Calcolo di una base di Gröbner

Algoritmo di Buchberger
Input: $g_1, \ldots, g_s \in P^r$, t.o. σ;
Output: $\mathcal{G}$, σ-base di Gröbner di $M = \langle g_1, \ldots, g_s \rangle \subseteq P^r$.

Sia $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$
$s' = s$; $\mathcal{G} = (g_1, \ldots, g_s)$
$B = \{(i,j) \mid 1 \le i < j \le s, \gamma_i = \gamma_j\}$;
while $B \neq \emptyset$ do
  scegli $(i,j) \in B$;
  $B = B \setminus \{(i,j)\}$;
  $S_{ij} = \phi(\sigma_{ij}) = \frac{1}{c_i} t_{ij} g_i - \frac{1}{c_j} t_{ji} g_j$;
  Calcola $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$, il ridotto di S_{ij} rispetto a $\mathcal{G}$;
  if $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) \neq 0$ then
    $s' = s' + 1$;
    $g_{s'} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$;
    $\mathcal{G} = \mathcal{G}, g_{s'}$;
    $B = B \cup \{(i, s') \mid 1 \le i < s',\ \gamma_i = \gamma_{s'}\}$;
  end if;
end while;
return $\mathcal{G}$.

Esempio

Sia $P = \mathbb{Q}[x,y]$ e sia $\mathcal{G} = (g_1, g_2, g_3)$ con $g_1, g_2, g_3 \in P^2$ definiti da:

$$g_1 = (x^2y - 1, 0), \quad g_2 = (xy^2 - 1, x), \quad g_3 = (0, xy + 1)$$

Sui termini $\mathbb{T}\langle e_1, e_2 \rangle$ di P^2 definiamo il term order σ dato da `PosLex`, quindi $t_1 e_i <_\sigma t_2 e_j$ se $i > j$ o, se $i = j$, allora se $t_1 <_{\mathrm{Lex}} t_2$. Pertanto vale:

$$\mathrm{LM}_\sigma(g_1) = x^2 y e_1, \quad \mathrm{LM}_\sigma(g_2) = xy^2 e_1, \quad \mathrm{LM}_\sigma(g_3) = xy e_2$$

Calcolo della base di Gröbner con l'algoritmo di Buchberger:
$s' = 3; \mathcal{G} = (g_1, g_2, g_3)$
$B = \{(1,2)\}$
scegliamo $(1,2) \in B$;
$B = \emptyset$
$S_{12} = (x - y, -x^2)$. S_{12} è ridotto modulo $\mathcal{G}$. Pertanto:
$s' = 4$; $g_4 = (x - y, -x^2)$; $\mathcal{G} = \mathcal{G}, g_4$;
$B = \{(1,4), (2,4)\}$;
Scegliamo $(1,4) \in B$;
$B = \{(2,4)\}$;
$S_{14} = (xy^2 - 1, x^3 y)$; La riduzione con $\mathcal{G}$ dà:
$S_{14} - g_2 - x^2 g_3 = (0, -x^2 - x)$; pertanto $s' = 5, g_5 = (0, -x^2 - x)$, $\mathcal{G} = \mathcal{G}, g_5$;
$B = \{(2,4), (3,5)\}$

Scegliamo $(2,4) \in B$;
$B = \{(3,5)\}$;
$S_{24} = (y^3 - 1, x^2y^2 + x)$; La riduzione con $\mathcal{G}$ dà:
$S_{24} - xyg_3 + g_3 = (y^3 - 1, x+1)$; pertanto $s' = 6, g_6 = (y^3 - 1, x+1)$, $\mathcal{G} = \mathcal{G}, g_6$;
$B = \{(3,5),(1,6),(2,6),(4,6)\}$
Scegliamo $(3,5) \in B$;
$B = \{(1,6),(2,6),(4,6)\}$
$S_{35} = (0, -xy + x)$; La riduzione con $\mathcal{G}$ dà:
$S_{35} + g_3 = (0, x+1)$; pertanto $s' = 7, g_7 = (0, x+1)$, $\mathcal{G} = \mathcal{G}, g_7$;
$B = \{(1,6),(2,6),(4,6),(3,7),(5,7)\}$
Scegliamo $(5,7) \in B$
$B = \{(1,6),(2,6),(4,6),(3,7)\}$
$S_{57} = 0$
Scegliamo $(3,7) \in B$
$B = \{(1,6),(2,6),(4,6)\}$
$S_{37} = (0, -y+1)$; è ridotto rispetto a $\mathcal{G}$
$s' = 8, g_8 = (0, -y+1), \mathcal{G} = \mathcal{G}, g_8$;
$B = \{(1,6),(2,6),(4,6),(3,8),(5,8),(7,8)\}$
Da qui in poi si vede che la forma ridotta di S_{ij} vale sempre 0 per ogni $(i,j) \in B$. Pertanto una σ-base di Gröbner del modulo M è data da:

