Βάσεις Gröbner

Ώρες γραφείου : 11:00-13:00 κάθε μέρα.

[Τελευταίο μάθημα.]

18/01/2018

Άσκηση: Βρείτε μια βάση Gröbner για το ιδεώδες $I = \langle xy^n - z \mid n \in \mathbb{N} \rangle \subseteq \mathbb{R}[x,y,z]$ με διάταξη την λεξικογραφική $lex_{x>y>z}$

Λύση:

$$I = \langle xy^n - z \mid n \in \mathbb{N} \rangle = \langle xy - z, xy^2 - z, xy^3 - z, \dots, xy^n - z, \dots \rangle$$

έχω άπειρους γεννήτορες άρα δεν μπορώ να εφαρμόσω Buchberger.

Θα βρω ποιό είναι αυτό το ιδεώδες και αν έχει πεπερασμένο πλήθος γεννητόρων, αλλιώς ο αλγόριθμος Buchberger δεν θα τελειώσει ποτέ.

Σίγουρα θέλω στους γεννήτορες το πολυώνυμο με τον μικρότερο βαθμό: $xy - z$.

Αφού $xy - z$ και $xy^2 - z$ ανήκουν στο I τότε ισχύει και αυτό που θα προκύψει από την διαίρεση:

$$xy^2 - z \xrightarrow{xy-z} xy^2 - z - y(xy - z) = (yz - z) \in I.$$

Τώρα πρέπει νδο αυτά τα 2 δημιουργούν όλα τα στοιχεία του I, αν δεν συμβαίνει αυτό, βρίσκω και ένα τρίτο.

$$xy^3 - z \xrightarrow{xy-z} xy^3 - z - y^2(xy - z) = (y^2 z - z) \xrightarrow{yz-z} y^2 z - z - y(yz - z) = (yz - z) \xrightarrow{yz-z} 0$$

Άρα $\langle xy - z, yz - z \rangle \subseteq I$.

Τώρα το τυχαίο πολυώνυμο $xy^n - z$ μας δίνει:

$$xy^n - z \xrightarrow{xy-z} xy^n - z - y^{n-1}(xy - z) = y^{n-1}z - z \xrightarrow{yz-z} \underset{\text{άπειρες φορές}}{\dots} \xrightarrow{yz-z} \dots$$

Ισχυριζόμαστε:

$$xy^n - z = y(xy^{n-1} - z) + (yz - z)$$

δηλαδή ότι $xy^n - z \in \langle xy - z, yz - z \rangle$

Για $n=1$: $xy - z \in \langle xy - z, yz - z \rangle$ που ισχύει.

Έστω ότι ισχύει $xy^n - z \in \langle xy - z, yz - z \rangle$

Θδο ισχύει $xy^{n+1} - z \in \langle xy - z, yz - z \rangle$

Είναι $xy^{n+1} - z = y(xy^n - z) - (yz - z) \in \langle xy - z, yz - z\rangle$

$\in \langle xy - z, yz - z\rangle$. άρα $I \subseteq \langle xy - z, yz - z\rangle$

Άρα πλέον, έχω ένα ιδεώδες που παράγεται από 2 μόνο γεννήτορες:

$$\boxed{I = \langle xy - z, yz - z\rangle.}$$

Έχουμε τώρα:

$g_1 = xy - z$
$g_2 = yz - z.$
$g_3 = zx - z^2.$

S-πολυώνυμα

$\cancel{S(g_1, g_2)}$, $\cancel{S(g_1, g_3)}$, $\cancel{S(g_2, g_3)}$

$S(g_1, g_2) = \frac{xyz}{xy}(xy - z) - \frac{xyz}{yz}(yz - z) = zx - z^2 = xz - z^2.$ δεν διαιρείται άλλο γιατί κανένας από τους αρχικούς όρους xy και yz δεν το διαιρεί.

