25/11/19

Ορισμός (S - πολυώνυμα)

Έστω $f, g \overset{\neq 0}{\in} \mathbb{K}[x_1, \dots, x_n]$, $<$ μονω. διάταξη και έστω $L = $ Ε.Κ.Π.$(lm(f), lm(g))$. Τότε, ορίζουμε το S πολυώνυμο αυτών

$$S(f,g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g.$$

Πχ $f = 3x^2yz - y^3z^3$, $g = xy^2 + z^2 \in \mathbb{Q}[x,y,z]$

α) $\overset{<}{lex}$, $x>y>z$ $\quad L = $ Ε.Κ.Π.$(x^2yz, xy^2) = x^2y^2z$

$$S(f,g) = \frac{x^2y^2z}{3x^2yz}(3x^2yz - y^3z^3) - \frac{x^2y^2z}{xy^2}(xy^2+z^2)$$

$$= -\frac{1}{3}y^4z^3 - xz^3 = -xz^3 - \frac{1}{3}y^4z^3$$

β) deglex $\quad f = -y^3z^3 + 3x^2yz$, $\quad g = xy^2 + z^2$

$L = $ Ε.Κ.Π.$(y^3z^3, xy^2) = xy^3z^3$

$$S(f,g) = \frac{xy^3z^3}{-y^3z^3}(-y^3z^3 + 3x^2yz) - \frac{xy^3z^3}{xy^2}(xy^2+z^2)$$

$$= -3x^3yz - yz^5 = -yz^5 - 3x^3yz$$

(Buchberger)

Θεώρημα: Έστω $G = \{g_1, \dots, g_k\} \subseteq \mathbb{K}[x_1, \dots, x_n]$, $<$ μον. διάταξη. Το σύνολο G είναι βάση Gröbner (του $I = \langle g_1, \dots, g_k \rangle$) αν-ν $S(g_i, g_j) \xrightarrow[+]{G} 0 \quad \forall i \neq j$

Πχ Να βρεθεί βάση Gröbner του $I = \langle \overset{g_1}{x^2y+z}, \overset{g_2}{xz+y} \rangle \subseteq \mathbb{Q}[x,y,z]$ deglex, $x>y>z$

Έστω $G_1 = \{ f_1 = x^2y + z,\ f_2 = xz + y \}$

$S(f_1, f_2)$: $L = ΕΚΠ(x^2y, xz) = x^2yz$

Άρα $S(f_1,f_2) = \frac{x^2yz}{x^2y}(x^2y+z) - \frac{x^2yz}{xz}(xz+y)$

$= z^2 - xy^2 = -xy^2 + z^2$

$S(f_1, f_2) = -xy^2 + z^2 \xrightarrow{G_1} -xy^2 + z^2 \to$ ανάγωγο μόδιο G_1

(που δίνει το ίδιο)

Θεωρώ $G_2 = \{ f_1, f_2, f_3 = -xy^2 + z^2 \}$

Παρατηρώ ότι $S(f_1, f_2) \xrightarrow[+]{G_2} 0$

$L = ΕΚΠ(xy^2, xz) = xy^2z$

$S(f_2, f_3) = \frac{xy^2z}{xz}(xz+y) - \frac{xy^2z}{-xy^2}(-xy^2+z^2)$

$= y^3 + z^3$

$S(f_2, f_3) = y^3 + z^3$ ανάγωγο μόδιο G_2

Έστω $G_3 = \{ f_1, f_2, f_3, f_4 = y^3 + z^3 \}$

$S(f_1, f_2), S(f_2, f_3) \xrightarrow[+]{G_3} 0$

Πρέπει να βρώ τα $S(f_1, f_3)$, $S(f_1, f_4)$, $S(f_2, f_4)$, $S(f_3, f_4)$

$L = ΕΚΠ(x^2y, xy^2) = x^2y^2$

$S(f_1, f_3) = \frac{x^2y^2}{x^2y}(x^2y+z) - \frac{x^2y^2}{-xy^2}(-xy^2+z^2)$

$= yz + xz^2 = xz^2 + yz \xrightarrow[f_2]{G_3} xz^2 + yz - \frac{xz^2}{xz}(xz+y)$

$= yz - yz = 0$

Το $S(f_1, f_3) \xrightarrow[+]{G_3} 0$. Κάνοντας τις πράξεις και τα υπόλοιπα πάνε στο 0

Άρα, το G_3 είναι β. Gröbner του I

Θεώρημα 1) Έστω $G=\{g_1,\dots,g_k\} \subseteq K[x_1,\dots,x_n]$
Ο αλγόριθμος Buchberger περιέχει βάση Gröbner για το $I=\langle g_1,\dots,g_k\rangle$

2) Έστω $f,g \in K[x_1,\dots,x_n]$ με $\mu\kappa\delta(lt(f), lt(g)) = 1$
$\Rightarrow S(f,g) \xrightarrow[+]{f,g} 0$

(σημαντικό ως προς τον όγκο των πράξεων)

Πχ Να βρεθεί βάση Gröbner για το ιδεώδες
$I = \langle x_1^2 + x_1x_2 + x_2^2,\ x_1+x_2,\ x_2\rangle \subseteq \mathbb{Q}[x_1,x_2]$
lex $x_2 > x_1$

Έστω $G_1 = \{f_1 = x_2^2 + x_2x_2 + x_1^2,\ f_2 = x_2 + x_1,\ f_3 = x_2\}$

$\to S(f_1,f_2) = \frac{x_2^2}{x_2^2}(x_2^2 + x_2x_2 + x_1^2) - \frac{x_2^2}{x_2}(x_2+x_1)$

