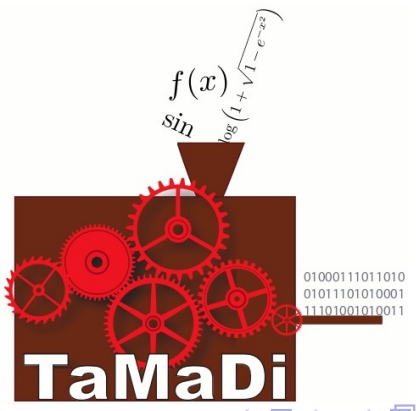
Approches "sums of squares" et autres pour borner l'erreur d'évaluation polynomiale

Jean-Michel Muller, CNRS

très inspiré de l'article de Sylvain Chevillard, Mioara Joldes, John Harrison et Christoph Lauter

8 avril 2011



Distance entre f et des polynômes

- L-algorithme et SLZ : on découpe le domaine d'entrée en nombreux sous-intervalles ;
- dans chaque sous-intervalle : la fonction f est approchée par un polynôme (SLZ : degré ≥ 2, L : degré 1 avec construction hiérarchique des approximations) ;
- on doit certifier l'erreur d'approximation pour chaque sous-intervalle (L : pour un des étages de l'approche hiérarchique) ;
- grand nombre de sous-intervalles (a priori exponentiel en la précision) $\longrightarrow$ nécessité d'être très rapide.

Distance entre f et des polynômes

- ne pas oublier : coq sera lent. Il vaut parfois mieux faire une quantité significative de calculs préliminaires pour fabriquer un certificat très facile à tester (ex. sums of squares) ;
- $||f - p||$ plus difficile que $||p_1 - p_2||$;
- solution possible : pour un nombre (assez large) de sous-intervalles consécutifs, une approximation polynomiale $\mathcal{P}_H$ de haut degré et d'erreur connue (p.ex. Taylor). Dans chaque sous-intervalle, approximation $\mathcal{P}_\ell$. On borne une bonne fois pour toutes $||f - \mathcal{P}_H||_\infty$, et pour chaque sous-intervalle $[a, b]$, on borne $||\mathcal{P}_H - \mathcal{P}_\ell||_{\infty,[a,b]}$.

Montrer que $||\mathcal{P}_H - \mathcal{P}_\ell||_{\infty,[a,b]} \leq \epsilon$

C'est montrer que

$$\epsilon - \mathcal{P}_H + \mathcal{P}_\ell \geq 0 \text{ sur } [a, b]$$

et que

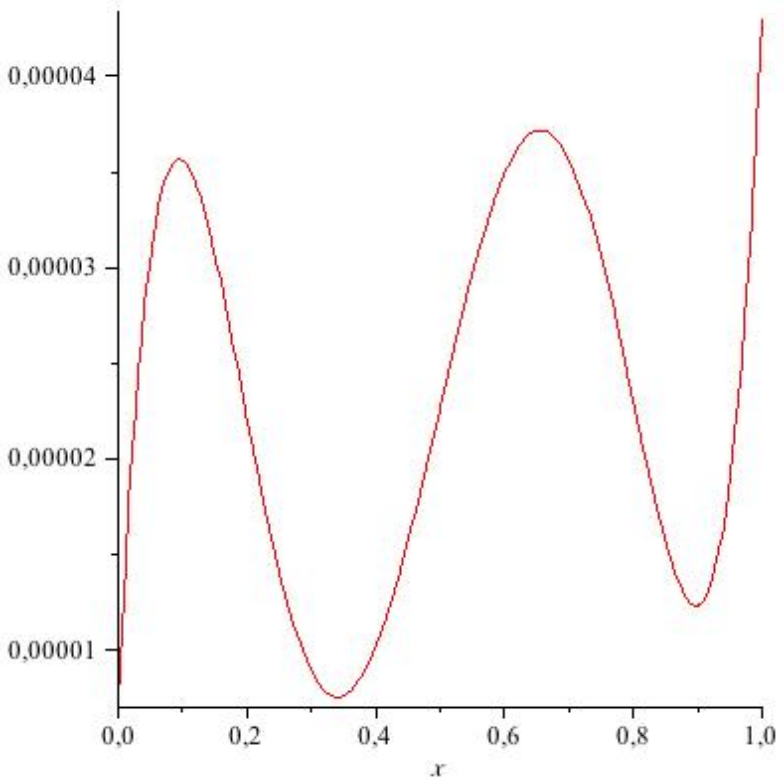
$$\mathcal{P}_H - \mathcal{P}_\ell + \epsilon \geq 0 \text{ sur } [a, b].$$

$\Rightarrow$ dans tous les cas, c'est montrer qu'un certain polynôme $\mathcal{P}$ est ≥ 0 sur $[a, b]$.

