

Théorie de l'élimination

PIROUTET Alban, PICHERY Léo

02/10/2024

Objectif

Éliminer des variables d'un système d'équations polynomiales

Objectif

Éliminer des variables d'un système d'équations polynomiales

Pour comprendre un peu la différence avec ce que nous avons l'habitude de voir, voici deux exemples.

Exemple 1

Système d'équations linéaires

$$\begin{cases} 2x - y - 3z &= 1 \\ 3x + 2y - 2z &= -4 \\ -x - 4y + 6z &= 22 \end{cases}$$

Exemple 1

Système d'équations polynomiales

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases} \quad (1)$$

Résolution de l'exemple 1

On s'intéresse à l'idéal $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$

Résolution de l'exemple 1

On s'intéresse à l'idéal $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$
Une base de Gröbner de I (pour l'ordre lexicographique) est :

$$\begin{cases} g_1 = x + y + z^2 - 1 \\ g_2 = y^2 - y - z^2 + z \\ g_3 = 2yz^2 + z^4 - z^2 \\ g_4 = z^6 - 4z^4 + 4z^3 - z^2 \end{cases} \quad (2)$$

Résolution de l'exemple 1

Les systèmes (1) et (2) ont les mêmes solutions.

Résolution de l'exemple 1

Les systèmes (1) et (2) ont les mêmes solutions.

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2 = z^2(z - 1)(z^2 + 2z - 1) \implies z =$$

$$\begin{cases} 0 \\ 1 \\ -1 + \sqrt{2} \\ -1 - \sqrt{2} \end{cases}$$

Résolution de l'exemple 1

Les systèmes (1) et (2) ont les mêmes solutions.

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2 = z^2(z - 1)(z^2 + 2z - 1) \implies z =$$

$$\begin{cases} 0 \\ 1 \\ -1 + \sqrt{2} \\ -1 - \sqrt{2} \end{cases}$$

On substitue dans $g_2 = 0$ et $g_3 = 0$ ce qui nous permet de déterminer les valeurs possibles de y puis on substitue dans $g_1 = 0$ et cela nous donne les valeurs de x possibles.

Résolution de l'exemple 1

Finalement on obtient 5 solutions :

$$\left\{ \begin{array}{l} (1, 0, 0) \\ (0, 1, 0) \\ (0, 0, 1) \\ (-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}) \\ (-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}) \end{array} \right.$$

Méthode de résolution

Comment a-t-on trouver les solutions ?

Méthode de résolution

Comment a-t-on trouver les solutions ?

1) Etape d'élimination

Méthode de résolution

Comment a-t-on trouver les solutions ?

- 1) Etape d'élimination
- 2) Etape d'extension

Les idéaux d'éliminations

Définition

Soit $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$. Le i^{eme} idéal d'élimination de I est l'idéal de $k[x_{i+1}, \dots, x_n]$ défini par :

$$I_i = I \cap k[x_{i+1}, \dots, x_n]$$

Les idéaux d'éliminations

Définition

Soit $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$. Le j^{ieme} idéal d'élimination de I est l'idéal de $k[x_{l+1}, \dots, x_n]$ défini par :

$$I_l = I \cap k[x_{l+1}, \dots, x_n]$$

On vérifie aisément que I_l est un idéal de $k[x_{l+1}, \dots, x_n]$.

Remarque

- Si l'on ordonne différemment les variables, alors on trouve des idéaux d'éliminations différents.

Remarque

- Si l'on ordonne différemment les variables, alors on trouve des idéaux d'éliminations différents.
- Eliminer $x_1, \dots, x_l$ signifie trouver des polynômes non nuls dans I_l .

Remarque

- Si l'on ordonne différemment les variables, alors on trouve des idéaux d'éliminations différents.
- Eliminer $x_1, \dots, x_l$ signifie trouver des polynômes non nuls dans I_l .
- Une solution de l'étape d'élimination signifie donner une procédure systématique pour trouver des éléments de I_l .

Théorème d'élimination

Théorème d'élimination

Soit $I \subseteq k[x_1, \dots, x_n]$ un idéal et G une base de Gröbner de I qui respecte l'ordre lexicographique où $x_1 > \dots > x_n$. Alors $\forall l \in \llbracket 0; n \rrbracket$: l'ensemble $G_l = G \cap k[x_{l+1}, \dots, x_n]$ est une base de Gröbner de I_l .

