenim, doncs, la contradicció esperada, i per tant, si l'expressió de f en termes dels g_i correspón a δ mínim, llavors

$$\operatorname{multideg}(f) = \delta$$

el que implica que $\operatorname{lm}(f) \in \langle \operatorname{lm}(g_1), \ldots, \operatorname{lm}(g_s) \rangle$, tal com voliem demostrar. $\square$

9. Algorisme de Buchberger

Teorema 9.1. *Sigui $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un ideal de $K[\overline{x}]$. Llavors, l'algorisme següent construeix una base de Gröbner en un nombre finit de passos:*

Input: $F = [f_1, \ldots, f_s]$. Un ordre monomial $\succ$.
Output: $G = [g_1, \ldots, g_m]$, base de Gröbner de $\mathcal{I}$, amb $F \subset G$.

$G := F$
REPETIR
  $G' := G$
  PER cada parell $\{p, q\} \in G'$, $p \neq q$ FER
    $S := \overline{S(p,q)}^{G'}$
    SI $S \neq 0$ LLAVORS $G := G \cup \{S\}$
FINSQUE $G = G'$.

Demostració. En primer lloc, $G \subset \mathcal{I}$, ja que ho és incialment, i durant l'algorisme, únicament s'afegeixen a G polinomis de $\mathcal{I}$. Per construcció, també $F \subset G$.

En segon lloc, l'algorisme acaba quan $G = G'$, es a dir quan tots els $\overline{S(p,q)}^{G} = 0$ per cada $(p, q) \in G$. Pel teorema 8.5, això implica que G és una base de Gröbner de $\langle G \rangle = \mathcal{I}$.

Només cal provar que l'algorisme acaba. Però observem que passa al final de cada pas del bucle principal. Tindrem

$$\big\langle \operatorname{lm}(G') \big\rangle \subset \langle \operatorname{lm}(G) \rangle$$

ja que $G' \subset G$. Però si $G \neq G'$ demostrarem que $\langle \operatorname{lm}(G') \rangle$ és estrictament menor que $\langle \operatorname{lm}(G) \rangle$. En efecte, si $G \neq G'$, és que, abans d'acabar el bucle, s'ha afegit algun residu r no nul d'un S-polinomi dividit per G'. Per tant, cap monomi de r és divisible per cap monomi principal de G'. Per tant,

$\mathrm{lm}(r) \notin \langle \mathrm{lm}(G') \rangle$. En canvi $\mathrm{lm}(r) \notin \langle \mathrm{lm}(G) \rangle$, i per tant la inclusió és estricta.

Si considerem la succesió de $\langle \mathrm{lm}(G) \rangle$'s de cada pas del bucle, és una cadena d'ideals estrictament ascencent. Per ser $K[\overline{x}]$ un anell Noetherià, la cadena estabilitza. Arribarà un moment en que $\langle \mathrm{lm}(G') \rangle = \langle \mathrm{lm}(G) \rangle$. Com que la succesió és estrictament creixent, això s'ha de produir en un nombre finit de passos de l'algorisme. Per tant, l'algorisme acaba. $\square$

Cal observar que la versió donada de l'algorisme de Buchberger és molt ineficient, ja que verifica moltes més coses de les necessàries. Més endavant donarem una versió més pràctica.

10. Millores de l'algorisme de Buchberger

L'algorisme de Buchberger té una complexitat intrínseca elevada. Quan volem implementar un algorisme matemàtic, a més de posar atenció en la seva correcció, hem de posar émfasi en altres qüestions i en particular en la seva eficiència. Hem d'intentar minimitzar els càlculs que fem. La versió donada en la secció anterior és exclussivament teòrica, ja que verifica a cada pas tots els residus dels S-polinomis. Anem a veure algunes millores que el fan més pràctic.

Definició 10.1. Donats un conjunt $G = \{g_1, \ldots, g_s\} \subset K[\overline{x}]$ i un ordre monomial $\succ$, direm que $f \in K[\overline{x}]$ **redueix a zero mòdul** G i posarem $f \to_G 0$, si

(i) existeix una expressió de la forma

$$f = q_1\, g_1 + \cdots + q_s\, g_s$$

(ii) tal que si $q_i\, g_i \neq 0$, llavors

$$\mathrm{multideg}(f) \succeq \mathrm{multideg}(q_i\, g_i)$$

Obviament, si $\overline{f}^G = 0$ llavors $f \to_G 0$. En canvi el recíproc no és cert en general.