Note : si ça nous arrange plus, on peut chercher à montrer que $\mathcal{P} > 0$.

On ne manipule pas n'importe quels polynômes

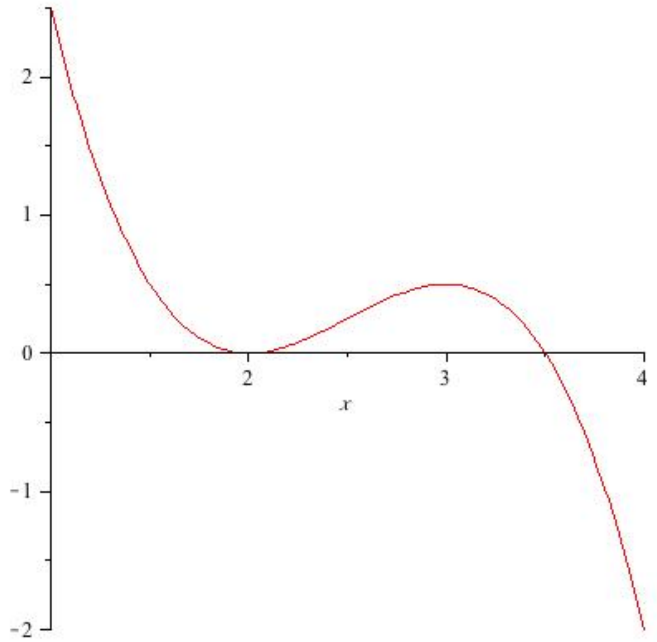
Courbe d'erreur d'approximation "décalée" d'une estimation/majoration de l'erreur max.



$\longrightarrow$ en général, aucune racine sur $[a, b]$. Si on a trouvé exactement l'erreur d'approximation, on peut avoir des racines multiples.

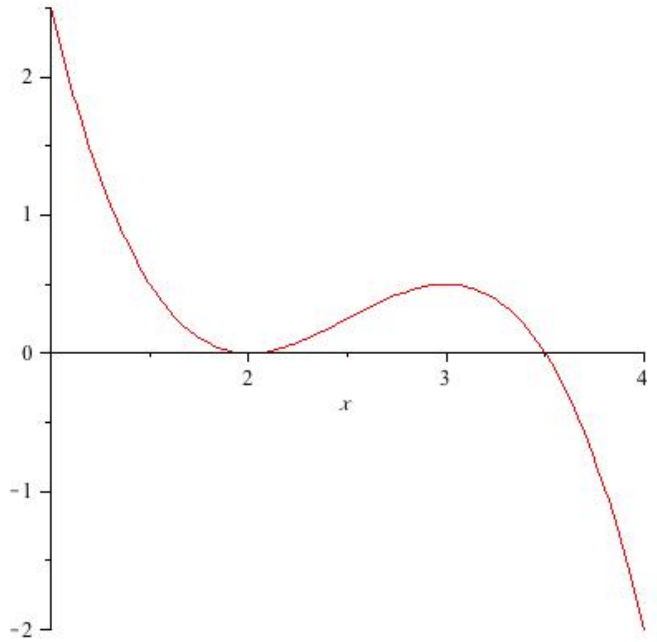
Montrer que $\mathcal{P} \geq 0$ (ou $\mathcal{P} > 0$) sur $[a, b]$

- en supposant $\mathcal{P}(a) > 0$, c'est montrer que $\mathcal{P}$ n'a aucune racine réelle de multiplicité impaire (ou aucune racine réelle) sur $[a, b[$;



