Devoir en temps libre d'algorithmique
à rendre le mardi 26 octobre 1999

Bases de Gröbner

Soit K un corps commutatif, par exemple celui des réels. On se place dans l'anneau des polynômes à plusieurs variables $K[X_1, \ldots, X_n]$. Rappelons qu'un polynôme f s'écrit de manière unique comme une somme finie $\sum a_i m_i$ où les a_i sont des éléments non nuls de K, les m_i sont distincts, chaque m_i étant un monôme $X_1^{k_1} \cdots X_n^{k_n}$ où les k_i sont des entiers strictement positifs. Le degré d'un tel monôme est $\sum k_j$. On dit que a_i est le coefficient de m_i dans f. On note (idéal engendré) :

$$\langle f_1, \ldots, f_k \rangle = \{f_1 g_1 + \cdots + f_k g_k \mid g_1, \ldots, g_k \in K[X_1, \ldots, X_n]\} .$$

Si J est un idéal (i.e. un sous-ensemble clos par addition et par multiplication par un polynôme quelconque) on note $g \equiv_J h$ si et seulement si $g - h \in J$.

Le problème est : étant donné $J = \langle f_1, \ldots, f_k \rangle$ décider $\equiv_J$, i.e. trouver un algorithme qui prend deux polynômes g et h en entrée et renvoie OUI si $g \equiv_J h$ et NON si $g \not\equiv_J h$. Cela revient à se demander si $g - h \equiv_J 0$. La technique employée est la réécriture. Le principe est le suivant. Supposons que $J = \langle f \rangle$. Si f est un polynôme dans lequel apparaît un monôme m_1 avec le coefficient a on peut "couper" f en am_1 et $\hat{f} = f - am_1$. On a $am_1 \equiv_J -\hat{f}$ que l'on regarde comme une règle de réécriture (ou de calcul) $am_1 \rightarrow -\hat{f}$. On applique cette règle de la manière suivante: si $g = bm_1m_2 + g_1$ est un polynôme dont l'un des monômes est divisé par m_1, on écrit

$$g \rightarrow g' = -(b/a)\hat{f}m_2 + g_1 .$$

On a $g \equiv_J g'$ (car $g' = g - (b/a)fm_2$) avec g' "plus simple" pour peu que l'on ait choisi m_1 "maximal" dans f. On dit que m_1m_2 est le pivot de la réduction. Il faut donc définir un ordre sur les monômes. En voici un ($>_{lex}$ est l'ordre lexicographique) :

$$X_1^{k_1} \cdots X_n^{k_n} \succ X_1^{l_1} \cdots X_n^{l_n} \Leftrightarrow \begin{cases} (\sum k_j > \sum l_j) \text{ ou} \\ (\sum k_j = \sum l_j) \text{ et } ((k_1, \ldots, k_n) >_{lex} (l_1, \ldots, l_n)) . \end{cases}$$

(A) Montrer que $\succ$ est bien fondé (pas de suite infinie strictement décroissante).

Soit f un polynôme. On note $H(f)$ son plus grand monôme (selon $\succ$). On supposera toujours sans perte de généralité que le coefficient de $H(f)$ dans f est 1 (soit $a = 1$ ci-dessus). On pose $R(f) = f - H(f)$. On note $\rightarrow_f$ la relation $\rightarrow$ de ci-dessus obtenue avec ce découpage de f, soit :

$$g + bH(f)m \ \rightarrow_f \ g - bR(f)m$$

Si $G = \{f_1, \ldots, f_k\}$ on note $\rightarrow_G = \bigcup \rightarrow_{f_i}$. Soulignons que $\rightarrow_G$ dépend du choix des générateurs $f_1, \ldots, f_k$ de $J = \langle f_1, \ldots, f_k \rangle$ (cf. la distinction entre un espace vectoriel et une base particulière de cet espace).

(B) Soit $G = \{f_1, \ldots, f_k\}$ et $J = \langle f_1, \ldots, f_k \rangle$. Montrer que $\equiv_J$ est la clôture réflexive, symétrique et transitive $\leftrightarrow^*_G$ de $\rightarrow_G$.

(C) Montrer que la relation $\rightarrow_G$ est bien fondée.

On pose ensuite la définition suivante : $G = \{f_1, \ldots, f_k\}$ est appelé base de Gröbner (pour $J = \langle f_1, \ldots f_k \rangle$) si $\rightarrow_G$ est confluent, i.e. si

$$\forall f, g, h \ \ ((f \ \rightarrow^*_G \ g \text{ et } f \ \rightarrow^*_G \ h) \Rightarrow (\exists k \ \ g \ \rightarrow^*_G \ k \text{ et } h \ \rightarrow^*_G \ k)) \ .$$

Les deux résultats qui suivent sont des lemmes généraux.

(D1) Montrer que si $\rightarrow_G$ est confluent alors pour tous f et g si $f \ \leftrightarrow^*_G \ g$ alors f et g ont un réduit commun.

