30/11/17

Άσκηση - Παράδειγμα (πάνω στο Buchberger)

Έστω $Q[x,\psi]$ με διάταξη "lex" με $x>\psi$ και
$I = \langle g_1 = \psi^2 + x\psi + x^2,\ g_2 = \psi + x,\ g_3 = \psi \rangle$
Να βρώ την Βάση Gröbner του I

Λύση

Αρχικά δεν γνωρίζω τα g_1, g_2, g_3 (εδώ είναι καλά)
Σύμφωνα με τον αλγόριθμο του Buchberger σχηματικά θα έχω:

G: $g_1 = \psi^2 + x\psi + x^2$, $g_2 = \psi + x$, $g_3 = \psi$, $g_4 = x$, $g_5 = x$

$\mathcal{G}$: $\cancel{S(g_1,g_2)}$, $\cancel{S(g_2,g_3)}$, $\cancel{S(g_1,g_3)}$, $\cancel{S(g_1,g_4)}$, $\cancel{S(g_2,g_4)}$, $\cancel{S(g_3,g_4)}$, $\cancel{S(g_4,g_5)}$, $\cancel{S(g_2,g_5)}$, $\cancel{S(g_1,g_5)}$, $\cancel{S(g_3,g_5)}$

Έχω ότι:

- $S(g_1,g_2) = \frac{\psi^2}{\psi^2}(\psi^2 + x\psi + x^2) - \frac{\psi^2}{\psi}(\psi + x) = \psi x + x^2 - \psi x = x^2$, το οποίο είναι ανάγωγο

Άρα το προσθέτω στο G, σαν g_4 και άρα στο $\mathcal{G}$ προκύπτουν τα $S(g_1,g_4)$, $S(g_2,g_4)$, $S(g_3,g_4)$.

Άρα έχω:

- $S(q_2,q_3) = \frac{\psi^2}{\psi^2}(\psi^2+x\psi+x^2) - \frac{\psi^2}{\psi}\cdot\psi = \psi x + x^2 \xrightarrow{q_2} \psi x + x^2 - \frac{\psi x}{\psi}(\psi+x) =$
$= x^2 - x^2 = 0.$

Άρα δεν προσθέτω τίποτα καινούριο.

- $S(q_2,q_3) = \frac{\psi}{\psi}(\psi+x) - \frac{\psi}{\psi}\psi = x$, το οποίο είναι ανάγωγο, διότι $\neq 0$

Άρα το προσθέτω στο G σαν q_5 και άρα θα πρέπει να υπολογίσω και τα
$S(q_1,q_5)$, $S(q_2,q_5)$, $S(q_3,q_5)$, $S(q_4,q_5)$

Άρα έχω:

- $S(q_1,q_4) \xrightarrow{G}_+ 0$ (Αφού $ΜΚΔ(\psi^2,x^2)=1$.)
- $S(q_2,q_4) \xrightarrow{G}_+ 0$ (Αφού $ΜΚΔ(\psi,x^2)=1$)
- $S(q_3,q_4) \xrightarrow{G}_+ 0$ (Αφού $ΜΚΔ(\psi,x)=1$)
- $S(q_1,q_5) \xrightarrow{G}_+ 0$ (Αντίστοιχα).
- $S(q_2,q_5) \xrightarrow{G}_+ 0$ (—"—)
- $S(q_3,q_5) \xrightarrow{G}_+ 0$ (—"—)
- $S(q_4,q_5) = \frac{x^2}{x^2}\cdot x^2 - \frac{x^2}{x}\cdot x = 0.$

Άρα δεν προσθέτω τίποτα καινούριο.
Άρα τελειώνω τον έλεγχο.
Άρα $G=\{q_1,q_2,q_3,q_4,q_5\}$ είναι βάση Gröbner.

Θεώρημα: Ο αλγόριθμος του Buchberger τερματίζει σε πεπερασμένο πλήθος βημάτων.

Β) Παρατήρηση.

(Για την προηγούμενη άσκηση.)

Είναι η $G=\{g_1,g_2,g_3,g_4,g_5\}$ μοναδική βάση Gröbner του I;

Λύση

Όχι δεν είναι η μοναδική.

Έστω $G=\{g_1,g_2,g_3,g_4,g_5,g_6, h_1g_1+h_2g_2+h_3g_3\}$

Έστω $f\in I$, $f\neq 0$.

Άρα $\exists\, i\in\{1,\dots,5\}$ τ.ω. $lm(g_i) \mid lm(f)$

Άρα $\{g_1,g_3\}$ ή $\{g_3,g_5\}$ αποτελούν μια βάση Gröbner αντίστοιχα

Επίσης $\{g_4+f(x,y)\}$ είναι και αυτή μια βάση Gröbner.

