Réécriture : Réduction polynômiale et Bases de Gröbner

Laure Danthony

D'après le cours de Pierre Lescanne, avril 2001

Table des matières

1 Le cadre de l'étude

On se place sur l'anneau des polynômes à plusieurs indéterminées sur un corps $\mathbb{K}$, c'est à dire que l'on considère les éléments de $\mathbb{K}[X_1, \ldots, X_n]$. Un tel polynôme s'écrit par exemple $X_1X_2^2 - 2X_1X_2$.

DÉFINITION 1 (IDÉAL)
Un idéal est un ensemble J non vide de polynômes de $\mathbb{K}[X_1, \ldots, X_n]$ vérifiant :

- si f et g sont dans J, alors $f + g$ est dans J.
- si $f \in J$ et $g \in K[X_1, \ldots, X_n$ alors $f.g \in J$.

La question qui se pose (notamment pour des recherches de zéros de polynômes) est : étant donnés un polynôme r et un idéal J, est-ce-que $r \in J$?
Pour résoudre ce problème, on va présenter J sous la forme d'un ensemble de règles de réécriture R tel que $r \in J \Leftrightarrow r \xrightarrow[R]{*} 0$, ce qui est plus facile à vérifier.

2 Idéal engendré et congruence

DÉFINITION 2 (IDÉAL ENGENDRÉ)
L'**idéal engendré** par $f_1, f_2, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_k]$ est l'ensemble :

$$< f_1, \ldots, f_k >= \{f_1.g_1 + f_2.g_2 + \ldots + f_k.g_k | g_1, \ldots g_k \in \mathbb{K}[X_1, \ldots X_k]\}.$$

On sait que c'est le plus petit idéal contenant les f_i.

DÉFINITION 3 (CONGRUENCE D'IDÉAL)
Etant donné un idéal J, on définit la congruence $\equiv_J$ par $f \equiv_J g \Leftrightarrow f - g \in J$.

On a donc à ce stade réduit le problème d'appartenance à un idéal au problème de la congruence à 0, ce qui est déjà un peu plus simple.

3 Notion d'ordre admissible

Appelons $M_n = \{X_1^{k_1} \ldots X_n^{k_n} | k_1, \ldots, k_n \in \mathbb{N}\}$ l'ensemble des monômes de $\mathbb{K}[X_1, \ldots, X_n]$.

DÉFINITION 4 (ORDRE ADMISSIBLE)
Un ordre $\prec$ total sur M_n est dit **admissible** si :

1. $m_1 | m_2 \Rightarrow m_1 \preceq m_2$ (il contient l'ordre de divisibilité) ;
2. il est compatible avec la multiplication : $m_1 \prec m_1 \Rightarrow m.m_1 \prec m.m_2$ $(\forall m)$.

EXEMPLE 1 *On montre facilement que l'ordre défini par :*
$X_1^{k_1} \ldots X_n^{k_n} > X_1^{l_1} \ldots X_n^{l_n}$ *ssi :*

- $\sum_{i=1}^{n} k_i > \sum_{i=1}^{n} l_i$ *ou*
- $\sum_{i=1}^{n} k_i = \sum_{i=1}^{n} l_i$ *et* $(k_1, \ldots k_n) >_{lex} (l_1, \ldots l_n)$.

est un ordre total admissible sur M_n.

LEMME 1 *Tout ordre admissible termine.*

Dans la suite on supposera un ordre admissible fixé. De plus, on fait les restrictions suivantes :

- les polynômes considérés seront non nuls, car si l'un des f_i est nul, on peut le supprimer et l'idéal engendré sera inchangé.
- les polynômes engendrant seront normalisés, *i.e.* leur terme de plus haut degré aura pour coefficient 1, en effet, on a $< f_1, \ldots, f_k >=< c_{f_1}^{-1} f_1, \ldots, f_k >$ si c_{f_1} est le coefficient du terme dominant de f_1. On peut évidemment faire de même pour les autres f_i.

4 Construction des règles de réécriture à l'aide des f_i

Dans un premier temps, étant donné un polynôme f normalisé (qui joue le rôle d'un des f_i), on l'écrit sous la forme : $f = t_f + r_f$, t_k étant le monôme de tête et r_f le reste du polynôme. On construit la règle $t_f \xrightarrow[f]{} -r_f$. De la sorte on obtient : $g \xrightarrow[f]{} g'$ ssi :

- g contient un monôme m avec coefficient de tête $a \neq 0$;
- il existe un monôme m', tel que $m = t_f.m'$;
- g' s'écrit $g' = g - am'.f$.