Exemple 10.2. Si posem $f = 2\,x^2\,y^2 - x\,y$, $g_1 = x^2 + y^2$, $g_2 = 2\,x\,y - 1$, el resultat de dividir f entre $[g_1, g_2]$ és

$$f = (2\,y^2)\,g_1 + (-\frac{1}{2})\,g_2 + (-2\,y^4 - \frac{1}{2})$$

i per tant $\overline{f}^G = -2\,y^4 - \frac{1}{2} \neq 0$. En canvi si dividim f entre $[g_2, g_1]$ el resultat és

$$f = (x\,y)\,g_1 + 0\,g_2$$

i per tant $f \to_G 0$.

L'interés d'aquesta definició radica en el fet que permet rebaixar la hipòtesi del teorema 8.5 substituint divisió per reducció, ja que de fet, és la única cosa que hem utilitzat en la demostració. Tenim doncs

Teorema 10.3. *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal. Llavors $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ és una base de Gröbner de $\mathcal{I}$ per un ordre monomial $\succ$ donat, ssi per cada parell $i \neq j$, $S(g_i, g_j) \to_G 0$.*

La següent proposició ens evitarà calcular alguns residus de S-polinomis.

Proposició 10.4. *Donat un conjunt $G \subset K[\overline{x}]$ i un ordre monomial, siguin $f, g \in G$. Si $\mathrm{lp}(f)$ i $\mathrm{lp}(g)$ no tenen variables en comú (és a dir, si $\mathrm{lcm}(\mathrm{lp}(f), \mathrm{lp}(g)) = \mathrm{lp}(f) \cdot \mathrm{lp}(g)$), llavors $S(f, g) \to_G 0$.*

Demostració. Siguin

$$f = a\, x^\alpha + f_r, \quad g = b\, x^\beta + g_r$$

on $\mathrm{multideg}(f_r) \prec \mathrm{multideg}(f)$ i $\mathrm{multideg}(g_r) \prec \mathrm{multideg}(g)$. Si es cumpleix la hipòtesi tenim

$$\begin{aligned} S(f,g) &= \frac{b\, x^\beta}{a\, b} f - \frac{a\, x^\alpha}{a\, b} g \\ &= \frac{1}{a\, b}\left((g - g_r)f - (f - f_r)g\right) = \frac{1}{a\, b}\left(f_r\, g - g_r\, f\right) \end{aligned}$$

i a més a més

$$\mathrm{multideg}(S(f,g)) = \max\left(\mathrm{multideg}(f_r\, g), \mathrm{multideg}(g_r\, f)\right),$$

ja que si hagués cancel.lació de monomis principals això implicaria la igualtat $x^\beta\ \mathrm{lp}(f_r) = x^\alpha\ \mathrm{lp}(g_r)$. Però tenint en compte que x^α i x^β són primers entre si, caldria que $x^\beta \mid \mathrm{lp}(g_r)$, el que és impossible. $\square$

Exemple 10.5. Amb aquesta proposició és immediat comprovar que

$$G = \left\{x^3 - y\, z^2 + 3, y\, z^2 - z^5, u^3 + 2\, u^2 + u\right\}$$

és una base de Gröbner respecte a l'ordre lex $x \succ y \succ z \succ u$.

En efecte, com que els monomis principals són primers entre si dos a dos, els tres S-polinomis redueixen a zero, i el teorema 10.3 assegura que G és una base de Gröbner.

Exemple 10.6. Anàlogament, aquesta proposició assegura immediatement que la base produïda per eliminació gaussiana en un sistema lineal, és una base de Gröbner minimal, ja que els monomis principals tenen variables disjuntes.

La següent definició generalitza el concepte de S-polinomi.

Definició 10.7 (Syzygies). Sigui $F = [f_1, \ldots, f_s] \in (K[\overline{x}])^s$. Una syzygia sobre els monomis principals dels polinomis de F és una s-tupla de polinomis $S = [h_1, \ldots, h_s] \in (K[\overline{x}])^s$ tal que

$$\sum_{i=1}^{s} h_i\ \mathrm{lm}(f_i) = 0.$$

Anomenarem $S(F)$ al subconjunt d'elements de $(K[\overline{x}])^s$ format per totes les syzygies sobre els monomis principals de F.

Podem considerar una syzygia com un vector de $(K[\overline{x}])^s$. Si denotem $\mathbf{e}_i = [0, \dots, 0, 1, 0, \dots, 0]$ els elements de la base canònica de K^s, llavors la syzygia de la definció pot expressar-se en la forma $S = \sum_{i=1}^{s} h_i \, \mathbf{e}_i$.

