TP6 : Bases de Gröbner et systèmes de polynômes multivariés

Résumé du TP

Bertrand Meyer

18 ± 2 décembre 2019

Introduction

Les **systèmes d'équations polynomiales multivariés**

- modélisent une grande variété de situation (par ex : mouvement des robots)
- sont difficiles à manipuler
- [version théorie du complot] dirigent le monde en secret.

Exemple : Cryptographie à clé publique multivariée
Basée sur la NP-difficulté à trouver les zéros d'un système général d'équations.

Candidate dans la compétition NIST post-quantique.

Bases de Gröbner
Outils pour la manipulation des systèmes.

Menace cryptographique.

Division

La division dans $\mathbb{K}[x]$

Outil principal dans $\mathbb{K}[x]$: la division euclienne ($\rightarrow$ pgcd)

Entrée : dividende f, diviseur g
Sortie : quotient q, reste r
Répéter :
    Si $td(f) = x^\alpha \cdot td(g)$:
        $f \leftarrow f - x^\alpha \cdot g$;
        $q \leftarrow q + x^\alpha$
Renvoyer q et $r = f$.

$\mathbb{K}[x]$ est principal :

être engendré par une famille $\leftrightarrow$ être multiple du générateur (le pcgd)

Dans $\mathbb{K}[\mathbf{x}]$ (avec $\mathbf{x} = x_1, \ldots, x_n$) : pas de division *a priori*.

Une pseudo-division dans $\mathbb{K}[\mathbf{x}]$

On ordonne les monômes (par ex : ordre lexicogaphique).

Algorithme de pseudo-division de f par g_1, g_2, …, g_s par imitation.

Entrée : dividende f, diviseurs g_1, …, g_s
Sortie : quotients g_1, …, g_s, reste r
Répéter :
Si $td(f) = x^\alpha \cdot td(g_i)$ pour un certain i :
$f \leftarrow f - x^\alpha \cdot g_i$;
$q_i \leftarrow q_i + x^\alpha$
Renvoyer q_1, …, q_i et $r = f$.

Idéal $\mathfrak{I} = \{q_1 g_1 + \cdots + q_s g_s\}$, non principal !

Problème

Pas de caractérisation du reste par rapport à $\mathfrak{I}$ quand $(g_1, g_2, \ldots, g_s)$ est quelconque. Le reste de $t_1 \cdot g_1 + \cdots + t_s \cdot g_s$ peut être non nul.

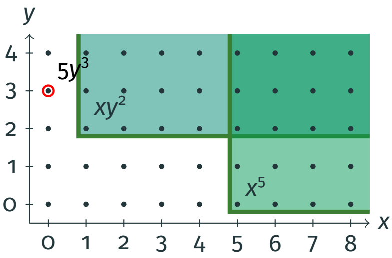
Les monômes du reste sont dans la partie non-couverte du diagramme en escalier

Exemple

$$f = -x^7 + x^6y + 2x^5 - 2x^4y - 5x^2 + 3xy^3 + 5xy + 11y^3 + 10$$

$$g_1 = xy^2 + 2y^2 \quad \text{et} \quad g_2 = x^5 + 5.$$

$$q_1 = -3y, \quad q_2 = -x^2 + xy + 2 \quad \text{et} \quad r = -2x^4y + 5y^3.$$



Les bases de Gröbner

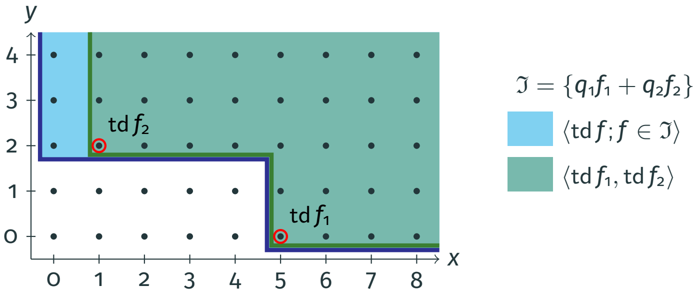
Définition

La famille $g_1, \ldots, g_s$ est une base de Gröbner de l'idéal $\mathfrak{I}$ si un t.d. d'un polynôme de $\mathfrak{I}$ est engendré par les t.d. de la base.

Contre exemple

$$f_1 = xy^2 + 2y^2 \text{ et } f_2 = x^5 + 5.$$

y^2 fait partie de l'idéal aussi :-(



Calcul d'une base de Gröbner

Algorithme

Soit G_0 une famille génératrice de l'idéal $\mathfrak{I}$, pour obtenir une base de Gröbner de $\mathfrak{I}$, on sature G_0 avec les restes des polynômes de syzygie

$$S(g,h) = \frac{\operatorname{ppcm}\left(\operatorname{td}(g),\operatorname{td}(h)\right)}{\operatorname{td}(g)} g - \frac{\operatorname{ppcm}\left(\operatorname{td}(g),\operatorname{td}(h)\right)}{\operatorname{td}(h)} h \quad \operatorname{rem} G.$$

Exemple

$$f_1 = xy^2 + 2y^2 \text{ et } f_2 = x^5 + 5.$$
$$s = S(f_1, f_2) = 2x^4y^2 - 5y^2 = (2x^3 - 4x^2 + 8x - 16) \cdot f_1 + 0 \cdot f_2 + 27y^2$$

Comme $f_1 \operatorname{rem} \langle f_2, s \rangle = 0$, (f_2, s) est une base de Gröbner.

Applications

Appartenance à un idéal

Dans $\mathbb{K}[x]$, f est multiple de g ssi la division de f par g renvoie un reste nul.

Dans $\mathbb{K}[\mathbf{x}]$, quand G est une base de Gröbner, f est appartient à l'idéal $\mathfrak{I}$ engendré par G ssi la division de f par G renvoie un reste nul.

Zéros d'un système d'équations polynomiales

Triangulation de sytèmes

Lorsque l'ordre est l'ordre lexicographique, $G \cap \mathbb{K}[x_{t+1}, \dots, x_n]$ est aussi une base de Gröbner de $\mathfrak{I} \cap \mathbb{K}[x_{t+1}, \dots, x_n]$.

Les bases de Gröbner triangularisent un système !

En pratique : on trouve les valeurs possibles de x_n en resolvant les dernières équations (qui ne dépendent que de x_n), on réinjecte dans les précédentes et on réitère.