EXEMPLE 2 *Le polynôme $X_1^2X_2 - 2X_1X_2 + 3X_2$ induit la règle $X_1^2X_2 \to 2X_1X_2 - 3X_2$. Si l'on veut réduire $2X_1^2X_2^2 + 2X_1X_2^2 + X_1X_2$, on remplace $X_1^2X_2^2 = X_2(X_1^2X_2)$ par ce qu'il faut. Tous calculs faits, on obtient $6X_1X_2^2 - 6X_2^2 + X_1X_2$, ce qui est plus petit pour l'ordre naturel sur les polynômes à plusieurs indéterminées.*

On obtient plus ou moins facilement les résultats suivants :

PROPOSITION 1 *Si f, g, h désignent des polynômes, f étant normalisé :*

- $f \xrightarrow[f]{} 0$ *(rassurant !)*
- $g \xrightarrow[f]{} g' \Rightarrow bm.g \xrightarrow[f]{} bm.g'$ *($b \in \mathbb{K}^*$ et m monôme)*
- $g \xrightarrow[f]{} g' \Rightarrow h + g$ *et* $h + g'$ *ont même forme normale pour la réduction* $\xrightarrow[f]{}$

Ces résultats servent à montrer le :

THÉORÈME 1 *Si on note $F = \{f_1, \ldots, f_n\}$ et $J =< f_1, \ldots, f_n >$ alors on a :*

$$\equiv_J = \xleftrightarrow[F]{*}$$

Comme de plus, $\to_F$ termine toujours (autre résultat important), on a : si $\to_F$ est confluente, alors $\equiv_J$ est décidable, donc le problème de l'appartenance à un idéal aussi. On s'est donc ramené à un "simple" problème de confuence.

5 Bases de Gröbner

On a montré dans le paragraphe précédent que si l'idéal est engendré par un nombre fini de polynômes normalisés qui induisent un ensemble de règles qui est confluent, alors le problème de l'appartenance à un idéal est décidable, ce qui nous motive pour la définition suivante :

DÉFINITION 5
$G = \{f_1, \ldots, f_k\}$ est une **base de Gröbner** de l'idéal J si :

1. $J =< f_1, \ldots, f_k >$;

2. $\xrightarrow[G]{}$ est confluent.

Savoir calculer une base de Gröbner d'un idéal J est donc utile, comme cela on pourra vérifier d'un polynôme est dans l'idéal.

DÉFINITION 6 (S-POLYNÔMES)
Soient deux polynômes normalisés f et g, soit $m = ppcm(t_f, t_g)$. Soient m_f et m_g définis par $m = mf.t_f$ et $m = m_g.t_g$. Le **S-polynôme de f et g** est défini par :

$$S(f,g) = m_f.f - m_g.g$$

REMARQUE 1 Les S-polynômes jouent pour $\xrightarrow[G]{}$ le même rôle que les paires critiques pour une relation quelconque.

THÉORÈME 2 *Soit $G = \{f_1, \ldots, f_k\}$. G est une base de Gröbner de J engendré par les f_i : $J =< f_1, \ldots, f_n >$ ssi tous les S-polynômes de G se réduisent à 0.*

6 Algorithme de Buchberger

But : On se donne :

- Un ensemble fini de polynômes $\{f_1, ..., f_n\}$ de coefficient de tête 1.
- Un ordre admissible

On retournera : un ensemble fini de polynômes G_i qui est une base de Gröbner de $< f_1, ..., f_n >$.

Algorithme
Initialisation

- $i := 0$;
- $G_0 := F$;
- $B_0 := \{(f,g) \mid f, g \in F, f \neq g\}$;

Tant que $B_i \neq \emptyset$ 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
  - $B_{i+1} := (B_i - (f,g)) \cup \{(k, c_h^{-1}h) \mid k \in G_i\}$;
  - $G_{i+1} := G_i \cup \{c_h^{-1}h\}$;
  - $i := i + 1$;

- Si $h = 0$, alors
  - $B_{i+1} := (B_i - (f, g))$;
  - $G_{i+1} := G_i$;
  - $i := i + 1$.

Retourne G_i

THÉORÈME 3 *L'algorithme de Buchberger termine et renvoie une base de Gröbner.*