Systèmes polynomiaux. Bases de Gröbner.

Bruno Salvy

INRIA

Introduction

1. Questions décidables
2. Idéaux et variétés

I. Bases de Gröbner

1. Ordres de termes
2. Réduction
3. Ordres admissibles
4. Bases de Gröbner

II. Applications

1. Lien avec les solutions
2. Réduction
3. Résolution
4. Élimination

III. Calcul

1. Algorithme de Buchberger
2. Complexité

Bibliographie

Questions décidables

$$\begin{cases} P_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ P_k(x_1, \ldots, x_n) = 0 \end{cases}$$

– Y a-t-il des solutions ?

– Les solutions sont-elles en nombre fini ?

– Est-ce que $Q(x_1, \ldots, x_n) = 0$ lorsque $(x_1, \ldots, x_n)$ est solution ?

Idéaux et variétés

Définition. Soit $\mathbb{A}$ un anneau, $\mathcal{I} \subset \mathbb{A}$ est un *idéal* lorsque

$$0 \in \mathcal{I},$$
$$\forall u, v \in \mathcal{I}, \qquad u + v \in \mathcal{I},$$
$$\forall a \in \mathbb{A}, \forall u \in \mathcal{I}, \qquad au \in \mathcal{I}.$$

Définition. Soit $\mathbb{K}$ un corps. Une *variété* de $\mathbb{K}^n$ est l'ensemble des zéros communs d'un nombre fini de polynômes $p_1, \ldots, p_k$ de $\mathbb{K}[x_1, \ldots, x_n]$.

Exemples. $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_n]$, $p_1, \ldots, p_k \in \mathbb{A}$,

$$\langle p_1, \ldots, p_k \rangle = \{a_1 p_1 + \cdots + a_k p_k, a_i \in \mathbb{A}, i = 1, \ldots, k\}$$

idéal *engendré* par les p_i;

$$\mathcal{I}(V) = \{p \in \mathbb{A} \mid \forall x \in V, p(x) = 0\}$$

l'idéal de V.

Théorème [Hilbert]. Tout idéal de $\mathbb{K}[x_1, \ldots, x_n]$ admet une base finie.

Théorème [Hilbert]. Si $\mathbb{K}$ est algébriquement clos,

$$P \in \mathcal{I}(V(p_1, \ldots, p_k)) \Longrightarrow \exists m \geq 1, P^m \in \langle p_1, \ldots, p_k \rangle.$$

Définition. $\sqrt{\mathcal{I}} = \{P \mid \exists m \geq 1, P^m \in \mathcal{I}\}$, le *radical* de l'idéal.

I. Bases de Gröbner

Ordres de termes

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} > x_1^{\beta_1} \cdots x_n^{\beta_n}$$

Exemples d'ordre sur les k-uplets $(\alpha_1, \ldots, \alpha_n)$:

- *lexicographique*: $\alpha_1 > \beta_1$ ou $(\alpha_1 = \beta_1$ et $\alpha_2 > \beta_2)$ ou $\ldots$;
- *degré total*: $\alpha_1 + \cdots + \alpha_n > \beta_1 + \cdots + \beta_n$ ou $\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$ et $(\alpha_n, \ldots, \alpha_1) >_{\mathrm{lex}} (\beta_n, \ldots, \beta_1)$;
- *ordre de k-élimination*: $k < n$ fixé $(\alpha_1, \ldots, \alpha_k) >_{\mathrm{deg}} (\beta_1, \ldots, \beta_k)$ ou $[(\alpha_1, \ldots, \alpha_k) = (\beta_1, \ldots, \beta_k)$ et $(\alpha_{k+1}, \ldots, \alpha_n) >_{\mathrm{deg}} (\beta_{k+1}, \ldots, \beta_n)]$.

Réduction

Généralisation de la division euclidienne.

Ordre $\rightarrow$ monôme dominant $\rightarrow$ division.

$f \in \mathbb{K}[x_1, \ldots, x_n]$ est *réduit* par rapport à $g \in \mathbb{K}[x_1, \ldots, x_n]$ si le monôme dominant de g ne divise pas celui de f.

Ordres admissibles

$$(\alpha_1, \ldots, \alpha_n) > (\beta_1, \ldots, \beta_n)$$

L'ordre $>$ est *admissible* lorsque

- $>$ est *total* sur $\mathbb{Z}^n$;
- si $\alpha > \beta$ et $\gamma \in \mathbb{Z}^n$, $\alpha + \gamma > \beta + \gamma$;
- $\alpha \geq 0$ pour tout $\alpha \in \mathbb{N}^n$.