En particular, els S-polinomis són syzygies relatives a dos polinomis (d'aquí el seu nom de Syzygia-polinomi):

$$S_{ij} = \frac{x^{\gamma_{ij}}}{\operatorname{lm}(f_i)} \mathbf{e}_i - \frac{x^{\gamma_{ij}}}{\operatorname{lm}(f_j)} \mathbf{e}_j$$

La relació amb l'S-polinomi és:

$$S(g_i, g_j) = S_{ij} \cdot G$$

És immediat veure que $S(F)$ és tancat per suma (de vectors) i per multiplicació per polinomis (escalars). Per tant formen l'anàleg d'un espai vectorial, però sobre l'anell $K[\overline{x}]$. Aquesta estructura s'anomena mòdul. Les syzygies formen, doncs un $K[\overline{x}]$-mòdul.

Una particularitat essencial de $S(F)$ és que admet una base finita. Abans de demostrar-ho ens cal aprofundir un xic més sobre les syzygies.

En primer lloc, definim el concepte de syzygia homogènia.

Definició 10.8. Un element de $S(F)$ és **homogènia de multigrau** $\delta \in \mathbb{Z}^n_{\geq 0}$, si és de la forma

$$S = [c_1 \, x^{\alpha_1}, \dots, c_s \, x^{\alpha_s}],$$

on $c_i \in K$ i $\alpha_i + \operatorname{multideg}(f_i) = \delta$ si $c_i \neq 0$.

En particular, la syzygia S_{ij}, associada al S-polinomi $S(g_i, g_j)$, és una syzygia homogènia de multigrau γ_{ij}.

Lema 10.9. *Tot element de $S(F)$ pot expressar-se de forma única com a suma de syzygies homènies de $S(F)$.*

Demostració. Sigui $S = [h_1, \dots, h_s] \in S(F)$. Fixat un exponent δ, sigui $h_{i\delta}$ el monomi de h_i, si existeix, tal que $h_{i\delta} \operatorname{lm}(f_i)$ té multigrau δ. S'ha de cumplir que $\sum_{i=1}^{s} h_{i\delta} \operatorname{lm}(f_i) = 0$. Per tant, $S_\delta = [h_{1\delta}, \dots, h_{s\delta}]$ és una syzygia homogènia de $S(F)$. Obviament, $S = \sum_\delta S_\delta$.

Com el component $h_{i\delta}$ és un monomi $c_i x^{\alpha(i)}$ de h_i, i és l'unic component de h_i de multigrau igual a $\delta - \operatorname{multideg}(f_i)$, està unívocament determinat. $\square$

Proposició 10.10. *Donat $F = [f_1, \dots, f_s]$.*

(i) *Cada element $S \in S(F)$ pot posar-se en la forma*

$$S = \sum_{ij} u_{ij} \, S_{ij}$$

on $u_{ij} \in K[\overline{x}]$ i S_{ij} són les syzygies corresponents als S-polinomis.

(ii) *En la descomposició anterior es manté el multigrau δ d'homogeneitat.*

Demostració. Pel lema anterior, podem suposar que S és homogènia de multigrau δ. Siguin i, j dues components no nules de S amb $i < j$ (necessàriament n'ha de tenir al menys dues). Siguin aquestes $c_i\, x^{\alpha_i}$ i $c_j\, x^{\alpha_j}$. Llavors $\alpha_i + \text{multideg}(f_i) = \alpha_j + \text{multideg}(f_j) = \delta$. Per tant $x^{\alpha_i} \mid x^{\delta}$ i $x^{\alpha_j} \mid x^{\delta}$. En conseqüència $x^{\gamma_{ij}} \mid x^{\delta}$, on $x^{\gamma_{ij}} = \text{lcm}(x^{\alpha_i}, x^{\alpha_j})$. Llavors

$$S' = S - c_i \ \text{lc}(f_i) x^{\delta - \gamma_{ij}} S_{ij}$$

té la seva component i-èsima nula. Apart de la component i, l'única altra component de S' diferent de S és la j que haurà variat en el seu coeficient de K. Hem obtingut una nova syzygia S' de multigrau δ, amb una component menys que S i sense alterar el multigrau δ d'homogeneitat. Continuant el procediment amb la component j i la següent component no nul.la de S' acabarem expressant S com a combinació de les S_{ij}. $\square$

Aquesta proposició precisa la idea de que tota cancel·lació de monomis principals pot expresar-se en termes de S-polinomis.

Hem demostrat que les S_{ij} per $i < j$ formen una base de totes les syzygies de $S(F)$. Però observem que no sempre són independents.

