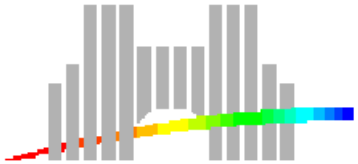
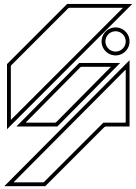
Pseudozéros et PGCD de polynômes en précision finie

Stef GRAILLAT

sous la direction de Philippe LANGLOIS

3e année ENSIMAG – DEA MA
Juin 2001





Introduction et motivations

But :
Travailler avec des polynômes ayant des données (coefficients ou racines) connues avec une incertitude : recherche de racines, calcul de PGCD, etc.

Raisons :

- Résultats provenant d'expériences.
- Représentation des nombres en machine.

Applications :

- Traitement du signal et d'images.
- Robotique.
- Biologie moléculaire.

Exemples du PGCD

- **Exemple 1** :
  Soient p et q deux polynômes unitaires et $\deg p > 1$.
  On suppose de plus que p divise $q \Longrightarrow \gcd(p, q) = p$.
  Or pour toute constante $\varepsilon > 0$, on a $\gcd(p, q + \varepsilon) = 1$.

- **Exemple 2** :

$$\begin{aligned} p &= z^2 - 3.0001z + 1.9999 \approx (z-1)(z-2), \\ q &= z^2 - 1.9999z + 1.0001 \approx (z-1)^2. \end{aligned}$$

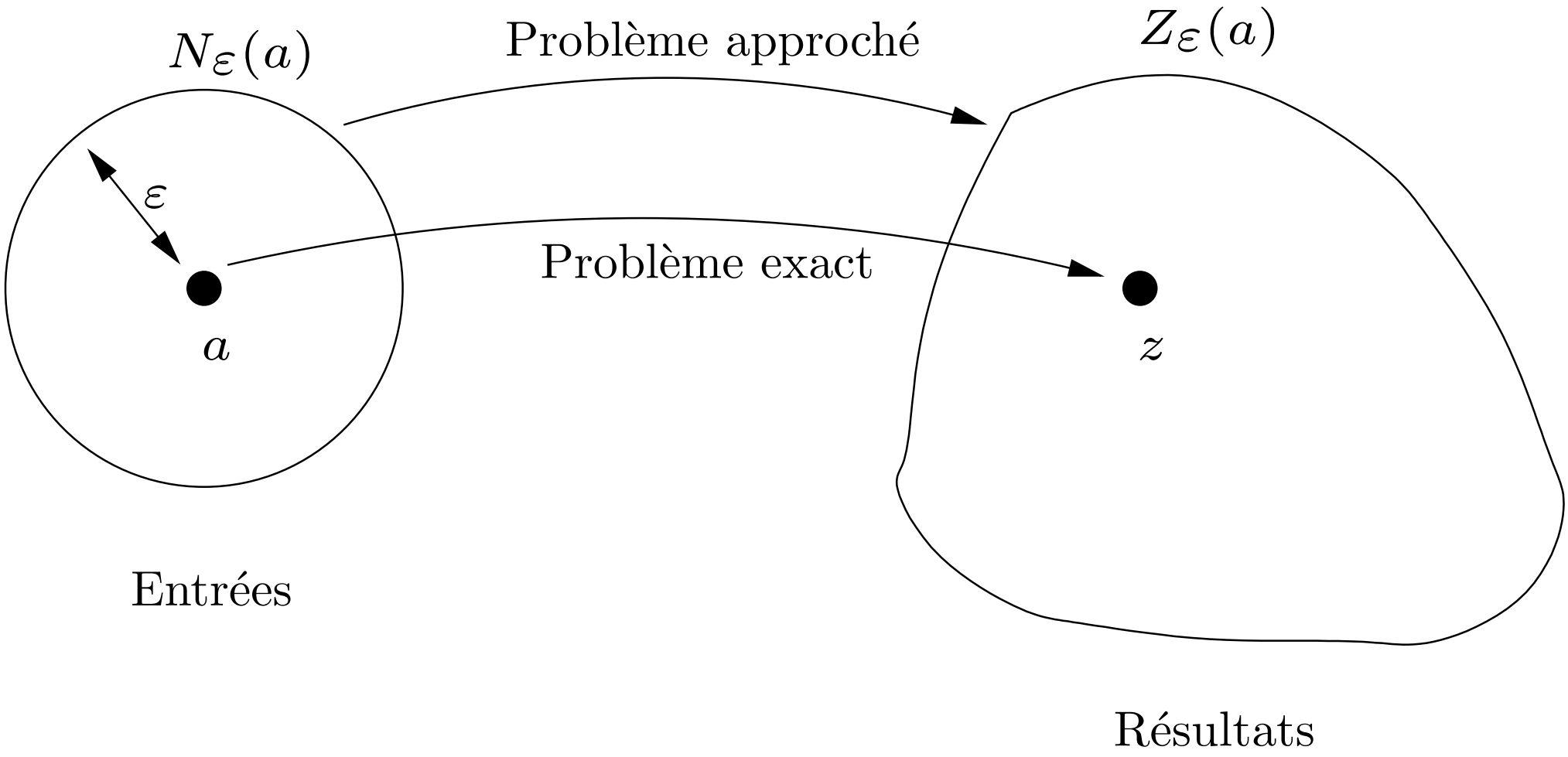
  Pour ε une perturbation sur les coefficients, on aimerait dire :

