Introduction au Calcul formel

Algorithmes et complexité

Frédéric Chyzak

frederic.chyzak@inria.fr

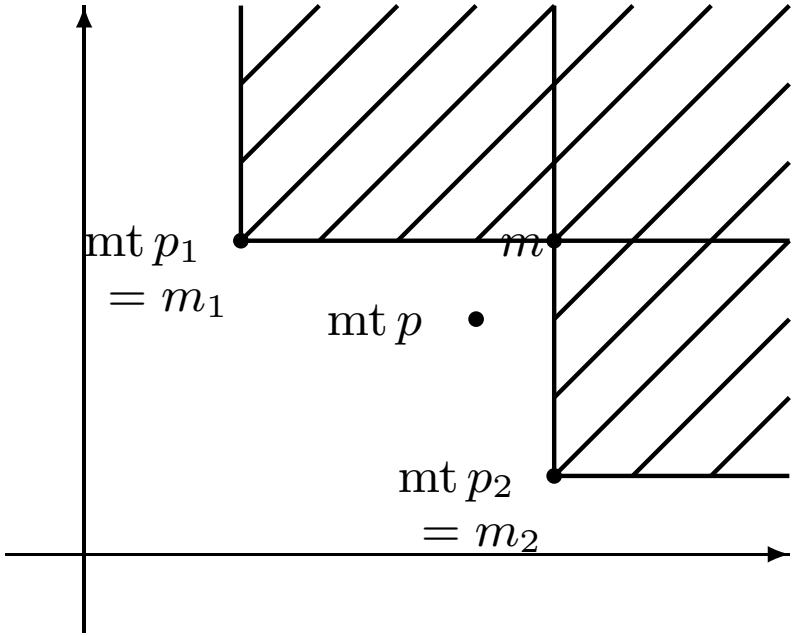
http://www.enseignement.polytechnique.fr/profs/informatique/Frederic.Chyzak/

Bases de Gröbner, la définition (rappel)

Définition. Soit I un idéal de $A = \mathbb{C}[X_1, \ldots, X_n]$ et $\prec$ un ordre monomial. Un ensemble fini $G \subseteq I$ est une base de Gröbner de I pour l'ordre $\prec$ si l'une quelconque des propriétés équivalentes est vérifiée :

1. la partie stable de M engendrée par $\mathrm{mt}(G)$ est $\mathrm{mt}(I)$;
2. $\mathrm{mt}(G)$ et $\mathrm{mt}(I)$ engendrent le même idéal ;
3. tout $f \in I$ non nul est réductible par G ;
4. pour tout $f \in A$, il existe un unique $r \in A$ tel que $f - r \in I$ et dont aucun monôme n'est divisible par un monôme de $\mathrm{mt}(G)$;
5. pour tout $f \in I$, le reste de la division de f par G est nul.

S-polynômes, le problème



$$\begin{cases} p = \sum_i l_i p_i \\ \mathrm{mt}\, p \notin \bigcup_i M\, \mathrm{mt}\, p_i \end{cases} \quad \Longrightarrow \quad \text{annulation des termes de tête !}$$

S-polynômes, la définition

Définition. Soient deux polynômes p_1 et p_2 et posons $m_1 = \mathrm{mt}\, p_1$, $m_2 = \mathrm{mt}\, p_2$ et $m = \mathrm{ppcm}(m_1, m_2) = n_i m_i$. On appelle *S-polynôme* de p_1 et p_2 toute combinaison linéaire de la forme $l_1 p_1 + l_2 p_2$ pour tous polynômes l_i tels que $\mathrm{mt}\, l_i = n_i$ et $\mathrm{tt}\, l_1\, \mathrm{tt}\, p_1 + \mathrm{tt}\, l_2\, \mathrm{tt}\, p_2 = 0$.