$S(g_1, g_3) = \frac{xyz}{xy}(xy - z) - \frac{xyz}{xz}(xz - z^2) = -z^2 + yz^2 = yz^2 - z^2 \xrightarrow{yz - z = g_2}$

$\rightarrow yz^2 - z^2 - \frac{yz^2}{yz}(yz - z) = -z^2 + z^2 = 0$. (δεν έχω να προσθέσω κάτι από S-πολυώνυμα)

$S(g_2, g_3) = \frac{xyz}{yz}(yz - z) - \frac{xyz}{xz}(xz - z^2) = -xz + yz^2 \xrightarrow{xz - z^2 = g_3}$

$\rightarrow -xz + yz^2 - \frac{-xz}{zx}(zx - z^2) = yz^2 - z^2 \xrightarrow{yz - z = g_2} yz^2 - z^2 - \frac{yz^2}{yz}(yz - z) = z^2 - z^2 = 0$

Αφού έφυγαν και τα 3 S-πολυώνυμα, βρήκα την βάση Gröbner

Η βάση Gröbner είναι:

$g_1 = xy - z$, $g_2 = yz - z$, $g_3 = zx - z^2$.

είναι ελαχιστική, είναι ανάγωγη.

<u>Βρείτε την καθολική βάση Gröbner:</u>

Η καθολική βάση Gröbner <u>είναι</u> η ένωση όλων των αναγώγων βάσεων Gröbner.

Θα πάρω όλες τις δυνατές περιπτώσεις

Έχω το ιδεώδες $I = \langle \underset{g_1}{xy - z}, \underset{g_2}{yz - z} \rangle$, $g_3 = zx - z^2$.

στο g_2 το z διαιρεί το yz άρα είναι πιο μεγάλο.

$\boxed{1^{η}\text{ περίπτωση}}$: $xy > z$ $\qquad S(g_1, g_2) = zx - z^2$ άρα θα πάρω δύο περιπτώσεις τις (1α) και (1β)

$yz > z$

(1α) $zx > z^2 \Rightarrow x > z$

(1β) $z^2 > zx \Rightarrow z > x$

(1α) Έχω ότι g_1, g_2, g_3 είναι ανάγωγη βάση Gröbner ∀ διάταξη με $xy > z$ και $x > z$.

(Δηλαδή για την (1α) έχω υπολογίσει ήδη τα S-πολυώνυμα)

(1β) Ελέγχω τα S-πολυώνυμα των $g_1 = xy - z$, $g_2 = yz - z$, $g_3 = z^2 - zx$

$S(g_1, g_3) \xrightarrow{g_1, g_3}_{+} 0$ $[\mu\kappa\delta(xy, z^2) = 1]$

$S(g_2, g_3) = z(yz - z) - y(z^2 - zx) = -z^2 + zyx = xyz - z^2 \xrightarrow{g_1}$

$\rightarrow zyx - z^2 - \frac{zyx}{xy}(xy - z) = z^2 - z^2 = 0$

Αυτό σημαίνει ότι είναι βάση Gröbner και μάλιστα ανάγωγη,

δηλαδή η $g_1 = xy - z$, $g_2 = yz - z$, $g_3 = z^2 - zx$ $\longrightarrow$

αν δεν ήταν βάση Gröbner θα βρίσκαμε και g_4.
Είναι ανάγωγη γιατί κανένας από τους μεγιστοβάθμιους όρους δεν διαιρεί τα υπόλοιπα g_1, g_2, g_3. Αν διαιρούσε θα πραγματοποιούσαμε την διαίρεση.

Επομένως η g_1, g_2, g_3 είναι βάση Gröbner

ή

$g_1, g_2, -g_3$.

$\boxed{2^{η} \text{ περίπτωση}}$: $f_1 = z - xy$, $f_2 = yz - z$. γιατί $z > xy$.

θα κάνω την γνωστή διαδικασία με τα S-πολυώνυμα και τις διαιρέσεις

$$\boxed{\begin{array}{l} f_1, f_2. \\ f_3 = xy^2 - xy \end{array}} \qquad \boxed{\begin{array}{l} S(f_1,f_2), \; S(f_1,f_3) \\ S(f_2,f_3), \end{array}}$$

$$S(f_1,f_2) = \frac{yz}{z}(z-xy) - \frac{yz}{yz}(yz-z) = -xy^2 + z \xrightarrow{f_1}$$

την διαίρεση την συνεχίζω χωρίς να με ενδιαφέρει πιο είναι το πιο μεγάλο.

$$\rightarrow -xy^2 + z - \frac{z}{z}(z-xy) = -xy^2 + xy$$

αφού $y > 1 \Rightarrow xy^2 > xy$

άρα xy^2 πιο μεγάλο.

