Modélisation et résolutions numérique et symbolique de problèmes via les logiciels Maple et MATLAB (MODEL)

Cours n°4 : Polynômes univariés, isolation de solutions réelles et algorithme d'Euclide

Stef Graillat & Mohab Safey El Din

Université Pierre et Marie Curie (Paris 6)

Résumé des notions précédemment vues

- Codes correcteurs d'erreurs linéaires
- Espaces vectoriels et matrices
- Dimension, Rang
- Calculs élémentaires en algèbre linéaire
- Corps fini de cardinalité un nombre premier
- Application à des codes spécifiques

Et maintenant on passe à un monde moins discret...

Résumé des notions précédemment vues

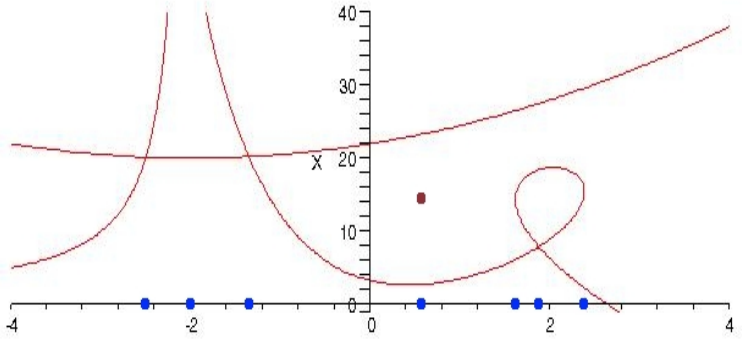
- Codes correcteurs d'erreurs linéaires
- Espaces vectoriels et matrices
- Dimension, Rang
- Calculs élémentaires en algèbre linéaire
- Corps fini de cardinalité un nombre premier
- Application à des codes spécifiques

Et maintenant on passe à un monde moins discret...

Solutions réelles de polynômes : Contexte applicatif

- En algèbre linéaire : apparaissent naturellement (valeurs propres de matrices)
- Valeurs propres en image :
  - Technique d'analyse en composantes principales (télédétection et image multi-spectrale)
  - Courbes algébriques apparaissent naturellement (Bézier patches)
- En IA :
  - Valeurs propres aussi !
  - Problèmes d'optimisation non linéaires $\rightsquigarrow$ s'expriment souvent polynmialement (algébriquement)
- En Calcul scientifique :
  - Sciences de l'ingénieur : Robotique, vision 3d, stabilisation de systèmes dynamiques
  - Gros progrès algorithmiques récents

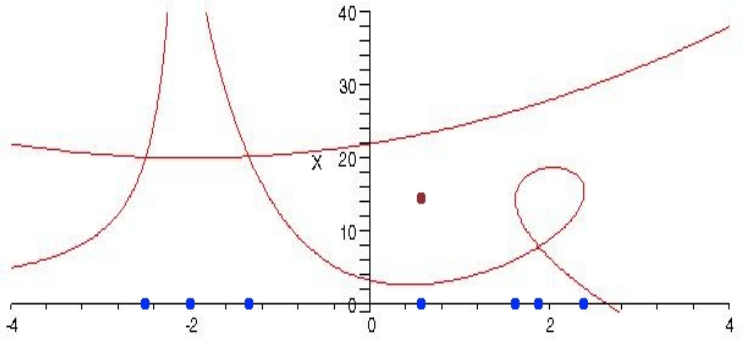
Un exemple : le tracé de courbes certifié



- Algorithme naif de balayage perpendiculairement à un axe ;
- Identifier les points où une « catastrophe » (points critiques, asymptotes) se produit par rapport à notre axe ;
- On peut commencer par identifier leurs projections sur notre axe.

On a besoin de savoir isoler les racines d'un polynômes en une variable.