Fonctionnement de l'algorithme sur l'exemple 1

$$I_1 = I \cap \mathbb{C}[y, z] = \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2 \rangle$$

$$I_2 = I \cap \mathbb{C}[z] = \langle z^6 - 4z^4 + 4z^3 - z^2 \rangle$$

Remarque

- Le dernier polynôme que nous obtenons n'est pas une façon aléatoire d'éliminer x et y de nos 4 équations : c'est la meilleure façon car les autres polynômes permettant de les éliminer sont des multiples de celui-ci.

Remarque

- Le dernier polynôme que nous obtenons n'est pas une façon aléatoire d'éliminer x et y de nos 4 équations : c'est la meilleure façon car les autres polynômes permettant de les éliminer sont des multiples de celui-ci.
- Le théorème d'élimination montre qu'une base de Gröbner pour l'ordre lexicographique ne permet pas seulement d'éliminer la première variable, mais aussi la seconde, troisième etc.

L'étape d'extension

Définition

Soit $I \subseteq k[x_1, \dots, x_n]$ un idéal. On définit :

$$V(I) = \{(a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0, \forall f \in I\}$$

$V(I)$ est une variété affine.

Définition

Soit $l \in \llbracket 1; n \rrbracket$. Cela nous donne l'idéal d'élimination I_l . On appelle solution partielle $(a_{l+1}, \dots, a_n) \in V(I_l)$ une solution partielle du système d'équation initial

Problème

Les équations que l'on obtient n'ont peut être pas de racines en commun i.e. peut être qu'il y a des solutions partielles qui ne peuvent pas être étendues.

Problème

Les équations que l'on obtient n'ont peut être pas de racines en commun i.e. peut être qu'il y a des solutions partielles qui ne peuvent pas être étendues.

Exemple

$$\begin{cases} xy = 1 \\ xz = 1 \end{cases} \quad (3)$$

Problème

Les équations que l'on obtient n'ont peut être pas de racines en commun i.e. peut être qu'il y a des solutions partielles qui ne peuvent pas être étendues.

Exemple

$$\begin{cases} xy = 1 \\ xz = 1 \end{cases} \quad (3)$$

$I = \langle xy - 1, xz - 1 \rangle$. Une base de Gröbner de I est $\langle xz - 1, y - z \rangle$

En appliquant le théorème d'élimination, $y - z$ génère I_1 . Les solutions partielles données par (a, a) pour $a \in \mathbb{C}$ s'étendent en solution complète par $(\frac{1}{a}, a, a)$ SAUF pour $a = 0$.

But

Déterminer à l'avance quelles solutions partielles vont pouvoir être complétées en solution complète.

Théorème d'extension

Théorème d'extension

Soit $I = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ et I_1 le premier idéal d'élimination de I . $\forall i \in \llbracket 1; s \rrbracket$ on suppose que l'on peut écrire f_i de la forme : $f_i = c_i(x_2, \dots, x_n)x_1^{N_i} + *i$ où $\deg(*i) < N_i$ et $N_i \geq 0$ et $c_i \in \mathbb{C}[x_2, \dots, x_n] \neq 0$.

Supposons $(a_2, \dots, a_n)$ une solution partielle $\in V(I_1)$. Si $(a_2, \dots, a_n) \notin V(c_1, \dots, c_s)$ alors $\exists a_1 \in \mathbb{C}$ tel que $(a_1, \dots, a_n) \in V(I)$.

Théorème d'extension

Théorème d'extension

Soit $I = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ et I_1 le premier idéal d'élimination de I . $\forall i \in \llbracket 1; s \rrbracket$ on suppose que l'on peut écrire f_i de la forme : $f_i = c_i(x_2, \dots, x_n)x_1^{N_i} + *i$ où $\deg(*i) < N_i$ et $N_i \geq 0$ et $c_i \in \mathbb{C}[x_2, \dots, x_n] \neq 0$.

Supposons $(a_2, \dots, a_n)$ une solution partielle $\in V(I_1)$. Si $(a_2, \dots, a_n) \notin V(c_1, \dots, c_s)$ alors $\exists a_1 \in \mathbb{C}$ tel que $(a_1, \dots, a_n) \in V(I)$.

Démonstration : La semaine prochaine !

