TD 13 : Bases de Gröbner et complétion

{lionel.rieg,paolo.tranquilli}@ens-lyon.fr

Exercice 1. *Complétion*

1. Rappeler le lemme de Newman et celui de Knuth-Bendix.

2. En déduire une méthode pour transformer un système de réécriture noethérien en système de réécriture confluent. C'est l'idée qui sous-tend l'algorithme de complétion de Knuth-Bendix.

3. Adapter cet algorithme pour calculer des formes normales modulo un ensemble d'égalités. Quel type d'égalités peut poser problème ? Que se passe-t-il dans ce cas ?

Exercice 2. *Bases de Gröbner et algorithme de Buchberger*

Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est principal et tout idéal est engendré par le pgcd de ses polynômes générateurs. Ainsi, l'idéal $\left\langle X^3 - X, X^3 + 1 \right\rangle$ est engendré par $\mathrm{pgcd}(X^3 - X, X^3 + 1) = X + 1$: $\left\langle X^3 - X, X^3 + 1 \right\rangle = \langle X + 1 \rangle = (X + 1)\mathbb{K}[X]$. En revanche, il n'en est pas de même pour les polynômes multi-variés.

1. Si on prend l'idéal $\mathcal{I}$ généré par $\left\{ X^2Y - Y, XY^2 - X \right\}$, donner un polynôme admettant deux restes modulo $\mathcal{I}$ premiers entre eux.

Un ordre $\prec$ sur les monômes est dit *admissible* si

a) il est total,

b) il contient l'ordre divise sur les monômes : $m_1 | m_2 \implies m_1 \preceq m_2$,

c) il est compatible avec le produit : $m_1 \prec m_2 \implies m \cdot m_1 \prec m \cdot m_2$.

2. Montrer que l'ordre *divise* est un bel ordre, c.-à-d. que pour toute suite de monômes $(m_i)_{i \in \mathbb{N}}$, il existe deux indices $i < j$ tels que $m_i | m_j$.

3. Montrer qu'un ordre admissible est nœthérien.

Etant donné un polynôme f, on définit :
– le monôme de tête t_f, c'est le plus grand monôme de f pour l'ordre $\prec$
– le coefficient de tête c_f, c'est le coefficient de t_f dans f
– le reliquat du polynôme $r_f = f - c_f t_f$.
Pour simplifier, on supposera dans la suite qu'aucun des polynômes f_i n'est nul.
Si f est un polynôme unitaire, alors on définit une règle de réduction $t_f \xrightarrow{f} -r_f$, qui oriente l'égalité $t_f = -r_f$ de $\mathbb{K}[\vec{X}]/\langle f \rangle$.
Si $F = \{ f_1, \ldots, f_k \}$, alors on pose

$$\xrightarrow{F} = \bigcup_{i=1}^{k} \xrightarrow{f_i} = \xrightarrow{f_1} \cup \cdots \cup \xrightarrow{f_k}$$

4. Soient $f, g, g', h \in \mathbb{K}[X_1, \dots, X_n]$ avec f unitaire, m un monôme et b dans $\mathbb{K}^*$. Montrer les trois propriétés suivantes :

a) $f \xrightarrow{f} 0$

b) $g \xrightarrow{f} g' \implies bm \cdot g \xrightarrow{f} bm \cdot g'$

c) $g \xrightarrow{f} g' \implies h + g \xrightarrow{f} h + g'$

Une base de Gröbner G est un ensemble fini de polynômes générateurs d'un idéal $\mathcal{I}$ qui permet de décider l'appartenance à $\mathcal{I}$ et assure l'unicité du résidu modulo $\mathcal{I}$. La propriété qui la caractérise est que l'ensemble $\{ t_g \mid g \in G \}$ engendre l'idéal $\{ t_f \mid f \in \mathcal{I} \}$, ce qui implique en particulier que G engendre $\mathcal{I}$.
Elle peut être calculée par l'algorithme de Buchberger donné ci-dessous.

Données – Un ensemble fini de polynômes unitaires $F = \{ f_1, \dots, f_k \}$
– Un ordre admissible

Résultat Un ensemble fini de polynômes G_i qui est une base de Gröbner de $\langle f_1, \dots, f_k \rangle$.

i := 0 ;
G_0 := F ;
$B_0 := \{ \{f, g\} \subset F \mid f \neq g \}$;
Tant que $B_i = \emptyset$, faire
  Choisir une paire $\{f, g\} \in B_i$,
  Calculer le S-polynôme $S(f, g)$,
  Calculer une $\xrightarrow{G_i}$ forme normale h de $S(f, g)$,
  Si $h \neq 0$, alors
    $B_{i+1} := (B_i \setminus \{ \{f, g\} \}) \cup \{ \{ k, c_h^{-1} h \} \mid k \in G_i \}$;
    $G_{i+1} := G_i \cup \{ c_h^{-1} h \}$;
    i := i + 1;
  Si $h = 0$, alors
    $B_{i+1} := B_i \setminus \{ \{f, g\} \}$;
    $G_{i+1} := G_i$;
    i := i + 1.
Retourne G_i

où le S-polynôme $S(f, g)$ est la différence des réduits de la plus petite paire critique des règles $\xrightarrow{f}$ et $\xrightarrow{g}$.

5. Calculer $S(f, g)$ en fonction de f et g.

6. Appliquez l'algorithme de Buchberger pour calculer une base de Gröbner de l'ensemble de polynômes $\{ X^2Y - Y, XY^2 - X \}$.

7. Le polynôme $Y^5 - Y^3$ appartient-il à l'idéal engendré par $\{ X^2Y - Y, XY^2 - X \}$? On donnera une démonstration fondée sur la base de Gröbner calculée à la question précédente.

8. Montrer que l'algorithme de Buchberger retourne une base de Gröbner. Est-elle optimale ? Peut-on faire mieux ?

9. Montrer que l'algorithme de Buchberger termine. Quelle est sa complexité ?