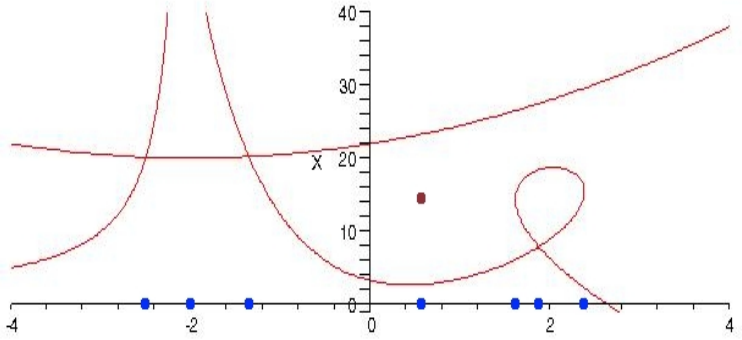
Un exemple : le tracé de courbes certifié



- Algorithme naif de balayage perpendiculairement à un axe ;
- Identifier les points où une « catastrophe » (points critiques, asymptotes) se produit par rapport à notre axe ;
- On peut commencer par identifier leurs projections sur notre axe.

On a besoin de savoir isoler les racines d'un polynômes en une variable.

Un exemple : le tracé de courbes certifié

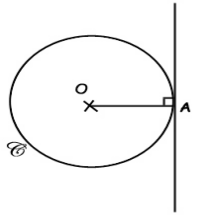


- Algorithme naif de balayage perpendiculairement à un axe ;
- Identifier les points où une « catastrophe » (points critiques, asymptotes) se produit par rapport à notre axe ;
- On peut commencer par identifier leurs projections sur notre axe.

On a besoin de savoir isoler les racines d'un polynômes en une variable.

Objectif 1 : Résoudre $f(X, Y) = g(X, Y) = 0$

Soit $\mathscr{C}$ une courbe définie par $f(X, Y) = 0$ et $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathscr{C}$ telle que $\frac{\partial f}{\partial X}(\mathbf{z}) \neq 0$ ou $\frac{\partial f}{\partial Y}(\mathbf{z}) \neq 0$.



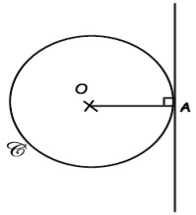
1. Une droite de vecteur directeur $\mathbf{v} = (\mathbf{a}, \mathbf{b})$ est tangente à $\mathscr{C}$ en $(\mathbf{x}, \mathbf{y})$ ssi elle contient $\mathbf{x}$ et $\mathbf{a}\frac{\partial f}{\partial X}(\mathbf{z}) + \mathbf{b}\frac{\partial f}{\partial Y}(\mathbf{z}) = \mathbf{v}.\mathrm{grad}_{\mathbf{z}}(f)0$. Elle est normale au vecteur gradient de f en z.

   On peut aussi dire que $\mathbf{v} = \lim_{\mathbf{z}' \to \mathbf{z}} \frac{\mathbf{zz}'}{||\mathbf{zz}'||}$.
2. Si on projette sur l'axe des absisses (celui des X), les « points critiques » sont précisément ceux pour lesquels $f(X, Y) = \frac{\partial f}{\partial Y} = 0$

⇝ Pour résoudre, on va se ramener au cas d'une variable.

Objectif 1 : Résoudre $f(X, Y) = g(X, Y) = 0$

Soit $\mathscr{C}$ une courbe définie par $f(X, Y) = 0$ et $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathscr{C}$ telle que $\frac{\partial f}{\partial X}(\mathbf{z}) \neq 0$ ou $\frac{\partial f}{\partial Y}(\mathbf{z}) \neq 0$.



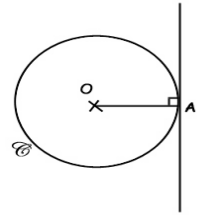
1. Une droite de vecteur directeur $\mathbf{v} = (\mathbf{a}, \mathbf{b})$ est tangente à $\mathscr{C}$ en $(\mathbf{x}, \mathbf{y})$ ssi elle contient $\mathbf{x}$ et $\mathbf{a}\frac{\partial f}{\partial X}(\mathbf{z}) + \mathbf{b}\frac{\partial f}{\partial Y}(\mathbf{z}) = \mathbf{v}.\mathrm{grad}_{\mathbf{z}}(f)0$. Elle est normale au vecteur gradient de f en $\mathbf{z}$.