En pratique, on se restreint à des termes et on pose :

$$\mathrm{Spoly}(p_1, p_2) = l_1 p_1 + l_2 p_2 \quad \text{pour} \quad l_1 = \mathrm{ct}(p_2) n_1, \quad l_2 = -\mathrm{ct}(p_1) n_2.$$

Propriété caractéristique des bases de Gröbner

Posons $P = \{p_k\}$. Si tous les $\mathrm{Spoly}(p_i, p_j)$ se réduisent à 0 par P, alors P est une base de Gröbner.

Preuve : Soit $p = \sum_i l_i p_i$ réduit. Sans perte de généralité, on peut supposer que $\delta = \max\{\mathrm{mt}\, l_i p_i\}$ est minimal, et que $\mathrm{mt}\, l_i p_i = \delta \succ \mathrm{mt}\, l_j p_j$ pour $i \leq k < j$. Alors,

$$p = \sum_{i=1}^{k} \mathrm{tt}(l_i) p_i + \sum_{i=1}^{k} (l_i - \mathrm{tt}\, l_i) p_i + \sum_{i>k} l_i p_i = \sum_{i=1}^{k} \mathrm{tt}(l_i) p_i + (\text{termes} \prec \delta).$$

Tant que $k > 1$, on fait :

$$\begin{aligned} \mathrm{tt}(l_k) p_k + \mathrm{tt}(l_{k-1}) p_{k-1} &= t_k\, \mathrm{ct}(p_{k-1}) n_k p_k + t_{k-1}\, \mathrm{ct}(p_k) n_{k-1} p_{k-1} \\ &= t_k\, \mathrm{Spoly}(p_k, p_{k-1}) + (t_{k-1} + t_k)\, \mathrm{ct}(p_k) n_{k-1} p_{k-1} \end{aligned}$$

Algorithme de Buchberger, version rudimentaire

INPUT: un ensemble fini P de polynômes p_i, un ordre monomial $\preceq$
OUTPUT: une base de Gröbner G pour le même idéal

1. initialiser G à P et S à l'ensemble des paires d'éléments de G ;
2. tant que S n'est pas vide,
   (a) choisir une paire $p = \{g, g'\}$ et la retirer de S ;
   (b) calculer $\mathrm{Spoly}(g, g')$ et le réduire par G ;
   (c) si le reste r est non nul, alors
      i. adjoindre à S tous les paires $\{g, r\}$ pour $g \in G$;
      ii. adjoindre r à G ;
3. renvoyer G.

Réductions à zéro

Pour éviter des réductions à zéro :

- paires triviales = se réduisent trivialement à 0 :

  Si $\operatorname{ppcm}(\operatorname{mt} p_1, \operatorname{mt} p_2) = \operatorname{mt}(p_1) \operatorname{mt}(p_2)$, alors $\operatorname{Spoly}(p_1, p_2)$ se réduit à zéro par $\{p_1, p_2\}$.

- paires inutiles = calculs redondants :

  Si $\operatorname{mt}(g_k)$ divise $\operatorname{ppcm}(\operatorname{mt} g_i, \operatorname{mt} g_j)$ et si les paires $\{g_i, g_k\}$ et $\{g_j, g_k\}$ ont déjà été réduites et les restes correspondants introduite, alors le S-polynôme de $\{g_i, g_j\}$ se réduit à zéro.

Bases de Gröbner réduites

On peut toujours remplacer un élément d'une base de Gröbner par le reste de sa division par les autres éléments.

Preuve : Ce faisant, on ne change pas les monômes de tête engendrés.

On peut toujours supprimer un élément d'une base de Gröbner dont le monôme de tête est divisible par celui d'un autre élément.

Preuve : La première étape de la division est en fait le calcul d'un S-polynôme, lequel se réduit à zéro.

Définition. Une *base de Gröbner réduite* est une base de Gröbner dont aucun élément n'est réductible par les autres, y compris s'agissant des monômes sous le monôme de tête, et dont les coefficients de tête sont normalisés à 1.

À ordre monomial donné, tout idéal admet une unique base de Gröbner réduite.

