Etude d'une base de Gröbner en deux variables

Philippe TAN
Jarod XIE

Sorbonne Université

27 Mai 2024

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Conclusion

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Conclusion

Introduction

- Soit un système d'équations polynomiales $f_0 = \cdots = f_r = 0$ que l'on souhaite résoudre.
- $f_0, \ldots, f_r$ sont des polynômes en x et y.
- Les termes des polynômes ont des coefficients dans un corps $\mathbb{K}$.
- On note $F = \{f_0, \ldots, f_r\}$ l'ensemble contenant les polynômes de notre système.
- Avec l'algorithme de Buchberger, on transforme l'ensemble F en un nouvel ensemble G.
- Cet ensemble $G = \{g_0, \ldots, g_k\}$ est appelé base de Gröbner de F.

Introduction

Système d'équations polynomiales $f_1 = \cdots = f_r = 0$

$$F = \{f_1, \ldots, f_r\} \xrightarrow{\text{Algorithme de Buchberger}} G = \{g_1, \ldots, g_k\}$$

Quels sont les avantages de cette base de Gröbner ?

Introduction

Système d'équations polynomiales $f_1 = \cdots = f_r = 0$

$$F = \{f_1, \ldots, f_r\} \xrightarrow{\text{Algorithme de Buchberger}} G = \{g_1, \ldots, g_k\}$$

Quels sont les avantages de cette base de Gröbner ?

- G admet le même ensemble de solutions que F.
- Les polynômes de G possèdent des propriétés facilitant la résolution du système considéré.

Introduction

Système d'équations polynomiales $f_1 = \cdots = f_r = 0$

$$F = \{f_1, \ldots, f_r\} \xrightarrow{\text{Algorithme de Buchberger}} G = \{g_1, \ldots, g_k\}$$

Quels sont les avantages de cette base de Gröbner ?

- G admet le même ensemble de solutions que F.
- Les polynômes de G possèdent des propriétés facilitant la résolution du système considéré.

Exemples d'application

- En géométrie algébrique : trouver les points d'intersection entre différentes courbes ou surfaces définies par des équations polynomiales
- En cryptographie : problème des courbes elliptiques et schémas de chiffrement à base de polynômes.

Sommaire

Introduction

Cas simple d'interpolation
- Coordonnées x distinctes
- Répétition avec la même abscisse x

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Sommaire

Introduction

Cas simple d'interpolation
Coordonnées x distinctes
Répétition avec la même abscisse x

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Coordonnées x distinctes

- On considère des k paires de coordonnées (x, y) : $((x_0, y_0), \ldots, (x_{k-1}, y_{k-1}))$
- Aucune paire de coordonnées partage la même abscisse x_i

Comment trouver un polynôme $h(x, y)$ qui s'annule sur tous nos points (x_i, y_i) ?

Coordonnées x distinctes

- On considère des k paires de coordonnées (x, y) : $((x_0, y_0), \ldots, (x_{k-1}, y_{k-1}))$
- Aucune paire de coordonnées partage la même abscisse x_i

Comment trouver un polynôme $h(x, y)$ qui s'annule sur tous nos points (x_i, y_i) ?

Solution simple

Décomposition de $h(x, y)$ en $h_1(x)$ et $h_2(y)$ où :

$$h(x,y) = h_1(x) + h_2(y) \text{ ou } h_1(x) \cdot h_2(y) \begin{cases} h_1(x) = \prod_{i=0}^{k-1}(x - x_i) \\ h_2(y) = \prod_{i=0}^{k-1}(y - y_i) \end{cases}$$

Ou même simplement $h(x, y) = h_1(x)$ ou $h(x, y) = h_2(y)$.

