Calcul déterministe de racines approchées de systèmes polynomiaux en complexité moyenne polynomiale

---

Journée nationales de calcul formel
Cluny, 4 novembre 2015

Pierre Lairez
TU Berlin

Le 17^e problème de Smale

« Peut-on calculer une racine approchée de n équations polynomiales à coefficients complexes en n inconnues en temps polynomial en moyenne avec un algorithme uniforme ? » *(S. Smale, 1998)*

Racine approchée

Un point depuis laquelle l'itération de Newton converge quadratiquement.

Temps polynomial en moyenne

Complexité par rapport à la taille de l'entrée, pour une distribution raisonnable de l'entrée, typiquement, une distribution gaussienne.

Algorithme uniforme

Une machine BSS : opérations arithmétiques sur des nombres réels exacts à cout unitaire.

Symbolique contre numérique

Symbolique

Connaitre une racine, c'est les connaitre toutes ;
or le nombre de racines est surpolynomial.

Numérique

L'itération de Newton permet d'approcher une seule racine.
$\rightsquigarrow$ une complexité polynomiale est envisageable.

Typiquement

- n équations de degré 2 en n inconnues.
- Taille de l'entrée : $N = n\binom{n+2}{2} \sim \frac{1}{2}n^3$.
- Nombre de racines : $\mathcal{D} = 2^n$, c'est surpolynomial en N.

Symbolique contre numérique

Symbolique

Connaitre une racine, c'est les connaitre toutes ;
or le nombre de racines est surpolynomial.

Numérique

L'itération de Newton permet d'approcher une seule racine.
$\rightsquigarrow$ une complexité polynomiale est envisageable.

Typiquement

- n équations de degré n en n inconnues.
- Taille de l'entrée : $N = n\binom{2n}{n} \sim Cn^{1/2}4^n$.
- Nombre de racines : $\mathcal{D} = n^n$, c'est surpolynomial en N.

Notations

- n et D des entiers naturels.
- $\mathcal{H}$, l'espace vectoriel complexe des systèmes de n équations de degré D en n inconnues ; fonctions $\mathbb{C}^n \to \mathbb{C}^n$.
- N, la dimension de $\mathcal{H}$.

- $\mathcal{H}$ est muni d'un produit scalaire hermitien.
- $\mathbb{S}(\mathcal{H})$, les systèmes polynomiaux de norme 1.

La méthode homotopique

Entrée

$f \in \mathcal{H}$, un système à résoudre.

Point de départ

On choisit un autre $g \in \mathcal{H}$ dont on connait une racine $\zeta \in \mathbb{C}^n$.

Homotopie

$$h_0 = g \qquad h_{k+1} = h_k + \delta_k \cdot (f - g)$$
$$z_0 = \zeta \qquad z_{k+1} = z_k - (\mathrm{d}_{z_k} h_{k+1})^{-1}(h_{k+1}(z_k)).$$

Point d'arrivée

Si $h_K = f$, alors z_K est une racine approchée de f.

- Comment choisir les δ_k ?
- Comment choisir la paire système-racine (g, ζ) ?

Historique (I)

Shub, Smale (années 90)

– Choix des δ_k, complexité de la méthode d'homotopie en terme du conditionnement le long de l'homotopie.

– Pour chaque n et chaque D, il existe un point de départ (g, ζ) pour l'homotopie qui est efficace en moyenne.

Beltrán, Pardo (2009)

– Choix aléatoire de (g, ζ).

Historique (I)

Shub, Smale (années 90)

– Choix des δ_k, complexité de la méthode d'homotopie en terme du conditionnement le long de l'homotopie.

– Pour chaque n et chaque D, il existe un point de départ (g, ζ) pour l'homotopie qui est efficace en moyenne.

Beltrán, Pardo (2009)

– Choix aléatoire de (g, ζ).

