Complexité topologique des algorithmes

Victoria LEBED

Pb : trouver les racines d'un polynôme $p = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$
$\in$ $Poly_n$

Pb^ε : — // — "ε-racines" — // —
approximations avec la précision ε

Points de vue :

1) Algèbre : sur $\mathbb{C}$, f a n racines.

2) Analyse :

racines polynômes coeff^s

$$\mathbb{C}^n \xrightarrow{pol} Poly_n \simeq \mathbb{C}^n$$

$$z_1, \dots, z_n \longmapsto \prod_i (x - z_i) \longrightarrow \text{fonctions symétriques en } z_i$$

$$\boxed{\mathbb{C}^n/\mathfrak{S}_n \xrightarrow[\text{homéom-sme}]{pol^*} \mathbb{C}^n}$$

$\mathfrak{S}_n$: gpe symétrique

Qu. : Y a-t-il une section continue ?

Ex. : $n = 2$ NON

$$\mathbb{C}^2 \overset{?}{\dashleftarrow} \mathbb{C}^2/\mathfrak{S}_2 \xleftarrow{rac^*} \mathbb{C}^2$$

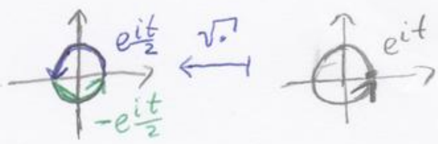
$$\frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2} \longleftarrow (a_1, a_0)$$

supposons qu'une section $\mathbb{C}^2 \overset{rac}{\longleftrightarrow} \mathbb{C}^2$ existe :

$$(e^{\frac{it}{2}}, -e^{\frac{it}{2}}) \xleftarrow{rac} (0, -e^{it}),\ t \in [0, 2\pi]$$

$t \to +0$: $(1, -1)$; $t \to 2\pi - 0$: $(-1, 1)$; $(1,-1) \neq (-1,1)$

$t \to +0$ ou $t \to 2\pi - 0$: $(0, 1)$



$\rightsquigarrow$ pb autour de $f = x^2$

Obstacle :

- naïf : $\nexists\ z \longmapsto \sqrt[k]{z}$ continue ($k \geq 2$)
- plus profond : la projection $\mathbb{C}^n \twoheadrightarrow \mathbb{C}^n/\mathfrak{S}_n$ n'admet pas de section continue.

Idée naïve : $\mathbb{C}^n_{\leq} := \{ \bar{z} \in \mathbb{C}^n \mid z_i \leq z_{i+1}\ \forall i \} \xrightarrow{pol} \mathbb{C}^n$ - bijection

$\leq$: $Re\, z_i < Re\, z_{i+1}$ ou $Re\, z_i = Re\, z_{i+1}$ & $Im\, z_i \leq Im\, z_{i+1}$

Pb : son inverse n'est pas continu :

$\varepsilon > 0$: $\xi_\varepsilon := (a + bi, a + \varepsilon + ci, z_3, \dots, z_n) \longleftrightarrow pol(\xi_\varepsilon)$, $b < c$

$\not\downarrow\ \varepsilon \to +0$ $\qquad$ $\downarrow\ \varepsilon \to +0$

$\xi := (a + ci, a + bi, z_3, \dots, z_n) \longleftrightarrow pol(\xi)$

3) Analyse numérique

<u>Qu. E</u> : Y a-t-il une "ε-section" continue de pol ?

$$\mathbb{C}^n \xleftarrow{rac_\varepsilon} B^n := \{\bar a \in \mathbb{C}^n \mid \|a\|_\infty \le 1\} \text{ t.q. } \forall f \in B^n \ \exists \bar z \in pol^{-1}(f) \text{ avec } \|\bar z - rac_\varepsilon(f)\|_\infty < \varepsilon.$$

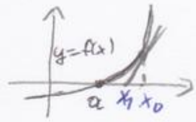
<u>Ex.</u> : $\{$Méthode de Newton$\}$

$f \in C^2(I \subset \mathbb{R}, \mathbb{R})$, $x_0 \in I$

<u>Idée</u> : $f(a) = 0 \Rightarrow 0 = f(a) \simeq f(x_0) + f'(x_0)(a - x_0) \Rightarrow a \approx x_0 - \frac{f(x_0)}{f'(x_0)} =: x_1$

<u>Itération</u> : $x_{k+1} := x_k - \frac{f(x_k)}{f'(x_k)}$.

<u>Pb</u> : On veut $f'(x_k) \neq 0 \ \forall k$!



<u>Rmq_I</u> : Si $f \in Poly_n(\mathbb{R})$, alors $x_k = \frac{P_k(x_0)}{Q_k(x_0)}$, avec P_k & $Q_k \in \mathbb{Z}[a_0, \dots, a_{n-1}][X]$.

