TD sur la séance Applications des bases de Gröbner

Frédéric Chyzak

Le 8 novembre 2006

1 Retour sur le résultant

Écrire une fonction qui calcule à un facteur entier près le résultant de deux polynômes P et Q de $\mathbb{Q}[X, Y]$ par rapport à l'indéterminée Y à l'aide d'une élimination par un calcul de base de Gröbner. (Ce calcul reste très proche de celui par algorithme d'Euclide naïf.)

2 Géométrie analytique et polynômes à coefficients trigonométriques

On considère la surface S paramétrée par

$$\begin{aligned} x &= (2 + \cos u) \cos t, \\ y &= (2 + \cos u) \sin t, \\ z &= \sin u, \end{aligned}$$

ainsi que la courbe C tracée sur S et paramétrée par

$$\begin{aligned} x &= (2 + \cos 2s) \cos 3s, \\ y &= (2 + \cos 2s) \sin 3s, \\ z &= \sin 2s. \end{aligned}$$

1. Obtenir une équation implicite de S.

2. Obtenir des équations implicites de C. On rappelle que

$$\cos 2x = 2\cos^2 x - 1, \qquad \sin 2x = 2 \cos x \sin x,$$
$$\cos 3x = 4 \cos^3 x - 3 \cos x, \qquad \sin 3x = 4 \cos^2 x \sin x - \sin x.$$

3. Vérifier à l'aide des équations implicites que la courbe C est tracée sur la surface S.

3 Ordres définis par des matrices de poids

On définit d'autres ordres monomiaux en se donnant des matrices de poids. Ces ordres plus généraux permettent de retrouver tous les ordres déjà vus.

Étant donnée une matrice inversible $W = (w_{i,j})_{1 \leq i,j \leq n}$, le poids d'un monôme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ est le vecteur colonne $W \cdot {}^{\mathrm{t}}(\alpha_1, \dots, \alpha_n)$. Deux monômes sont ensuite comparés en comparant lexicographiquement leurs poids respectifs. Autrement dit, pour comparer $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ et $X_1^{\beta_1} \dots X_n^{\beta_n}$: on compare

$$w_{1,1}\alpha_1 + \cdots + w_{1,n}\alpha_n \qquad \text{et} \qquad w_{1,1}\beta_1 + \cdots + w_{1,n}\beta_n \;;$$

si ces deux nombres sont différents, on statue sur l'ordre des monômes, sinon, on continue avec

$$w_{2,1}\alpha_1 + \cdots + w_{2,n}\alpha_n \qquad \text{et} \qquad w_{2,1}\beta_1 + \cdots + w_{2,n}\beta_n,$$

et ainsi de suite. La nature inversible de la matrice assure qu'on n'aura pas égalité jusqu'à la n-ième ligne.

Par exemple, l'ordre lexicographique $\prec_{\mathrm{lex}}$ est donné par la matrice identité, l'ordre lexicographique gradué $\prec_{\mathrm{grevlex}}$ est donné par la matrice

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & 0 & \dots & -1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & -1 & \dots & 0 & 0 \\ 0 & -1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

(première ligne et antidiagonale à 1).

1. Écrire une fonction qui prend en entrée un idéal et une permutation σ de $\{1, \dots, n\}$, donnée sous forme de séquence Magma, calcule la matrice de poids correspondant à l'ordre $\mathrm{lex}(X_{\sigma(1)}, \dots, X_{\sigma(n)})$, puis retourne la base de Gröbner pour cet ordre.

2. Écrire une autre fonction qui itère sur l'ensemble des permutations des variables d'un système de polynômes pour calculer toutes les bases lexicographiques en n'affichant que les monômes de tête de chaque polynôme.

3. Appliquer ces programmes les deux premiers systèmes donnés dans le fichier annexe (accessible depuis la page des TD). Les bases de Gröbner ainsi obtenues sont-elles toutes les mêmes ? Le nombre d'éléments dans chaque base est-il toujous le même ? Le même jeu de monômes de tête peut-il être obtenu pour deux ordres différents ? La même base de Gröbner peut-elle être obtenue pour deux ordres différents ?