Exemple 10.11. Sigui $F = [x^2\, y^2 + z^2, x\, y^2 + y^2, x^2\, y + y\, z]$ i considerem l'ordre lex amb $x \succ y \succ z$. Les tres syzygies corresponents als tres S-polinomis són:

$$S_{12} = [1, -x, 0], \quad S_{23} = [1, 0, -y], \quad S_{23} = [0, x, -y].$$

Observem que $S_{23} = S_{13} - S_{12}$. Per tant, S_{23} és combinació de les altres dues i pot elimnar-se de la base.

Exemple 10.12. Sigui $G = [x^2yz - y^2, xy^2z - x + y^3, xyz^2 - xz - y, x^2y^2 + z^2]$. Considerem ordre lex amb $x \succ y \succ z$.

a) Determinem totes les syzygies corresponents a S-polinomis.
b) Expressem la syzygia $S = [2xyz, -x^2z, 3x^2y, -4xz^2]$ en termes de les anteriors.
c) Trobem una base mínima de syzygies.

a) Les syzygies corresponents als S-polinomis són:

$$\begin{array}{rcl} S_{12} & = & [\ y, \ -x, \ 0, \ 0\ ] \\ S_{13} & = & [\ z, \ 0, \ -x, \ 0\ ] \\ S_{14} & = & [\ y, \ 0, \ 0, \ -z\ ] \\ S_{23} & = & [\ 0, \ z, \ -y, \ 0\ ] \\ S_{24} & = & [\ 0, \ x, \ 0, \ -z\ ] \\ S_{34} & = & [\ 0, \ 0, \ xy, \ -z^2\ ] \end{array}$$

b) Per determinar S en termes de les syzygies corresponents als S-polinomis, fem

$$\begin{array}{rcccl} S_1 & = & S - 2xzS_{12} & = & [\ 0, \ x^2z, \ 3x^2y, \ -4xz^2\ ] \\ S_2 & = & S_1 - x^2S_{23} & = & [\ 0, \ 0, \ 4x^2y, \ -4xz^2\ ] \\ S_3 & = & S_2 - 4xS_{34} & = & [\ 0, \ 0, \ 0, \ 0\ ] \end{array}$$

Finalment, doncs,

$$S = 2xzS_{12} + x^2 S_{23} + 4xS_{34}$$

c) Observem ara que aquest mateix procés el podem fer per expressar algunes de les syzygies corresponents a S-polinomis en termes de les altres. Així:

$$\begin{array}{rcrcccccl} S_{14} - S_{24} & = & & [& y, & -x, & 0, & 0 &] = S_{12} \\ S_{34} - zS_{24} & = & & [& 0, & -zx, & xy, & 0 &] \\ & = & x & [& 0, & -z, & y, & 0 &] = -xS_{23} \end{array}$$

Teorema 10.13. *Un conjunt $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ és una base de Gröbner de l'ideal $\mathcal{I} \subset K[\overline{x}]$ per un ordre monomial donat, si per cada element $S = [h_1, \ldots, h_s]$ d'una base homogènia de syzygies de $S(G)$ es verifica*

$$S \cdot G = \sum_{i=1}^{s} h_i\, g_i \to_G 0.$$

Demostració. Pel teorema 8.5, G és una base de Gröbner si totes les syzygies redueixen a zero. Tenint en compte que en la descomposició d'una syzygia en una base de syzygies el multigrau d'homogeneitat es manté, és obvi que si les syzygies d'una base redueixen a zero, les restants syzygies també redueixen a zero mòdul G. □

Ara hem de saber com fer més petita una base de syzygies. Hi ha manera d'obtenir bases minimals, però una forma general de reduir-les es basa en la següent proposició

Proposició 10.14. *Donat $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$, suposem que un subconjunt $S \subset \{S_{ij} \; : \; 1 \leq i < j \leq s\}$ és una base de les syzygies $S(G)$. Suposem además que existeixen elements diferents $g_i, g_j, g_k \in G$ tals que*

$$\mathrm{lp}(g_k) \mid \mathrm{lcm}(\mathrm{lp}(g_i), \mathrm{lp}(g_j)).$$

Si $S_{ik}, S_{jk} \in S$, llavors $S - \{S_{ij}\}$ també és una base de $S(G)$.