<u>Convergence</u> : Taylor $\Rightarrow C|x_k - a| \le (\underbrace{C|x_0 - a|}_{\text{on veut : } < 1})^{2^n}$, avec $C = \frac{M_2}{2m_1}$,

quadratique

• $M_2 = \max_{x \in I} |f''(x)| \underset{\text{si } f \in B^n}{\le} M(n)$

• $m_1 = \min_{x \in I} |f'(x)|$

$$\Updownarrow$$

$$\frac{m_1}{|x_0 - a|} > \frac{M_2}{2}$$

"Petit" m_1 au voisinage d'un zéro de f est lié à l'existence d'une fonction avec un zéro double proche de $f \overset{\text{déf}}{\Leftarrow}$ "mauvaise" fonction.

<u>Rmq_II</u> : La méthode marche aussi sur $\mathbb{C} \rightsquigarrow$ fractales de Newton.

<u>Bilan</u> : Pour un $f \in B^n$ "éloigné" des mauvais polynômes, on obtient une fonction rationnelle $\mathbb{C} \xleftarrow{rac_\varepsilon^{(1)}} \underset{\text{un voisinage de } f}{U_{(f)}} \subset B^n$ qui donne une "ε-racine" d'un polynôme.

4) Théorie topologique des algorithmes

Arbre de calcul :

entrée (racine) B^n

calcul $\boxed{f}$ $f : \mathbb{C}^n \supset \mathcal{U} \xrightarrow{\text{cont.}} \mathbb{C}^n$ ~~rationnelle~~

branchements: un des $\varphi_i > 0$? — oui / non $\varphi_i : \mathbb{C}^n \supset \mathcal{U} \xrightarrow{\text{cont.}} \mathbb{R}^{k_i}$, ~~rationnelle~~

résultat (feuille) $\mathbb{C}^n$

Rmq : Weierstrass $\Rightarrow$ on peut remplacer "continue" par "rationnelle" & simplifier les conditions de branchement : $\varphi > 0$, $\varphi : \mathcal{U} \to \mathbb{R}$.

complexité topologique d'un algo : $=$ # branchement $+ 1 =$ # feuilles

$TC(n,\varepsilon) := \min_{A \text{ résout } \mathcal{P}_n^\varepsilon} (\text{c-té top.}(A))$

(A) Majoration

Th. (Vassil'ev, 89) : $\boxed{TC(n,\varepsilon) \leq n}$

$\mathbb{C}^n_{<,\varepsilon,0} := \{ \bar{z} \in \mathbb{C}^n \mid \frac{\varepsilon}{2n} < \operatorname{Re} z_{i+1} - \operatorname{Re} z_i \ \forall i \} \xrightarrow[\text{Roméo}]{\text{pol}} V_0 \subset \mathbb{C}^n$

$\mathrm{rac}_\varepsilon^{(0)} := \text{Weierstrass}(\text{pol}^{-1})$

$\mathbb{C}^n_{<,\varepsilon,1} := \left\{ \bar{z} \in \mathbb{C}^n \mid \exists i \text{ t.q. } |\operatorname{Re} z_{i+1} - \operatorname{Re} z_i| < \frac{\varepsilon}{n} \ \& \ \frac{\varepsilon}{2n} < \operatorname{Re} z_{j+1} - \operatorname{Re} z_j \ \forall j \neq i. \right\} \xrightarrow{\text{pol}} V_1 \subset \mathbb{C}^n$, $\mathrm{rac}_\varepsilon^{(1)}$

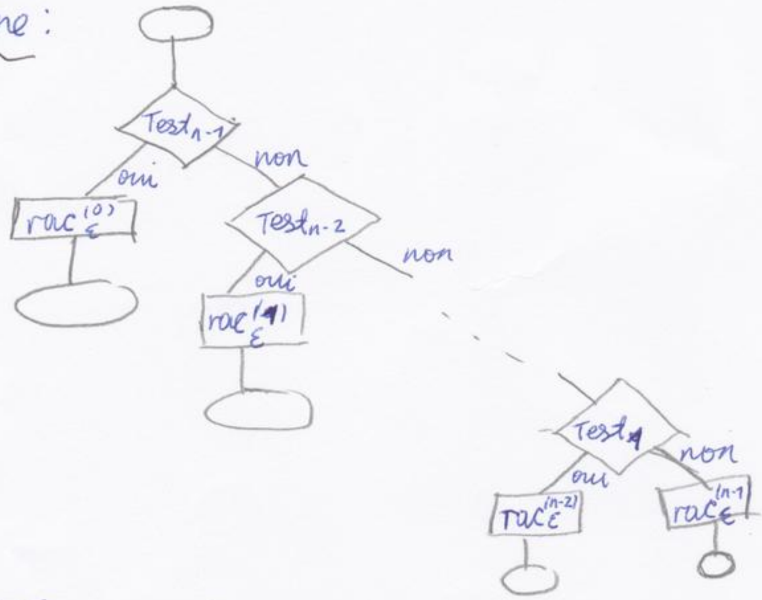
$\left(z_1, \dots, z_{i-1}, \frac{\operatorname{Re} z_i + \operatorname{Re} z_{i+1}}{2} + i \min\{\operatorname{Im} z_i, \operatorname{Im} z_{i+1}\}, \frac{\operatorname{Re} z_i + \operatorname{Re} z_{i+1}}{2} + i \max\{\operatorname{Im} z_i, \operatorname{Im} z_{i+1}\}, z_{i+2}, \dots, z_n\right) \longleftarrow \text{pol}(\bar{z})$