(D2) Montrer que la bonne fondation de $\rightarrow_G$ implique que $\rightarrow_G$ est confluente si et seulement si la propriété suivante (appelée confluence locale) est vérifiée:

$$\forall f, g, h \ \ ((f \ \rightarrow_G \ g \text{ et } f \ \rightarrow_G \ h) \Rightarrow (\exists k \ \ g \ \rightarrow^*_G \ k \text{ et } h \ \rightarrow^*_G \ k))$$

(un seul pas de réduction dans chacune des hypothèses).

On retourne aux polynômes. La question suivante montre l'intérêt des bases de Gröbner.

(E1) Montrer que si $G = \{f_1, \ldots, f_n\}$ est une base de Gröbner pour $J = \langle f_1, \ldots, f_k \rangle$, alors $\equiv_J$ est décidable.

(E2) Trouver des polynômes f_1, f_2 tels que $\{f_1, f_2\}$ ne soit pas une base de Gröbner.

(E3) Pour tous g_1, g_2 on pose $S(g_1, g_2) = m_1 g_1 - m_2 g_2$ où m_1 et m_2 sont tels que $m_1 H(g_1) = m_2 H(g_2)$ est le plus petit commun multiple de $H(g_1)$ et $H(g_2)$. Montrer que $G = \{f_1, \ldots, f_k\}$ est une base de Gröbner si et seulement si $(S(f_i, f_j) \ \to_G^\star \ 0)$ pour toutes les paires i, j.

L'étape finale du problème consiste à trouver une base de Gröbner pour un idéal donné $J = \langle f_1, \ldots, f_k \rangle$. Si $\{f_1, \ldots, f_k\}$ satisfait déjà le critère (E3) il n'y a rien à faire. Sinon on utilise l'algorithme suivant. On pose $(G_0, B_0) = (\{f_1, \ldots, f_k\}, \{(f_l, f_r) \mid 1 \leq l < r \leq k\})$ et on définit le système formel suivant ($\underline{h}$ désigne le polynôme kh ($k \in K$) tel que le coefficient du monôme de tête ait le coefficient 1) :

$$\frac{(f_l, f_r) \in B \quad S(f_l, f_r) \ \to_G^\star \ h \ \neq 0 \text{ et irréductible pour } \to_G}{(G, B) \ \longrightarrow \ (G \cup \{\underline{h}\}, B \cup \{(\underline{h}, f) \mid f \in G\} \setminus \{(f_l, f_r)\})}$$

$$\frac{(f_l, f_r) \in B \quad S(f_l, f_r) \ \to_G^\star \ 0}{(G, B) \ \longrightarrow \ (G, B \setminus \{(f_l, f_r)\})}$$

(F1) Montrer que si $(G, B) = (G_p, B_p)$ est une forme normale de (G_0, B_0) pour ce système alors G est une base de Gröbner pour J.

(F2) Montrer que le système termine toujours en admettant le résultat suivant (objet de la question (G)) : si $m_1, \ldots, m_n, \ldots$ est une suite infinie de monômes alors il existe $i < j$ tel que m_i divise m_j.

Pour prouver la propriété utilisée en (F2) il reste un petit peu de travail et cela passe par la notion de bon ordre partiel. Un bon ordre partiel est un ensemble ordonné X tel que pour toute suite infinie $x_1, \ldots, x_n, \ldots$ d'éléments de X il existe i, j tels que $i < j$ et $x_i \leq x_j$. Cette propriété implique la bonne fondation, car s'il existait une suite $x_1, \ldots, x_n, \ldots$ telle que $x_n > x_{n+1}$ pour tout n alors on ne pourrait avoir $i < j$ tels que $x_i \leq x_j$ (antisymétrie de $\leq$). Réciproquement si l'ordre est total il est facile de voir que la bonne fondation implique la propriété de bon ordre partiel.

Si X et Y sont des ordres partiels l'ordre produit sur $X \times Y$ est défini par $(x_1, y_1) \leq (x_2, y_2)$ si et seulement si $x_1 \leq x_2$ et $y_1 \leq y_2$. Il est facile de voir que si X et Y sont bien fondés alors $X \times Y$ est bien fondé. Mais c'est le résultat plus fort que $X \times Y$ est un bon ordre partiel qui nous intéresse (noter que si X et Y sont des ordres totaux, $X \times Y$ n'est pas total sauf cas trivial: $(3, 5)$ versus $(4, 2)$).

(G1) Montrer que dans un bon ordre partiel X tout suite infinie $x_1, \ldots, x_n, \ldots$ admet une sous-suite croissante $x_{i_1} \leq \cdots \leq x_{i_n} \leq \cdots$.

(G2) Prouver que si X et Y sont des bons ordres partiels alors $X \times Y$ est un bon ordre partiel.

(G3) Prouver l'hypothèse faite dans la question (F2).