$S(f_1,f_3) \xrightarrow{f_1, f_3}_{+} 0$ γιατί $\text{μκδ}(z, xy^2) = 0$

$$S(f_2,f_3) = \frac{xy^2z}{yz}(yz-z) - \frac{xy^2z}{xy^2}(xy^2-xy) = -xyz + xyz = 0$$

Άρα είναι η f_1, f_2, f_3 βάση Gröbner, όμως <u>όχι</u> ανάγωγη και <u>όχι</u> ελαχιστική

$\longrightarrow$

Δεν μπορώ να την κάνω ελαχιστική χωρίς να είναι βάση Gröbner, γι'αυτό την κάνω ελαχιστική στο τέλος:

Παρατηρώ ότι $z \mid yz$ άρα η ελαχιστική είναι η $f_1 = z - xy$, $f_3 = xy^2 - xy$

και

$z \nmid xy^2 \quad xy^2 \nmid z$

$z \nmid xy \quad xy^2 \nmid xy$ Άρα f_1, f_3 ανάγωγη.

<u>Ποιά είναι η καθολική βάση Gröbner;</u>

$\{g_1, g_2, g_3, -g_3, -g_1, f_3 = xy^2 - xy\} \rightarrow$ 6 στοιχεία

και επειδή δεν με ενδιαφέρει το πρόσημο ουσιαστικά περιέχει 4 στοιχεία:

$\{g_1, g_2, g_3, f_3\} \longrightarrow$ <u>ΠΟΤΕ</u> ελαχιστική (η ελαχιστική έχει ή 3 ή 2 στοιχεία)

Παρ'όλο που είχα άπειρες διατάξεις κατάφερα να βρώ την καθολική βάση Gröbner.

<u>Άσκηση:</u> Έστω G μια βάση Gröbner για το ιδεώδες $I \subset K[x_1, x_2, \ldots, x_n]$ ως προς κάποια μονωνυμική διάταξη. Έστω $f, r \in K[x_1, x_2, \ldots, x_n]$ και το r είναι ανάγωγο modulo G. Δείξτε ότι αν $f - r \in I$ τότε $f \xrightarrow{G}_+ r$

<u>Λύση:</u> Έστω $f \xrightarrow{G}_+ r_1$ και θέλω νδο $r_1 = r$, με r_1 ανάγωγο. και $f - r \in I$ άλλα με αφαίρεση αυτών $\Rightarrow$

Άρα $f - r_1 \in I$

$\Rightarrow r - r_1 \in I$.

Θέλω $r - r_1 = 0$. Έστω $r - r_1 \neq 0$ και $r - r_1 \in I \Rightarrow \exists\, i$ τω: $lm(g_i) \mid lm(r - r_1) \Rightarrow$

$\Rightarrow lm(g_i)$ διαιρεί κάποιο μονώνυμο του r. Άτοπο αφού r ανάγωγο

ή

$lm(g_i)$ διαιρεί κάποιο μονώνυμο του r_1. Άτοπο αφού r ανάγωγο.

Καταλήξαμε σε άτοπο γενικά, άρα $r = r_1 : f \xrightarrow{G}_+ r$

Άσκηση: Να υπολογίσετε μια βάση και την διάσταση του K-διανυσματικού χώρου

$K[x,y]/I$ όπου $I = \langle x^2y + xy^2 + 1,\ x^3 - 1 \rangle$

Λύση: Πρέπει να υπολογίσω αρχικά μια βάση Gröbner.
Διαλέγω την λεξικογραφική διάταξη: lex $y > x$

Με καθοδηγεί η άσκηση στο να επιλέξω $y>x$ γιατί έτσι x^3 και θα είναι πιο μικρό άρα θα κάνω λιγότερους υπολογισμούς. Ουσιαστικά και $x>y$ να επέλεγα θα έβγαζα ίδια διάσταση αλλά διαφορετική βάση Gröbner.

