Projet Cassiopée: Méthodes algébriques d'inversion de systèmes polynomiaux

Clément Aubert - Erwan Tesson

18 février 2018

Première partie

Bases de Gröbner

Chapitre 1

Rappels d'Algèbre

1.1 Définitions

Définition 1.1. Soit A un ensemble de deux lois de composition interne $+$ et $\times$. On dit que $(A, +, \times)$ est un *anneau* si :
- $(A, +)$ est un groupe commutatif
- $\times$ est associative.
- $\times$ est distributive par rapport à l'addition.

Définition 1.2. Une partie I de l'anneau A est appelé *idéal* de l'anneau A si :
- $(I, +)$ est un sous-groupe de $(A, +)$
- $\forall x \in I$ et $\forall a \in A$, alors ax et xa sont éléments de I.

Définition 1.3. On appelle *idéal* de $K[x_1, ..., x_n]$ toute partie I de $K[x_1, ..., x_n]$ vérifiant :
- le polynome nul est dans I
- si P_1 et P_2 sont dans I, il en est de même pour $P_1 - P_2$
- si P est dans I et si Q est un polynôme quelconque, PQ appartient à I.

Propriété 1.1. L'ordre doit être total, compatible à la multiplication et bien ordonné :
- $\text{LEX}_{X_1>X_2>...>X_n}$: le plus grand monôme est celui qui contient le plus de X_1, puis le plus de X_2
- $\text{DEGLEX}_{X_1>X_2>...>X_n}$: par degrès puis par ordre $\text{LEX}_{X_1>X_2>...>X_n}$
- $\text{DEGREVLEX}_{X_1>X_2>...>X_n}$: par degrès puis par ordre $\text{LEX}_{X_1>X_2>...>X_n}$ "inversé"

Théorème. *(Hilbert)* Pour tout Idéal I de $K[x_1, ..., x_n]$, il existe un système fini de générateur $(g_1, ..., g_k)$ de polynômes tel que $I = \text{Id}(g_1, ..., g_k)$

Théorème. (Croissance d'idéaux) Si $(I_i)_{i \in \mathbb{N}}$ une famille d'idéaux tels que :

$$I_1 \subset I_2 \subset I_3 \subset ...$$

alors $\exists N \in \mathbb{N}$ tel que

$$I_N = I_{N+1} = I_{N+2} = ...$$

1.2 Notations

— $K[x_1, ..., x_n]$: l'anneau des polynomes à valeur dans K

Chapitre 2

Bases de Gröbner

2.1 Définition

Définition 2.1. On fixe un ordre monomial. Soit $I = \langle f_1, ..., f_m \rangle$ un idéal de $K[x_1, ..., x_n]$

— $\mathrm{LT}(I) = \langle \{lt(f) : f \in I\} \rangle$ est appelé idéal initial de I

— $\{g_1, ..., g_s\} \subset I$ est une base de Gröbner de I si :

$$\langle lt(g_1), ..., lt(g_s) \rangle = \mathrm{LT}(I)$$

Propriété 2.1. Soit $f \in K[x_1, ..., x_n]$,si G est une base de Gröbner de $I = \langle f_1, ..., f_m \rangle$ alors :

— $\overline{f^G} = 0 \Leftrightarrow f \in I$

— le reste $\overline{f^G}$ est unique

Chapitre 3

Résolution de systèmes polynomiaux

3.1 Définitions

Définition 3.1. *Soit* $(f_1, f_2, ..., f_s) \in K[x_1, ..., x_n]$*, on définit une variété affine comme :*

$$\boldsymbol{V}(f_1, f_2, ..., f_s) = \{(a_1, ..., a_n) \in k^n : f_i(a_1, ..., a_n) = 0, \forall i \in [1, s]\}$$

3.2 Théorie de l'élimination

Définition 3.2. $I_I = I \cap K[x_{I+1}, ..., x_n]$ est un idéal de $K[x_{I+1}, ..., x_n]$ appelé I-ème idéal d'élimination.

Deuxième partie

Exemples d'utilisation des Bases de Gröbner

Chapitre 4

Réduction par le pivot de Gauss

Principe

La méthode du pivot de Gauss est un procédé qui résulte des bases de Gröbner.

Exemple

On a F= {x+3y+4z-5, 3x+4y+5z-2}.
On cherche à simplifier l'expression de F

$$\Leftrightarrow S = \begin{cases} 2x + 3y + 4z = 5 \\ 3x + 4y + 5z = 2 \end{cases}$$

$$\Leftrightarrow S = \begin{cases} 2x + 3y + 4z = 5 \\ y + 2z = 11 \end{cases}$$

$$\Leftrightarrow S = \begin{cases} 2x - 2z = -28 \\ y + 2z = 11 \end{cases}$$

$$\Leftrightarrow S = \begin{cases} x = z - 14 \\ y = -2z + 11 \end{cases}$$

On a donc G= {-z+14, y+2z-11}.

Bibliographie

Voici la liste des documents utilisés pour nos recherches :

— https ://moodle.polytechnique.fr/pluginfile.php/66308/mod$_{r}esource/content/3/Cours8.pdf$
http : //denis.monasse.free.fr/denis/articles/grobner.pdf

— http ://www.lifl.fr/jncf2015/files/lecture-notes/faugere.pdf

— http ://iml.univ-mrs.fr/ kohel/tch/M2-Agreg/CM/08$_{g}eometrie_{s}uite.pdf$

Ces documents s'ajoutent à ceux proposés sur le sujet de notre projet Cassiopée :

— J.-F. Cardoso. Blind signal separation : statistical principles. Proc. IEEE, 9(10) :20092025, Oct. 1998.

— M. Castella. Inversion of polynomial systems and separation of nonlinear mixtures of nite-alphabet sources. IEEE Trans. Signal Process., 56(8, Part 2) :39053917, Aug. 2008.

— P. Comon. Independent component analysis, a new concept ? Signal Process., 36(3) :287 314, Apr. 1994.

— D. Cox, J. Little, and D. O'Shea. Ideal, Varieties, and Algorithms. Springer, third edition edition, 2007.