Précision p-adique, échelonnement matriciel et bases de Gröbner

Tristan Vaccon

Université de Rennes I

15 mai 2013

Besoin de calculs p-adiques

Quelques motivations

- Dans l'étude des représentations p-adiques du groupe de Galois absolu d'un corps p-adique : besoin de Calcul Effectif en Théorie de Hodge p-adique ;
- Applications cryptographiques possibles : comptage de point sur des variétés.

1 Précision p-adique et algorithme de Gauss
- Puissance de la précision p-adique
- Analyse de la perte de précision dans l'échelonnement de Gauss

2 Application aux bases de Gröbner
- L'algorithme F5
- Considérations p-adiques

Plan de l'exposé

1 Précision p-adique et algorithme de Gauss
- Puissance de la précision p-adique
- Analyse de la perte de précision dans l'échelonnement de Gauss

2 Application aux bases de Gröbner
- L'algorithme F5
- Considérations p-adiques

Définition de la précision

p-adiques à précision fixée

Les éléments de $\mathbb{Q}_p$ sont de la forme $\sum_{i=-l}^{+\infty} a_i p^i$, avec $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ et p un nombre premier.
Nécessairement, en machine, on se restreint au début de ce développement en série, et on ne considère que des éléments de la forme suivante : $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, avec $l \in \mathbb{Z}$.

Définition de la précision

p-adiques à précision fixée

Les éléments de $\mathbb{Q}_p$ sont de la forme $\sum_{i=-l}^{+\infty} a_i p^i$, avec $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ et p un nombre premier.
Nécessairement, en machine, on se restreint au début de ce développement en série, et on ne considère que des éléments de la forme suivante : $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, avec $l \in \mathbb{Z}$.

Définition

L'**ordre**, ou la **précision absolue** de $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ est d. Sa **précision relative** correspond au nombre de ses chiffres significatifs, et est donnée par $d - \min\{i \in \mathbb{Z}, a_i \neq 0\}$.

Définition de la précision

p-adiques à précision fixée

Les éléments de $\mathbb{Q}_p$ sont de la forme $\sum_{i=-l}^{+\infty} a_i p^i$, avec $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ et p un nombre premier.
Nécessairement, en machine, on se restreint au début de ce développement en série, et on ne considère que des éléments de la forme suivante : $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, avec $l \in \mathbb{Z}$.

Définition

L'**ordre**, ou la **précision absolue** de $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ est d. Sa **précision relative** correspond au nombre de ses chiffres significatifs, et est donnée par $d - \min\{i \in \mathbb{Z}, a_i \neq 0\}$.

Exemple

L'ordre de $3 * 7^{-1} + 4 * 7^0 + 5 * 7^1 + 6 * 7^2 + O(7^3)$ est 3, et sa précision relative $4 = 3 - (-1)$.

Précision p-adique contre précision réelle

L'essence de l'étude de la précision p-adique provient de la remarque suivante :

Proposition (Les erreurs de précision ne se cumulent pas)

On a :

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

Autrement dit, si a et b sont connus avec une précision $O(p^k)$, alors $a + b$ aussi.

Précision p-adique contre précision réelle

L'essence de l'étude de la précision p-adique provient de la remarque suivante :

Proposition (Les erreurs de précision ne se cumulent pas)

On a :

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

Autrement dit, si a et b sont connus avec une précision $O(p^k)$, alors $a + b$ aussi.

Précision p-adique contre précision réelle

L'essence de l'étude de la précision p-adique provient de la remarque suivante :

Proposition (Les erreurs de précision ne se cumulent pas)

On a :

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

Autrement dit, si a et b sont connus avec une précision $O(p^k)$, alors $a + b$ aussi.

Remarque

Ceci est le contraire du cas réel, et de ses **erreurs d'arrondis** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

Autrement dit, si a et b sont connus avec une précision 10^{-n}, alors $a + b$ est connu à $10^{(-n+1)}$.

Précision p-adique contre précision réelle

L'essence de l'étude de la précision p-adique provient de la remarque suivante :

Proposition (Les erreurs de précision ne se cumulent pas)

On a :

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

Autrement dit, si a et b sont connus avec une précision $O(p^k)$, alors $a + b$ aussi.

Remarque

Ceci est le contraire du cas réel, et de ses **erreurs d'arrondis** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

Autrement dit, si a et b sont connus avec une précision 10^{-n}, alors $a + b$ est connu à $10^{(-n+1)}$.