Demostració. Suposem, per simplificar que $i < j < k$ i siguin $x^{\gamma_{ij}}, x^{\gamma_{ik}}, x^{\gamma_{jk}}$ els habituals lcm's. La hipòtesi implica que $x^{\gamma_{ik}} \mid x^{\gamma_{ij}}$ i $x^{\gamma_{jk}} \mid x^{\gamma_{ij}}$. Per tant resulta

$$\begin{aligned} S_{ij} &= \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}}\left(\frac{x^{\gamma_{ik}}}{\mathrm{lm}(g_i)}\mathbf{e}_i - \frac{x^{\gamma_{ik}}}{\mathrm{lm}(g_k)}\mathbf{e}_k\right) + \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}}\left(\frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_k)}\mathbf{e}_k - \frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_j)}\mathbf{e}_j\right) \\ &= \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}}S_{ik} - \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}}S_{jk} \end{aligned}$$

quedant demostrada la proposició. □

Ara incorporarem les proposicions 10.4 i 10.14 en un algorisme de Buchberger més eficient que l'emprat per la demostració. Farem servir els parells ordenats $[i, j]$ amb $i < j$ per identificar les syzygies a que ens referim.

Donem a continuació l'algorisme de Buchberger millorat. Sigui $\mathcal{I} = \langle F \rangle$.

Algorisme de Buchberger

Input: $F = [f_1, \ldots, f_s]$. Un ordre monomial $\succ$.
Output: $G = [g_1, \ldots, g_m]$, base de Gröbner de $\mathcal{I}$, amb $F \subset G$.

$B := \{[i,j] \ : \ 1 \leq i < j \leq s\}$
$G := F$
$m := s$
MENTRE $B \neq \phi$ FER
    Seleccionar un element $[i,j] \in B$
    $B := B - \{[i,j]\}$
    SI variables(lp(f_i)) $\cap$ variables(lp(f_i)) $\neq \phi$ I
        Criteri(f_i, f_j, B) és fals LLAVORS
        $S := \overline{S(f_i, f_j)}^G$
        SI $S \neq 0$ LLAVORS
            $m := m + 1$
            $f_m := S$
            $G := G \cup \{f_m\}$
            $B := B \cup \{[n,m] \ : \ 1 \leq n < m\}$

La funció Criteri(f_i, f_j, B) retorna cert si existeix algún $k \notin \{i,j\}$ pel qual $[i,k]$ i $[j,k]$ no estan a B i tal que $\mathrm{lp}(f_k) \mid \mathrm{lcm}(\mathrm{lp}(f_i), \mathrm{lp}(f_j))$.

Nota: cal anar amb compte amb els parells ordenats $[i,k]$, ja que si $k < i$ cal canviar-lo per $[k,i]$.

La funció Criteri està basada en la proposició 10.14, i el primer criteri per evitar calcular residus de S-polinomis en la proposició 10.4.

L'algorisme donat pot amillorar-se. Per una discusió més detallada consultar [3] i [4].

Normalment, després de calcular una base de Gröbner, s'acaba determinant primer una base minimal i finalment una base reduida. Els programes de càlcul simbòlic determinen, en general, la base reduida.

Acabem comentant una mica la complexitat de l'algorisme. A pesar de les millores actuals de l'algorisme, resulta fàcil donar exemples de bases per les quals l'algorisme queda colapsat en temps i memòria.

Entre d'altres problemes el grau dels polinomis intermitjos que es produeixen durant l'evolució de l'algorisme pot creixer molt. També solen crèixer molt el tamany dels coeficients.

En general, l'ordre monomial que sol donar menor grau dels polinomis intermitjos és grevlex, mentre que lex sol donar una major complexitat [1],[2].

Actualment hi han noves millores de l'algorisme i hi ha molt treball de recerca sobre el tema.

11. Generalització per polinomis sobre un anell Noetherià

Aquesta secció és la generalització de les seccions 5 i 6 per polinomis a coeficients en un anell, i pot deixar-se de banda en una primera lectura. En moltes aplicacions interessa considerar polinomis a $\mathcal{R}[\overline{x}]$, on $\mathcal{R}$ és un anell Noetherià. Els resultats obtinguts en les dues seccions esmentades poden generalitzar-se sense gaires dificultats, si be cal anar amb compte, ja que ara no podem utilitzar la divisió. En tota la secció, $\mathcal{R}$ serà un anell Noetherià, i no exigirem res més. En particular no exigim que sigui un UFD.

Un monomi a $\mathcal{R}[\overline{x}]$ serà una expressió de la forma $a\,x^\alpha$, on $a \in \mathcal{R}$. Continuem utilitzem les notacions $a = \mathrm{lc}$, $x^\alpha = \mathrm{lp}$, i $a\,x^\alpha = \mathrm{lm}$, com en el cas anterior.

