Réécriture

Bases de Gröbner

1 Les monômes à n-variables

Soit K un corps.
Un monôme est une formule $X_1^{d_1}...X_n^{d_n}$.
Le degré d'un monôme est

$$deg(X_1^{d_1}...X_n^{d_n}) = \sum_{i=1}^{n} d_i.$$

Un monôme affecté d'un coefficient $c \in K$ est une formule $cX_1^{d_1}...X_n^{d_n}$.

2 L'anneau des polynômes à n-variables sur K

Un polynôme P est une somme finie d'un ensemble[1] de monômes $\{m_1, ..., m_k\}$ affectés de coefficients :

$$P = \sum_{j=1}^{k} c_j m_j$$

C'est surtout un ensemble de paires $\{(c_1, m_1), ..., (c_k, m_k)\}$, sans répétition de m_i.

Les polynômes à coefficients dans K forment un anneau noté $K[X_1, ..., X_n]$, c'est l'anneau des polynômes à n-variables.

Exemple :
$X_1^2X_2 - 2X_1X_2 + 3X_2$ est un polynôme dont les monômes sont : $X_1^2X_2$, X_1X_2,X_2.

▶Remarquons que dans les polynômes en tant que formules, les $X_1, ..., X_n$ jouent le rôle de constantes.

3 Idéaux

- Un idéal est un sous-ensemble $J \subseteq K[X_1, ..., X_n]$ tel que
  1. $f, g \in J \implies f + g \in J$.

[1] pas d'un multiensemble, donc il ne doit pas y avoir de répétitions.

2. $f \in J$ et $g \in K[X_1, ..., X_n] \implies f \cdot g \in J$.

- L'idéal engendré par $f_1, ..., f_k \in K[X_1, ..., X_n]$ est l'ensemble

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

On démontre que c'est le plus petit idéal qui contient l'ensemble $\{f_1, ..., f_k\}$.

4 Liens entre congruences et idéaux

Une congruence est une relation d'équivalence $\equiv$ telle que
pour tous $g_1, g_2 \in K[X_1, ..., X_n]$,
$f_1 \equiv f_1'$ et $f_2 \equiv f_2' \implies f_1 \cdot g_1 + f_2 \cdot g_2 \equiv f_1' \cdot g_1 + f_2' \cdot g_2$.

▶ On a les résultats suivants :

- L'ensemble des polynômes congrus à 0 forment un idéal.
- Si J est un idéal, la relation $\equiv_J$ définie par

$$f \equiv_J \iff g \quad f - g \in J$$

est une congruence dont la classe de congruence du polynôme 0 est précisément J.

5 L'appartenance à un idéal

Le problème de l'appartenance à un idéal est le suivant

Instance : $f, f_1, ..., f_k \in K[X_1, ..., X_n]$

Question : Est-ce que $f \in \langle f_1, ..., f_k \rangle$?

6 Comment utiliser les congruences pour réduire ?

▶ Idée : puisque les idéaux sont liés aux congruences. On va d'abord parler en termes de congruences.

▶ Étant donné un polynôme f, pour savoir s'il appartient à un idéal, il suffit de trouver un «polynôme plus simple» et de tester l'appartenance à l'idéal sur ce polynôme plus simple.

▶ «Idéalement», 0 est bon candidat pour ce polynôme plus simple. Il faut donc utiliser les congruences pour réduire.

▶ On va voir que $f \in J \Leftrightarrow f \equiv_J 0$ et pour montrer $f \equiv_J 0$, on construit à l'aide des f_i un ensemble de règles $\xrightarrow[F]{}$ tel que $f \equiv_J 0 \Leftrightarrow f \xrightarrow[F]{*} 0$. Ce qui est plus facile à déterminer.

Question : Comment construire cet ensemble de règles ?

▶ Solution : Étant donné un idéal J qui contient un polynôme

$$f = \sum_{j=1}^{k} c_j m_j$$

congru à 0 et dont le monôme le plus «grand» est m_k, on a

$$m_k \equiv_J -c_k^{-1} \sum_{j=1}^{k-1} c_j m_j.$$

et on peut utiliser la règle

$$m_k \to -c_k^{-1} \sum_{j=1}^{k-1} c_j m_j.$$

Tout instance de m_k peut-être remplacée par $-c_k^{-1} \sum_{j=1}^{k-1} c_j m_j$.

Exemple ON considère $X_1^2X_2 - 2X_1X_2 + 3X_2$ Le monôme le plus grand est clairement $X_1^2X_2$ et la règle que l'on engendre est $X_1^2X_2 \to 2X_1X_2 - 3X_2$. Dans le polynôme $2X_1^2X_2^2 + 2X_1X_2^2 + X_1X_2$, cela revient à remplacer le monôme $X_1^2X_2^2 = (X_1^2X_2)X_2$ par $2X_1X_2^2 - 3X_2^2$, ce qui donne $4X_1X_2^2 - 6X_2^2 + 2X_1X_2^2 + X_1X_2$ soit encore $6X_1X_2^2 - 6X_2^2 + X_1X_2$, qui est «manifestement» plus simple.

7 Les ordres sur les monômes

Les ordres que l'on considère sont totaux,mais on a le choix entre plusieurs et c'est crucial pour l'efficacité de la complétion.