   On peut aussi dire que $\mathbf{v} = \lim_{\mathbf{z}' \to \mathbf{z}} \frac{\mathbf{z}\mathbf{z}'}{||\mathbf{z}\mathbf{z}'}$.
2. Si on projette sur l'axe des absisses (celui des X), les « points critiques » sont précisément ceux pour lesquels $f(X, Y) = \frac{\partial f}{\partial Y} = 0$

$\rightsquigarrow$ Pour résoudre, on va se ramener au cas d'une variable.

Objectif 1 : Résoudre $f(X, Y) = g(X, Y) = 0$

Soit $\mathscr{C}$ une courbe définie par $f(X, Y) = 0$ et $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathscr{C}$ telle que $\frac{\partial f}{\partial X}(\mathbf{z}) \neq 0$ ou $\frac{\partial f}{\partial Y}(\mathbf{z}) \neq 0$.



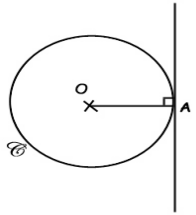
1. Une droite de vecteur directeur $\mathbf{v} = (\mathbf{a}, \mathbf{b})$ est tangente à $\mathscr{C}$ en $(\mathbf{x}, \mathbf{y})$ ssi elle contient $\mathbf{x}$ et $\mathbf{a}\frac{\partial f}{\partial X}(\mathbf{z}) + \mathbf{b}\frac{\partial f}{\partial Y}(\mathbf{z}) = \mathbf{v}.\mathrm{grad}_{\mathbf{z}}(f)0$. Elle est normale au vecteur gradient de f en $\mathbf{z}$.

   On peut aussi dire que $\mathbf{v} = \lim_{\mathbf{z}' \to \mathbf{z}} \frac{\mathbf{z}\mathbf{z}'}{||\mathbf{z}\mathbf{z}'}$.
2. Si on projette sur l'axe des absisses (celui des X), les « points critiques » sont précisément ceux pour lesquels $f(X, Y) = \frac{\partial f}{\partial Y} = 0$

$\rightsquigarrow$ Pour résoudre, on va se ramener au cas d'une variable.

Objectif 1 : Résoudre $f(X, Y) = g(X, Y) = 0$

Soit $\mathscr{C}$ une courbe définie par $f(X, Y) = 0$ et $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathscr{C}$ telle que $\frac{\partial f}{\partial X}(\mathbf{z}) \neq 0$ ou $\frac{\partial f}{\partial Y}(\mathbf{z}) \neq 0$.