4. Appliquer le programme sur le troisième système du fichier. Que se passe-t-il ?

5. Modifier le programme pour calculer avec les ordres $\mathrm{grlex}(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ au lieu des ordres lexicographiques, puis relancer le calcul.

4 Polynômes symétriques

On sait que tout polynôme symétrique de n indéterminées peut se récrire à l'aide des polynômes symétriques élémentaires

$$\begin{aligned}
&e_1 = X_1 + \cdots + X_n,\\
&e_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n,\\
&\ldots\\
&e_n = X_1 \ldots X_n,
\end{aligned}$$

donnés par la formule de Newton

$$(U - X_1) \ldots (U - X_n) = U^n - e_1U^{n-1} + \cdots + (-1)^n e_n.$$

Pour simplifier, on pourra traiter l'exercice en se fixant une petite valeur pour n ($n = 3, 4$). (L'exercice est assez technique pour un n générique.)

1. Introduire l'algèbre de polynômes en les indéterminées $X_1, \ldots, X_n, S_1, \ldots, S_n$. Les calculs qui vont suivre viseront à éliminer les X_i. Déterminer une base de Gröbner de l'idéal engendré par les polynômes $S_1 - e_1, \ldots, S_n - e_n$.

2. Exprimer maintenant le polynôme symétrique

$$(X_1^5 + X_2^5)(X_1^5 + X_3^5) \ldots (X_{n-1}^5 + X_n^5) = \prod_{1 \leq i < j \leq n} \left(X_i^5 + X_j^5\right)$$

en termes des polynômes symétriques élémentaires $e_1, \ldots, e_n$.

5 Optimisation d'une fonction polynomiale sur la sphère et résolution de systèmes polynomiaux

On s'intéresse à calculer le lieu des valeurs extrêmes de la fonction polynomiale

$$\phi : (x, y, z) \mapsto x^3 + 2xyz - z^2$$

sur la sphère de rayon 1 centrée à l'origine, donnée par l'annulation de la fonction puissance analytique

$$s : (x, y, z) \mapsto x^2 + y^2 + z^2 - 1.$$

Par la méthode du multiplicateur de Lagrange, ces extrêmes sont aux points où les gradients des fonctions ϕ et s sont colinéaires. Autrement dit, on a à déterminer les triplets (x, y, z) où il existe un t tel que

$$\begin{aligned}
\frac{\partial \phi}{\partial x}(x, y, z) &= t\frac{\partial s}{\partial x}(x, y, z),\\
\frac{\partial \phi}{\partial y}(x, y, z) &= t\frac{\partial s}{\partial y}(x, y, z),\\
\frac{\partial \phi}{\partial z}(x, y, z) &= t\frac{\partial s}{\partial z}(x, y, z),\\
s &= 0.
\end{aligned}$$

Cet exercice demandant de résoudre des polynômes d'une indéterminée, on se placera sur une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$. Tous les calculs se feront pour l'ordre lexicographique. On s'intéresse à calculer un lieu géométrique, aussi va-t-on négliger toute multiplicité éventuelle des zéros de polynômes d'une variable.

1. Éliminer l'indéterminée T de l'idéal engendré par les polynômes donnés par le système d'équations ci-dessus.

2. Écrire une fonction qui, prenant en entrée un idéal I de $\bar{\mathbb{Q}}[X_1, \ldots, X_n]$ et un entier k tel que I ne fasse intervenir que $X_1, \ldots, X_k$, calculera par une élimination un polynôme de la variable X_k dont les k-ièmes coordonnées des solutions du système doivent être solution.

3. Prolonger la fonction de la question précédente en résolvant ce polynôme dans $\bar{\mathbb{Q}}$ et en produisant successivement tous les idéaux obtenus par évaluation de X_k en une racine. Observer que chacun de ces idéaux (que l'on demande seulement d'afficher) ne fait intervenir que $X_1, \ldots, X_{k-1}$.

4. Enfin, rendre la fonction récursive pour qu'elle renvoie l'ensemble de toutes les solutions de l'idéal en entrée, chaque solution étant représentée comme une liste de coordonnées. Pour ce faire, pour chaque idéal calculé à la question précédente, on calculera récursivement ses solutions, de longueur $k - 1$, que l'on prolongera en listes de longueur k.