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

1. il est total,
2. il est contient l'ordre divise sur les monômes,

$$m_1 | m_2 \quad \Longrightarrow \quad m_1 \prec m_2,$$

3. il est compatible avec le produit :

$$m_1 \prec m_2 \quad \Longrightarrow \quad m \cdot m_1 \prec m \cdot m_2.$$

Lemme : Tout ordre admissible termine.

Démonstration :

- L'ordre divise sur les monômes est l'ordre produit (composante par composante) de l'ordre naturel sur $\mathbb{N}$.
- C'est donc un beau préordre.
- Donc comme les ordres admissibles contiennent un beau préordre, ils sont aussi de beaux préordres, donc ils terminent.

N. B. Ce résultat est parfois appelé le lemme de Dixon (1910).

Exemple : L'ordre défini par

1. $deg(X_1^{d_1}...X_n^{d_n}) > deg(X_1^{e_1}...X_n^{e_n})$,
2. ou $deg(X_1^{d_1}...X_n^{d_n}) = deg(X_1^{e_1}...X_n^{e_n})$ et $(d_1,...,d_n) >_{lex} (e_1,...,e_n)$.

est admissible.

8 Quelques définitions

On se donne un ordre admissible $\prec$. Étant donné un polynôme f, on définit

- le monôme de tête t_f, c'est le plus grand monôme pour l'ordre $\prec$ qui apparaît dans f,
- le coefficient de tête c_f, c'est le coefficient dans f de t_f,
- le reliquat du polynôme r_f défini par

$$f = c_f t_f + r_f.$$

.

▶ Restrictions :

- Dans la suite on ne s'intéressera qu'aux polynômes f_i avec $c_{f_i} = 1$.En effet,

$$\langle f_1,...,f_n\rangle = \langle c_{f_1}^{-1} f_1,...,c_{f_n}^{-1} f_n\rangle.$$

- On peut aussi supposer qu'aucun f_i n'est le polynôme 0.

9 Règle et réduction

- Si f est un polynôme de coefficient de tête 1, alors on définit une règle

$$t_f \xrightarrow[f]{} -r_f.$$

- La règle $t_f \xrightarrow[f]{} -r_f$ engendre une réduction $g \xrightarrow[f]{} g'$ ainsi
  1. g contient un monôme m avec coefficient a tel que,

2. $m = t_f \cdot m'$
3. et $g' = g - am' \cdot f$.

- Si $F = \{f_1, ..., f_n\}$ alors

$$\xrightarrow[F]{} \quad = \quad \bigcup_{k=1}^{n} \xrightarrow[f_k]{} .$$

Lemme : Soient $f, g, g', h \in K[X_1, ..., X_n]$,
m un monôme,
$b \in K^*$.
Supposons que f a 1 comme coefficient de tête.

1. $f \xrightarrow[f]{} 0$,
2. $g \xrightarrow[f]{} g' \implies bm \cdot g \xrightarrow[f]{} bm \cdot g'$,
3. $g \xrightarrow[f]{} g' \implies h + g \downarrow_f h + g'$.

▶ La démo est laissée en exercice

Si on note :

$$\begin{aligned} F &= \{f_1, ..., f_n\} \\ J &= \langle f_1, ..., f_k \rangle \end{aligned}$$

on a :

Théorème : $\equiv_J \quad = \quad \xleftrightarrow[F]{*}$

10 Bases de Gröbner

$G = \{f_1, ..., f_n\}$ est une base de Gröbner de l'idéal J si

1. $J = \langle f_1, ..., f_n \rangle$, ($f_i$ normalisés).
2. $\xrightarrow[G]{}$ est confluent.

11 S-polynômes

▶ Les S-polynômes sont en quelque sorte les paires critiques des règles.
Soient deux polynômes f et g de coefficients de tête 1.
Soit $m = ppcm(t_f, t_g)$.
Soient

- m_f tel que $m = m_f \cdot t_f$,
- m_g tel que $m = m_g \cdot t_g$,

Le S-polynôme de f et g est défini par

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

Théorème : Soit $G = \{f_1, ..., f_n\}$. G est une base de Gröbner de $J = \langle f_1, ..., f_k \rangle$ ssi tous les S-polynômes de G se réduisent à 0.

L'algorithme de Buchberger

Données

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

Résultat

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

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 : L'algorithme de Buchberger termine et retourne une base de Gröbner.

Démonstration :

- (Correction) Soit $J = \langle f_1, ..., f_n \rangle$.
  On remarque que pour chaque étape on a $\langle G_i \rangle = J$.
  - Les $S(f,g) \in J$, car $f, g \in J$.
  - De même si $S(f,g) \in J = \langle G_i \rangle$ et $S(f,g) \xrightarrow[G_i]{} h$, on a $c_h^{-1} \in J$.

  Le résultat est une base de Gröbner.
- (Terminaison) cf All That.

▶ Remarquons que l'algorithme présenté n'interréduit pas les polynômes. Même après iterréduction, l'algorithme est sensible à l'ordre admissible choisi. Il aussi indispensable d'implanter des critères de paires critiques pour ne pas calculer toutes les S-polynômes.