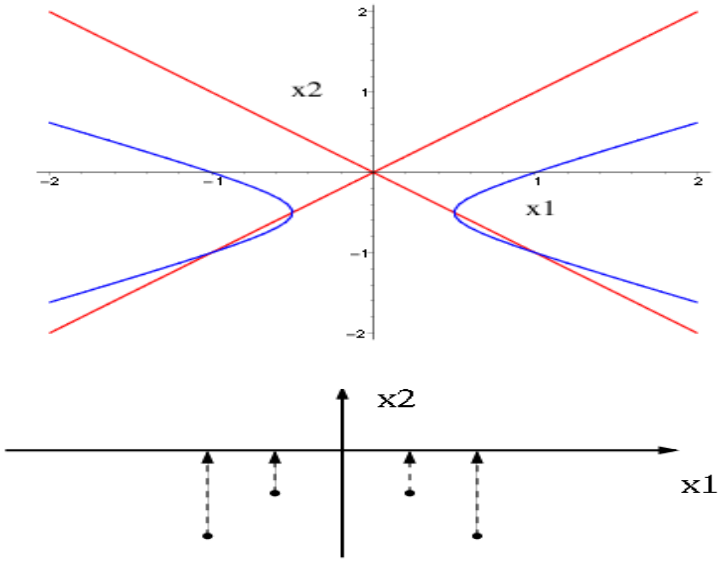


1. Une droite de vecteur directeur $\mathbf{v} = (\mathbf{a}, \mathbf{b})$ est tangente à $\mathscr{C}$ en $(\mathbf{x}, \mathbf{y})$ ssi elle contient $\mathbf{x}$ et $\mathbf{a}\frac{\partial f}{\partial X}(\mathbf{z}) + \mathbf{b}\frac{\partial f}{\partial Y}(\mathbf{z}) = \mathbf{v}.\mathrm{grad}_{\mathbf{z}}(f)0$. Elle est normale au vecteur gradient de f en $\mathbf{z}$.

   On peut aussi dire que $\mathbf{v} = \lim_{\mathbf{z}' \to \mathbf{z}} \frac{\mathbf{z}\mathbf{z}'}{||\mathbf{z}\mathbf{z}'}$.
2. Si on projette sur l'axe des absisses (celui des X), les « points critiques » sont précisément ceux pour lesquels $f(X, Y) = \frac{\partial f}{\partial Y} = 0$

$\rightsquigarrow$ Pour résoudre, on va se ramener au cas d'une variable.

Objectif 2 : Isoler les solutions réelles de $f(X) = 0$



Polynômes univariés : codage et propriétés élémentaires

1. Soit $\mathbb{K}$ un corps et X une indéterminée.

$$\mathbb{K}[X] = \{\sum_{i=0}^{D} c_i X^i \mid c_i \in \mathbb{K},\ D \in \mathbb{N}\}$$

2. Le degré de f est le plus petit entier D tel que $c_i \neq 0$
3. Codage dense : tableau des coefficients.
4. Codage creux : tableau des coefficients non-nuls et des exposants.
5. L'ensemble des polynômes est un $\mathbb{K}$-espace vectoriel (de dimension infinie).
6. L'ensemble des polynômes de degré $\leq D$ est un $\mathbb{K}$-espace vectoriel de dimension finie $D+1$.

Polynômes univariés : propriétés (suite)

1. Les fonctions polynomiales sont continues et dérivables.
2. Un polynôme univarié de degré D a D racines complexes (comptées avec multiplicité).
3. Le Théorème des valeurs intermédiaires s'applique : pour tout $c \in [f(a), f(b)]$, il existe $u \in [a, b]$ tel que $f(u) = c$.
4. Le Théorème de Rolle s'applique : soit $a < b$ tel que $f(a)f(b) < 0$, alors il exists $c \in [a, b]$ tel que $f'(c) = 0$.

Stratégie d'isolation

Soit $f \in \mathbb{Q}[X]$.

Isolation dans un intervalle $I = [a, b]$

1. Compter le nombre de racines de f dans $[a, b]$
2. S'il n'y a pas de racines retourner une liste vide
3. S'il y a une et une seule racine retourner I
4. Procéder par dichotomie (appels récursifs avec $I_1 = [a, \frac{a+b}{2}]$ et $I_2 = [\frac{a+b}{2}, b]$

Pour généraliser sur les réels, on a besoin d'une borne sur le max des valeurs absolues des racines.

Stratégie d'isolation

Soit $f \in \mathbb{Q}[X]$.

Isolation dans un intervalle $I = [a, b]$

1. Compter le nombre de racines de f dans $[a, b]$
2. S'il n'y a pas de racines retourner une liste vide
3. S'il y a une et une seule racine retourner I
4. Procéder par dichotomie (appels récursifs avec $I_1 = [a, \frac{a+b}{2}]$ et $I_2 = [\frac{a+b}{2}, b]$

Pour généraliser sur les réels, on a besoin d'une borne sur le max des valeurs absolues des racines.

Stratégie d'isolation

Soit $f \in \mathbb{Q}[X]$.