Definició 11.1 (Ideal de monomis)**.** Direm que $\mathcal{I} \subset \mathcal{R}[\overline{x}]$ és un ideal de monomis si existeix un conjunt $A \subset \mathbb{Z}^n_{\geq 0}$ (finit o infinit) i una funció $a : A \to \mathcal{R}$ tal que

$$\begin{aligned} \mathcal{I} &= \langle a(\alpha)\,x^\alpha \ : \ \alpha \in A\rangle \\ &= \left\{ \sum_{\alpha\in A} h_\alpha\, a(\alpha)\,x^\alpha \ : \ h_\alpha \in \mathcal{R}[\overline{x}] \right\} \end{aligned}$$

Exemple 11.2. $\mathcal{I} = \left\langle a\,x^3\,y^2, b\,x^3\,y^2, c\,x\,y, d\,x^2\,y^3.\right\rangle \subset \mathcal{R}[x,y]$.

Lema 11.3. *Sigui $\mathcal{I} = \langle a(\alpha)\,x^\alpha \ : \ \alpha \in A\rangle$ un ideal de monomis de $\mathcal{R}[\overline{x}]$.*

(i) *El conjunt d'elements de $\mathcal{R}$ donat per*

$$\mathcal{I}_\beta = \left\{ b \in \mathcal{R} \ : \ b\,x^\beta \in \mathcal{I} \right\}$$

és un ideal de $\mathcal{R}$.

(ii) *Si $x^\alpha \mid x^\beta$, llavors $\mathcal{I}_\alpha \subseteq \mathcal{I}_\beta$.*

(iii) *Un monomi $b\,x^\beta \in \mathcal{I}$ ssi existeix $\alpha \in A$ tal que $x^\alpha \mid x^\beta$ i $b \in \mathcal{I}_\beta$.*

Demostració. (i) Exercici.

(ii) Si $a \in \mathcal{I}_\alpha$, llavors $a\,x^\alpha \in \mathcal{I}$. Si $x^\alpha \mid x^\beta$, existeix $\gamma \in \mathbb{Z}_{\geq 0}$ tal que $x^\beta = x^\gamma\,x^\alpha$. En conseqüència $a\,x^\beta \in \mathcal{I}$ i $a \in \mathcal{I}_\beta$.

(iii) $\Rightarrow$: Obvi per la definició de $\mathcal{I}_\beta$. Si x^β és múltiple d'algún x^α per algún $\alpha \in A$, llavors $\mathcal{I}_\beta \neq \phi$.

$\Leftarrow$: Si $b\,x^\beta \in \mathcal{I}$, llavors $b\,x^\beta = \sum_{k=1}^s h_{\alpha(k)}\,a(\alpha(k))\,x^{\alpha(k)}$, per certs $h_{\alpha(k)} \in \mathcal{R}[\overline{x}]$ i $\alpha(k) \in A$. Expandint el producte tindrem

$$b\,x^\beta = \sum_{k=1}^{s}\sum_{j=1}^{t_k} c_{kj}\,a(\alpha(k))\,x^{\gamma(k,j)+\alpha(k)}$$

on $c_{kj} \in \mathcal{R}$. Un cop expandit el producte, únicament no es cancel.len els monomis corresponents a productes de potències d' exponent β. Per cada un dels monomis restants és $\gamma(k,j) + \alpha(k) = \beta$. Per tant x^β és divisible per cada un dels $x^{\alpha(k)}$ que no s'hagin cancel.lat. Ademés s'ha de cumplir $\sum_{kj} c_{kj} a(\alpha(k)) = b$. Per (ii), pels $\alpha(k)$ que han quedat, $a(\alpha(k)) \in \mathcal{I}_\beta$ i per tant $b \in \mathcal{I}_\beta$. □

Així, els monomis de l'ideal de l'exemple 11.2 seran:

$$\langle a,b,c\rangle\ x^3\,y^2,\ \langle c\rangle\ x\,y,\ \langle c,d\rangle\ x^2\,y^3$$

Lema 11.4. *Sigui $\mathcal{I}$ un ideal de monomis i $f\in\mathcal{R}[\overline{x}]$. Són equivalents les afirmacions següents:*

(i) *$f\in\mathcal{I}$.*
(ii) *Cada terme de f pertany a $\mathcal{I}$.*
(iii) *f és una $\mathcal{R}$-combinació lineal de monomis de $\mathcal{I}$.*

Demostració. Obviament (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). Només cal provar que (i) implica (iii). La demostració és anàloga a la del lema anterior. Sigui $f\in\mathcal{I}$. Llavors, existeixen certs $h_k\in\mathcal{R}[\overline{x}]$ i $\alpha(k)\in A$, tals que

$$f=\sum_{k=1}^{s}h_k\,a(\alpha(k))\,x^{\alpha(k)}=\sum_{k=1}^{s}\sum_{j=1}^{t_k}c_{kj}\,a(\alpha(k))\,x^{\gamma(k,j)+\alpha(k)}$$

on $c_{kj}\in\mathcal{R}$. Per tant, cada subterme de f és múltiple d'algún $a(\alpha(k))\,x^{\alpha(k)}$ i per tant pertany a $\mathcal{I}$. La suma dels termes que són de la forma $d_j\,x^{\delta(j)}$ serà tal que $d_j\in\mathcal{I}_{\delta(j)}$, i $x^{\delta(j)}$ és divisible per algún $x^{\alpha(k)}$. Per tant, cada monomi $d_j\,x^{\delta(j)}\in\mathcal{I}$. $\square$