$$\begin{array}{llll} g_1 = (x^2y - 1, 0), & g_2 = (xy^2 - 1, x), & g_3 = (0, xy+1), & g_4 = (x - y, -x^2) \\ g_5 = (0, -x^2 - x), & g_6 = (y^3 - 1, 1 + x), & g_7 = (0, x+1), & g_8 = (0, -y+1) \end{array}$$

Dal procedimento usato per il calcolo della base di Gröbner $\{g_1, \dots, g_8\}$ con l'algoritmo di Buchberger, si vede anche come otterenere ciascun g_i come combinazione lineare dei generatori di partenza (cioè di g_1, g_2, g_3). Ad esempio g_4 è stato ottenuto da S_{12}, cioè $g_4 = yg_1 - xg_2$, mentre $g_5 = S_{14} - g_2 - x^2g_3$, quindi $g_5 = g_1 - xy(yg_1 - xg_2) - g_2 - xyg_3$, cioè $g_5 = (-xy^2+1)g_1 + (x^2y-1)g_2 + (-x^2)g_3$. In questo modo si vede che, se chiamiamo $\mathcal{H}$ la matrice 1×3 la cui riga è costituita dai generatori $h_1 = g_1, h_2 = g_2, h_3 = g_3$ del modulo M e $\mathcal{G}$ la matrice 1×8 costituita dalla base di Gröbner $g_1, \dots, g_8$, si può costruire una matrice 8×3, $\mathcal{A}$, ad entrate polinomiali, tale che

$$\mathcal{G} = \mathcal{H} \cdot \mathcal{A}$$

La matrice $\mathcal{A}$ vale:

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

Base di Gröbner minimale

I leading term della base di Gröbner scritta sopra sono:

$$\begin{array}{llll} \mathrm{LT}_\sigma(g_1) = x^2ye_1, & \mathrm{LT}_\sigma(g_2) = xy^2e_1, & \mathrm{LT}_\sigma(g_3) = xye_2, & \mathrm{LT}_\sigma(g_4) = xe_1, \\ \mathrm{LT}_\sigma(g_5) = x^2e_2, & \mathrm{LT}_\sigma(g_6) = y^3e_1, & \mathrm{LT}_\sigma(g_7) = xe_2, & \mathrm{LT}_\sigma(g_8) = ye_2. \end{array}$$

Come si vede, alcuni leading term sono multipli di altri (ad esempio $\mathrm{LT}_\sigma(g_1)$ e $\mathrm{LT}_\sigma(g_2)$ sono multipli di $\mathrm{LT}_\sigma(g_4)$, mentre $\mathrm{LT}_\sigma(g_3)$ è multiplo di $\mathrm{LT}_\sigma(g_7)$). Se dalla base di Gröbner $g_1, \ldots, g_8$ togliamo quegli elementi i cui leading term sono multipli di altri, otteniamo ancora una base di Gröbner di M. Quindi gli elementi che rimangono in questo esempio sono: g_4, g_6, g_7, g_8. Questa è una base di Gröbner minimale di M, in accordo con la:
Definizione: una base di Gröbner $g_1, \ldots, g_s$ si dice *minimale* se $\mathrm{LT}_\sigma(g_i)$ non è multiplo di $\mathrm{LT}_\sigma(g_j)$ per ogni $i \neq j$ e se $\mathrm{LC}_\sigma(g_i) = 1$ per ogni i.
Infine si noti che alcuni elementi della base $\{g_4, g_6, g_7, g_8\}$ possono essere ridotti rispetto agli altri. Ad esempio g_6 può essere ridotto rispetto a g_7 (infatti $g_6 \to_{\{g_7\}} (y^3 - 1, 0) = g_6 - g_7$) e così pure g_4 si può ridurre con g_7 (infatti $g_4 \to_{\{g_7\}} (x - y, -1) = g_4 + xg_7 - g_7$). Si ottengono così i seguenti elementi di P^2:

