Algorithmique et Programmation
TD n° 12 : Systèmes d'équations polynomiales

Ecole normale supérieure
Département d'informatique
td-algo@di.ens.fr

2012-2013

1 Rappel

- Un idéal I est (dans notre contexte) un ensemble de polynômes en n variables tel que
  - *i)* $0 \in I$
  - *ii)* $\forall x, y \in I, x + y \in I$
  - *iii)* $\forall x \in I, \forall y \in \mathbb{K}[x_1, \ldots, x_n], xy \in I$
- L'idéal engendré par $F = \{f_1, \ldots, f_n\}$ est le plus petit idéal contenant F. C'est en fait l'ensemble des combinaisons polynomiales des f_i. On le note parfois $\langle f_1, \ldots, f_s \rangle$.
- Étant donné un polynôme $f \in \mathbb{K}[x_1, \ldots, x_n]$, on note $LT(f)$ le terme de tête de f, c'est-à-dire le monôme de f (avec son coefficient dans $\mathbb{K}$) qui est le plus grand pour l'ordre sur les monômes qu'on utilise.
- Si I est un idéal, alors on note $LT(I) = \{LT(f) \mid f \in I\}$.
- Un ensemble fini de polynômes G est une base de Gröbner de l'idéal I si a) I est engendré par G et b) L'idéal $< LT(I) >$ est engendré par $LT(g_1), \ldots, LT(g_s)$. Tous les idéaux admettent une base de Gröbner.

2 Division de Polynômes multivaries et bases de Gröbner

Exercice 1 : Division de Polynômes multivariés.

1. Donnez l'algorithme de la division euclidienne des polynômes à une variable (qui écrit $f = q \cdot g + r$ où $\deg r \leq \deg g$).
2. Proposez une généralisation multivariée évidente de l'algorithme précédent. On suppose qu'on nous donne un ordre admissible sur les monômes. Donnez un algorithme qui, étant donné une famille $g_1, \ldots, g_s$ de polynômes en n variables, écrit :

   $$f = a_1 \cdot g_1 + \cdots + a_s \cdot g_s + r$$

   où les a_i et r sont des polynômes multivariés, et où r satisfait des conditions raisonnables de non-divisibilité par les g_i qu'il vous faudra préciser.

Dans toute la suite on note $\overline{f}^G$ le reste donné par l'algorithme de division multivarié en divisant f par $G = \{g_1, \ldots, g_s\}$

3. Calculez la division de $f = x^7y^2 + x^3y^2 - y + 1$ par $g_1 = xy^2 - x$ et $g_2 = x - y^3$, en utilisant l'ordre lexicographique, puis l'ordre grevlex (le tout avec $x > y$).
4. Démontrez que le reste r dépend de l'ordre des g_i. Donnez un exemple.
5. Démontrez que r est unique si $G = \{g_1, \ldots, g_s\}$ est une base de Gröbner (d'un idéal I). Déduisez-en un algorithme pour tester l'appartenance à un idéal de polynômes multivariés.
6. Déduisez-en les propriétés suivantes des bases de Gröbner : a) la division de tout polynôme $f \in I$ par G donne zéro, et b) le terme de tête de n'importe quel polynôme de I est divisible par le terme de tête d'un g_i.
7. Déduisez-en le résultat suivant : étant donné un polynôme f arbitraire, on peut écrire $f = g + r$, où $g \in I$, et aucun monôme de r n'est divisible par le terme de tête d'un polynôme de I. En d'autres termes, le "reste de la division de f par l'idéal I" est bien défini.

Exercice 2 : Autour de l'algorithme de Buchberger.

On rappelle l'algorithme de Buchberger

function BUCHBERGER($f_1, \ldots, f_t$)
  $G \leftarrow F$
  repeat
    $G' \leftarrow G$
    for all pair $p \neq q$ in G' **do**
      $S \leftarrow \overline{\mathrm{Spol}(p,q)}^{G}$
      if $S \neq 0$ **then** $G \leftarrow G \cup \{S\}$
    end for
  until $G = G'$
  return G
end function

On admettra que l'algorithme termine et qu'il renvoie une base de Gröbner (non-minimale, non-réduite).

1. Un polynôme est dit homogène si tous ses monômes sont de même degré. Un idéal est dit homogène s'il possède un ensemble de générateurs homogènes. Démontrez qu'il possède alors une base de Gröbner formée de polynômes homogènes.
2. La description de l'algorithme de Buchberger donnée ici est volontairement très très très simplifiée. Par exemple, que se passe-t-il lorsqu'on choisi une paire $\{p, q\}$ pour la deuxième fois ? Commment améliorer cet aspect des choses ?
3. Que se passe-t-il si on lance l'algorithme de Buchberger sur un ensemble de polynômes en n variables, mais de degré 1 ?

Exercice 3 : . Une base de Groebner G d'un ideal I est dite réduite si

-$LC(p) = 1$ pour tout $p \in G$.

-Pour tout $p \in G$, les monômes de p ne sont pas dans $< LT(G - \{p\}) >$.

1. Prouver que si G et G' sont deux bases de Groebner réduites, alors $LT(G) = LT(G')$. En déduire que s'il existe une base réduite, alors elle est unique.
2. Soit $A = (a_{ij})$ une matrice $n \times m$ à coefficients dans un corps k et soit $f_i = a_{i1}x_1 + \ldots + a_{im}x_m$ les polynômes linéaires dans $k[x_1, \ldots x_m]$ déterminés par les coefficients de A. Soit $B = (b_{ij})$ la forme échelon réduite de A et soit $g_1, \ldots g_t$ les polynômes linéaires associés aux lignes non-nules de B ($t \leq n$). Montrer que $g_1, \ldots g_t$ est la base réduite de l'ideal $\langle f_1, \ldots f_n \rangle$.