Έχουμε: $f_1 = xy^2 + x^2y + 1$, $f_2 = x^3 - 1$ → καλά διατεταγμένο γιατί το 1 είναι το πιο μικρό από όλα

και θα κάνουμε αλγόριθμο Buchberger:

f_1, f_2, $f_3 = y^2 + xy + x^2$	~~$S(f_1,f_2)$~~, $S(f_1,f_3)$, ~~$S(f_2,f_3)$~~

$$S(f_1,f_2) = \frac{x^3y^2}{xy^2}(xy^2 + x^2y + 1) - \frac{x^3y^2}{x^3}(x^3-1) = x^4y + x^2 + y^2 = \underset{\text{διάταξη}}{y^2 + x^4y + x^2} \xrightarrow{f_2}$$

$$\longrightarrow y^2 + x^4y + x^2 - \frac{x^4y}{x^3}(x^3-1) = y^2 + xy + x^2$$ άρα $f_3 = y^2 + xy + x^2$.

$S(f_2,f_3) \xrightarrow{f_2,f_3}_{+} 0$ γιατί μκδ$(x^3, y^2) = 1$.

$$S(f_1,f_3) = \frac{xy^2}{xy^2}(xy^2 + x^2y + 1) - \frac{xy^2}{y^2}(y^2 + xy + x^2) = x^2y + 1 - x^2y - x^3 = -x^3 + 1 \xrightarrow{f_2} 0$$

Άρα $f_1 = xy^2 + x^2y + 1$, $f_2 = x^3 - 1$, $f_3 = y^2 + xy + x^2$ βάση Gröbner.

Μπορώ να την κάνω ελαχιστική. Παρατηρώ ότι $y^2 \mid xy^2$, άρα η ελαχιστική βάση Gröbner είναι η f_2, f_3 γιατί $x^3 \nmid y^2$ και $y^2 \nmid x^3$. Είναι και ανηγμένη γιατί το x^3 και το y^2 δεν διαιρεί τίποτα

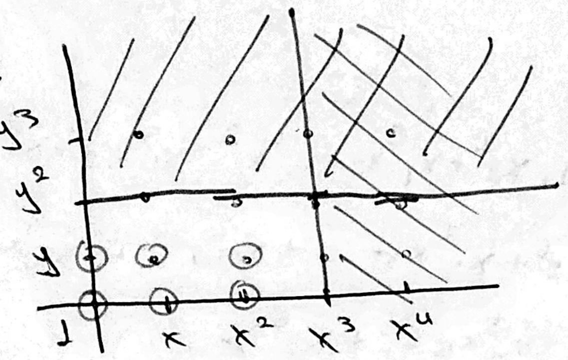
Πηγαίνουμε τώρα στον δακτύλιο πηλίκο:

$\{M+I \mid M \notin lt(I)\}$ είναι βάση του $K[x,y]/I$.

$\|$

$\{M+I \mid M \notin \langle x^3, y^2 \rangle\}$ $\rightsquigarrow$ είναι στο επίπεδο

Γεωμετρικά:



Άρα $\{1+I,\ x+I,\ x^2+I,\ y+I,\ xy+I,\ x^2y+I\} = \{M+I \mid M \notin lt(I)\}$

$$\boxed{\dim K[x,y]/I = 6.}$$

Άρα αυτά δεν είναι βάση Gröbner, είναι βάση διανυσματικού χώρου.

Άσκηση: Έστω $f = 2x^3y^5z^4 + 3x^7y^7 + x^8y^3z \in \mathbb{Z}_{17}[x,y,z]$

Δείξτε ότι δεν υπάρχει μονωνυμική διάταξη του $\mathbb{Z}_{17}[x,y,z]$ με $lt(f) = 2x^3y^5z^4$

Λύση: Έστω ότι υπάρχει τέτοια μονωνυμική διάταξη:

$x^3y^5z^4 > y^7z^7$ και $x^3y^5z^4 > x^8y^3z$

$\Downarrow$

$x^3 > y^2z^3$

γιατί αν $x^3 < y^2z^3$ θα ήταν $x^3y^5z^4 < \cancel{y^7z^7}$ άτοπο!

$\Downarrow$

$y^2z^3 > x^5$

γιατί αν $x^5 > y^2z^3$ θα ήταν $x^3y^5z^4 < x^8y^3z$ άτοπο!

Μπορώ και να πολ/ω και να διαιρέσω ένα μονώνυμο με ένα άλλο αρκεί να μην μου βγει αρνητικό

Δηλαδή $x^3 > y^2z^3 > x^5 \Rightarrow x^3 > x^5 \Rightarrow 1 > x^2$ Άτοπο!