  - $\gcd(p, q) = z - 1$ pour $\varepsilon \geq 0.0001$.
  - p et q sont premiers entre eux pour $\varepsilon < 0.0001$.

Pourquoi en faire un sujet d'étude ?

- Problèmes difficiles.
- On doit rechercher les "singularités".
- La démarche générale :
  - Donner une définition précise de ce que l'on veut calculer.
  - Trouver des algorithmes pour ce calcul (souvent des heuristiques).
  - Certifier les résultats.
- appliquée à
  - (ε-pseudo)zéros.
  - (ε-)diviseurs.
  - (ε-)PGCD.

Principe des calculs approchés



Plan de l'exposé

- Introduction : le calcul algébrique approché.
- Partie 1 : Les pseudozéros : définition, calcul et utilité.

BUT : Montrer que les pseudozéros permettent de résoudre des problèmes.

- Partie 2 : PGCD approché : définition et calcul.
- Partie 3 : Étude de la primalité de deux polynômes.
- Conclusion et perspectives.

Partie 1

Les pseudozéros : définition, calcul et utilité

Historique

- Mosier (1986).
- Repris par Trefethen et Toh (1994).
- Chatelin et Frayssé (1996).
- Stetter (1999).

Notre contribution

- **Expression calculable pour $presque$ toutes les normes.**

Pseudozéros : définition

- Perturbation :
  Voisinage du polynôme p

$$N_\varepsilon(p) = \{\widehat{p} \in \mathbb{P}_n : \|p - \widehat{p}\| \leq \varepsilon\}\,.$$

- Définition de l'ensemble des ε-pseudozéros :

$$Z_\varepsilon(p) = \{z \in \mathbb{C} : \widehat{p}(z) = 0 \text{ pour } \widehat{p} \in N_\varepsilon(p)\}\,.$$

Calcul

- **Théorème** :
  L'ensemble des pseudozéros vérifie

$$Z_\varepsilon(p) = \left\{ z \in \mathbb{C} : |g(z)| := \frac{|p(z)|}{\|\underline{z}\|_*} \leq \varepsilon \right\},$$

  où $\underline{z} = (1, z, \ldots, z^n)$ et $\|\cdot\|_*$ est la norme duale de $\|\cdot\|$.

- **Idée de la preuve** :
  "$\subset$" : Inégalité de Hölder généralisée ($i.e.$ $|x^* y| \leq \|x\| \|y\|_*$) :

$$|p(z)| = |p(z) - \widehat{p}(z)| = |\sum_{i=0}^{n} (p_i - \widehat{p}_i) z^i| \leq \|p - \widehat{p}\| \|\underline{z}\|_*.$$