$\varphi_i(\bar{z}) := \operatorname{Re} z_{i+1} - \operatorname{Re} z_i - \frac{\varepsilon}{2n}$

$\mathbb{C}^n_{<,\varepsilon,k} := \left\{ \bar{z} \in \mathbb{C}^n \mid \varphi_i(\bar{z}) > 0 \text{ pour } k \text{ indices } \& \ |\operatorname{Re} z_{i+1} - \operatorname{Re} z_i| < \frac{\varepsilon}{n} \text{ pour les autres} \right\} \xrightarrow{\text{pol}} V_k$, $\mathrm{rac}_\varepsilon^{(k)}$

$\text{Test}_k := \exists\, i_1 < i_2 < \dots < i_k$ avec $f_{i_j} > 0\ \forall j$.

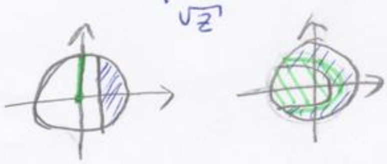
Algorithme :



Rmq : Ces idée permettent de munir $\mathbb{C}^n/\mathfrak{S}_n$ d'une structure de CW-complexe.

Ex : $f = x^2 - a$ racines : coeff^s

$$\mathbb{C} \underset{\sqrt{z}}{\overset{z^2}{\rightleftarrows}} \mathbb{C}$$



Ⓑ Minorations

$\forall \varepsilon \le \varepsilon(n)$,

- $\boxed{TC(n,\varepsilon) \ge (\log_2 n)^{2/3}}$ (Smale, 87)
- $\boxed{TC(n,\varepsilon) \ge n+1-Dig_p(n)}$ $\forall$ p premier (Vassil'ev, 89)

  où $Dig_p(\sum c_k p^k) = \sum c_k$

Rmq: les minorations ne dépendent pas de ε.

Crl: $TC(p^k,\varepsilon) = p^k$ pour p premier.

Idées:

- $TC(n,\varepsilon) \ge Recouv(\mathbb{C}^n - \underset{\exists z_i = z_j,\ i\neq j}{\Delta} \xrightarrow{\pi} \underbrace{\mathbb{C}^n/S_n - \pi(\Delta)}_{=: \widetilde{\mathbb{C}^n}})$

Pour $f \in C(U,V)$, Recouv(f) $= \min\{k \mid \exists V = \bigcup_{i=1}^{k} \underset{\text{ouverts}}{V_i}$ & sections $U \xleftarrow{s_i} V_i\}$

Ex.: $f(x) = x^3 - x : \mathbb{R} \to \mathbb{R}$

Recouv(f) = 2.

- Recouv(π) est lié avec l'homologie de $\widetilde{\mathbb{C}^n}$

Gpe fondamental: $\pi_1(\underset{\text{espace top.}}{M}, \underset{\in M}{z}) :=$ z-lacets ds M / z-lacets triviaux

$\boxed{\pi_1(\widetilde{\mathbb{C}^n}, \{1,2,\dots,n\}) \simeq Br_n}$ ← gpe de tresses:

Mieux: $\widetilde{\mathbb{C}^n}$ est l'espace d'Eilenberg-MacLane $K(Br_n, 1)$.

Questions liées :

1) Généraliser ces idée à d'autres pb ?

2) (Arnol'd, 70') : f^ns algébriques : $\underset{n\text{ var.}}{f} \overset{?}{=} \underbrace{f_1 \circ f_2}_{k<n\text{ var.}}$? Génériquement impossible pour $k < n - Dig_2(n)$.
(p)

3) Complexité usuelle

<u>Ex.</u> : Pb des éléments égaux : $\bar{x} \in \mathbb{R}^n \rightsquigarrow \exists ?\ x_i = x_j$, $i \neq j$.

Sol^n naïve : complexité n^2

Algo de tri efficace : $n \log n$

$\prod_{i<j} (x_i - x_j)$: $n \log n$

(80') : Arguments topologiques $\Rightarrow\ \geq n \log n$

4) (McMullen, 85) : $\cdot \not\exists$ algorithmes itératif "généralement convergents" pour notre pb pour $n \geq 4$;
• polynômes qui posent des problèmes (e.g. x^d) sont "noués"

5) (Farber, 00') : robotique

Bonus : énigme sur les polynômes.