Montrer que $\mathcal{P} \geq 0$ (ou $\mathcal{P} > 0$) sur $[a, b]$

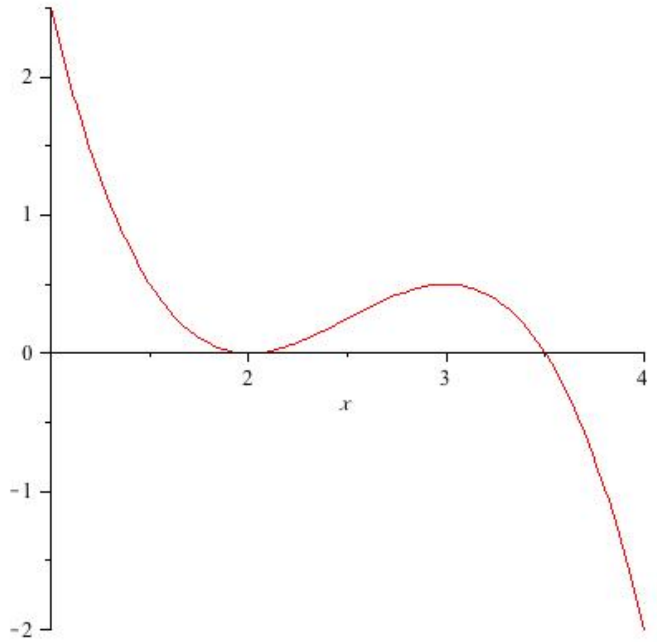
- en supposant $\mathcal{P}(a) > 0$, c'est montrer que $\mathcal{P}$ n'a aucune racine réelle de multiplicité impaire (ou aucune racine réelle) sur $[a, b[$;



- Règle des signes de Descartes ;

Montrer que $\mathcal{P} \geq 0$ (ou $\mathcal{P} > 0$) sur $[a, b]$

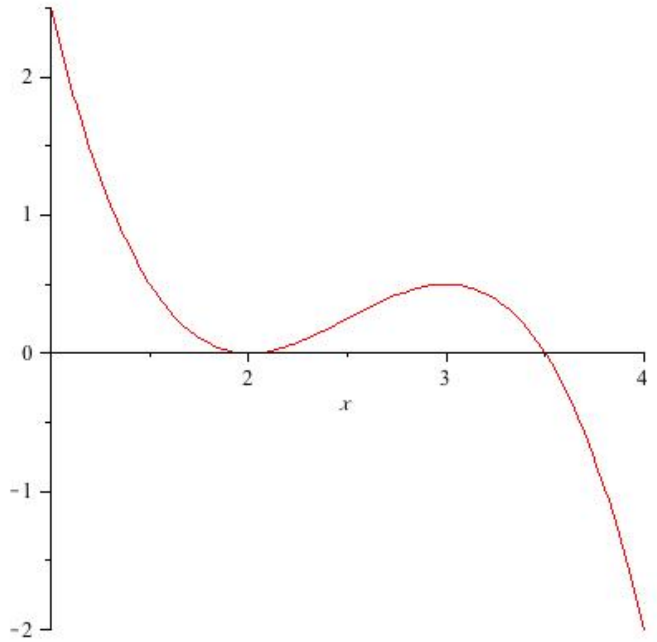
- en supposant $\mathcal{P}(a) > 0$, c'est montrer que $\mathcal{P}$ n'a aucune racine réelle de multiplicité impaire (ou aucune racine réelle) sur $[a, b[$;



- Règle des signes de Descartes ;
- Théorème de Sturm ;

Montrer que $\mathcal{P} \geq 0$ (ou $\mathcal{P} > 0$) sur $[a, b]$

- en supposant $\mathcal{P}(a) > 0$, c'est montrer que $\mathcal{P}$ n'a aucune racine réelle de multiplicité impaire (ou aucune racine réelle) sur $[a, b[$;



- Règle des signes de Descartes ;
- Théorème de Sturm ;
- Décomposition de $\mathcal{P}$ en somme de carrés.

Règle des signes de Descartes

Le nombre ν de racines réelles positives d'un polynôme $\mathcal{P}$ est majoré par le nombre m de changements de signes entre 2 coefficients consécutifs non nuls. Il a de plus la même parité que $m \longrightarrow$ quand m vaut 0 ou 1, $\nu = m$.