"$\supset$" : Soit $u \in \mathbb{C}$ tel que $|p(u)| \leq \varepsilon \|\underline{u}\|_*$. Notons $\underline{u} = (1, u, u^2, \ldots, u^n)$.
Alors $\exists\ d \in \mathbb{C}^{n+1}$ vérifiant $d^* \underline{u} = \|\underline{u}\|$ et $\|d\| = 1$.
Définissons les polynômes r et p_u par

$$\begin{aligned} r(z) &= \sum_{k=0}^{n} r_k z^k \quad \text{avec} \quad r_k = \overline{d}_k, \\ p_u(z) &= p(z) - \frac{p(u)}{r(u)} r(z). \end{aligned}$$

p_u : polynôme le plus proche de p ayant u comme racine.
$r(u) = d^* \underline{u} = \|\underline{u}\|_*$ et $p_u(u) = 0$. Donc

$$\|p - p_u\| = \frac{|p(u)|}{|r(u)|} \|r\| \leq \|\overline{d}\| \varepsilon.$$

Hypothèse : $\|\overline{d}\| = \|d\|$.

$$\|p - p_u\| \leq \varepsilon.$$

Algorithme de calcul

Algorithme utilisé dans notre package MATLAB de tracé de ε-pseudozéros :

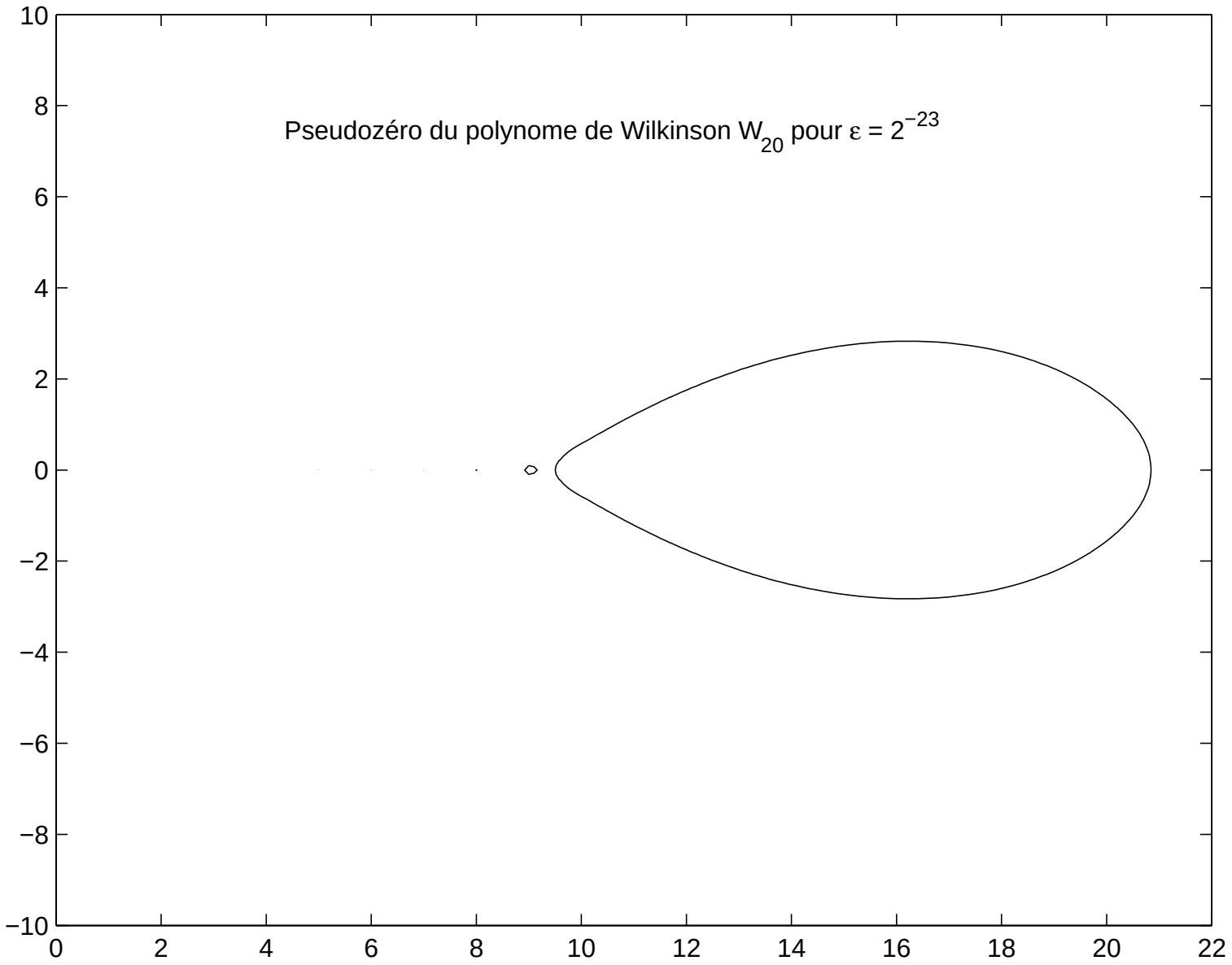
- On maille un carré contenant toutes les racines de p à l'aide de la commande MATLAB `meshgrid`.
- On calcule $g(z)$ pour tous les points z de la grille.
- On affiche la ligne de niveau $|g(z)| = \varepsilon$ à l'aide de la commande MATLAB `contour`.