$= x_2x_1 + x_1^2 - x_1x_2 = x_1^2 \xrightarrow[+]{G_1} x_1^2 = f_4$

Θεωρώ το $G_2 = \{f_1, f_2, f_3, f_4 = x_1^2\}$ όπου $S(f_1,f_2) \xrightarrow[+]{G_2} 0$

και καθώς $\mu\kappa\delta\left(lt(f_4), \begin{matrix} lt(f_1) \\ lt(f_2) \\ lt(f_3)\end{matrix}\right) = 1 \Rightarrow S(f_1,f_4), S(f_2,f_4), S(f_3,f_4) \xrightarrow[+]{G_2} 0$

$\to S(f_2,f_3) = \frac{x_2}{x_2}(x_2+x_1) - \frac{x_2}{x_2}\cdot x_2 = x_1$ ανάγωγο μόδιο G_2

* Αν ξεκινούσα από το $S(f_2,f_3)$ δεν θα είχα το f_4 στη βάση

Θεωρώ $G_3 = \{f_1, f_2, f_3, f_4, f_5 = x_1\}$ και καθώς $\mu\kappa\delta\left(lt(f_5), \begin{matrix} lt(f_1) \\ lt(f_2) \\ lt(f_3)\end{matrix}\right) = 1$
$\Rightarrow S(f_1,f_5), S(f_2,f_5), S(f_3,f_5) \xrightarrow[+]{G_3} 0$

$S(f_2, f_3) = x_1 \xrightarrow[+]{G_3} 0$ και $S(f_1, f_3)$, $S(f_4, f_5) \xrightarrow[+]{G_3} 0$

Άρα, το G_3 είναι βάση Gröbner για το I.

¥ Προτιμάμε τις χαμηλές δυνάμεις στα S πολυώνυμα

¥ Από κάθε βάση Gröbner προκύπτουν άπειρες βάσεις Gröbner.

Ορισμός (Ελαχιστική Βάση Gröbner)
Έστω βάση Gröbner $G = \{g_1, \ldots, g_k\} \subseteq \mathbb{K}[x_1, x_n]$. Η G καλείται ελαχιστική αν i) $lc(g_i) = 1$, $\forall i = 1, \ldots, k$
και ii) $\nexists i, j \in \{1, \ldots, k\} : lm(g_i) \mid lm(g_j)$
με $i \neq j$

ΠΧ $\mathbb{Q}[x_1, x_2]$ $\leq_{lex}$ με $x_1 > x_2$

$G = \{-\frac{1}{2}x_1^2 + x_2, x_2^3, x_1x_2 + x_2\}$ Δεν είναι ελαχιστική γιατί δεν ισχύει το i)
$\downarrow$
$G' = \{x_1^2 - 2x_2, x_2^3, x_1x_2 + x_2\}$
(πολ/ζω με -2)

ΠΧ $G = \{\cancel{f_1 = x_2^2 + x_2x_1 + x_1^2}, f_2 = \cancel{x_2 + x_1}, f_3 = x_2, \cancel{f_4 = x_1^2}, f_5 = x_1\}$
(διώχνω ότι διαιρείται από άλλο)

Παρατηρώ ότι μία ελαχιστική βάση Gröbner είναι η
$G' = \{f_3 = x_2, f_5 = x_1\}$

ή

μία άλλη ελαχιστική βάση είναι η
$G'' = \{f_2 = x_2 + x_1, f_5 = x_1\}$

Θεώρημα. Έστω $G_1 = \{g_1, \dots, g_k\}$ και $G_2 = \{f_1, \dots, f_s\}$ δύο ελαχιστικές βάσεις Gröbner ενός $I \subseteq \mathbb{K}[x_1, \dots, x_n]$, $<$ μον. Τότε, $k = s$ και μπορώ να αριθμήσω έτσι τα στοιχεία των G_1, G_2, έτσι ώστε

$lt(f_i) = lt(g_i)$, $\forall i = 1, \dots, k = s$

Ορισμός. Έστω $G = \{g_1, \dots, g_k\}$ βάση Gröbner ενός ιδεώδους $I \subseteq \mathbb{K}[x_1, \dots, x_n]$, $<$ μονωμ. διάταξη.
Η G θα καλείται ανάγωγη βάση Gröbner αν

i) $lc(g_i) = 1$, $\forall i = 1, \dots, k$ και

ii) g_i ανάγωγο μόδιο $G \setminus \{g_i\}$, $\forall i = 1, \dots, k$)

($\forall i = 1, \dots, k$ δεν υπάρχει όρος του g_i ο οποίος να διαιρείται από $lm(g_j)$)

$\hookrightarrow g_j \in G \setminus \{g_i\}$

Π.χ. $G'' = \{f_2 = x_2 + x_1, f_5 = x_1\}$ lex $x_2 > x_1$

ελαχιστική ↗

Για να γίνει ανάγωγη εκτελούμε για όλα τα στοιχεία f' της ελαχιστικής (όπου είναι εφικτό) τη διαίρεση μόδιο $G'' \setminus \{f'\}$

$x_2 + x_1 \xrightarrow{G'' \setminus \{f_2\}}$;

$x_2 + x_1 - \frac{x_1}{x_1} \cdot x_1 = x_2$ ανάγωγο $\rightarrow G''' = \{x_2, x_1\}$ ανάγωγη