Άσκηση:

$G = (V, E)$

$V = \{v_1, v_2, v_3, v_4, v_5\}$

$E = \{ \{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_1, v_5\}, \{v_4, v_5\} \}$

χρωματίζεται με 7 χρώματα;

Λύση: $I_G \subseteq \mathbb{C}[x_1, x_2, x_3, x_4, x_5]$

$$I_G = \langle x_1^7 - 1, x_2^7 - 1, x_3^7 - 1, x_4^7 - 1, x_5^7 - 1, x_1^6 + x_1^5 x_2 + x_1^4 x_2^2 + x_1^3 x_2^3 + x_1^2 x_2^3 + x_1 x_2^5 + x_2^6,$$

$$x_1^6 + x_1^5 x_3 + \dots + x_3^6, \quad x_2^6 + x_2^5 x_3 + \dots + x_3^6, \quad x_3^6 + x_3^5 x_4 + \dots + x_4^6,$$

$$x_1^6 + x_1^5 x_5 + \dots + x_5^6, \quad x_4^6 + x_4^5 x_5 + \dots + x_5^6 \rangle.$$

Το γράφημα αυτό έχει 5 κορυφές και 6 ακμές

Έχουμε περισσότερες ακμές από τις κορυφές

το ιδεώδες $I_G \neq \langle 1 \rangle$

Άρα και χρωματίζεται με 7 χρώματα.

...σκηση:

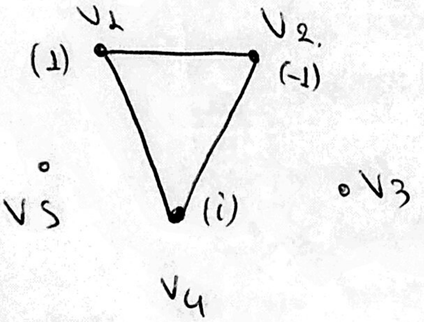
Το ιδεώδες:

$$I = \langle x_1^4 - 1, x_2^4 - 1, x_3^4 - 1, x_4^4 - 1, x_5^4 - 1, x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3,$$
$$x_1^3 + x_1^2 x_4 + x_1 x_4^2 + x_4^3, x_4^3 + x_4^2 x_2 + x_4 x_2^2 + x_2^3 \rangle.$$

Χρωματίζεται με 4 χρώματα;

Λύση:

Έχω 5 κορυφές και 3 ακμές.



Οι v5 και v3 χρωματίζονται με οποιοδήποτε χρώμα. Άρα χρωματίζεται με 3 χρώματα και με 4 χρώματα, όμως όχι με 2 λόγω του τριγώνου.

Δ Από τη στιγμή που γίνεται το σχήμα σημαίνει ότι $I_G \neq \langle 1 \rangle$; αν δεν μπορούσα να το κάνω τότε $I_G = \langle 1 \rangle$.

Άσκηση:

$$I = \langle x_1^{2017} - 2017x_7, x_2^{2016} - 2016x_7, x_3^{2015} - 2015x_7, x_4^{2014} - 2014x_7,$$
$$x_5^{2013} - 2013x_7, x_6^{2012} - 2012x_7, x_7 \rangle.$$

Γι' αυτό το ιδεώδες να υπολογίσετε μια ανάγωγη βάση Gröbner;

Λύση:

Θέλω να απλοποιήσω τους γεννήτορες. Το "κλειδί" είναι στο x_7.
Αν προσθέσω σε έναν γεννήτορα, έναν άλλον γεννήτορα, τότε δεν αλλάζει το ιδεώδες, παραμένει το ίδιο.

Διαλέγω οποιαδήποτε διάταξη με x_7 πιο μικρό:

lex $x_1 > x_2 > \dots > x_7$. Τα μεγιστοβάθμια όλα έχουν μκδ$=1$
Άρα όλα τα S πολυώνυμα $\to 0$ άρα βάση Gröbner. Είναι ελάχιστη

Είναι αναγωγή;

Όχι γιατί το x_7 διαιρεί πολλούς όρους.

Η αναγωγή είναι $\eta = x_1^{2017}, x_2^{2016}, x_3^{2015}, x_4^{2014}, x_5^{2013}, x_6^{2012}, x_7$.

Αν το πρόβλημα δεν επηρεάζεται από την διάταξη τότε έχω το δικαίωμα να αλλάξω διάταξη που να με βολεύει.