Sommaire

Introduction

Cas simple d'interpolation
Coordonnées x distinctes
Répétition avec la même abscisse x

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Répétition avec la même abscisse x

- On considère des paires de coordonnées (x, y) avec k abscisses x distinctes deux à deux.
- Il existe des paires de coordonnées partageant la même abscisse x_i avec des ordonnées y_i différentes : $((x_i, y_i), (x_i, y_i'))$

La méthode précédente fonctionne puisque $h_1(x)$ et $h_2(y)$ sont construites de manière à s'annuler sur tous les x_i et tous les y_i

Répétition avec la même abscisse x

Exprimons y en fonction de x. Cherchons un polynôme $p(x)$ et trouvons lui une expression.
On teste $p(x) = y \Rightarrow y - p(x) = 0$

$$y - p(x) = 0 \begin{cases} p(x_0) & = y_0 \\ & \vdots \\ p(x_{k-1}) & = y_{k-1} \end{cases}$$

$$\begin{cases} p(x_i) & = y_i \\ p(x_i) & = y_i' \end{cases} \Rightarrow y_i = y_i' \text{ impossible}$$

Mais on peut trouver une solution pour $y^2 + ay - p(x) = 0$

Répétition avec la même abscisse x

Exemple pour $y^2 + ay - p(x) = 0$ avec les points $\{(-1,0),(1,0),(1,1),(2,2)\}$

$$y^2 + ay - p(x) = 0 \begin{cases} y_0^2 + ay_0 - p(x_0) & = 0 \\ & \vdots \\ y_k^2 + ay_k - p(x_k) & = 0 \end{cases}$$

Répétition avec la même abscisse x

Exemple pour $y^2 + ay - p(x) = 0$ avec les points $\{(-1,0),(1,0),(1,1),(2,2)\}$

$$y^2 + ay - p(x) = 0 \begin{cases} y_0^2 + ay_0 - p(x_0) & = 0 \\ & \vdots \\ y_k^2 + ay_k - p(x_k) & = 0 \end{cases}$$

$$\iff \begin{cases} p(-1) & = 0^2 + a0 = 0 \\ p(1) & = 0^2 + a0 = 0 \\ p(1) & = 1^2 + a1 = 1 + a \\ p(2) & = 2^2 + a2 = 4 + 2a \end{cases}$$

Répétition avec la même abscisse x

Exemple pour $y^2 + ay - p(x) = 0$ avec les points $\{(-1,0),(1,0),(1,1),(2,2)\}$ (suite) :

$$\begin{cases} p(-1) & = 0^2 + a0 = 0 \\ p(1) & = 0^2 + a0 = 0 \\ p(1) & = 1^2 + a1 = 1 + a \\ p(2) & = 2^2 + a2 = 4 + 2a \end{cases}$$

$$\begin{cases} p(1) & = 0 \\ p(1) & = 1 + a \end{cases} \iff \begin{cases} a = -1 \end{cases}$$

On trouve une expression de a, mais est-ce une solution générale ?
On vérifie pour $x = 2$: on obtient $4 + 2(-1) = 0$

Répétition avec la même abscisse x

Exemple pour $y^2 + ay - p(x) = 0$ avec les points $\{(-1,0),(1,0),(1,1),(2,2)\}$ (suite) :

$$y^2 + ay - p(x) = 0 \begin{cases} y_0^2 + ay_0 - p(x_0) & = 0 \\ & \vdots \\ y_k^2 + ay_k - p(x_k) & = 0 \end{cases}$$

$$\iff \begin{cases} p(-1) & = 0^2 + a0 = 0 \\ p(1) & = 0^2 + a0 = 0 \\ p(1) & = 1^2 + a1 = 1 + a = 1 - 1 = 0 \\ p(2) & = 2^2 + a2 = 4 + 2a = 4 - 2(-1) = 0 \end{cases}$$

On a alors trouvé un polynôme $p(x)$ tel que $y^2 + ay - p(x) = 0$ est vrai pour toutes nos paires de coordonnées.

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Conclusion

Approche matricielle

Introduction :

- Utilisation des matrices pour représenter des systèmes d'équations.
- Exemple avec $k = 6$ paires de coordonnées (x_i, y_i).
- Représentation sous forme de polynôme $P(x, y) = ax^2 + by^2 + cxy + dx + ey + f$.