Formules de précision

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Formules de précision

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Formules de précision

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Proposition (division)

$$\frac{xp^a + O(p^b)}{yp^c + O(p^d)} = x * y^{-1}p^{a-c} + O(p^{min(d+a-2c,b-c)})$$

En particulier,

$$\frac{1}{p^c y + O(p^d)} = y^{-1}p^{-c} + O(p^{d-2c})$$

Plan de l'exposé

1 Précision p-adique et algorithme de Gauss
- Puissance de la précision p-adique
- Analyse de la perte de précision dans l'échelonnement de Gauss

2 Application aux bases de Gröbner
- L'algorithme F5
- Considérations p-adiques

Méthode de Gauss : Résultat

Théorème

Méthode de Gauss : Résultat

Théorème

Soit M une matrice $n \times m$ ($n \leqslant m$) dont les coefficients sont des entiers p-adiques connus avec la précision uniforme $O(p^k)$, et telles que son mineur principal $\Delta = det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})$ vérifie $val(\Delta) < k$.

Méthode de Gauss : Résultat

Théorème

Soit M une matrice $n \times m$ ($n \leqslant m$) dont les coefficients sont des entiers p-adiques connus avec la précision uniforme $O(p^k)$, et telles que son mineur principal $\Delta = det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})$ vérifie $val(\Delta) < k$.
Alors, la perte maximale de précision lorsque l'on effectue l'échelonnement de M par l'algorithme de Gauss peut être majorée par $val(\Delta)$ (autrement dit, on peut calculer les coefficients de la forme échelonnée à précision $O(p^{k-val(\Delta)})$).

Méthode de Gauss : Démonstration

Proof.

$$M = \begin{bmatrix} m_{1,1} + O(p^k) & \cdots & m_{1,n} + O(p^k) & \cdots \\ \vdots & m_{i,j} + O(p^k) & \vdots & \\ m_{n,1} + O(p^k) & \cdots & m_{n,n} + O(p^k) & \cdots \; m_{n,m} + O(p^k) \end{bmatrix}$$

□

Méthode de Gauss : Démonstration

Proof.

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & \cdots & m_{1,m}^{(1)} + O(p^k) \\ O(p^k) & m_{2,2}^{(1)} + O(p^k) & \cdots & m_{2,m}^{(1)} + O(p^k) \\ \vdots & \vdots & \ddots & \\ & & m_{i,j}^{(1)} + O(p^k) & \\ O(p^k) & m_{n,2}^{(1)} + O(p^k) & \cdots & m_{n,m}^{(1)} + O(p^k) \end{bmatrix}$$

$$\begin{aligned} L_1 &\leftarrow c_1^{-1} L_1 \\ L_2 &\leftarrow L_2 - \frac{m_{2,1}}{m_{1,1}} L_1 \\ &\vdots \\ L_n &\leftarrow L_n - \frac{m_{n,1}}{m_{1,1}} L_1 \end{aligned}$$

On prend comme pivot le coefficient sur la première colonne de **plus petite valuation**, mis sur la première ligne par un échange de lignes : $M_{1,1} = c_1 * p^{a_1} + O(p^k)$.
De plus, comme $a_1 \leqslant val(m_{j,1})$, $\frac{m_{n,1}}{m_{1,1}}$ est dans $\mathbb{Z}_p$, connu à l'ordre k au moins. □

Méthode de Gauss : Démonstration

Proof.

$$M \simeq \begin{bmatrix} p^{a1} + O(p^k) & \cdots & & m_{1,m}^{(2)} + O(p^k) \\ O(p^k) & p^{a2} + O(p^k) & \cdots & m_{2,m}^{(1)} + O(p^k) \\ \vdots & O(p^k) & m_{i,j}^{(2)} + O(p^k) & \\ O(p^k) & O(p^k) & m_{n,3}^{(2)} + O(p^k) \cdots & m_{n,m}^{(2)} + O(p^k) \end{bmatrix}$$

$$L_2 \leftarrow a_2^{-1} L_2$$
$$L_3 \leftarrow L_3 - \frac{m_{3,2}^{(1)}}{m_{2,2}^{(1)}} L_2$$
$$\vdots$$
$$L_n \leftarrow L_n - \frac{m_{n,2}^{(1)}}{m_{2,2}^{(1)}} L_2$$

(avec $M_{2,2} = c_2 * p^{a_2} + O(p^k)$)

□

Méthode de Gauss : Démonstration

Proof.