$$\overline{g}_1 = (0, x+1), \quad \overline{g}_2 = (0, y-1), \quad \overline{g}_3 = (x-y, -1), \quad \overline{g}_4 = (y^3 - 1, 0)$$

che sono ancora una base di Gröbner di M (perchè i loro LT_σ non sono stati alterati) e formano una base di Gröbner ridotta, in accordo con la:
Definizione: una base di Gröbner $g_1, \ldots, g_s$ si dice *ridotta* se è minimale e se g_i è ridotto modulo $\{g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_s\}$, per ogni $i = 1, \ldots, s$.

Si può dimostrare che da ogni base di Gröbner si può estrarre una base di Gröbner ridotta e la base di Gröbner ridotta è unica (per un fissato ordinamento).

Seguendo i calcoli che hanno permesso di ottenere la base di Gröbner ridotta a partire da $\{g_1, \ldots, g_8\}$, si può anche ora trovare una matrice, chiamiamola ancora $\mathcal{A}$, tale che $\overline{\mathcal{G}} = \mathcal{H} \cdot \mathcal{A}$, dove ora $\overline{\mathcal{G}} = \overline{g}_1, \ldots, \overline{g}_4$. La matrice $\mathcal{A}$ che si trova è:

$$\begin{pmatrix} -xy^3+y & -xy^4+y^2 & xy^3+xy^2-1 & xy^3-y^3-y \\ x^2y^2-y & x^2y^3-y^2 & -x^2y^2-x^2y-x+y+1 & -x^2y^2+xy^2+y+1 \\ -x^2y+x+1 & -x^2y^2+xy+y-1 & x^2y+x^2-x-1 & x^2y-xy-x \end{pmatrix}$$

Infine, poiché gli elementi di $\mathcal{H}$ (che sono i generatori di M) sono ovviamente elementi di M, devono ridursi a 0 con la base di Gröbner $\overline{\mathcal{G}}$, pertanto, applicando l'algoritmo di divisione, si ottiene, ad esempio: $h_1 = y\overline{g}_1 + y\overline{g}_2 + (xy+y^2)\overline{g}_3 + \overline{g}_4$ e così per tutti gli altri. In questo modo si può costruire una matrice 4×3, $\mathcal{B}$, tale che $\mathcal{H} = \overline{\mathcal{G}} \cdot \mathcal{B}$. La matrice $\mathcal{B}$ vale:

$$\begin{pmatrix} y & 1 & y \\ y & y+1 & -1 \\ xy+y^2 & y^2 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

Consideriamo ora la base di Gröbner $\{\overline{g}_1, \overline{g}_2, \overline{g}_3, \overline{g}_4\}$ scritta sopra. Poiché è una base di Gröbner, per il criterio di Buchberger l'S-vettore di $\overline{g}_i$ e $\overline{g}_j$ (quando è definito) deve ridursi a zero con $\{\overline{g}_1, \overline{g}_2, \overline{g}_3, \overline{g}_4\}$. Infatti si trova, con S_{12}: $(y-1)\overline{g}_1 - (x+1)\overline{g}_2 = 0$ da cui si costrisce la sizigia $\tau_{12} = (y-1)\varepsilon_1 - (x+1)\varepsilon_2$, analogamente, con S_{34} si ottiene: $(y^2+y+1)\overline{g}_2 + (y^3-1)\overline{g}_3 + (-x+y)\overline{g}_4 = 0$, da cui la sizigia $\tau_{34} = (y^2+y+1)\varepsilon_2+(y^3-1)\varepsilon_3+(-x+y)\varepsilon_4$ e quindi, per il teorema di Schereyer, τ_{12}, τ_{34} è una δ-base di Gröbner del modulo Siz $(\overline{g}_1, \overline{g}_2, \overline{g}_3, \overline{g}_4)$ (dove δ è il term-order definito nel teorema di Schreyer).