Système d'équations :

$$\begin{cases} ax_0^2 + by_0^2 + cx_0y_0 + dx_0 + ey_0 + f = 0 \\ ax_1^2 + by_1^2 + cx_1y_1 + dx_1 + ey_1 + f = 0 \\ \vdots \\ ax_5^2 + by_5^2 + cx_5y_5 + dx_5 + ey_5 + f = 0 \end{cases}$$

Matrice A associée :

$$\begin{pmatrix} 1 & x_0 & y_0 & x_0y_0 & x_0^2 & y_0^2 \\ 1 & x_1 & y_1 & x_1y_1 & x_1^2 & y_1^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_5 & y_5 & x_5y_5 & x_5^2 & y_5^2 \end{pmatrix}$$

Condition d'inversibilité :

- La matrice est inversible si et seulement si son déterminant est non nul.
- Les vecteurs formés par les coordonnées doivent être linéairement indépendants.

Cas $k = 2$:

$$\begin{pmatrix} 1 & x_0 & y_0 \\ 1 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Généralisation :

- Forme générale pour un polynôme de degré d en deux variables :

$$P(x, y) = \sum_{i=0}^{d} \sum_{j=0}^{d-i} c_{ij} x^i y^j$$

- Nombre de termes : $\frac{(d+2)(d+1)}{2}$

Conclusion :

- Fournit un moyen systématique d'analyser l'existence de polynômes qui s'annulent en des points précis.
- Lorsque le nombre de points augmente, i.e la taille du système, nous pouvons construire un polynôme approprié pour l'ensemble des points
- Établit un lien fondamental entre l'algèbre linéaire et l'algèbre polynomiale

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Conclusion

Interpolation de Lagrange

Introduction :

- L'interpolation de Lagrange est une méthode pour trouver un polynôme passant par un ensemble donné de points.
- Utilisation fréquente en analyse numérique et en géométrie algorithmique.

Formule de base :

- Polynôme de Lagrange pour des points $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$:

$$L(x) = \sum_{i=0}^{n} y_i \ell_i(x)$$

- où les $\ell_i(x)$ sont les polynômes de base de Lagrange tel que :

$$\ell_i(x) = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{x - x_j}{x_i - x_j}$$

Exemple pratique :

- Considérons trois points: (x_0, y_0), (x_1, y_1), et (x_2, y_2).
- Les polynômes de base de Lagrange sont:

$$\ell_0(x) = \frac{(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)}$$

$$\ell_1(x) = \frac{(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)}$$

$$\ell_2(x) = \frac{(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)}$$

Polynôme interpolé :

$$L(x) = y_0\ell_0(x) + y_1\ell_1(x) + y_2\ell_2(x)$$

Problème rencontré :

- Ne permet pas d'avoir deux points qui ont la même abscisse
- On va donc séparer en deux sous-ensembles D et E, tel que D contient l'ensemble des points avec des abscisses distinct deux à deux et E les couples de points qui ont leurs abscisses identiques
- On cherche dans cette partie un polynôme de la forme $G(x) = y^2 + yg_3(x) + g_4(x)$
- Exemple avec 4 points (0,0), (0,1), (1,4) et (1,-4)

Application et Utilité :

- Utilisé pour interpoler des données et approcher des fonctions complexes.
- Précision dépend de la distribution des points x_i.
- Couramment utilisé dans les calculs numériques et graphiques.

Limites :

- Sensible aux oscillations pour un grand nombre de points (phénomène de Runge).
- Nécessité d'ajuster la méthode pour des données bruyantes ou irrégulières.

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Conclusion

Application du du Théorème des Restes Chinois (CRT)

L'interpolation de Lagrange est un cas particulier du Théorème des Restes Chinois.

Application du Théorème des Restes Chinois (CRT)

Théorème des Restes Chinois (CRT)

Étant donné des entiers $n_1, \ldots, n_k$ qui sont deux à deux premiers entre eux et des entiers arbitraires $a_1, \ldots, a_k$, alors le système :

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

a une unique solution modulo $N = n_1 n_2 \cdots n_k$:

$$x = a_1 M_1 y_1 + \cdots + a_k M_k y_k$$

où $M_i = N/n_i$ et $y_i \equiv M_i^{-1} \pmod{n_i}$ avec $1 \leq i \leq k$.