Base de Gröbner

Définition. Pour un ordre admissible fixé, un sous-ensemble fini $G = \{g_1, \ldots, g_t\}$ d'un idéal $\mathcal{I}$ est une *base de Gröbner* de $\mathcal{I}$ lorsque le monôme dominant de tout élément de $\mathcal{I}$ est divisible par celui d'un des g_i.

Propriété. Pour un ordre admissible fixé, tout idéal de $\mathbb{K}[x_1, \ldots, x_n]$ autre que $\{0\}$ admet une base de Gröbner.

II. Applications

Lien avec les solutions

$$\begin{cases} P_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ P_k(x_1, \ldots, x_n) = 0 \end{cases}$$

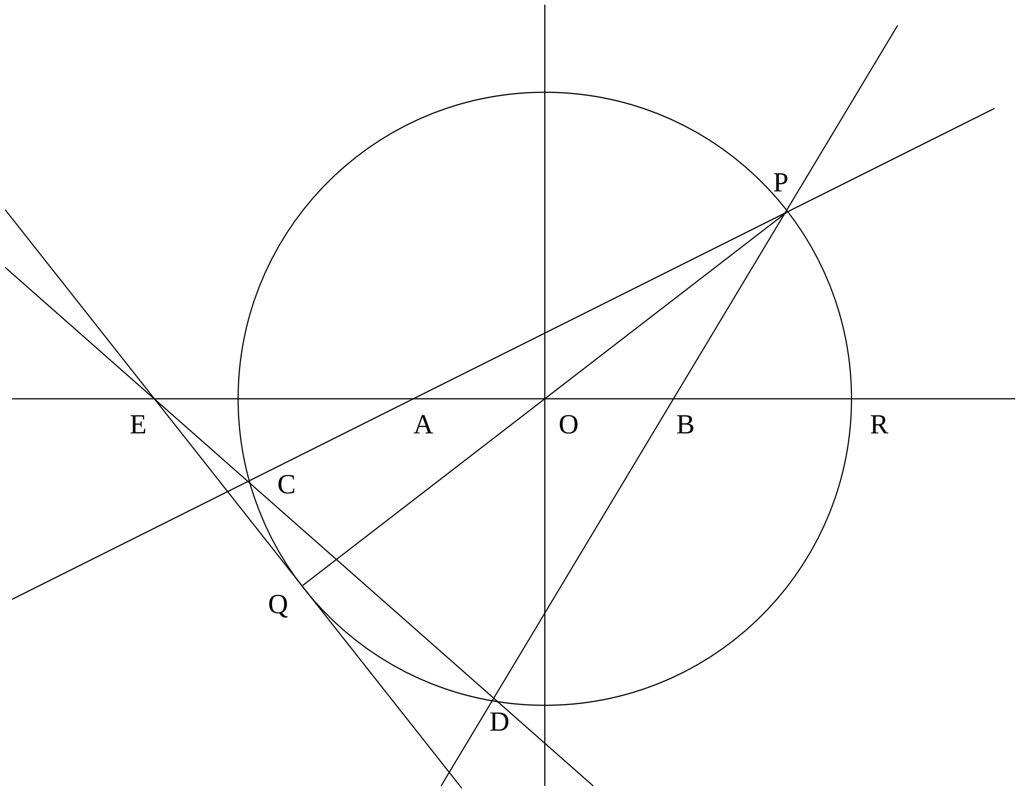
- Le système a des solutions ssi une base de Gröbner de $\langle P_1, \ldots, P_k \rangle$ est différente de $\{1\}$;
- le système a un nombre fini de solutions ssi chacun des x_i apparaît seul dans le monôme dominant d'un des éléments de la base (dimension 0).

Réduction

Généralisation du reste pour la division euclidienne.

- La réduction par une base de Gröbner donne un test d'appartenance à l'idéal ;
- la réduction donne une forme normale ;
- en dimension 0, la réduction ramène les calculs à de l'algèbre linéaire en dimension finie.

Un exercice de géométrie



Résolution

La base pour l'ordre lexicographique donne un système triangulaire ayant les mêmes solutions que le système de départ.

Dans le cas linéaire, équivalent à l'algorithme de Gauss.