Simulation numérique

Ensemble des pseudozéros du polynôme de Wilkinson

$$\begin{aligned} W_{20} &= (z-1)(z-2)\cdots(z-20), \\ &= z^{20} - 210z^{19} + \cdots + 20!, \end{aligned}$$

en ne perturbant que le coefficient de z^{19} avec une perturbation inférieure à $\varepsilon = 2^{-23}$.


Pseudozéro du polynome de Wilkinson W_{20} pour $\varepsilon = 2^{-23}$
10
8
6
4
2
0
−2
−4
−6
−8
−10
0
2
4
6
8
10
12
14
16
18
20
22

Partie 2

PGCD approché : définition et calcul

Exemples du PGCD

$p(z) = z^n$ et $q(z) = (z - 1/2)^n$

Mesure de la perturbation : $\delta = (\|\Delta p\|_2^2 + \|\Delta q\|_2^2)^{1/2}$

- $\widehat{p}(z) = z^n - (1/2)^n$ et $\widehat{q} = q = (z - 1/2)^n$
  PGCD $= z - 1/2$, $\delta = 1/2^n$

- $\widehat{p}(z) = z^n - (1/2)^{n-1} z$ et $\widehat{q} = (z - 1/2)^n - (-1/2)^{n-1}(z - 1/2)$
  PGCD $= z(z - 1/2)$, $\delta = 3/2^n$

$\Longrightarrow$ le degré du PGCD varie différemment pour des tailles de perturbations similaires.

Définition d'un PGCD approché

Définition classique :

Soient p et q des polynômes de degrés respectifs n et m et soit ε un nombre positif. On appelle :

- ε-**diviseur** (ou diviseur approché) : tout diviseur des polynômes perturbés $\widehat{p}$ et $\widehat{q}$ vérifiant
  - $\deg \widehat{p} \leq n$, $\deg \widehat{q} \leq m$ et
  - $\max(\|p - \widehat{p}\|, \|q - \widehat{q}\|) \leq \varepsilon$.
- ε-**PGCD** (PGCD approché) : un ε-diviseur de degré maximum.

Remarques :

- Tolérance sur les coefficients (nombres flottants / mesures).
- Unicité du degré mais non du ε-PGCD.

Synthèse de la bibliographie

Trois approches :

- Approche exacte : algorithme d'optimisation globale [Karmarkar et al. 1995].
- Heuristiques :
  - Adaptation de l'algorithme d'Euclide [Emiris et al. 1996].
  - Méthode matricielle : la SVD [Corless et al. 1997].
  - Par les racines [Pan 1996].
- Certification [Emiris et al. 1997, Rupprecht 2000].

Approche exacte

Algorithme d'optimisation de Karmarkar et Lakshman (1995)

- Principe :
  Chercher d de degré maximum, p_1 et q_1 tel que

$$\|p - p_1 d\| \leq \varepsilon \quad \text{et} \quad \|q - q_1 d\| \leq \varepsilon.$$

- Inconvénient :
  De complexité exponentielle en le degré du polynôme d car nécessite un algorithme de minimisation globale.

Adaptation de l'algorithme d'Euclide

- Principe : modifier la condition d'arrêt.
  Exact : arrêt au dernier reste non nul.
  Approché : arrêt au dernier reste de norme inférieure à la tolérance.

- Avantage : rapidité, $\mathcal{O}((n+m)^2)$.

- Inconvénient : donne un minorant sur le degré du ε-PGCD.