Isolation dans un intervalle $I = [a, b]$

1. Compter le nombre de racines de f dans $[a, b]$
2. S'il n'y a pas de racines retourner une liste vide
3. S'il y a une et une seule racine retourner I
4. Procéder par dichotomie (appels récursifs avec $I_1 = [a, \frac{a+b}{2}]$ et $I_2 = [\frac{a+b}{2}, b]$

Pour généraliser sur les réels, on a besoin d'une borne sur le max des valeurs absolues des racines.

Stratégie d'isolation

Soit $f \in \mathbb{Q}[X]$.

Isolation dans un intervalle $I = [a, b]$

1. Compter le nombre de racines de f dans $[a, b]$
2. S'il n'y a pas de racines retourner une liste vide
3. S'il y a une et une seule racine retourner I
4. Procéder par dichotomie (appels récursifs avec $I_1 = [a, \frac{a+b}{2}]$ et $I_2 = [\frac{a+b}{2}, b]$

Pour généraliser sur les réels, on a besoin d'une borne sur le max des valeurs absolues des racines.

Stratégie d'isolation

Soit $f \in \mathbb{Q}[X]$.

Isolation dans un intervalle $I = [a, b]$

1. Compter le nombre de racines de f dans $[a, b]$
2. S'il n'y a pas de racines retourner une liste vide
3. S'il y a une et une seule racine retourner I
4. Procéder par dichotomie (appels récursifs avec $I_1 = [a, \frac{a+b}{2}]$ et $I_2 = [\frac{a+b}{2}, b]$

Pour généraliser sur les réels, on a besoin d'une borne sur le max des valeurs absolues des racines.

Premières bornes

Soit $f = \sum_{i=0}^{D} X^i \in \mathbb{Q}[X]$.

Proposition 1

Si α est une racine complexe de f et que $a_D = 1$, alors $|\alpha| < 1 + \max(|a_i|, 0 \leq i \leq D-1)$.

Proposition 2 (Borne de Lagrange-MacLaurin)

Posons $m = \max(\{i \mid 0 \leq i \leq D-1, a_i < 0\})$ *et* $B = \max(\{-a_i \mid 0 \leq i \leq D-1,\ a_i < 0\})$ *($B = 0$ par convention si tous les a_i sont positifs ou nuls). Si α est une racine réelle positive de f alors, en supposant que $a_D = 1$ et que $a_0 \neq 0$, on a*

$$\alpha < 1 + \sqrt[n-m]{B}.$$

Majoration du nombre de racines

Définition 1

On définit le signe, $\mathrm{sign}(a)$, *d'un élément* $a \in \mathbb{R}$ *par un entier valant* 0 *si* $a = 0$, 1 *si* $a > 0$ *et* -1 *si* $a < 0$. *Le* nombre de changements de signes $V(a)$ *dans une suite,* $\underline{a} = a_1, \cdots, a_k$, *d'éléments de* $\mathbb{R} \setminus \{0\}$ *est défini par induction sur* k *par :*

$$V(a_1) = 0$$

$$V(a_1, \cdots, a_k) = \begin{cases} V(a_1, \cdots, a_{k-1}) + 1 & \text{si} \quad \mathrm{sign}(a_{k-1}a_k) = -1 \\ V(a_1, \cdots, a_{k-1}) & \text{sinon} \end{cases}$$

Si $f = \sum_{i=0}^{D} a_i X^i \in \mathbb{R}[X]$, on note $V(f)$ le nombre $V(a_0, \ldots, a_D)$.

Majoration du nombre de racines (suite)

Proposition 3 (Lemme de Descartes)

Soit $f \in \mathbb{R}[X]$ *non identiquement nul. Le nombre de racines réelles strictement positives (comptées avec multiplicités) de* f

- *est égal à* $V(f)$ *modulo 2.*
- *est borné par* $V(f)$.

Conséquence : Soit $f = \sum_{i=0}^{D} a_i X^i \in \mathbb{R}[X]$.