Application du Théorème des Restes Chinois (CRT)

CRT pour résoudre un système d'équation polynomiales :

- Pour chaque point (x_i, y_i) de D, on a une entrée dans notre système de congruence : $G \equiv y - y_i \pmod{x - x_i}$
- Pour chaque paire de points $((x_i, y_i), (x_i, y_i'))$ de E, on a une entrée dans notre système de congruence : $G \equiv (y - y_i)(y - y_i') \pmod{x_i}$

Application du Théorème des Restes Chinois (CRT)

CRT pour résoudre un système d'équation polynomiales :

- Pour chaque point (x_i, y_i) de D, on a une entrée dans notre système de congruence : $G \equiv y - y_i \pmod{x - x_i}$
- Pour chaque paire de points $((x_i, y_i), (x_i, y_i'))$ de E, on a une entrée dans notre système de congruence : $G \equiv (y - y_i)(y - y_i') \pmod{x_i}$

$$\begin{cases} G \equiv y - y_0 \pmod{x - x_0} \\ \vdots \\ G \equiv y - y_{d-1} \pmod{x - x_{d-1}} \\ G \equiv (y - y_d)(y - y_d') \pmod{x - x_d} \\ \vdots \\ G \equiv (y - y_{d+e-1})(y - y_{d+e-1}') \pmod{x - x_{d+e-1}} \end{cases}$$

Application du Théorème des Restes Chinois (CRT)

- On peut alors rassembler les éléments issus de D ensemble, et ceux issu de E ensemble :

$$\begin{cases} G & \equiv (y - h_1(x))(y - h_2(x)) \pmod{\prod_{i=d}^{d+e-1}(x - x_i)} \\ G & \equiv (y - h_3(x)) \pmod{\prod_{i=0}^{d-1}(x - x_i)} \end{cases}$$

- Puis on retrouve G avec la formule du CRT, qui est l'unique solution de ce système de congruence.

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Premier cas (g_0, g_1)

Second cas (g_0, g_1, g_2)

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Premier cas (g_0, g_1)

Second cas (g_0, g_1, g_2)

Premier cas (g_0, g_1)

- On considère les paires de coordonnées (x_i, y_i) sans répétition (de x_i) (éléments dans D).
- On note :

$$g_0(x) = \prod_{i=0}^{d-1}(x - x_i)$$

$g_1(x, y) = y - L(x)$ où $L(x)$ est un polynôme interpolateur de Lagrange

Premier cas (g_0, g_1)

- On considère les paires de coordonnées (x_i, y_i) sans répétition (de x_i) (éléments dans D).
- On note :

$$g_0(x) = \prod_{i=0}^{d-1}(x - x_i)$$

$g_1(x, y) = y - L(x)$ où $L(x)$ est un polynôme interpolateur de Lagrange

- Supposons maintenant qu'on ait un polynôme $P(x, y)$ qui s'annule sur tous nos points (x_i, y_i). Montrons qu'il existe deux polynômes $q_0(x, y)$ et $q_1(x, y)$ tels que :

$$P(x, y) = g_0(x)q_0(x, y) + g_1(x, y)q_1(x, y) \qquad (1)$$

Preuve 1

- Soit le polynôme $P(x, y) = yP_1(x) + P_0(x)$ s'annulant sur toutes nos paires de coordonnées (x_i, y_i).