- Se ramener à $[a, b]$? changement de variable

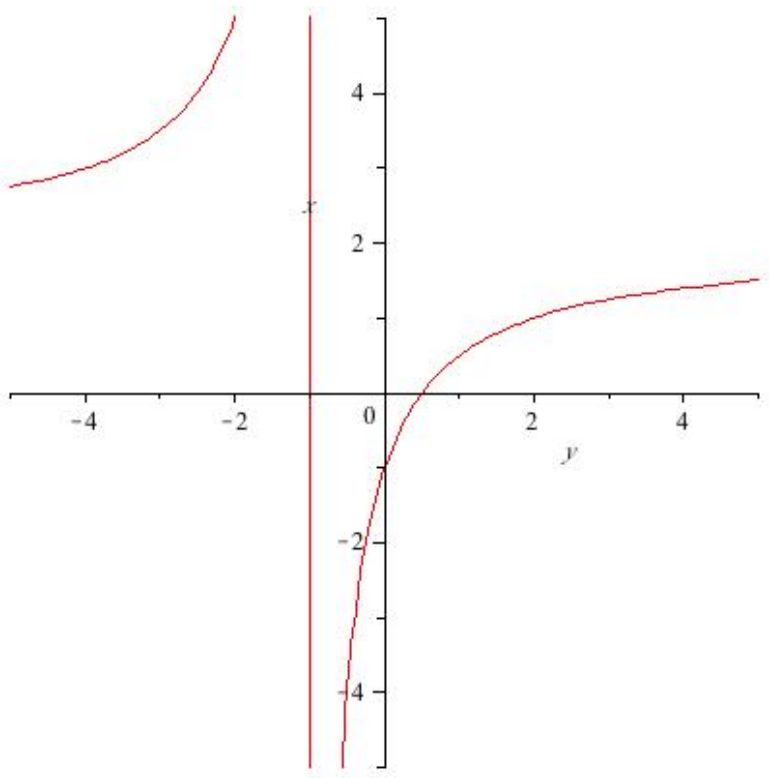
$$x = \frac{a + by}{1 + y}.$$

on a

$$\mathcal{P}(x) = 0 \Leftrightarrow \mathcal{P}\left(\frac{a + by}{1 + y}\right) = 0$$

- se ramener à un polynôme :

$$\mathcal{P}\left(\frac{a + by}{1 + y}\right) \times (1 + y)^n.$$



Cas $[a, b] = [-1, 2]$.

Collins & Akritas, Rouiller & Zimmermann

- Intervalle considéré : $[0,1]$ (chgt de variable). P de degré n ;
- pour $c < 2^k$ $(k, c \in \mathbb{N})$, on définit

$$I_{k,c} = \left]\frac{c}{2^k}, \frac{c+1}{2^k}\right[, \text{ et } P_{k,c} = 2^{kn} P\left(\frac{x+c}{2^k}\right);$$

- racines de $P_{k,c}$ sur $[0,1] \leftrightarrow$ racines de P sur $I_{k,c}$;
- Collins & Akritas : si on applique itérativement des transformations $P \to P\left(\frac{x}{2}\right)$ et $P \to P\left(\frac{x+1}{2}\right)$ à n'importe quel polyôme sans facteurs carrés P, au bout d'un nombre fini d'étapes on obtient un polynôme pour lequel la règle de Descartes donne comme borne 0 ou 1 sur le nombre de racines dans $[0,1]$.
- Stratégie de Bissection : On repère itérativement les $I_{k,c}$ pour lequels la borne de Descarte est > 1, et on les "coupe" (en passant à $k+1$).

Collins & Akritas, Rouiller & Zimmermann

- Diverses variantes du parcours d'arbre explorées par Rouiller et Zimmermann (et leur "petite main" Hanrot ?). En particulier, donnent une version où on n'a en mémoire qu'un polynôme à chaque pas ;
- ceci dit
  - la méthode est intéressante pour isoler les racines. Ici on veut montrer qu'il n'y en a pas ;
  - adaptations : tout arrêter dès qu'on trouve une borne impaire, revoir la stratégie en tenant compte du fait qu'il n'y a (a priori) pas de racines ;
  - s'assurer que P est sans facteurs carrés : calculer le pgcd de P et P'... quand on a fait ça, on a fait le plus gros de la méthode de Sturm.