1. Si $V(f) = 0$, alors f n'a pas de racines réelles strictement positives ;
2. Si $V(f) = 1$, alors f a une et une seule racine réelle strictement positive.

Majoration du nombre de racines (suite)

Proposition 3 (Lemme de Descartes)

Soit $f \in \mathbb{R}[X]$ *non identiquement nul. Le nombre de racines réelles strictement positives (comptées avec multiplicités) de* f

- *est égal à* $V(f)$ *modulo 2.*
- *est borné par* $V(f)$.

Conséquence : Soit $f = \sum_{i=0}^{D} a_i X^i \in \mathbb{R}[X]$.

1. Si $V(f) = 0$, alors f n'a pas de racines réelles strictement positives ;
2. Si $V(f) = 1$, alors f a une et une seule racine réelle strictement positive.

Calcul du nombre de racines : Suite de Sturm

Définition 2

Soit $f \in \mathbb{R}[X]$. *Une suite de Sturm associée à* f *pour un intervalle donné* $[a, b] \in \mathbb{R}$ *est une suite de polynômes de* $\mathbb{R}[X]$ $[f_0(X), \ldots f_s(X)]$ *tels que :*

1. $f_0 = f$
2. f_s *n'a aucune racine réelle dans* $[a, b]$;
3. *pour* $0 < i < s$, *si* $\alpha \in [a, b]$ *est tel que* $f_i(\alpha) = 0$, *alors* $f_{i-1}(\alpha) f_{i+1}(\alpha) < 0$:
4. *si* $\alpha \in [a, b]$ *est tel que* $f_0(\alpha) = 0$, *alors*

$$\begin{cases} f_0 f_1(\alpha - \epsilon) < 0 \\ f_0 f_1(\alpha + \epsilon) > 0 \end{cases}$$

pour toute valeur de ϵ *suffisamment petite (*$f_0 f_1$ *est une fonction croissante en* α*).*

Calcul du nombre de racines : Vers le Théorème de Sturm

Soit $f \in \mathbb{R}[X]$ et $S(X) = [f_0(X), \dots f_s(X)]$ une suite de Sturm associée à f sur I. On note $V_{stu}(f(c)) = V(f_0(c), \dots f_s(c))$ pour tout $c \in \mathbb{R}$.
Si $I = \mathbb{R}$, on définit $V_{stu}(f(+\infty))$ (resp. $V_{stu}(f(-\infty))$) comme étant le nombre de variations de signes dans la suite des coefficients de plus haut degré des polynômes de $S(X)$ (resp. $S(-X)$).

Proposition 4

Si $I = [a, b]$ alors $V_{stu}(f(b)) - V_{stu}(f(a))$ est égal au nombre de racines réelles de f dans $[a, b]$.

Corollaire 1

$V_{stu}(f(+\infty)) - V_{stu}(f(-\infty))$ est égal au nombre de racines réelles de f dans $\mathbb{R}$.

Calcul du nombre de racines : Vers le Théorème de Sturm

Soit $f \in \mathbb{R}[X]$ et $S(X) = [f_0(X), \dots f_s(X)]$ une suite de Sturm associée à f sur I. On note $V_{stu}(f(c)) = V(f_0(c), \dots f_s(c))$ pour tout $c \in \mathbb{R}$.
Si $I = \mathbb{R}$, on définit $V_{stu}(f(+\infty))$ (resp. $V_{stu}(f(-\infty))$) comme étant le nombre de variations de signes dans la suite des coefficients de plus haut degré des polynômes de $S(X)$ (resp. $S(-X)$).

Proposition 4

Si $I = [a, b]$ alors $V_{stu}(f(b)) - V_{stu}(f(a))$ est égal au nombre de racines réelles de f dans $[a, b]$.

Corollaire 1

$V_{stu}(f(+\infty)) - V_{stu}(f(-\infty))$ est égal au nombre de racines réelles de f dans $\mathbb{R}$.