Élimination

Analogue du résultant en k variables

Théorème. Soit $\mathcal{I}$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et G une base de Gröbner de $\mathcal{I}$ pour l'ordre lexicographique ou pour un ordre de k-élimination, alors l'ensemble

$$G \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$$

est une base de Gröbner de

$$\mathcal{I} \cap \mathbb{K}[x_{k+1}, \ldots, x_n].$$

Exemples

– Triangularisation

– Résultant

– Dépendence algébrique

– Fonctions symétriques des racines

– Calculs d'enveloppe

– Optimisation linéaire en nombres entiers

Calcul d'enveloppes

$$f(x, y, \lambda) = 0$$

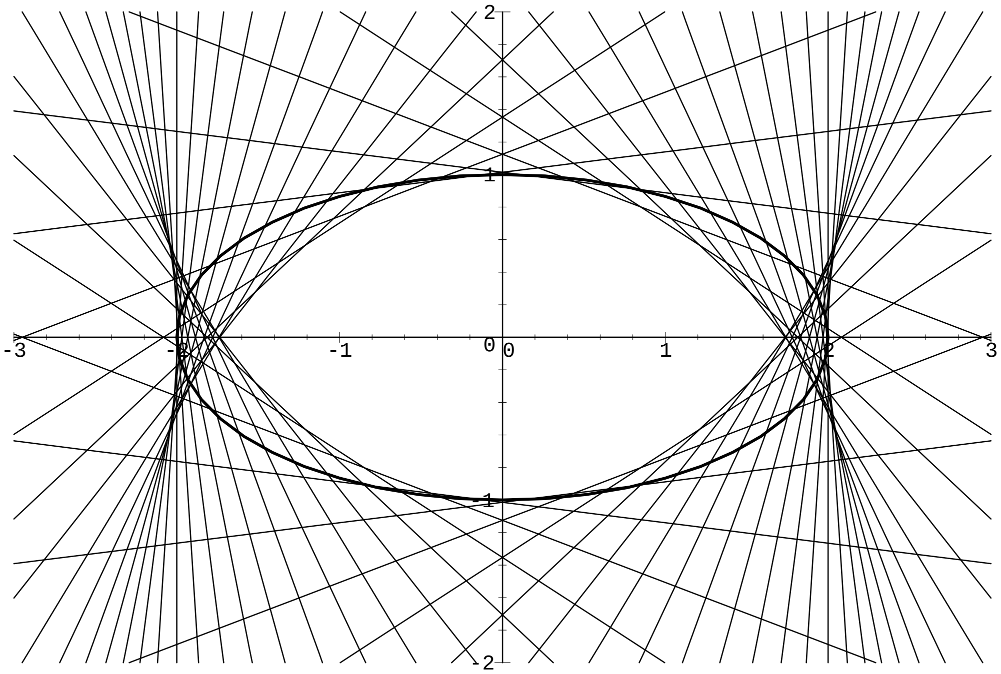
famille paramétrée de courbes (f polynôme)

Enveloppe :

$$\begin{cases} f(x, y, \lambda) = 0, \\ f'_\lambda(x, y, \lambda) = 0. \end{cases}$$

Exemple

Perpendiculaires aux diamètres d'une ellipse en leurs extrémités.



III. Calcul

Algorithme de Buchberger

Définition. $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ avec pour monômes dominants

$$c_f x_1^{\alpha_1} \cdots x_n^{\alpha_n} \qquad \text{et} \qquad c_g x_1^{\beta_1} \cdots x_n^{\beta_n}.$$

Soit $\gamma_i = \max(\alpha_i, \beta_i)$, $i = 1, \ldots, n$. Le *S-polynôme* de f et g (relativement à l'ordre) est

$$S(f, g) = x^{\gamma-\alpha} f - x^{\gamma-\beta} g.$$

Théorème. Une base G d'un idéal $\mathcal{I}$ de $\mathbb{K}[x_1, \ldots, x_n]$ est une base de Gröbner ssi pour tout $(f, g) \in G^2$,

$$S(f, g) \to_G 0.$$

Algorithme. Tant que l'un des S-polynômes ne se réduit pas à 0, on le rajoute à la base.

Complexité

Complexité théorique très élevée :

$$O(d^{n^2}).$$

En pratique,

- une dizaine de variables, degré 2 ;
- deux ou trois variables, degré 7-8 ;
- très variable.

L'ordre du degré est généralement plus rapide.

Systèmes spécialisés.

Bibliographie

Zippel (Richard). – *Effective Polynomial Computation.* – Kluwer Academic Publishers, 1993.

Cox (D.), Little (J.), and O'Shea (D.). – *Ideals, Varieties, and Algorithms.* – Springer-Verlag, 1992.