PGCD numérique de deux polynômes

Action incitative INRIA Fiable

Olivier BEAUMONT — ENS Lyon

Bernard PHILIPPE — INRIA/IRISA – Rennes

Comment définir le PGCD numérique

Problème Soient p et q deux polynômes qui peuvent provenir de calculs antérieurs.
Comment définir leurPGCD ?
Le calcul exact n'est pas adapté
$\Longrightarrow$ définition par voisinage:
p et q ont un PGCD de degré k à ϵ près $\Longleftrightarrow$

$$k = \max_i \left(\left\{ \begin{array}{ll} \exists \Delta p, & ||\Delta p|| \leq \epsilon \\ \exists \Delta p, & ||\Delta p|| \leq \epsilon \end{array} \right. , deg(PGCD(p + \delta p, p + \delta p)) = i \right).$$

Comment obtenir une majoration du degré du PGCD?

Matrice de Sylvester:

$$S(p,q) = \begin{pmatrix} p_0 & p_1 & \cdots & p_n & & & & \\ & p_0 & p_1 & & \cdots & p_n & & \\ & & \ddots & & & & \ddots & \\ & & & p_0 & & p_1 & \cdots & p_n \\ q_0 & q_1 & \cdots & q_m & & & & \\ & q_0 & q_1 & & \cdots & q_m & & \\ & & \ddots & & & & \ddots & \\ & & & q_0 & & q_1 & \cdots & q_m \end{pmatrix}$$

On sait que

$$dim(Ker(S(p,q))) = deg(pgcd(p,q)).$$

Il suffit de surestimer la taille du noyau de $S(p,q)$.

Comment obtenir une majoration du degré?

- Faire une QR avec pivot de S

$$R = \begin{pmatrix} r_{1,1} & & & & & \\ & \ddots & & & & \\ & & \ddots & & & \\ & & & r_{i,i} & & \\ & & & & \ddots & \\ & & & & & r_{n+m,n+m} \end{pmatrix}, \quad r_{i,i} \leq r_{j,j}, \quad i < j.$$

Calcul d'erreur: $|\widehat{r_{i,i}} - r_{i,i}| \leq (n+m)^{1.5}\epsilon |r_{1,1}|$

- On considère que $r_{i,i}$ peut être nul dès que

$$\widehat{r_{i,i}} \leq (n+m)^{1.5}\epsilon.$$

Comment obtenir une approximation du PGCD?

On connaît une base du noyau $Q^{(i)} = \begin{pmatrix} q_1 & q_2 & \dots & q_i \end{pmatrix}$.
On sait que si $\lambda_1, \lambda_2, \dots, \lambda_i$ sont les racines communes, alors

$$\begin{pmatrix} \lambda_1 & \dots & \lambda_i \\ \lambda_1^2 & \dots & \lambda_i^2 \\ \vdots & & \vdots \\ \lambda_1^{n+m} & \dots & \lambda_i^{n+m} \end{pmatrix}$$ est une base de $Q^{(i)}$.

Si le PGCD s est de la forme $s = s_0 + s_1 X + \dots + s_i X^i$ alors

$$\forall j, Q^{(i)}(j : j + i, 1 : j)s = -Q^{(i)}(1 + j + i, 1 : j).$$

On peut donc retrouver s en résolvant un système linéaire de petite taille.

Conclusion à la fin de la première phase

On a déterminé s et par division euclidienne on peut obtenir

$$\begin{cases} p = b_p s + r_p \\ q = b_q s + r_q \end{cases},$$

où r_p et r_q sont a priori petits.
On peut donc vérifier que

$$\begin{cases} p - r_p = b_p s \\ q - r_q = b_q s \end{cases},$$

ce qui nous donne une idée de PGCD numérique puisque $(p - r_p)$ et $(q - r_q)$ admettent s comme diviseur commun.

Raffinement du résultat

Dans ce qui suit, on va chercher deux polynômes $p+\delta p$ et $q+\delta q$ dont le degré du PGCD est $deg(s)$.
On cherche $\delta b_p, \quad \delta b_q$ et δs vérifiant

$$\left\{\begin{array}{l} p = (b_p+\delta b_p)(s+\delta s) \\ q = (b_q+\delta b_q)(s+\delta s) \end{array}\right. ,$$

soit, au premier ordre,

$$\left\{\begin{array}{l} p = b_p s + \delta b_p s + b_p \delta s \\ q = b_q s + \delta b_q s + b_q \delta s \end{array}\right. .$$

On obtient ainsi un système à $n+m+2$ équations et $n+m-degre(s)+3$, qu'on peut résoudre par les moindres carrés.

Résultats numériques (1)

$$\left\{ \begin{array}{l} p = \prod_{i=1}^{10} (X - i) \\ q = \prod_{i=9}^{15} (X - i) \end{array} \right. .$$

Le degré du PGCD de p et q est majoré par 2.

	$\frac{\text{norme du résidu}}{\text{norme de } p}$	$\frac{\text{norme du résidu}}{\text{norme de } q}$
Avant raffinement	$6 \;\; 10^{-6}$	$1 \;\; 10^{-9}$
Après raffinements (2)	$1 \;\; 10^{-16}$	$9 \;\; 10^{-17}$

	avant raffinement	après raffinements
racine 1	10.000038	9.99999999997
racine 2	8.999986	9.00000000003

Résultats numériques (2)

$$\begin{cases} p = T_{12}(X) + .3090169943752925X \\ q = T_{10}(X) \end{cases}.$$

Le degré du PGCD de p et q est majoré par 4.

	$\frac{\text{norme du résidu}}{\text{norme de } p}$	$\frac{\text{norme du résidu}}{\text{norme de } q}$
Avant raffinement	$1 \quad 10^{-13}$	$4 \quad 10^{-13}$
Après raffinements (1)	$1 \quad 10^{-16}$	$9 \quad 10^{-17}$

Résultats numériques (3)

$$\begin{cases} p = \sum_{i=0}^{13*3-1} X^i \\ q = \sum_{i=0}^{13*5-1} X^i \end{cases} .$$

Le degré du PGCD de p et q est majoré par 12.

	$\frac{\text{norme du résidu}}{\text{norme de } p}$	$\frac{\text{norme du résidu}}{\text{norme de } q}$
Avant raffinement	$5 \;\; 10^{-13}$	$5 \;\; 10^{-14}$
Après raffinements (4)	$1 \;\; 10^{-16}$	$1 \;\; 10^{-16}$

Résultats numériques (4)

$$\left\{ \begin{array}{l} p = \prod_{i=1}^{10} (X - 2i) \\ q = \prod_{i=9}^{15} (X - 2i) \end{array} \right. .$$

Le degré du PGCD de p et q est majoré par 3.

	$\frac{\text{norme du résidu}}{\text{norme de } p}$	$\frac{\text{norme du résidu}}{\text{norme de } q}$
Avant raffinement	$5 \ \ 10^{-3}$	$5 \ \ 10^{-4}$
Après raffinements (4)	$9 \ \ 10^{-13}$	$4 \ \ 10^{-13}$

	avant raffinement	après raffinement
racine 1	20-1e-8	19.28+2.31 i
racine 2	18-1e-8	19.28 - 2.31 i
racine 3	17.53	17.54

Remarques finales

- le critère sur la taille du noyau donne de bons résultats et le raffinement est efficace

- à la fin, on est sûr de rien... La majoration du degré du PGCD est assurée pour p et q, mais pas dans le voisinage (mais elle tellement large...).

- il serait intéressant de pouvoir considérer des perturbations structurées sur p et q.