Calcul du nombre de racines : Vers le Théorème de Sturm

Soit $f \in \mathbb{R}[X]$ et $S(X) = [f_0(X), \dots f_s(X)]$ une suite de Sturm associée à f sur I. On note $V_{stu}(f(c)) = V(f_0(c), \dots f_s(c))$ pour tout $c \in \mathbb{R}$.
Si $I = \mathbb{R}$, on définit $V_{stu}(f(+\infty))$ (resp. $V_{stu}(f(-\infty))$) comme étant le nombre de variations de signes dans la suite des coefficients de plus haut degré des polynômes de $S(X)$ (resp. $S(-X)$).

Proposition 4

Si $I = [a, b]$ alors $V_{stu}(f(b)) - V_{stu}(f(a))$ est égal au nombre de racines réelles de f dans $[a, b]$.

Corollaire 1

$V_{stu}(f(+\infty)) - V_{stu}(f(-\infty))$ est égal au nombre de racines réelles de f dans $\mathbb{R}$.

Calcul du nombre de racines : Vers le Théorème de Sturm

Soit $f \in \mathbb{R}[X]$ sans racince réelle multiple dans $[a, b]$.

Proposition 5

On pose $f_0 = f$, $f_1 = f'$. et on construit par induction les polynômes f_i $i = 2 \dots s$ en posant $f_{i-2} = f_{i-1}g_i - f_i$ et en stoppant la construction à l'indice s tel que f_s n'admet aucune racine réelle dans $[a, b]$. La suite ainsi construite est une suite de Sturm associée à f pour $[a, b]$.

Théorème de Sturm : On pose $f_0 = f$, $f_1 = -f'$. et on construit par induction les polynômes f_i $i = 2 \dots s$ en posant $f_{i-2} = f_{i-1}g_i - f_i$, $deg(f_i) < deg(f_{i-1})$, et en stoppant la construction à l'indice s tel que $f_{s-2} = f_{s-1}g_s$, g_s étant le PGCD de f et f'. La suite ainsi construite est une suite de Sturm associée à f pour $[a, b]$ avec a, b tels que $f(a)f(b) \neq 0$.

Algorithme d'isolation

1. Borner le max. des valeurs absolues des racines réelles de f (voir les bornes précédemment données).
   $\rightsquigarrow$ on obtient un intervalle $I = [a, b]$.
2. Construire une suite de Sturm S
3. Si $V_{stu}(f(b)) - V_{stu}(f(a)) = 0$ retourner []
4. Si $V_{stu}(f(b)) - V_{stu}(f(a)) = 1$ retourner I
5. Sinon procéder par dichotomie.

$\rightsquigarrow$ L'algorithme est récursif et pour analyser sa complexité, on doit borner la profondeur de la récursion $\rightsquigarrow$ Pour cela, il faut connaitre la distance minimale entre deux racines de f (voir TD).

Algorithme d'isolation

1. Borner le max. des valeurs absolues des racines réelles de f (voir les bornes précédemment données).
   $\rightsquigarrow$ on obtient un intervalle $I = [a, b]$.
2. Construire une suite de Sturm S
3. Si $V_{stu}(f(b)) - V_{stu}(f(a)) = 0$ retourner []
4. Si $V_{stu}(f(b)) - V_{stu}(f(a)) = 1$ retourner I
5. Sinon procéder par dichotomie.

$\rightsquigarrow$ L'algorithme est récursif et pour analyser sa complexité, on doit borner la profondeur de la récursion $\rightsquigarrow$ Pour cela, il faut connaitre la distance minimale entre deux racines de f (voir TD).

S. Graillat & M. Safey (Univ. Paris 6) MODEL (cours nr4) 16 / 20

Algorithme d'isolation

1. Borner le max. des valeurs absolues des racines réelles de f (voir les bornes précédemment données).
   $\rightsquigarrow$ on obtient un intervalle $I = [a, b]$.
2. Construire une suite de Sturm S
3. Si $V_{stu}(f(b)) - V_{stu}(f(a)) = 0$ retourner []
4. Si $V_{stu}(f(b)) - V_{stu}(f(a)) = 1$ retourner I
5. Sinon procéder par dichotomie.