Au bout de $n-1$ étapes, nous sommes ramenés au cas d'une matrice échelonnée à $O(p^k)$ près :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{i,j}^{(n-1)} + O(p^k) \\ O(p^k) & p^{a_2} + O(p^k) & & \\ \vdots & \ddots & \ddots & \\ O(p^k) & \cdots & O(p^k) & p^{a_n} + O(p^k) \end{bmatrix}$$

Méthode de Gauss : Démonstration

Proof.

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(n)} + O(p^k) \\ \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_2} + O(p^{k-a_1}) & & \\ & O(p^{k-a_1}) & & m_{i,j}^{(n)} + O(p^{k-a_1}) \\ & & \ddots & \\ & O(p^{k-a_1}) \cdots & O(p^{k-a_1}) & p^{a_n} + O(p^{k-a_1}) \end{bmatrix}.$$

$$L_2 \leftarrow L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$L_3 \leftarrow L_3 - \frac{M_{3,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$\vdots$$

$$L_n \leftarrow L_n - \frac{M_{n,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

En effet, $M_{2,1}^{(n-1)} - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} * M_{1,1}^{(n-1)} = 0$.

Par ailleurs, $\frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} = \frac{O(p^k)}{p^{a_1}+O(p^k)} = O(p^{k-a_1})$, donc $L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1 = L_2 + O(p^{k-a_1})L_1$.

Méthode de Gauss : Démonstration

Proof.

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(n)} + O(p^k) \\ \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_2} + O(p^{k-a_1}) & & \\ & O(p^{k-a_1}) & & m_{i,j}^{(n)} + O(p^{k-a_1}) \\ & & \ddots & \vdots \\ & O(p^{k-a_1}) \cdots & O(p^{k-a_1}) & p^{a_n} + O(p^{k-a_1}) \end{bmatrix}.$$

$$L_2 \leftarrow L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$L_3 \leftarrow L_3 - \frac{M_{3,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$\vdots$$

$$L_n \leftarrow L_n - \frac{M_{n,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

En effet, $M_{2,1}^{(n-1)} - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} * M_{1,1}^{(n-1)} = 0$.

Par ailleurs, $\frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} = \frac{O(p^k)}{p^{a_1} + O(p^k)} = O(p^{k-a_1})$, donc $L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1 = L_2 + O(p^{k-a_1}) L_1$.

Méthode de Gauss : Démonstration

Proof.

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(n)} + O(p^k) \\ \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_2} + O(p^{k-a_1}) & & \\ & O(p^{k-a_1}) & & m_{i,j}^{(n)} + O(p^{k-a_1}) \\ & O(p^{k-a_1}) \cdots & O(p^{k-a_1}) & p^{a_n} + O(p^{k-a_1}) . \end{bmatrix}$$

$$\begin{aligned} L_2 &\leftarrow L_2 + O(p^{k-a_1})L_1 \\ L_3 &\leftarrow L_3 + O(p^{k-a_1})L_1 \\ &\vdots \\ L_n &\leftarrow L_n + O(p^{k-a_1})L_1 \end{aligned}$$

En effet, $M_{2,1}^{(n-1)} - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} * M_{1,1}^{(n-1)} = 0$.

Par ailleurs, $\frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} = \frac{O(p^k)}{p^{a_1}+O(p^k)} = O(p^{k-a_1})$, donc $L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1 = L_2 + O(p^{k-a_1})L_1$.

□

Méthode de Gauss : Démonstration

Proof.

On fait de même avec les colonnes suivantes :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & & \\ \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_2} + O(p^{k-a_1}) & & & \\ & \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_3} + O(p^{k-a_1-a_2}) & & \\ & & O(p^{k-a_1-a_2}) & \ddots & \\ & & \vdots & & \\ & & O(p^{k-a_1-a_2}) & \cdots & O(p^{k-a_1-a_2}) \end{bmatrix} \begin{matrix} m_{1,j}^{(n+1)} + O(p^k) \\ m_{2,j}^{(n+1)} + O(p^{k-a_1}) \\ m_{3,j}^{(n+1)} + O(p^{k-a_1-a_2}) \\ \cdots \\ \cdots \\ p^{a_n} + O(p^{k-a_1-a_2}) \end{matrix}$$

□

Méthode de Gauss : Démonstration

Proof.