Algorithme de Buchberger, version classique

INPUT: un ensemble fini P de polynômes p_i, un ordre monomial $\preceq$
OUTPUT: une base de Gröbner G pour le même idéal

1. initialiser G à P et S à l'ensemble des paires d'éléments de G ;
2. tant que S n'est pas vide,
   (a) choisir une paire $p = \{g, g'\}$ et la retirer de S ;
   (b) si p est inutile ou triviale, passer à la paire suivante ;
   (c) calculer $\mathrm{Spoly}(g, g')$ et le réduire par G ;
   (d) si le reste r est non nul, alors
      i. adjoindre à S tous les paires $\{g, r\}$ pour $g \in G$;
      ii. retirer de G les polynômes dont le monôme de tête est divisible par celui de r et y adjoindre r ;
3. inter-réduire G et renvoyer le résultat.

Exemple de calcul

Exercice. Calculer une base de Gröbner pour l'ordre lexicographique de l'idéal engendré par $Y - X^2$ et $Z - X^3$.

Stratégies

Liberté sur le choix des paires et dans les réductions → plusieurs stratégies :

- « normale » (due à Buchberger),
- « du sucre » (due à Giovini, Mora, Niesi, Robbiano et Traverso),
- de Gebauer et Möller.

Maintenant dépassé par l'algorithme F_5 (dû à Faugère).

Buchberger $\supset$ Euclide

Pour deux polynômes $p_1 = c_1 X^{d_1} + \cdots$ et $p_2 = c_2 X^{d_2} + \cdots$ de $\mathbb{C}[X]$, avec $\deg p_1 = d_1 > d_2 = \deg p_2$,

$$\mathrm{Spoly}(p_1, p_2) = c_2 p_1 - c_1 X^{d_1 - d_2} p_2$$

est la première étape élémentaire d'une division euclidienne.

La réduction de $\mathrm{Spoly}(p_1, p_2)$ par $\{p_2\}$ fournit le reste p_3 de la division euclidienne de p_1 par p_2 (à multiplication par une constante près).

L'algorithme de Buchberger crée les paires $\{p_1, p_3\}$ et $\{p_2, p_3\}$. La première devient redondante si on traite la seconde.

Buchberger $\supset$ Gauss

Système linéaire :

$$a_{i,1}x_1 + \cdots + a_{i,n}x_n = 0, \qquad 1 \leq i \leq m.$$

La réduction de Gauss renvoie un système triangulaire équivalent :

$$\begin{aligned} b_{1,1}x_1 + \cdots + b_{1,r}x_r + \cdots + b_{1,n}x_n &= 0, \\ &\cdots \\ b_{r,r}x_r + \cdots + b_{r,n}x_n &= 0. \end{aligned}$$

Pour l'ordre lexicographique, les $b_{i,i}X_i + \cdots + b_{i,n}X_n$ sont une base de Gröbner de l'idéal engendré par les $a_{i,1}X_1 + \cdots + a_{i,n}X_n$. Une base de Gröbner réduite fournit un système linéaire triangulaire réduit : la matrice $(b_{i,j})_{1 \leq i,j \leq r}$ est diagonale.

Modules

Définition. Un *module* M sur un anneau A est un groupe additif stable par action par tout élément de A.

Exemple. Tout idéal de A est un A-module. Les quotients de la forme A/I pour un idéal I de A sont des modules sur A.

Exemple. Étant donnée une famille $(g_u)_{u\in U}$ d'éléments de A^r, les combinaisons linéaires finies à coefficients dans A forment un module noté $\sum_{u\in U} Ag_u$. Les quotients de la forme $A^r / \sum_{u\in U} Ag_u$ sont des modules sur A.

Ordres sur les modules

Soit $B = (b_i)_{1 \leq i \leq p}$ la base canonique de A^r :

$$A^r = Ab_1 \oplus \cdots \oplus Ab_r.$$

Deux façons naturelles d'étendre les ordres monomiaux à $M \times B$:

- top = *term over position* (mb_i triés sur m puis sur i),
- pot = *position over term* (mb_i triés sur i puis sur m).

On obtient ainsi : $\prec_{\text{top,lex}}$, $\prec_{\text{pot,lex}}$, $\prec_{\text{top,grevlex}}$, $\prec_{\text{pot,grevlex}}$, etc.