Théorème d'extension

Corollaire

Soit $I = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ et I_1 le premier idéal d'élimination de I . $\forall i \in \llbracket 1; s \rrbracket$ on suppose que l'on peut écrire f_i de la forme : $f_i = c_i x_1^{N_i} + *_{i}$ où $\deg(*_{i}) < N_i$ et $N_i \geq 0$ et $c_i \in \mathbb{C} \setminus \{0\}$.

Supposons $(a_2, \dots, a_n)$ une solution partielle $\in V(I_1)$ alors $\exists a_1 \in \mathbb{C}$ tel que $(a_1, \dots, a_n) \in V(I)$.

Généralisation du théorème d'élimination

Définition

Fixons un entier $1 \leq l \leq n$. Un ordre monomial $>$ sur $k[x_1, \dots, x_n]$ est de type l -élimination si pour tout monôme impliquant l'une des variables $x_1, \dots, x_l$ est plus grand que tous les monômes de $k[x_{l+1}, \dots, x_n]$.

L'ordre lexicographique est un ordre de type l -élimination pour n'importe quel l , ce qui en fait un outil très utile pour éliminer les variables progressivement dans les calculs de bases de Gröbner.

Généralisation du théorème d'élimination

Théorème

Si I est un idéal dans $k[x_1, \dots, x_n]$ et G est une base de Gröbner de I par rapport à un ordre monomial de type I -élimination, alors $G \cap k[x_{I+1}, \dots, x_n]$ est une base de Gröbner de l'idéal d'élimination $I_I = I \cap k[x_{I+1}, \dots, x_n]$.

Exemple

Considérons les équations

$$\begin{aligned}xy &= 4, \\ y^2 &= x^3 - 1.\end{aligned}$$

En utilisant l'ordre lexicographique avec $x > y$, la base de Gröbner est donnée par

$$\begin{aligned}g_1 &= 16x - y^2 - y^4, \\ g_2 &= y^5 + y^3 - 64,\end{aligned}$$

mais si nous procédons comme d'habitude, nous découvrons que $y^5 + y^3 - 64$ n'a pas de racines rationnelles. Une option est de calculer les racines numériquement. On obtient

$$y = 2.21363, -1.78719 \pm 1.3984i, \text{ ou } 0.680372 \pm 2.26969i.$$

Conceptuellement

L'élimination correspond à la projection d'une variété sur un espace de plus petite dimension.

Définition

Soit $V = V(f_1, \dots, f_s) \subseteq \mathbb{C}^n$. Pour éliminer les premières l variables $x_1, \dots, x_l$, nous considérons l'application de projection

$$\pi_l : \mathbb{C}^n \rightarrow \mathbb{C}^{n-l}$$

qui envoie $(a_1, \dots, a_n)$ sur $(a_{l+1}, \dots, a_n)$. Si nous appliquons π_l à $V \subseteq \mathbb{C}^n$, alors nous obtenons

$$\pi_l(V) \subseteq \mathbb{C}^{n-l}.$$

Lemme

Soit $I_l = \langle f_1, \dots, f_s \rangle \cap \mathbb{C}[x_{l+1}, \dots, x_n]$ le l^{ieme} idéal d'élimination. Dans $\mathbb{C}^{n-l}$:
 $\pi_l(V) \subseteq V(I_l)$.

Remarque

Les points de $V(I_I)$ sont appelés les solutions partielles. A l'aide du lemme, on peut écrire : $\pi_I(V) = \{(a_{I+1}, \dots, a_n) \in V(I_I) \mid \exists a_1, \dots, a_I \in \mathbb{C} \text{ tel que } (a_1, \dots, a_I, a_{I+1}, \dots, a_n) \in V\}$.

Remarque

Les points de $V(I_I)$ sont appelés les solutions partielles. A l'aide du lemme, on peut écrire : $\pi_I(V) = \{(a_{I+1}, \dots, a_n) \in V(I_I) \mid \exists a_1, \dots, a_I \in \mathbb{C} \text{ tel que } (a_1, \dots, a_I, a_{I+1}, \dots, a_n) \in V\}$.
Donc $\pi_I(V)$ contient exactement toutes les solutions partielles qui peuvent s'étendre en des solutions complètes.