À la fin, on obtient :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(2n-2)} + O(p^k) \\ & p^{a_2} + O(p^{k-a_1}) & & \\ 0 & & \ddots & m_{i,j}^{(2n-2)} + O(p^{k-a_1 \cdots - a_{i-1}}) \\ & & & \\ 0 & & 0 \quad p^{a_n} + O(p^{k-a_1 \cdots - a_{n-1}}) & \end{bmatrix}$$

La perte de précision sur la ligne i est $\sum_{j=1}^{i-1} a_j$.

□

Méthode de Gauss : Démonstration

Proof.

À la fin, on obtient :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(2n-2)} + O(p^k) \\ & p^{a_2} + O(p^{k-a_1}) & & \\ 0 & & \ddots & m_{i,j}^{(2n-2)} + O(p^{k-a_1 \cdots - a_{i-1}}) \\ & & & \\ 0 & & 0 \quad p^{a_n} + O(p^{k-a_1 \cdots - a_{n-1}}) & \end{bmatrix}$$

La perte de précision sur la ligne i est $\sum_{j=1}^{i-1} a_j$.
Or, $val(det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})) = \sum_{j=1}^{n} a_i$, et les a_i sont positifs.
La perte de précision est donc bien majorée par
$val(det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n}))$.

□

Plan de l'exposé

1 Précision p-adique et algorithme de Gauss
- Puissance de la précision p-adique
- Analyse de la perte de précision dans l'échelonnement de Gauss

2 Application aux bases de Gröbner
- L'algorithme F5
- Considérations p-adiques

Une brève présentation

Notations

Dans ce qui suit, k est un corps, $n, s \in \mathbb{N}$, et on note $R = k[X_1, \ldots, X_n]$.
On note R_d pour les polynômes homogènes de degré d de R.
On prend ω un ordre monomial sur R.

Une brève présentation

Notations

Dans ce qui suit, k est un corps, $n, s \in \mathbb{N}$, et on note $R = k[X_1, \ldots, X_n]$.
On note R_d pour les polynômes homogènes de degré d de R.
On prend ω un ordre monomial sur R.

Proposition (D. Lazard 83)

Pour un idéal I engendré par des polynômes homogènes $f_1, \ldots, f_s \in R$, alors $I \cap R_d$ est engendré par les $x^\alpha f_i$ où $|\alpha| + \deg(f_i) = d$.

Une brève présentation

Définition (Matrice de Macaulay)

On note $Mac_d(f_1, \ldots, f_s)$ la matrice

$$x^{d_1} > \quad \ldots \quad > \quad \ldots \quad > x^{d\binom{n-1}{n+d-1}}$$

$$\begin{matrix} x^{\alpha_{1,1}} f_1 \\ \vdots \\ x^{\alpha_{1,\binom{n-1}{n+d-d_1-1}}} f_1 \\ x^{\alpha_{2,1}} f_2 \\ \vdots \\ x^{\alpha_{s,\binom{n-1}{n+d-d_s-1}}} f_s \end{matrix} \begin{bmatrix} & & \\ & x^{\alpha} f_i \quad \text{dans la} \quad \text{base des} \quad x^{d_i} & \\ & & \end{bmatrix}$$

dont les lignes sont les polynômes $x^{\alpha} f_i$ écrits dans la base $x^{d_1}, \ldots, x^{d\binom{n-1}{n+d-1}}$, avec $|\alpha| + \deg(f_i) = d$.

Une brève présentation

Principe de l'algorithme F5 matriciel

L'idée est d'échelonner successivement les matrices $Mac_d(f_1, \ldots, f_i)$ en faisant croitre d et i.
La connaissance du profil de $Mac_d(f_1, \ldots, f_i)$ donne les termes de têtes de $LT((f_1, \ldots, f_i)_d)$ et des informations sur les lignes inutiles des $Mac_{d'}(f_1, \ldots, f_{i'})$ pour $d' > d$ et $i' > i$.

Plan de l'exposé

1 Précision p-adique et algorithme de Gauss
- Puissance de la précision p-adique
- Analyse de la perte de précision dans l'échelonnement de Gauss

2 Application aux bases de Gröbner
- L'algorithme F5
- Considérations p-adiques

Le problème de la position de l'idéal de tête

Souci des tests à zéro

Un souci majeur apparait lorsqu'on ne considère que des données connues à précision fixée : celui de ne pas savoir si une colonne est sans pivot ou si la précision est insuffisante.