Théorème de Sturm

- $P_0 = \mathcal{P}$, de degré n, $P_1 = \mathcal{P}'$;
- algorithme d'Euclide appliqué à P_0 et P_1, en prenant les opposés des restes :
  - $P_0 = P_1 Q_1 - P_2$;
  - $P_1 = P_2 Q_2 - P_3$;
  - ...
  - on s'arrête dès que P_m est constant ($m \leq n$)
- si $P_m \neq 0$, $\mathcal{P}$ n'a pas de racine multiple dans $\mathbb{R}$. Soit $V(x)$ le nombre de changements "stricts" de signes dans la suite

$$P_0(x), P_1(x), P_2(x), \ldots, P_m(x).$$

  Le nombre de racines réelles de $\mathcal{P}$ dans $]a, b[$ est $V(a) - V(b)$.
- si $P_m = 0$, P a des racines multiples (*pas forcément dans* $[a, b]$). Même chose en divisant P_0, P_1, ..., P_{m-1} par P_{m-1}.

Exemple : $P_0(x) = x^3 - 19x + 30$ sur $[1, 4]$

- $P_1(x) = P_0'(x) = 3x^2 - 19$;

Exemple : $P_0(x) = x^3 - 19x + 30$ sur $[1, 4]$

- $P_1(x) = P_0'(x) = 3x^2 - 19$;
- division euclidienne de P_0 par P_1 : reste $-38/3x + 30$

$$P_2(x) = \frac{38}{3}x - 30$$

Exemple : $P_0(x) = x^3 - 19x + 30$ sur $[1, 4]$

- $P_1(x) = P_0'(x) = 3x^2 - 19$;
- division euclidienne de P_0 par P_1 : reste $-38/3x + 30$

$$P_2(x) = \frac{38}{3}x - 30$$

- division euclidienne de P_1 par P_2 : reste $-784/361$

$$P_3(x) = \frac{784}{361}$$

Exemple : $P_0(x) = x^3 - 19x + 30$ sur $[1, 4]$

- $P_1(x) = P_0'(x) = 3x^2 - 19$;
- division euclidienne de P_0 par P_1 : reste $-38/3x + 30$

$$P_2(x) = \frac{38}{3}x - 30$$

- division euclidienne de P_1 par P_2 : reste $-784/361$

$$P_3(x) = \frac{784}{361}$$

$$P_0(1) = 12 \quad P_1(1) = -16 \quad P_2(1) = -\frac{52}{3} \quad P_3(1) = \frac{784}{361} \quad V(1) = 2$$
$$P_0(4) = 18 \quad P_1(4) = 29 \quad P_2(4) = \frac{62}{3} \quad P_3(4) = \frac{784}{361} \quad V(4) = 0$$

Exemple : $P_0(x) = x^3 - 19x + 30$ sur $[1, 4]$

- $P_1(x) = P_0'(x) = 3x^2 - 19$;
- division euclidienne de P_0 par P_1 : reste $-38/3x + 30$

$$P_2(x) = \frac{38}{3}x - 30$$

- division euclidienne de P_1 par P_2 : reste $-784/361$

$$P_3(x) = \frac{784}{361}$$

$$P_0(1) = 12 \quad P_1(1) = -16 \quad P_2(1) = -\tfrac{52}{3} \quad P_3(1) = \tfrac{784}{361} \quad V(1) = 2$$
$$P_0(4) = 18 \quad P_1(4) = 29 \quad P_2(4) = \tfrac{62}{3} \quad P_3(4) = \tfrac{784}{361} \quad V(4) = 0$$

Il y a donc $V(1) - V(4) = 2$ racines...