Υπάρχουν άπειρες βάσεις Gröbner

Ορισμός: Μια βάση Gröbner $G=\{g_1,\dots,g_t\}$ λέγεται ελαχιστική αν

i) $\forall\, i\in\{1,\dots,t\}$ ισχύει $lc(g_i)=1$

ii) Για οποιουσδήποτε δείκτες $i\neq j$ με $i\neq j$ το αρχικό μονώνυμο $lm(g_i)$ δεν διαιρεί το αρχικό μονώνυμο $lm(g_j)$ (δηλ. $lm(g_i)\nmid lm(g_j)$)

Πρόταση: Έστω $G=\{g_1,g_2,\dots,g_s\}$ βάση Gröbner του I.

Αν $lm(g_2)\mid lm(g_1)$ τότε το $G'=\{g_2,g_3,\dots,g_s\}$ είναι βάση Gröbner του I

Απόδειξη

Έχω ότι G: βάση Gröbner $\Rightarrow \exists\, i\in\{1,\dots,t\}$ τ.ω. $lm(g_i)\mid lm(f)$.

Έστω $f\in I$, $f\neq 0$

Έστω δηλαδή ότι $lm(g_1)\mid lm(f)$ τότε όπως $lm(g_2)\mid lm(g_1) \Rightarrow lm(g_2)\mid lm(f)$.

Άρα για κάθε $f\in I$, $f\neq 0$ $\exists\, i\in\{2,\dots,s\}$ τ.ω. $lm(g_i)\mid lm(f)$

Άρα $G'=\{g_2,\dots,g_s\}$ είναι βάση Gröbner εξ' ορισμού.

• Αλγόριθμος Εύρεσης Ελαχιστικής βάσης Gröbner

Είσοδος: $F=\{f_1,\dots,f_s\} \subset k[x_1,\dots,x_n]$ βάση Gröbner του I.
Έξοδος: $G=\{g_1,\dots,g_t\}$ ελαχιστική βάση Gröbner του I.

Αρχή

$$G=\left\{ g_1=\frac{f_1}{lc(f_1)},\ g_2=\frac{f_2}{lc(f_2)},\ \dots,\ g_s=\frac{f_s}{lc(f_s)} \right\}$$

Αν $\exists\,(i,j)$ με $i\neq j$ τ.ω.: $lm(g_i)\mid lm(g_j)$ τότε
αφαίρεσε το g_j από το G και συνέχισε
τέλος ~

Πρόταση: Αν $G=\{g_1,\dots,g_t\}$ και $F=\{f_1,\dots,f_s\}$ είναι ελαχιστικές βάσεις Gröbner ενός ιδεώδους $I \Rightarrow s=t$ και μπορούμε να τις ξαναριθμήσουμε έτσι ώστε $lm(g_i)=lm(f_i)$, $\forall\, i\in\{1,\dots,t\}$

Απόδειξη

Έχω ότι: $\left.\begin{array}{l} g_1\in I \\ g_1\neq 0 \end{array}\right\} \xRightarrow{F:\text{ βάση Gröbner}} \exists\, i\in\{1,\dots,s\}$ τ.ω.: $lm(f_i)\mid lm(g_1)$

Αναδιατάσσω λοιπόν την βάση έτσι ώστε $lm(f_1)\mid lm(g_1)$.

Αντίστοιχα έχω: $\left.\begin{array}{l} f_1\in I \\ f_1\neq 0 \end{array}\right\} \xRightarrow{G:\text{ βάση Gröbner}} \exists\, j\in\{1,\dots,t\}$ τ.ω.: $lm(g_j)\mid lm(f_1)$

Άρα έχω: $\left.\begin{array}{l} \cdot\ lm(g_j)\mid lm(f_1) \\ \cdot\ lm(f_1)\mid lm(g_1) \end{array}\right\} \Rightarrow lm(g_j)\mid lm(g_1) \xRightarrow{G:\text{ ελαχιστική}} j=1.$

Άρα $\left.\begin{array}{l} \cdot\ lm(g_1)\mid lm(f_1) \\ \cdot\ lm(f_1)\mid lm(g_1) \end{array}\right\} \Rightarrow lm(g_1)=lm(f_1)$

Έχω ότι: $\left.\begin{array}{l} g_2\in I \\ g_2\neq 0 \end{array}\right\} \xRightarrow{F:\text{ βάση Gröbner}} \exists\, i\in\{2,\dots,s\}$ τ.ω.: $lm(f_i)\mid lm(g_2)$

! Αν είχα $i=1 \Rightarrow$
$lm(f_1)=lm(g_1)\mid lm(g_2)$ Άτοπο
αφού G: ελαχιστική.

Αποδείξαμε δηλαδή την βάση έχει ώστε $lm(f_2) \mid lm(g_2)$

Αντίστοιχα έχω: $\left.\begin{array}{l} f_2 \in I \\ f_2 \neq 0 \end{array}\right\} \xrightarrow{G: \text{βάση Gröbner}} \exists\, j \in \{1, \dots, t\}$ τ.ω.