Problème de la détermination de l'idéal de tête

$$\begin{bmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 1+O(p^k) & 1+O(p^k) & 0 & 1+O(p^k) \end{bmatrix}$$

$$L_2 \leftarrow L_2 - \frac{M_{2,1}}{M_{1,1}} L_1$$

Le problème de la position de l'idéal de tête

Souci des tests à zéro

Un souci majeur apparait lorsqu'on ne considère que des données connues à précision fixée : celui de ne pas savoir si une colonne est sans pivot ou si la précision est insuffisante.

Problème de la détermination de l'idéal de tête

$$\begin{bmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & -1+O(p^k) & 1+O(p^k) \end{bmatrix} \qquad L_2 \leftarrow L_2 - (1+O(p^k))L_1$$

Le problème de la position de l'idéal de tête

Souci des tests à zéro

Un souci majeur apparait lorsqu'on ne considère que des données connues à précision fixée : celui de ne pas savoir si une colonne est sans pivot ou si la précision est insuffisante.

Problème de la détermination de l'idéal de tête

$$\begin{bmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & -1+O(p^k) & 1+O(p^k) \end{bmatrix} \qquad L_2 \leftarrow L_2 - (1+O(p^k))L_1$$

Quel est le terme de tête pour la deuxième ligne ?

Conjecture de Moreno-Socias

Définition (Idéal faiblement ω)

Si ω est un ordre monomial sur R, et si I est un idéal de R. On dit que I est **faiblement**-ω si : pour tout x^α qui est un terme de tête d'une base de Gröbner minimale de I pour l'ordre ω, alors $LT(I)$ contient tout les monômes de degré $|\alpha|$ qui sont plus grand que x^α pour l'ordre ω.

Conjecture de Moreno-Socias

Définition (Idéal faiblement ω)

Si ω est un ordre monomial sur R, et si I est un idéal de R. On dit que I est **faiblement**-ω si : pour tout x^α qui est un terme de tête d'une base de Gröbner minimale de I pour l'ordre ω, alors $LT(I)$ contient tout les monômes de degré $|\alpha|$ qui sont plus grand que x^α pour l'ordre ω.

Conjecture (Moreno-Socias)

Si k est infini, si $d_1, \ldots, d_s \in \mathbb{N}^*$, il existe un ouvert de Zariski non-vide U de $k[X_1, \ldots, X_n]_{d_1} \times \cdots \times k[X_1, \ldots, X_n]_{d_s}$ tel que pour tout $(f_1, \ldots, f_s) \in U$:

Conjecture de Moreno-Socias

Définition (Idéal faiblement ω)

Si ω est un ordre monomial sur R, et si I est un idéal de R. On dit que I est **faiblement**-ω si : pour tout x^α qui est un terme de tête d'une base de Gröbner minimale de I pour l'ordre ω, alors $LT(I)$ contient tout les monômes de degré $|\alpha|$ qui sont plus grand que x^α pour l'ordre ω.

Conjecture (Moreno-Socias)

Si k est infini, si $d_1, \ldots, d_s \in \mathbb{N}^*$, il existe un ouvert de Zariski non-vide U de $k[X_1, \ldots, X_n]_{d_1} \times \cdots \times k[X_1, \ldots, X_n]_{d_s}$ tel que pour tout $(f_1, \ldots, f_s) \in U$: $(f_1, \ldots, f_s)$ engendre un idéal faiblement grevlex.

Conjecture de Moreno-Socias

Définition (Idéal faiblement ω)

Si ω est un ordre monomial sur R, et si I est un idéal de R. On dit que I est **faiblement**-ω si : pour tout x^α qui est un terme de tête d'une base de Gröbner minimale de I pour l'ordre ω, alors $LT(I)$ contient tout les monômes de degré $|\alpha|$ qui sont plus grand que x^α pour l'ordre ω.

Conjecture (Moreno-Socias)

Si k est infini, si $d_1, \ldots, d_s \in \mathbb{N}^*$, il existe un ouvert de Zariski non-vide U de $k[X_1, \ldots, X_n]_{d_1} \times \cdots \times k[X_1, \ldots, X_n]_{d_s}$ tel que pour tout $(f_1, \ldots, f_s) \in U$: $(f_1, \ldots, f_s)$ engendre un idéal faiblement grevlex.

Remarque

En conséquence, les suites régulières donnant un idéal faiblement grevlex seraient génériques.