Corol·lari 11.5. *Dos ideals de monomis són iguals ssi tenen els mateixos monomis.*

Teorema 11.6 (Lema de Dickson)**.** *Si $\mathcal{I}\subset\mathcal{R}[\overline{x}]$ és un ideal de monomis $\mathcal{I}=\langle a(\alpha)\,x^\alpha\ :\ \alpha\in A\rangle$, llavors podem extreure un subconjunt finit de monomis $\{a(\alpha(1))\,x^{\alpha(1)},\ldots,a(\alpha(s))\,x^{\alpha(s)}\}$ tal que*

$$\mathcal{I}=\left\langle a(\alpha(1))\,x^{\alpha(1)},\ldots,a(\alpha(s))\,x^{\alpha(s)}\right\rangle.$$

Demostració. La demostració és idèntica al cas de $K[\overline{x}]$, ja que el teorema de la base d'Hilbert i següent els hem demostrat a $\mathcal{R}[\overline{x}]$. $\square$

Passem ara a estudiar la generalització del teorema de les bases de Gröbner. La definició de l'ideal $\langle\mathrm{lm}(\mathcal{I})\rangle$ és similar al cas de $K[\overline{x}]$. Cal recordar però que inclou els coeficients que ara són elements de $\mathcal{R}$, i no poden ser menystinguts.

Proposició 11.7. *Sigui $\mathcal{R}$ un anell Noetherià i $\succ$ un ordre monomial. Si $\mathcal{I}\subset\mathcal{R}[\overline{x}]$ és un ideal, llavors $\langle\mathrm{lm}(\mathcal{I})\rangle$ és un ideal de monomis de $\mathcal{R}[\overline{x}]$.*

Demostració. Exercici. $\square$

Proposició 11.8 (Reducció)**.** *Sigui $b\,x^\beta$ un monomi de l'ideal de monomis*

$$\mathcal{I}=\langle a_1\,x^{\alpha_1},\ldots,a_s\,x^{\alpha_s}\rangle$$

Llavors

(i) *Existeix un subconjunt no buit S d'indexos, tal que $j\in S$, implica que $x^{\alpha_j}\mid x^\beta$.*

(ii) *Sigui* $S = \{i_1, \ldots, i_k\}$ *el conjunt màxim que verifica* (i). *Llavors,*

$$b \in \langle a_{i_1}, \ldots, a_{i_k} \rangle$$

(iii) *Existeixen monomis* $c_i\, x^{\gamma_i}$ *tals que*

$$b\, x^{\beta} = \sum_{i \in S} (c_i\, x^{\gamma_i})\, a_i\, x^{\alpha_i}$$

i $\beta = \gamma_i + \alpha_i$

Demostració. (i) El conjunt S és no buit pel punt (iii) del lema 11.3.

(ii) Posem $\mathcal{J} = \langle a_{i_1}, \ldots, a_{i_k} \rangle$. El lema esmentat en (i) implica a més a més que $b \in \mathcal{I}_\beta$. No més cal provar que $\mathcal{I}_\beta = \mathcal{J}$. Pel punt (ii) del lema 11.3, és obvi que $\mathcal{J} \subseteq \mathcal{I}_\beta$. Ara demostrarem la inclusió contraria $\mathcal{I}_\beta \subseteq \mathcal{J}$. Sigui $b \in \mathcal{I}_\beta$. Llavors $b\, x^{\beta} \in \mathcal{I}$, i per tant

$$b\, x^{\beta} = \sum_{i=1}^{s} h_i\, a_i\, x^{\alpha_i} = \sum_{i=1}^{s} \sum_{j=1}^{k_i} c_{ij}\, a_i\, x^{\gamma_{ij} + \alpha_i} \tag{11.1}$$

S'han de cancel·lar tots els termes de l'expressió anterior excepte aquells que tenen exponent total β. Per tant, únicament poden no cancel·lar-se en la suma aquells termes que corresponguin a indexos tals que $\beta = \gamma_{ij} + \alpha_i$, és a dir, que pertanyin a S. Per tant la suma no més s'extén als subindexos de S. Identificant coeficients tenim

$$b = \sum_{i \in S} \sum_{j=1}^{k_i} c_{ij}\, a_i$$

que prova que $b \in \mathcal{J}$.