$\rightsquigarrow$ L'algorithme est récursif et pour analyser sa complexité, on doit borner la profondeur de la récursion $\rightsquigarrow$ Pour cela, il faut connaitre la distance minimale entre deux racines de f (voir TD).

S. Graillat & M. Safey (Univ. Paris 6) MODEL (cours nr4) 16 / 20

Construction d'une suite de Sturm

Rappel : On pose $f_0 = f$, $f_1 = f'$. et on construit par induction les polynômes f_i $i = 2 \dots s$ en posant $f_{i-2} = f_{i-1}g_i - f_i$, $deg(f_i) < deg(f_{i-1})$, et en stoppant la construction à l'indice s tel que $f_{s-2} = f_{s-1}g_s$, g_s étant le PGCD de f et f'. La suite ainsi construite est une suite de Sturm associée à f pour $[a, b]$ avec a, b tels que $f(a)f(b) \neq 0$.

1. Étant donné f_0 et f_1, on peut définir f_2 comme le reste de la division euclidienne de f_0 par f_1.
2. ... et ainsi de suite.
3. Complexité de la division euclidienne de A par B (avec $\deg(A) \geq \deg(B)$: $O(\deg(B)(\deg(A) - \deg(B))$
   (voir les fonctions `rem` et `quo` en Maple).

Construction d'une suite de Sturm

Rappel : On pose $f_0 = f$, $f_1 = f'$. et on construit par induction les polynômes f_i $i = 2 \dots s$ en posant $f_{i-2} = f_{i-1}g_i - f_i$, $deg(f_i) < deg(f_{i-1})$, et en stoppant la construction à l'indice s tel que $f_{s-2} = f_{s-1}g_s$, g_s étant le PGCD de f et f'. La suite ainsi construite est une suite de Sturm associée à f pour $[a, b]$ avec a, b tels que $f(a)f(b) \neq 0$.

1. Étant donné f_0 et f_1, on peut définir f_2 comme le reste de la division euclidienne de f_0 par f_1.
2. ... et ainsi de suite.
3. Complexité de la division euclidienne de A par B (avec $\deg(A) \geq \deg(B)$: $O(\deg(B)(\deg(A) - \deg(B))$ (voir les fonctions `rem` et `quo` en Maple).

Construction d'une suite de Sturm

$\rightsquigarrow$ il suffit d'appliquer l'algorithme d'Euclide au couple (f, f')
Entrée : Deux polynômes A et B dans $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps) avec $\deg(A) \geq \deg(B)$.
Sortie : La suite des restes euclidiens.
Euclide

1. $A_0 = A$ et $A_1 = B$
2. Tant que $A_i \neq 0$
   - $A_{i+1} = A_{i-1}$ `rem` A_i
   - $i++$
3. Retourner les A_i.

Complexité : $O(D^2)$ où D est le degré de f.

Propriétés

- Le dernier élément non nul de la suite renvoyée par Euclide(A, B) est le PGCD de A et B.
- Implantation : Prendre garde à ne pas calculer 0 dans les divisions euclidiennes.
- Forte croissance des coefficients (à tester en TME).
- **Idée** : Faire du calcul modulaire et utiliser le Théorème des restes chinois (`chrem`)

Relation de Bézout

EuclideEtendu

1. $A_0 = A$ et $A_1 = B$ et $U_0 = 1$ et $V_0 = 0$
2. Tant que $A_i \neq 0$
   - $Q_i = A_{i-1}$ `div` A_i
   - $A_{i+1} = A_{i-1} - A_iQ_i$
   - $U_{i+1} = U_{i-1} - Q_iU_i$ et $U_{i+1} = U_{i-1} - Q_iU_i$
   - $i++$
3. Retourner les A_i.

Proposition 6

On a $A_0U_i + A_1V_i = A_i$.