– L'algorithme de Beltrán-Pardo, c'est une fonction

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times [0,1]^{\mathbb{N}} \to \mathbb{C}^n$$

telle que :

- $\mathrm{BP}(f, a)$ est une racine approchée de f, pour presque tout f et a ;
- si f et a sont uniformément distribués, alors $\mathbb{E}(\mathrm{cout}_{\mathrm{BP}}(f, a)) = O(nD^{3/2}N^2)$.

Historique (II)

Bürgisser, Cucker (2011)

– Algorithme déterministe en complexité moyenne $N^{O(\log\log N)}$.

– La complexité régularisée de l'algorithme de Beltrán-Pardo est polynomiale :

$$\sup_{f\in\mathcal{H}} \left[\mathbb{E}\left(\mathrm{cout}_{\mathrm{BP}}(f)\right)\right] = \infty$$

$$\text{mais } \sup_{f\in\mathcal{H}} \left[\mathbb{E}\left(\mathrm{cout}_{\mathrm{BP}}(f+\varepsilon)\right)\right] = O\left(\frac{1}{\sigma} nD^{3/2}N^2\right),$$

où $\varepsilon \in \mathcal{H}$ est une v.a. gaussienne isotrope de variance σ^2.

Lairez (2015)

– Algorithme déterministe en complexité moyenne $O(nD^{3/2}N^2)$.

Duplication de la distribution unif. sur $[0, 1]$

- $q > 0$ un entier.
- $x \in [0, 1]$ une v.a. uniformément distribuée.

- $\lfloor x \rfloor_q \stackrel{\text{def}}{=} 2^{-q} \lfloor 2^q x \rfloor \in [0, 1]$, la troncature de x à précision q.
- $\{x\}_q \stackrel{\text{def}}{=} 2^q x - \lfloor 2^q x \rfloor \in [0, 1]$, la partie fractionnaire.

Proposition

- La distribution de $\lfloor x \rfloor_q$ tend vers la distribution uniforme sur $[0, 1]$ quand $q \to \infty$.
- $\{x\}_q$ est uniformément distribuée sur $[0, 1]$.
- $\lfloor x \rfloor_q$ et $\{x\}_q$ sont indépendants.

Duplication de la distribution unif. sur $\mathbb{S}(\mathcal{H})$

- $q > 0$ un entier.
- $x \in \mathbb{S}(\mathcal{H})$ une v.a. uniformément distribuée.

- $\lfloor x \rfloor_q \stackrel{\text{def}}{=} [\ldots] \in \mathbb{S}(\mathcal{H})$, la troncature de x à précision q.
- $\{x\}_q \stackrel{\text{def}}{=} [\ldots] \in \mathbb{S}(\mathcal{H})$, la partie fractionnaire.

Proposition

- La distribution de $\lfloor x \rfloor_q$ tend vers la distribution uniforme sur $\mathbb{S}(\mathcal{H})$ quand $q \to \infty$.
- $\{x\}_q$ est *presque* uniformément distribuée sur $\mathbb{S}(\mathcal{H})$.
- $\lfloor x \rfloor_q$ et $\{x\}_q$ sont *presque* indépendants.

Un algorithme déterministe

Dérandomisation de l'algorithme de Beltrán-Pardo

Algorithme de Beltrán-Pardo

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times [0,1]^{\mathbb{N}} \to \mathbb{C}^n.$$

Un algorithme déterministe

Dérandomisation de l'algorithme de Beltrán-Pardo

Algorithme de Beltrán-Pardo modifié

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

Un algorithme déterministe

Dérandomisation de l'algorithme de Beltrán-Pardo

Algorithme de Beltrán-Pardo modifié

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

Un algorithme déterministe

Dérandomisation de l'algorithme de Beltrán-Pardo

Algorithme de Beltrán-Pardo modifié

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

L'algorithme, 1er essai

procédure BPD(f)
  $q \leftarrow$ un entier assez grand
  renvoyer $\mathrm{BP}\left(\lfloor f \rfloor_q, \{f\}_q\right)$
fin procédure