Preuve 1

- Soit le polynôme $P(x, y) = yP_1(x) + P_0(x)$ s'annulant sur toutes nos paires de coordonnées (x_i, y_i). On réécrit $P(x, y)$:

$$\begin{aligned} P(x, y) &= yP_1(x) + P_0(x) \\ &= (y - L(x))P_1(x) + L(x)P_1(x) + P_0(x) \end{aligned}$$

Preuve 1

- Soit le polynôme $P(x, y) = yP_1(x) + P_0(x)$ s'annulant sur toutes nos paires de coordonnées (x_i, y_i). On réécrit $P(x, y)$:

$$\begin{aligned} P(x, y) &= yP_1(x) + P_0(x) \\ &= (y - L(x))P_1(x) + L(x)P_1(x) + P_0(x) \\ &= g_1(x, y)P_1(x) + L(x)P_1(x) + P_0(x) \end{aligned}$$

Preuve 1

- Soit le polynôme $P(x, y) = yP_1(x) + P_0(x)$ s'annulant sur toutes nos paires de coordonnées (x_i, y_i). On réécrit $P(x, y)$:

$$\begin{aligned} P(x, y) &= yP_1(x) + P_0(x) \\ &= (y - L(x))P_1(x) + L(x)P_1(x) + P_0(x) \\ &= g_1(x, y)P_1(x) + L(x)P_1(x) + P_0(x) \end{aligned}$$

- Alors on définit :

$$r(x, y) = P(x, y) - g_1(x, y)P_1(x) = L(x)P_1(x) + P_0(x) \qquad (2)$$

Preuve 1 (suite)

- Puisque $r(x, y)$ est pûrement en x et qu'il s'annule sur tous nos points (x_i, y_i), on peut alors poser :

$$L(x)P_1(x) + P_0(x) = g_0(x)q_0(x, y)$$

Preuve 1 (suite)

- Puisque $r(x, y)$ est pûrement en x et qu'il s'annule sur tous nos points (x_i, y_i), on peut alors poser :

$$L(x)P_1(x) + P_0(x) = g_0(x)q_0(x, y)$$

- Au final on obtient :

$$P(x, y) = g_1(x, y)q_1(x, y) + g_0(x)q_0(x, y)$$

avec $q_1(x, y) = P_1(x)$

- On retrouve bien l'expression (1).

Preuve 1 (suite)

- Puisque $r(x, y)$ est pûrement en x et qu'il s'annule sur tous nos points (x_i, y_i), on peut alors poser :

$$L(x)P_1(x) + P_0(x) = g_0(x)q_0(x, y)$$

- Au final on obtient :

$$P(x, y) = g_1(x, y)q_1(x, y) + g_0(x)q_0(x, y)$$

avec $q_1(x, y) = P_1(x)$

- On retrouve bien l'expression (1).

- On a alors prouvé l'existence d'une solution $P(x, y)$ exprimée en fonction de $g_0(x)$ et $g_1(x, y)$.

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Premier cas (g_0, g_1)

Second cas (g_0, g_1, g_2)

Second cas (g_0, g_1, g_2)

- On considère les paires de coordonnées (x_i, y_i) avec répétition (de x_i) (éléments dans $D \cup E$).
- On note :

  $$g_0(x) = \prod_{i=0}^{d-1}(x - x_i)$$

  $g_1(x, y) = y - L(x)$ où $L(x)$ est un polynôme interpolateur de Lagrange

  $$g_2(x, y) = y^2 + l_1(x)y + l_0(x)$$

- Supposons maintenant qu'on ait un polynôme $P(x, y)$ qui s'annule sur tous nos points (x_i, y_i). Montrons qu'il existe trois polynômes $q_0(x, y)$, $q_1(x, y)$ et $q_2(x, y)$ tels que :

$$P(x, y) = g_0(x)q_0(x, y) + g_1(x, y)q_1(x, y) + g_2(x, y)q_2(x, y) \quad (3)$$

Preuve 2

- Soit le polynôme $P(x, y) = y^2 P_(x) + yP_1(x) + P_0(x)$ s'annulant sur toutes nos paires de coordonnées (x_i, y_i).