Proposition d'algorithme

Proposition (Algorithme F5 "faible")

On peut modifier l'algorithme F5 pour des idéaux faiblement ω de la façon suivante :

- *On procède d'abord à l'algorithme F5 normalement ;*

Proposition d'algorithme

Proposition (Algorithme F5 "faible")

On peut modifier l'algorithme F5 pour des idéaux faiblement ω de la façon suivante :

- *On procède d'abord à l'algorithme F5 normalement ;*
- *Mais, dès qu'on rencontre une colonne sans pivot dans l'échelonnement : on stoppe l'échelonnement, et on complète la matrice en remplaçant ses lignes non encore réduites par des multiples des lignes de $\widetilde{Mac}_{d-1,i}$ de manière à obtenir une matrice échelonnée.*

3 quadriques en 6 variables

Un exemple

Pour 3 quadriques génériques en 6 variables, on obtient après réduction pour la matrice de Macaulay en degré 3 :

$$\left[\begin{array}{c|c} \text{bloc 9x9 inversible} & \text{(perte de précision : déterminant de la matrice 9x9)} \\ \hline 0 & \text{9 lignes multiples des lignes de la matrice en degré 2} \end{array}\right].$$

Un résultat possible

Proposition

Soit $(f_1, \ldots, f_s)$ une suite régulière de polynôme homogènes dans $\mathbb{Q}_p[X_1, \ldots, X_n]$, telle que les $I_i = (f_1, \ldots, f_i)$ soient des idéaux faiblement ω.
Si les f_i sont connus avec une précision suffisante (i.e. plus grande que les valuations des mineurs non nuls maximaux sur les premières colonnes des matrices de Macaulay définies par les f_i), alors on peut calculer (par un algorithme F5) une approximation d'une base de Gröbner de I pour ω, et celle-ci est bien définie.

Remarque

La conjecture de Moreno-Socias nous permettrait d'en déduire qu'ainsi, on peut calculer une base de Gröbner pour l'ordre grevlex pour presque toute suite $(f_1, \ldots, f_s)$ de $\mathbb{Q}_p[X_1, \ldots, X_n]$ (avec $s \leqslant n$). On a de plus une expression pour la précision nécessaire.

Comment faire mieux ?

- Pour des calculs de base de Gröbner, on fixe un ordre monomial, et on ne tient pas du tout compte des valuations des coefficients :

Comment faire mieux ?

- Pour des calculs de base de Gröbner, on fixe un ordre monomial, et on ne tient pas du tout compte des valuations des coefficients :
  - Calcul de bases de bord ?

Comment faire mieux ?

- Pour des calculs de base de Gröbner, on fixe un ordre monomial, et on ne tient pas du tout compte des valuations des coefficients :
  - Calcul de bases de bord ?
  - Tenir compte de la valuation dans le choix du monôme dominant : "bases de Gröbner tropicales".

Comment faire mieux ?

- Pour des calculs de base de Gröbner, on fixe un ordre monomial, et on ne tient pas du tout compte des valuations des coefficients :
  - Calcul de bases de bord ?
  - Tenir compte de la valuation dans le choix du monôme dominant : "bases de Gröbner tropicales".
- estimation de la précision requise : (travail en cours),

$$\mathbb{P}(val(P(X_1,\ldots,X_n)) \geqslant a) \leqslant (1+\frac{1}{\sqrt{p}})^n \times \frac{p^{val(LC(P))/2d}}{p^{a/2d}},$$

où $LM(P) = X_1^{d_1}\ldots X_n^{d_n}$ et $d = max(d_1,\ldots,d_n)$.

Bardet, Magali

"Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie", thèse de doctorat, Université Paris VI, Décembre 2004.

Caruso, Xavier

Random matrix over a DVR and LU factorization, preprint.

Faugère, Jean-Charles

A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In Proceedings of the 2002 international symposium on Symbolic and algebraic computation, ISSAC '02, pages 75-83, New York, NY, USA, 2002. ACM.

Moreno-Socias, Guillermo

Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991.

Pardue, Keith

Generic Sequences of Polynomials, J. Algebra 324 (2010), no. 4, 579–590

Sasaki,T. & Kako,F.

Term cancellations in computing floating-point Gröbner bases. In Proceedings of CASC 2010, volume 6244 of Lecture Notes in Comput. Sci., pages 220–231, Berlin, 2010. Springer.