Méthode matricielle : la SVD

$$Syl(p,q) = \begin{bmatrix} p_0 & 0 & \cdots & 0 & q_0 & 0 & \cdots & 0 \\ p_1 & p_0 & \ddots & \vdots & q_1 & q_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ p_n & & \ddots & p_0 & q_m & & \ddots & q_0 \\ 0 & p_n & & p_1 & 0 & q_m & & q_1 \\ \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & p_n & 0 & \ldots & 0 & q_m \end{bmatrix} \in \mathbb{C}^{(n+m)\times(n+m)}.$$

- Principe : calculer le défaut de rang numérique de la matrice de Sylvester par SVD.
- Avantage : $\mathcal{O}((n+m)^3)$.
- Inconvénient : donne un majorant sur le degré du ε-PGCD.

Certification

- Principe :
  Utiliser l'algorithme d'Euclide modifié et des techniques de SVD pour obtenir un minorant et majorant du degré égaux.

Partie 3

Primalité de 2 polynômes

Définition de la ε-primalité

- **Définition :**
  Deux polynômes p et q sont ε-**premiers entre eux** si
  leur ε-**PGCD** est 1.

- **Calcul:**
  - Optimisation : algorithme de Karmarkar et Lakshman (1995).
  - Borne de Sylvester : algorithme COPRIME [Beckermann et Labahn 1998].
  - Graphique : les pseudozéros.

Algorithme de Karmarkar et Lakshman

Il s'agit d'un algorithme d'optimisation (moindre carré).

- **Entrée :** p et q deux polynômes.
- **Sortie :** $\widehat{p}$, $\widehat{q}$ et α tels que α soit racine commune de $\widehat{p}$ et $\widehat{q}$ avec $\|p-\widehat{p}\|_2^2 + \|q-\widehat{q}\|_2^2$ minimum.
- **Complexité :** polynomiale en n et m resp. les degrés de p et q.
- **Avantage :** fiable.
- **Inconvénient :** la complexité polynomiale.

Algorithme COPRIME

Algorithme de Beckermann et Labahn (1998).

- **Entrée :** p et q deux polynômes.
- **Sortie :** borne inférieure de $\epsilon(p,q)$ défini par

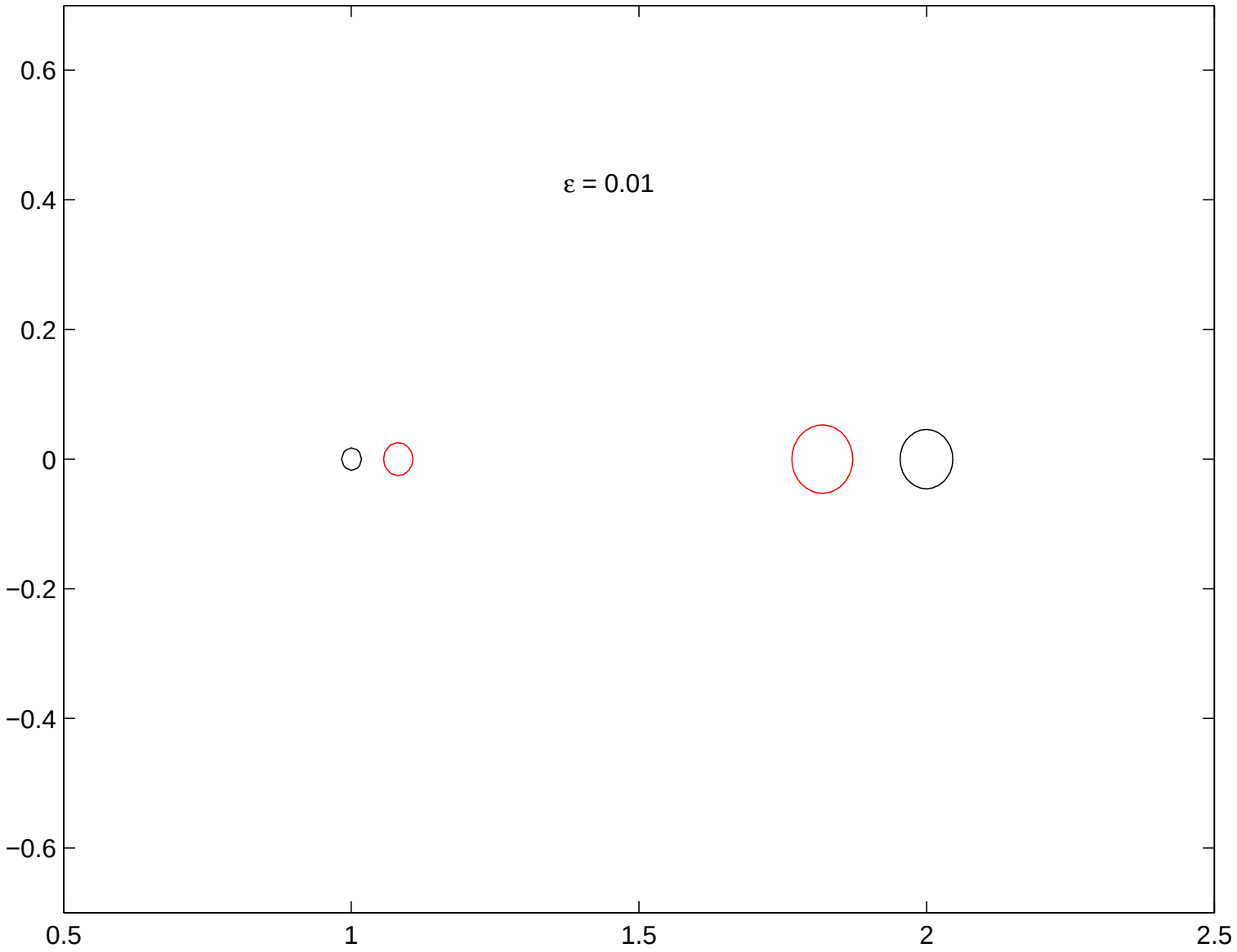
$$\epsilon(p,q) = \inf\{\|(p-\widehat{p}, q-\widehat{q})\| : (\widehat{p},\widehat{q}) \text{ ont une racine commune et}$$