Preuve 2

• Soit le polynôme $P(x, y) = y^2 P_(x) + yP_1(x) + P_0(x)$ s'annulant sur toutes nos paires de coordonnées (x_i, y_i). On réécrit $P(x, y)$:

$$\begin{aligned} P(x,y) = & \; y^2 P_2(x) + yP_1(x) + P_0(x) \\ = & \; g_2(x,y)P_2(x) - l_1(x,y)yP_2(x) - l_0(x,y)P_2(x) + yP_1(x) \\ & + P_0(x) \end{aligned}$$

Preuve 2

• Soit le polynôme $P(x,y) = y^2 P_(x) + yP_1(x) + P_0(x)$ s'annulant sur toutes nos paires de coordonnées (x_i, y_i). On réécrit $P(x,y)$:

$$\begin{aligned} P(x,y) &= y^2 P_2(x) + yP_1(x) + P_0(x) \\ &= g_2(x,y)P_2(x) - l_1(x,y)yP_2(x) - l_0(x,y)P_2(x) + yP_1(x) \\ &\quad + P_0(x) \\ &= g_2(x,y)P_2(x) + y\underbrace{(-l_1(x,y)yP_2(x) + yP_1(x))}_{\tilde{P}_1} \\ &\quad \underbrace{-l_0(x,y)P_2(x) + P_0(x)}_{\tilde{P}_0} \\ &= g_2(x,y)P_2(x) + y\tilde{P}_1(x) + \tilde{P}_0(x) \end{aligned}$$

Preuve 2 (suite)

$$P(x,y) = g_2(x,y)P_2(x) + y\tilde{P}_1(x) + \tilde{P}_0(x)$$

$$\underbrace{P(x,y) - g_2(x,y)P_2(x)}_{\text{cancel out on every}(x_i,y_i)} = y\tilde{P}_1(x) + \tilde{P}_0(x)$$

Preuve 2 (suite)

$$P(x,y) = g_2(x,y)P_2(x) + y\tilde{P}_1(x) + \tilde{P}_0(x)$$

$$\underbrace{P(x,y) - g_2(x,y)P_2(x)}_{\text{cancel out on every}(x_i,y_i)} = y\tilde{P}_1(x) + \tilde{P}_0(x)$$

$$= g_0(x)\tilde{q}_0(x,y) + g_1(x,y)\tilde{q}_1(x,y)$$

• On obtient la dernière ligne avec la preuve du cas 1 (slide 32)

Alors :

$$P(x,y) = g_2(x,y)q_2(x,y) + g_1(x,y)\tilde{q}_1(x,y) + g_0(x)\tilde{q}_0(x,y)$$

On retrouve bien l'expression (3)

Preuve 2 (suite)

$$P(x,y) = g_2(x,y)P_2(x) + y\tilde{P}_1(x) + \tilde{P}_0(x)$$

$$\underbrace{P(x,y) - g_2(x,y)P_2(x)}_{\text{cancel out on every}(x_i,y_i)} = y\tilde{P}_1(x) + \tilde{P}_0(x)$$

$$= g_0(x)\tilde{q}_0(x,y) + g_1(x,y)\tilde{q}_1(x,y)$$

• On obtient la dernière ligne avec la preuve du cas 1 (slide 32)

Alors :

$$P(x,y) = g_2(x,y)q_2(x,y) + g_1(x,y)\tilde{q}_1(x,y) + g_0(x)\tilde{q}_0(x,y)$$

On retrouve bien l'expression (3)

• On a alors prouvé l'existence d'une solution $P(x,y)$ exprimée en fonction de $g_0(x)$, $g_1(x,y)$ et $g_2(x,y)$.

Preuve de l'existence d'une solution avec nos polynômes

Conséquences :

- Polynôme $P(x, y)$ qui s'annule sur tous nos points :

$$P(x,y) = g_2(x,y)q_2(x,y) + g_1(x,y)\tilde{q_1}(x,y) + g_0(x)\tilde{q_0}(x,y)$$

Preuve de l'existence d'une solution avec nos polynômes

Conséquences :

- Polynôme $P(x, y)$ qui s'annule sur tous nos points :

$$P(x, y) = g_2(x, y)q_2(x, y) + g_1(x, y)\tilde{q_1}(x, y) + g_0(x)\tilde{q_0}(x, y)$$

- $P(x, y) \in \langle g_0(x), g_1(x, y), g_2(x, y) \rangle$

Preuve de l'existence d'une solution avec nos polynômes

Conséquences :