Théorème d'extension géométrique

Théorème d'extension géométrique

Soit $V = V(f_1, \dots, f_s) \subseteq \mathbb{C}^n$, soit $c_i \in \mathbb{C}[x_2, \dots, x_n]$ de la même forme que dans le théorème d'extension. Si I_1 est le premier idéal d'élimination de $\langle f_1, \dots, f_s \rangle$ alors on a dans $\mathbb{C}^{n-1}$: $V(I_1) = \pi_1(V) \cup (V(c_1, \dots, c_s) \cap V(I_1))$ où $\pi_1 : \mathbb{C}^n \rightarrow \mathbb{C}^{n-1}$ est la projection sur les $(n-1)^{ieme}$ coordonnées.

Théorème de fermeture

Théorème de fermeture

Soit $V = V(f_1, \dots, f_s) \subseteq \mathbb{C}^n$, et I_1 est le 1^{ier} idéal d'élimination de $\langle f_1, \dots, f_s \rangle$ alors :

- $V(I_1)$ est la plus petite variété affine contenant $\pi_1(V) \subseteq \mathbb{C}^{n-1}$
- Quand $V \neq \emptyset$, il y a une variété affine $W \subset V(I_1)$ telle que $V(I_1) \setminus W \subset \pi_1(V)$.

Remarque

Quand on dit "plus petite variété" on sous-entend au sens de l'inclusion de la théorie des ensembles i.e.

- $\pi_I(V) \subseteq V(I_I)$
- Si Z est une autre variété affine de $\mathbb{C}^{n-1}$ contenant $\pi_I(V)$ alors $V(I_I) \subseteq Z$

Théorème d'extension géométrique

Corollaire

Soit $V = V(f_1, \dots, f_s) \subseteq \mathbb{C}^n$ et supposons que $\forall i, f_i$ est de la forme : $f_i = c_i x_1^{N_i} + *$ où $*$ est une somme de termes où le degré de x_1 est $< N_i$ et $c_i \in \mathbb{C} \setminus \{0\}$ et $N_i > 0$. Si I_1 est le premier idéal d'élimination alors dans $\mathbb{C}^{n-1}$: $\pi_1(V) = V(I_1)$ où π_1 est la projection sur les $(n-1)^{ieme}$ dernières coordonnées.

Calcul de l'intersection de deux idéaux

Proposition

Soient I et J deux idéaux de $k[x_1, \dots, x_n]$, et soit w une nouvelle variable. Considérons l'idéal $\langle wI, (1-w)J \rangle$ dans $k[x_1, \dots, x_n, w]$. Alors, l'intersection de cet idéal avec $k[x_1, \dots, x_n]$ est donnée par :

$$I \cap J = \langle wI, (1-w)J \rangle \cap k[x_1, \dots, x_n].$$

On calcule donc une base de Gröbner pour ce nouvel idéal et on utilise les idéaux tronqués pour obtenir une base de Gröbner de $I \cap J$. On "tue" w en premier avec un ordre monomial avec $w > x_1, \dots, x_n$.

Application du calcul de l'intersection de deux idéaux

Considérons les idéaux suivants de $\mathbb{Q}[x, y]$:

$$I = (x^2 + y^3 - 1, x - yx + 3) \quad \text{et} \quad J = (x^2y - 1).$$

$$\langle w(x^2 + y^3 - 1), w(x - yx + 3), (1 - w)(x^2y - 1) \rangle \subset \mathbb{Q}[x, y, w]$$

$$G = \{x^3y^2 - x^3y - 3x^2y - xy + x + 3, x^2y^4 + x^4y - x^2y - y^3 - x^2 + 1,$$

$$12853w + 118x^4y + 9x^2y^3 - 357x^3y - 972x^2y^2 + 2152x^2y - 118x^2 - 9y^2 + 357x + 972y - 2152,$$

$$x^5y + 3x^2y^3 + 3x^2y^2 - x^3 + 3x^2y - 3y^2 - 3y - 3\}.$$

Ainsi, une base de Gröbner pour l'idéal $I \cap J$ est :

$$\{x^3y^2 - x^3y - 3x^2y - xy + x + 3, x^2y^4 + x^4y - x^2y - y^3 - x^2 + 1, x^5y + 3x^2y^3 + 3x^2y^2 - x^3 + 3x^2y - 3y^2 - 3y - 3\}.$$

Merci pour votre attention !