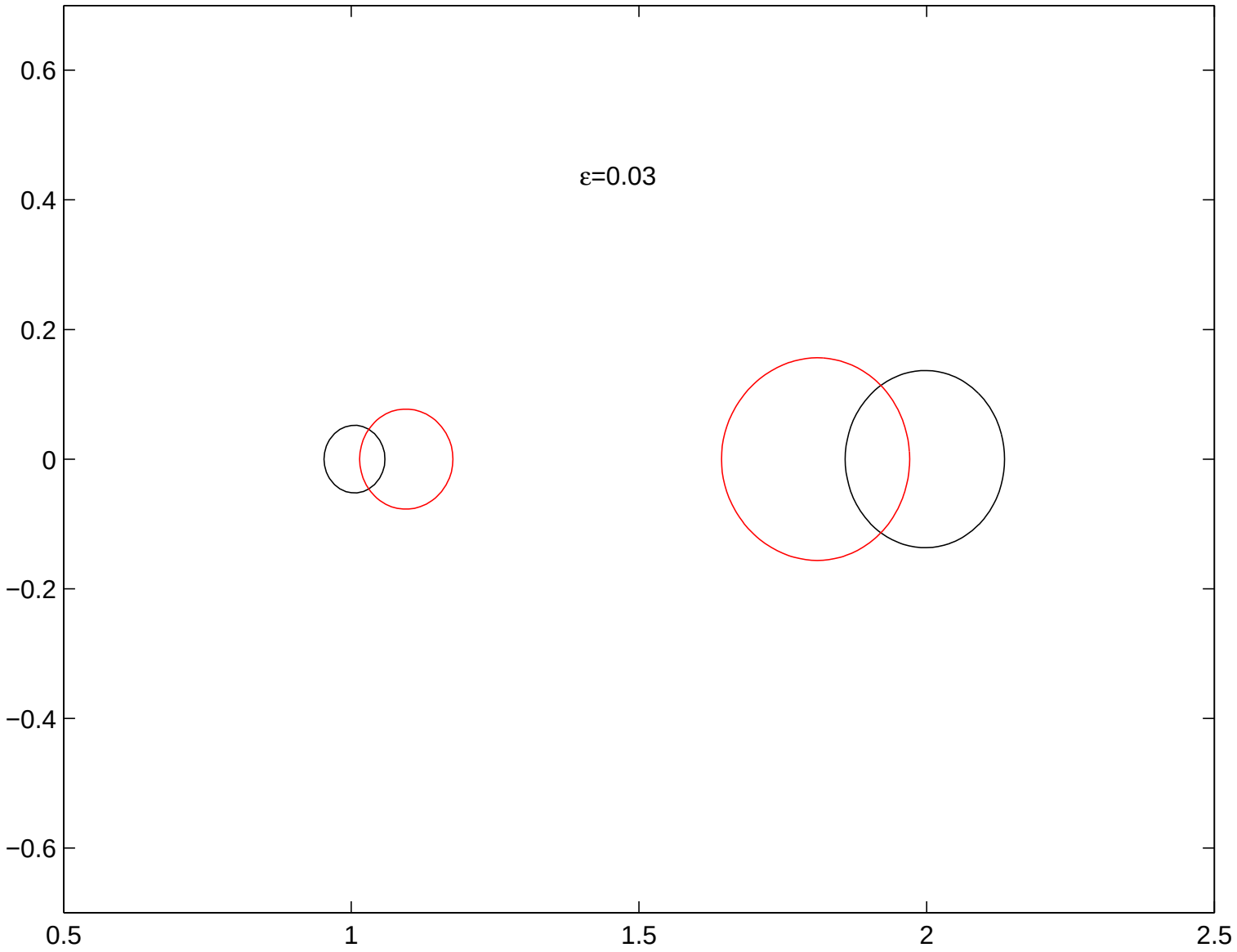
$$\deg\widehat{p} \leq n, \deg\widehat{q} \leq m\}.$$