- Polynôme $P(x, y)$ qui s'annule sur tous nos points :

$$P(x, y) = g_2(x, y)q_2(x, y) + g_1(x, y)\tilde{q_1}(x, y) + g_0(x)\tilde{q_0}(x, y)$$

- $P(x, y) \in \langle g_0(x), g_1(x, y), g_2(x, y)\rangle$
- $P(x, y)$ est lié à l'idéal engendré par les polynômes de F via la base de Gröbner G

Preuve de l'existence d'une solution avec nos polynômes

Conséquences :

- Polynôme $P(x, y)$ qui s'annule sur tous nos points :

$$P(x, y) = g_2(x, y)q_2(x, y) + g_1(x, y)\tilde{q_1}(x, y) + g_0(x)\tilde{q_0}(x, y)$$

- $P(x, y) \in \langle g_0(x), g_1(x, y), g_2(x, y)\rangle$
- $P(x, y)$ est lié à l'idéal engendré par les polynômes de F via la base de Gröbner G
- Toutes les solutions du système F sont racines de $P(x, y)$

Preuve de l'existence d'une solution avec nos polynômes

Conséquences :

- Polynôme $P(x, y)$ qui s'annule sur tous nos points :

$$P(x, y) = g_2(x, y)q_2(x, y) + g_1(x, y)\tilde{q_1}(x, y) + g_0(x)\tilde{q_0}(x, y)$$

- $P(x, y) \in \langle g_0(x), g_1(x, y), g_2(x, y)\rangle$
- $P(x, y)$ est lié à l'idéal engendré par les polynômes de F via la base de Gröbner G
- Toutes les solutions du système F sont racines de $P(x, y)$

Preuve de l'existence d'une solution avec nos polynômes

Conséquences :

- Polynôme $P(x, y)$ qui s'annule sur tous nos points :

$$P(x, y) = g_2(x, y)q_2(x, y) + g_1(x, y)\tilde{q_1}(x, y) + g_0(x)\tilde{q_0}(x, y)$$

- $P(x, y) \in \langle g_0(x), g_1(x, y), g_2(x, y)\rangle$
- $P(x, y)$ est lié à l'idéal engendré par les polynômes de F via la base de Gröbner G
- Toutes les solutions du système F sont racines de $P(x, y)$

$\Rightarrow$ Résoudre le système d'équations polynomiales F, c'est chercher les racines de $P(x, y)$.

Sommaire

Introduction

Cas simple d'interpolation

Approche matricielle

Interpolation de Lagrange

Application du Théorème des Restes Chinois (CRT)

Preuve de l'existence d'une solution avec nos polynômes

Conclusion

Conclusion

Nous avons vu :

- **Techniques d'interpolation**
  - Interpolation dans des cas très simple.
  - Interpolation de Lagrange un peu plus avancée.

Conclusion

Nous avons vu :

- **Techniques d'interpolation**
  - Interpolation dans des cas très simple.
  - Interpolation de Lagrange un peu plus avancée.
- **Approche matricielle**
  - Possibilité lier l'algèbre linéaire à l'algèbre polynomial.

Conclusion

Nous avons vu :

- **Techniques d'interpolation**
  - Interpolation dans des cas très simple.
  - Interpolation de Lagrange un peu plus avancée.
- **Approche matricielle**
  - Possibilité lier l'algèbre linéaire à l'algèbre polynomial.
- **Fondement théorique**
  - Mise en avant du Théorème des Restes Chinois pour répondre à notre problème

Conclusion

Nous avons vu :

- **Techniques d'interpolation**
  - Interpolation dans des cas très simple.
  - Interpolation de Lagrange un peu plus avancée.
- **Approche matricielle**
  - Possibilité lier l'algèbre linéaire à l'algèbre polynomial.
- **Fondement théorique**
  - Mise en avant du Théorème des Restes Chinois pour répondre à notre problème
- **Preuve d'existence**
  - Nous avons prouvé l'existence d'une solution en fonction des polynômes que nous avons interpolés.