Exemple : $P_0(x) = x^3 - 19x + 30$ sur $[1, 4]$

- $P_1(x) = P_0'(x) = 3x^2 - 19$;
- division euclidienne de P_0 par P_1 : reste $-38/3x + 30$

$$P_2(x) = \frac{38}{3}x - 30$$

- division euclidienne de P_1 par P_2 : reste $-784/361$

$$P_3(x) = \frac{784}{361}$$

$$P_0(1) = 12 \quad P_1(1) = -16 \quad P_2(1) = -\tfrac{52}{3} \quad P_3(1) = \tfrac{784}{361} \quad V(1) = 2$$
$$P_0(4) = 18 \quad P_1(4) = 29 \quad P_2(4) = \tfrac{62}{3} \quad P_3(4) = \tfrac{784}{361} \quad V(4) = 0$$

Il y a donc $V(1) - V(4) = 2$ racines. . . en fait

$$P_0(x) = (x - 2)(x - 3)(x + 5).$$

Approche "sommes de carrés"

Pour faire un peu d'histoire (et faire plaisir à Vincent), le 17ème problème de Hilbert : *Si un polynôme en n variables et à coefficients réels ne prend que des valeurs positives sur* $\mathbb{R}$*, est-il possible de le décomposer en une somme de carrés de fractions rationnelles ?*

- Emil Artin, 1926 : la réponse est oui
- dans le cas qui nous intéresse (une variable), somme de carrés de polynômes. . . et, surtout, bien plus facile !
- tombe bien : représenter un polynôme comme somme de carrés est une manière simple de prouver qu'il est ≥ 0. . . sur $\mathbb{R}$!

Intérêt ici : certificat simple. On fait du calcul "sale mais rapide" pour construire la décomposition en sommes de carrés. Il ne reste qu'à la vérifier ensuite.

Cas à une variable

$\mathcal{P} \in \mathbb{R}[X]$, positif ou nul sur $\mathbb{R}$:

- il est de degré pair et de coefficient de tête > 0 (sinon $\mathcal{P}(x)$ tend vers $-\infty$, soit en $+\infty$, soit en $-\infty$) ;
- ses racines réelles sont de multiplicité paire (déjà vu) ;
- bien sûr ses racines complexes sont conjuguées.

$$\mathcal{P}(x) = \lambda \cdot (x - (a_1 + ib_1)) \cdot (x - (a_2 + ib_2)) \cdots (x - (a_m + ib_m)) \cdot (x - (a_1 - ib_1)) \cdot (x - (a_2 - ib_2)) \cdots (x - (a_m - ib_m))$$