- **Complexité :** en $\mathcal{O}((n+m)^2)$.
- **Avantage :** rapide.
- **Inconvénient :** donne une borne $\varepsilon_{inf} \leq \epsilon(p,q)$.

Les pseudozéros

- **Entrée :** p et q deux polynômes.
- **Sortie :** un graphique.
- **Avantage :** fiable.
- **Inconvénient :** outil qualitatif.
- **Exemple :**
  $p = (z-1)(z-2) = z^2 - 3z + 2$
  $q = (z-1.08)(z-1.82) = z^2 - 2.9z + 1.9656$


ε = 0.01
0.6
0.4
0.2
0
−0.2
−0.4
−0.6
0.5
1
1.5
2
2.5


ε=0.03
0.6
0.4
0.2
0
−0.2
−0.4
−0.6
0.5
1
1.5
2
2.5

Conclusion et perspectives

- Travail effectué :
  - Formule explicite du plus proche polynôme avec une racine donnée.
  - Package de tracé de pseudozéros.
  - Application des pseudozéros à la primalité.
- Perspectives :
  - Mieux automatiser le tracé de pseudozéros.
  - Mieux comprendre l'instabilité de l'algorithme d'Euclide.
  - Étudier les algorithmes de certification d'un ε-PGCD.

Divers

Trucs utiles

Norme et vecteur duaux

- Norme duale de $\|\cdot\|$:

$$\|y\|_* = \sup_{\|x\|\neq 0} \frac{|y^* x|}{\|x\|} = \sup_{\|x\|=1} |y^* x|.$$

- Vecteur dual :

Théorème . *Pour tout vecteur y, il existe un vecteur z vérifiant*

$$z^* y = \|z\|_* \|y\|.$$

Décomposition en Valeurs Singulières

Théorème . *Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$ avec $\mathbb{K} = \mathbb{R}$ où $\mathbb{C}$ de rang k. Alors A peut s'écrire sous la forme*

$$A = UDV^*,$$

où $U \in \mathcal{M}_m(\mathbb{K})$ et $V \in \mathcal{M}_n(\mathbb{K})$ sont des matrices unitaires (on dit souvent orthogonales dans le cas réel). La matrice $D = (\sigma_{ij}) \in \mathcal{M}_{m,n}(\mathbb{K})$ vérifie $\sigma_{ij} = 0$ pour $i \neq j$ et $\sigma_{11} \geq \sigma_{22} \geq \cdots \geq \sigma_{kk} > \sigma_{k+1,k+1} = \cdots = \sigma_{qq} = 0$ où $q = \min(m, n)$.