Un algorithme déterministe

Dérandomisation de l'algorithme de Beltrán-Pardo

Algorithme de Beltrán-Pardo modifié

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

L'algorithme, 2e essai

procédure BPD(f)
  $q \leftarrow \lfloor \log_2 N \rfloor$
  répéter
    $q \leftarrow 2q$
    $z \leftarrow \mathrm{BP}\left(\lfloor f \rfloor_q, \{f\}_q\right)$
  tant que z n'est pas une racine approchée de f
  renvoyer z
fin procédure

Un algorithme déterministe

Dérandomisation de l'algorithme de Beltrán-Pardo

Algorithme de Beltrán-Pardo modifié

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

L'algorithme, le bon

procédure BPD(f)
  $q \leftarrow \lfloor \log_2 N \rfloor$
  répéter
    $q \leftarrow 2q$
    $z \leftarrow \mathrm{BP}\left(\lfloor f \rfloor_q, \{f\}_q\right)$ avec abandon anticipé
  tant que z n'est pas une racine approchée de f
  renvoyer z
fin procédure

Analyse de la complexité

- Soit $f \in \mathbb{S}(\mathcal{H})$ une v.a. uniformément distribuée.
- Soit Ω le nombre d'itérations dans BPD(f).
- $\mathbb{E}(\Omega) \leqslant 7$; queue très légère.
- $\mathrm{cout}_{\mathrm{BPD}}(f) = \sum_{k=1}^{\Omega} \left(O(Nq_k) + \mathrm{cout}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \right)$, où BP' = « BP avec abandon anticipé ».

Analyse de la complexité

- Soit $f \in \mathbb{S}(\mathcal{H})$ une v.a. uniformément distribuée.
- Soit Ω le nombre d'itérations dans BPD(f).
- $\mathbb{E}(\Omega) \leqslant 7$; queue très légère.
- $\mathrm{cout}_{\mathrm{BPD}}(f) = \sum_{k=1}^{\Omega} \left(O(Nq_k) + \mathrm{cout}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \right)$, où BP' = « BP avec abandon anticipé ».
- $\mathrm{cout}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \sim \mathrm{cout}_{\mathrm{BP}}(f, g)$, où $g \in \mathbb{S}(\mathcal{H})$ est une v.a. uniforme.

Analyse de la complexité

- Soit $f \in \mathbb{S}(\mathcal{H})$ une v.a. uniformément distribuée.
- Soit Ω le nombre d'itérations dans BPD(f).
- $\mathbb{E}(\Omega) \leqslant 7$; queue très légère.
- $\mathrm{cout}_{\mathrm{BPD}}(f) = \sum_{k=1}^{\Omega} \left(O(Nq_k) + \mathrm{cout}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \right)$, où BP' = « BP avec abandon anticipé ».
- $\mathrm{cout}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \sim \mathrm{cout}_{\mathrm{BP}}(f, g)$, où $g \in \mathbb{S}(\mathcal{H})$ est une v.a. uniforme.
- $\mathbb{E}(\mathrm{cout}_{\mathrm{BPD}}(f)) = O(nD^{3/2}N^2)$

Conclusion

✗ Construction artificielle.

✓ Réponse déterministe à la question de Smale.

✓ Approche justifiée par la pertinence de l'analyse régularisée.

✓ La précision q reste modérée, de l'ordre de $\log N$.

✓ L'aléa est déjà dans la question, dès sa formulation.

Problème no. 17bis — Peut-on calculer une racine approchée d'un système polynomial en temps polynomial par rapport à sa complexité d'évaluation, à son degré et au logarithme de son conditionnement ?

Conclusion

✗ Construction artificielle.

✓ Réponse déterministe à la question de Smale.

✓ Approche justifiée par la pertinence de l'analyse régularisée.

✓ La précision q reste modérée, de l'ordre de $\log N$.

✓ L'aléa est déjà dans la question, dès sa formulation.

Problème no. 17bis — Peut-on calculer une racine approchée d'un système polynomial en temps polynomial par rapport à sa complexité d'évaluation, à son degré et au logarithme de son conditionnement ?

Merci !