(avec $b_i = 0$ lorsque racine double réelle)
soit

$$\mathcal{P}(x) = \lambda \cdot (q(x) + ir(x)) \cdot (q(x) - ir(x))$$

$$= \lambda \cdot (q(x))^2 + \lambda \cdot (r(x))^2$$

Mais mon polynôme est ≥ 0 sur $[a, b]$, pas sur $\mathbb{R}$

Changement de variable

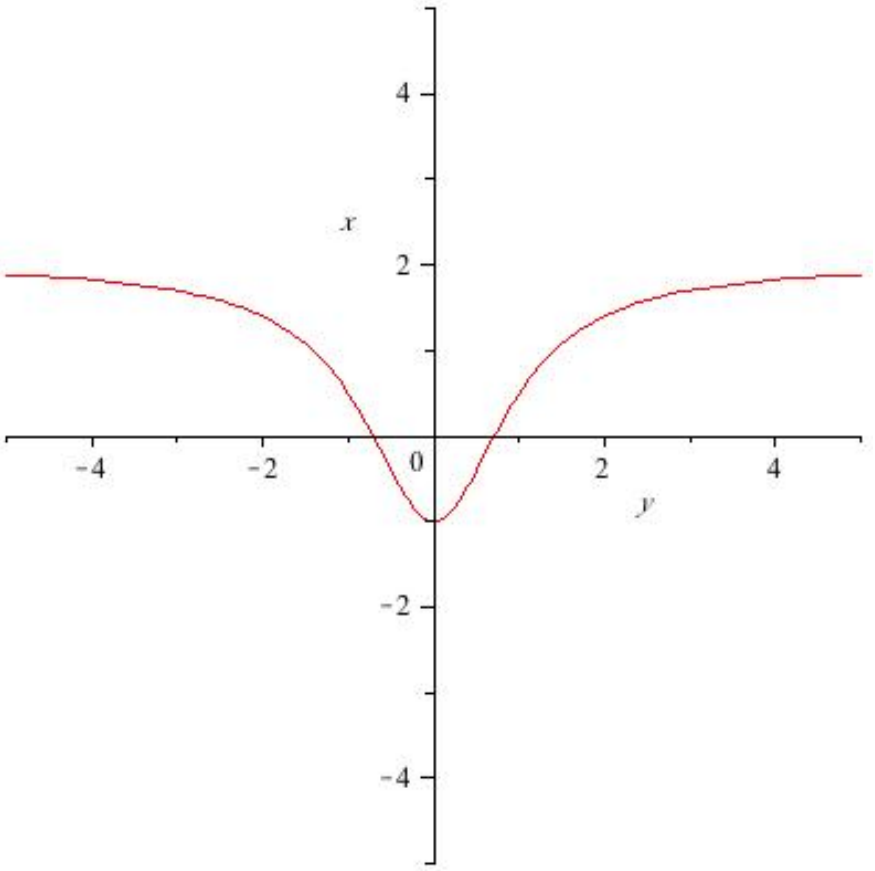
$$x = \frac{a + by^2}{1 + y^2}$$

Problème associé :

$$\forall y \in \mathbb{R}, \mathcal{P}\left(\frac{a + by^2}{1 + y^2}\right) \geq 0$$

On se ramène à un polynôme en multipliant $\mathcal{P}\left(\frac{a+by^2}{1+y^2}\right)$ par $(1 + y^2)^n$.

(pas gratuit : double le degré)



Je ne connais pas exactement les racines...

- calcul approché ;
- elles ne sont pas forcément dans $\mathbb{Q}[i]$

$\longrightarrow$ au lieu de $a_k \pm ib_k$ on a $a_k^* \pm ib_k^*$
$\longrightarrow$ donne $\mathcal{P}(x) = \lambda \cdot (q(x))^2 + \lambda \cdot (r(x))^2 + u(x)$.

On va pouvoir rendre u aussi petit qu'on veut, mais il n'est pas forcément > 0, donc on ne peut pas forcément le décomposer en somme de carrés.

$\longrightarrow$ Se donner un peu de marge avec un polynôme légèrement différent

Polynôme "perturbé"

$$\mathcal{P}_\epsilon(x) = \mathcal{P}(x) - \epsilon \cdot (1 + x + x^2 + \cdots + x^n).$$

- $\mathcal{P} > 0 \Rightarrow \exists \epsilon_0$ t.q. $(\epsilon < \epsilon_0 \Rightarrow \mathcal{P}_\epsilon > 0)$
- décomposition $\mathcal{P}_\epsilon(x) = (\lambda - \epsilon) \cdot (q(x))^2 + (\lambda - \epsilon) \cdot (r(x))^2$, mais comme on calcule des racines approchées, on a en fait

$$\mathcal{P}_\epsilon(x) = (\lambda - \epsilon) \cdot (q(x))^2 + (\lambda - \epsilon) \cdot (r(x))^2 + u(x),$$

où les coefficients de u sont aussi petits qu'on veut. On en déduit

$$\mathcal{P}(x) = (\lambda-\epsilon)\cdot(q(x))^2+(\lambda-\epsilon)\cdot(r(x))^2+\epsilon\cdot(1+x^2+\cdots+x^n)+u(x).$$

On a presque fini

$$\mathcal{P}(x) = (\lambda-\epsilon)\cdot(q(x))^2+(\lambda-\epsilon)\cdot(r(x))^2+\epsilon\cdot(1+x^2+\cdots+x^n)+u(x).$$

Posons $u(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ et $n = 2m$, il vient :

$$\begin{aligned}
&\epsilon \cdot (1 + x^2 + \cdots + x^n) + u(x) \\
&= \sum_{k=0}^{m-1} |a_{2k+1}| \left(x^{k+1} + \frac{\text{sign}(a_{2k+1})}{2} \cdot x^k\right)^2 \\
&+ \sum_{k=0}^{m} \left(\epsilon + a_{2k} - |a_{2k-1}| - \frac{|a_{2k+1}|}{4}\right) \cdot x^{2k}
\end{aligned}$$

$\longrightarrow$ dès que

$$\frac{|a_{2k+1}|}{4 - a_{2k} + |a_{2k+1}|} \leq \epsilon,$$

c'est une somme de carrés.