$\left.\begin{array}{l} \cdot\ lm(g_j) \mid lm(f_2) \\ \text{και έχω } lm(f_2) \mid lm(g_2) \end{array}\right\} \xrightarrow{G: \text{ελαχιστική}} j = 2 \Rightarrow \left.\begin{array}{l} lm(g_2) \mid lm(f_2) \\ \cdot\ lm(f_2) \mid lm(g_2) \end{array}\right\} \Rightarrow lm(f_2) = lm(g_2)$

⋮

Συνεχίζω όμοια

Ορισμός: Μια βάση Gröbner $G = \{g_1, \dots, g_t\}$ λέγεται ανάγωγη βάση Gröbner, αν

i) $\forall\, i \in \{1, \dots, t\}$ ισχύει $lc(g_i) = 1$.

ii) Για κάθε ζεύγος $i \neq j$ το αρχικό μονώνυμο $lm(g_i)$ δεν διαιρεί κανέναν όρο του g_j

Παράδειγμα

Έστω ο δακτύλιος $\mathbb{Q}[x, \psi]$ με διάταξη "lex", με $\psi > x$, τότε.

$\left.\begin{array}{l} \cdot\ G_1 = \{x, \psi + x\} \rightsquigarrow \text{όχι ανάγωγη} \\ \cdot\ G_2 = \{x, \psi\} \rightsquigarrow \text{ανάγωγη} \end{array}\right\} \rightsquigarrow$ ελαχιστικές

$\cdot\ G_3 = \{x, \psi + f(x)\} \rightsquigarrow$ όχι ανάγωγη

με $f(x) \neq 0$ και $f(0) = 0$ (δηλ. ο σταθερός όρος $= 0$)

Θεώρημα: κάθε ανάγωγη βάση Gröbner είναι ελαχιστική ($\not\Leftarrow$).

Scanned by CamScanner

Θεώρημα: Κάθε μη μηδενικό ιδεώδες I στον δακτύλιο $k(x_1,\dots,x_n)$ εφοδιασμένο με μια μονωνυμική διάταξη "$>$" διαθέτει μοναδική ανάγωγη βάση Gröbner ως προς την "$>$"

Απόδειξη

Έστω $\cdot\ I = \langle f_1,\dots, f_s\rangle$.

$\cdot\ F = \{f_1,\dots, f_s\} \xrightarrow[\text{Buchberger}]{\text{αλγόριθμος}} \{h_1,\dots, h_t\}$: βάση Gröbner $\Rightarrow$

$\Rightarrow G = \{g_1,\dots, g_t\}$: ελαχιστική

Έχω ότι:

- $g_1 \xrightarrow{H_1}_+ h_1$, όπου h_1 ανάγωγο modulo $H_1 = \{g_2,\dots, g_t\}$
με $h_1 = lm(g_1)+\dots$: κανένας όρος του h_1 δεν διαιρείται από κάποιο $lm(g_i)$,
- $g_2 \xrightarrow{H_2}_+ h_2$, όπου h_2 ανάγωγο modulo $H_2 = \{h_1, g_3,\dots, g_t\}$
με $h_2 = lm(g_2)+\dots$ ομοίως.

⋮

- $g_t \xrightarrow{H_t}_+ h_t$, όπου h_t ανάγωγο modulo $H_t = \{h_1, h_2,\dots, h_{t-1}\}$.

Άρα έχω:

$\cdot\ H = \{h_1, h_2,\dots, h_t\}$: ανάγωγη βάση Gröbner

$\cdot\ lm(g_1) = lm(h_1), \dots, lm(g_t) = lm(h_t)$

Θ.δ.ο. η ανάγωγη βάση είναι μοναδική

Έστω $G = \{g_1,\dots, g_t\}$ και $F = \{f_1,\dots, f_t\}$ δύο ανάγωγες βάσεις Gröbner και $lm(f_i) = lm(g_i)$, $\forall\, i \in \{1,\dots, t\}$

Έχω ότι $g_i \in I,\ f_i \in I \xRightarrow{\text{άρα}}$ $\left.\begin{array}{l} \cdot\ g_i - f_i \in I \\ \cdot\ g_i - f_i \neq 0 \end{array}\right\} \xRightarrow{G\text{: βάση Gröbner}} \exists\, j \neq i$ τ.ω.

$lm(g_j) \mid lm(g_i - f_i)$

Έχω ότι $\left.\begin{array}{l} lm(f_j) = lm(g_j) \Rightarrow lm(f_j) \mid lm(g_i - f_i) \end{array}\right\} \Rightarrow$

Άρα το $lm(f_j) = lm(g_j)$ διαιρεί κάποιον όρο του g_i ή του f_i

· 1η περίπτωση: Το $\mathrm{Im}(f_i) = \mathrm{Im}(g_i)$ διαιρεί κάποιον όρο του g_i.
Άτοπο γιατί G: ανάγωγη βάση Gröbner

· 2η περίπτωση: Το $\mathrm{Im}(f_i) = \mathrm{Im}(g_i)$ διαιρεί κάποιον όρο του f_i
Άτοπο γιατί F: ανάγωγη βάση Gröbner
Άρα δεν ισχύει $g_i - f_i \neq 0$
Άρα τελικά $g_i = f_i \Rightarrow G = F$.