S-polynômes pour les modules

Définition. Soient $p_1 = \sum_{i=1}^{r} p_{1,i} b_i$ et $p_2 = \sum_{i=1}^{r} p_{2,i} b_i$ deux éléments de M et posons $m_1 b_{i_1} = \operatorname{mt} p_1$, $m_2 b_{i_2} = \operatorname{mt} p_2$ et $m = \operatorname{ppcm}(m_1, m_2) = n_i m_i$.

Lorsque $i_1 = i_2$, on appelle *S-polynôme* de p_1 et p_2 toute combinaison linéaire de la forme $l_1 p_1 + l_2 p_2$ pour tous polynômes l_i tels que $\operatorname{mt} l_i = n_i$ et $\operatorname{tt} l_1 \operatorname{tt} p_{1,i} + \operatorname{tt} l_2 \operatorname{tt} p_{2,i} = 0$.

Lorsque $i_1 \neq i_2$, on dit que p_1 et p_2 *n'ont pas* de S-polynôme.

$$\operatorname{Spoly}(p_1, p_2) = \begin{cases} \operatorname{ct}(p_2) n_1 p_1 + \operatorname{ct}(p_1) n_2 p_2 & i_1 = i_2, \\ 0 & \text{sinon.} \end{cases}$$

Bases de Gröbner pour les modules

La notion de base de Gröbner et l'algorithme de Buchberger s'étendent tels quels modulo les deux extensions précédentes.

```
> Q:=RationalField();
> P<X,Y,Z>:=PolynomialRing(Q,3,"grevlex");
> M:=Module(P,2);
> S:=sub<M|(X^2-1)*M.1+(X*Y-Z)*M.2,(Y^2+X)*M.1+(3*Z-X)*M.2>;
> Groebner(S);
> Basis(S);
[
    (0   X*Y^3 + X^3 + X^2*Y - 3*X^2*Z - Y^2*Z - X*Z - X + 3*Z),
    (X^2 - 1 X*Y - Z),
    ( Y^2 + X -X + 3*Z)
]
>
```

Base de Gröbner en terme des polynômes originaux

Étant donnés des polynômes $p_1, \ldots, p_r$, on cherche à exprimer les éléments d'une base de Gröbner de l'idéal engendré I en terme des p_i.

Dans $A^{r+1} = \sum_{i=0}^{r} Ab_i$: une base de Gröbner pour un ordre *pot* du sous-module engendré par les $p_i b_0 - b_i$ contient :

- des éléments de la forme $gb_0 - \sum_{i=1}^{r} l_i b_i \ : \ g = \sum_{i=1}^{r} l_i p_i$.

  Les g constituent une base de Gröbner pour I.

- des éléments de la forme $\sum_{i=1}^{r} u_i b_i \ : \ \sum_{i=1}^{r} u_i p_i = 0$.

  Engendrent le module des relations entre les p_i.

Complexité, problèmes complets

Le problème général de la recherche d'une base de Gröbner réduite et le problème d'appartenance à un idéal générique de polynômes sont des problèmes EXPSPACE-complets (pour des coefficients dans $\mathbb{Q}$).

Restreints à des idéaux binomiaux (engendrés par des binômes $X^\alpha - X^\beta$), il en est de même pour les deux problèmes.

Restreint à des idéaux homogènes (engendrés par des polynômes dont tous les monômes ont même degré), le problème d'appartenance à un idéal n'est que PSPACE-complet.

Complexité, taille de la sortie

Les degrés des polynômes d'une base de Gröbner réduite d'un idéal $Ap_1 + \cdots + Ap_s \subseteq \mathbb{C}[X_1, \ldots, X_n]$, pour des p_i de degré au plus d, sont au plus

$$2\left(\frac{d^2}{2} + d\right)^{2^n - 1}.$$

Il existe des idéaux dont toutes les bases de Gröbner contiennent au moins $2^{2^{cn}}$ éléments et des éléments de degré au moins $2^{2^{c'n}}$, pour des constantes réelles $c, c' > 0$.