(iii) A l'expressió (11.1) hem vist que $\gamma_{ij} = \beta - \alpha_i$, i per tant no depén de j. Podem efectuar la suma referida a j i obtenir $c_i = \sum_{j=1}^{k_i} c_{ij}$, quedant provat (iii). □

Aquest lema juga pels polinomis a $\mathcal{R}[\overline{x}]$, un paper de substitut de la divisió, que ara no existeix com existia a $K[\overline{x}]$. Ens permetrà reduir termes principals.

Teorema 11.9 (Base de Gröbner). *Sigui* $\mathcal{I} \subset \mathcal{R}[\overline{x}]$ *un ideal diferent de* $\{0\}$. *Llavors*

(i) *Donat un ordre monomial* $\succ$, *existeix un conjunt finit* $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$, *tal que*

$$\langle \mathrm{lm}(\mathcal{I}) \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle \tag{11.2}$$

(ii) *Tot subconjunt* G *de* $\mathcal{I}$ *que verifiqui (11.2) és una base de* $\mathcal{I}$. *És a dir,*

$$\mathcal{I} = \langle g_1, \ldots, g_s \rangle\,.$$

Direm que és una **base de Gröbner** *de* $\mathcal{I}$.

Demostració. (i) Sigui $\succ$ un ordre monomial. Per la proposició 11.7, $\langle \mathrm{lm}(I) \rangle$ és un ideal de monomis. Pel lema de Dickson, existeix un subconjunt finit d'elements que el genera. Però els elements de $\langle \mathrm{lm}(I) \rangle$ són de la forma $\mathrm{lm}(f)$, on $f \in \mathcal{I}$. Per tant, existeix $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ tal que $\langle \mathrm{lm}(\mathcal{I}) \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle$.

(ii) Demostrem que el conjunt G de (i) verifica també $\mathcal{I} = \langle g_1, \ldots, g_s \rangle$. És evident que $\langle g_1, \ldots, g_s \rangle \subseteq \mathcal{I}$, ja que cada $g_i \in \mathcal{I}$.

Recíprocament, si $f \in \mathcal{I}$ tenim que

$$f = \mathrm{lm}(f) + f'$$

on $\mathrm{lm}(f') \prec \mathrm{lm}(f)$. Però $\mathrm{lm}(f) \in \mathrm{lm}(\mathcal{I})$, i per tant

$$\mathrm{lm}(f) \in \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle \, .$$

Pel punt (iii) del lema 11.8, existeixen monomis q_i, alguns possiblemet nuls, tals que

$$\mathrm{lm}(f) = q_1 \; \mathrm{lm}(g_1) + \cdots + q_s \; \mathrm{lm}(g_s).$$

i tals que $\mathrm{multideg}(\mathrm{lm}(f)) = \mathrm{multideg}(\mathrm{lm}(q_k \, g_k))$, per tots els que no són nuls. Per tant, al no haver cancel·lació del terme principal de cada sumand no idènticament nul, resulta

$$\mathrm{lm}(f) = \mathrm{lm}(q_1 \, g_1 + \cdots + q_s \, g_s).$$

Posant $f_0 = q_1 \, g_1 + \cdots + q_s \, g_s$, hem descomposat en suma $f = f_0 + f_1$, de tal manera que $f_0 \in \langle g_1, \ldots, g_s \rangle$, $\mathrm{lm}(f) = \mathrm{lm}(f_0)$, $f_1 \in \mathcal{I}$ i $\mathrm{multideg}(f_1) \prec \mathrm{multideg}(f)$. Continuant la reducció per f_1 i tenint en compte que l'ordre monomial és un bon ordre, acabarem expressant f com a combinació lineal dels g_i's i residu zero. □

Referències

[1] (1987) D. Bayer & M. Stillman, "A criterion for detecting m-regularity", Invent. Math. **87**, 1-11.

[2] (1987) D. Bayer & M. Stillman, "A theorem on refining division orders by the reverse lexicographic order", Duke J. Math. **55**, 321-328.

[3] (1985) B. Buchberger, "Gröbner bases: an algorithmic method in polynomial ideal theory" a "Multidimensional Systems Theory", ed. N.K. Bose, D. Reidel, Publishing Company, Dordrecht, 184-232.

[4] (1988) R. Gebauer & H.M. Möller, "On an installation of Buchberger's algorithm" a "Computational Aspects of Commutative Algebra", ed. L.Robbiano, Academic Press, New-York, 15-33.