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

Cours n°10 : Résolution de systèmes polynomiaux et méthode de Newton

Stef Graillat

Université Pierre et Marie Curie (Paris 6)

Résumé du cours précédent

- Étude des systèmes polynomiaux : idéaux, variétés
- Introduction à l'algèbre commutative et à la géométrie algébrique

Objectifs

1. Systèmes à 2 équations à 2 variables : PGCD, résultants
2. Méthode de Newton

Bibliographie

- Modern Computer Algebra, J. von zur Gathen et J. Gerhard, 2nd édition, Cambridge University Press, 2003
- Ideals, Varieties, and Algorithms, D. Cox, J. Little et D. O'Shea, 3e édition, Springer, 2007
- Cours de calcul formel - Corps finis, systèmes polynomiaux - Applications, Ph. Saux Picart et É. Rannou, Ellipses, 2002
- Mathématiques L3 - Mathématiques appliquées, Jacques-Arthur Weil et Alain Yger, Pearson, 2009
- Scientific Computing : An Introductory Survey, Michael T. Heath, McGraw-Hill, 2002

Rappel : Motivation initiale à la notion d'idéal

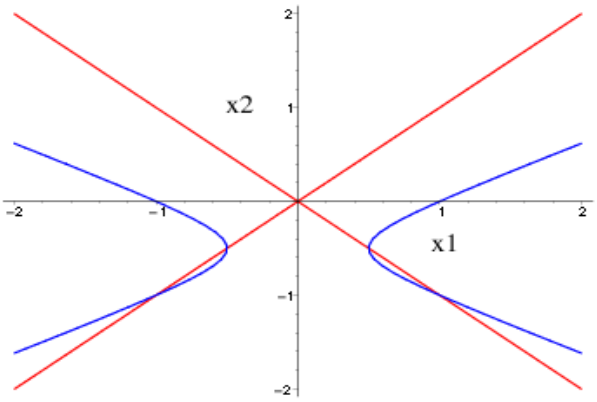
Solutions de $X^3 - X = 0$ et $X^2 - 3X + 2 = 0 \Longrightarrow$ PGCD $\rightarrow X - 1 = 0$

$(X+5)(X^2-3X+2)+1(X^3-X) = X-1$, **Combinaisons algébriques !**

V l'intersection des courbes définies par $A = -3Y^2 - 3Y + X^2 - 1$, $B = -Y^2 + X^2$
C'est un ensemble fini de points

$$(-1,-1),(1,-1),(-\frac{1}{2},-\frac{1}{2}),(\frac{1}{2},-\frac{1}{2})$$

$\deg(\mathrm{Gcd}(A(-1,Y),B(-1,Y)) \geq 1$
$\deg(\mathrm{Gcd}(A(1,Y),B(1,Y)) \geq 1$
$\deg(\mathrm{Gcd}(A(1/2,Y),B(1/2,Y)) \geq 1$
$\deg(\mathrm{Gcd}(A(-1/2,Y),B(-1/2,Y)) \geq 1$



Résolution complète des systèmes 2×2

Soit $A \in \mathbb{Q}[X,Y]$ et $B \in \mathbb{Q}[X,Y]$. On veut résoudre $A = B = 0$.

- Le système est-il de dimension 0 ?
  Algorithme pour **calculer la dimension** $\rightarrow$ se réduit à un calcul de PGCD !
- Résoudre = calculer des **approximations numériques** des solutions
  $\rightarrow$ Paramétrisation rationnelle

  Calculs modulo $\langle A, B\rangle$, réduire le problème à des **calculs de PGCD** en interprétant A et B comme des polynômes de $\mathbb{Q}[Y][X]$.
  Chercher un élément séparant pour $V(\langle A, B\rangle)$
- **Nombre maximal de solutions** ? (degré de $\langle A, B\rangle$)
- **Complexité** ? (Objectif : être polynomial en le nombre maximal de solutions)

Du PGCD à l'algèbre linéaire

D un anneau euclidien, **K** son corps de fraction,

$$\mathbf{D}_i[X] = \{f \in \mathbf{D}[X] \mid \deg(f) \leq i\}$$

$A = a_p X^p + \cdots + a_0$ et $B = b_q X^q + \cdots + b_0$ dans $\mathbf{D}[X]$ de degrés resp. p et q.

$\langle A, B\rangle = \langle R\rangle$ avec $\deg(R) < \min(p, q)$,

$$A = RV \text{ et } B = RU \Rightarrow UA + BV = 0$$
$$\Phi : (U, V) \in \mathbf{D}_{q-1}[X] \times \mathbf{D}_{p-1}[X] \to UA + VB \in \mathbf{D}_{p+q-1}[X]$$

$\mathbf{D}_i[X]$ est un D-espace vectoriel de dimension finie.

- Interpréter les polynômes de $\mathbf{D}_i[X]$ comme des **vecteurs de $\mathbf{D}^{i+1}$**
- **Représentation matricielle de Φ**

Du PGCD à l'algèbre linéaire

Matrice transposée de la matrice associée à cette application (**matrice de Sylvester**) :

$$\mathrm{Sylv}(A, B)^t = \begin{array}{c} \\ X^{q-1}A \\ \vdots \\ \vdots \\ A \\ X^{p-1}B \\ \vdots \\ \vdots \\ \vdots \\ B \end{array} \begin{bmatrix} a_p & \cdots & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & \vdots & \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & a_p & \cdots & \cdots & \cdots & \cdots & a_0 \\ b_q & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_q & \cdots & \cdots & \cdots & b_0 \end{bmatrix}$$

Le résultant de A et B est le déterminant de cette matrice

Propriétés du résultant (suite)

$\mathrm{Res}(A,B) = 0$ ssi il existe $U \in \mathbf{K}[X]$ et $V \in \mathbf{K}[X]$
avec $\deg(U) < q$ **et** $\deg(V) < p$ **tel que** $UA + VB = 0$.
$\mathrm{Res}(A,B) = 0$ **si et seulement si** A **et** B **ont un facteur commun dans** $\mathbf{K}[X]$.
Soit A et B dans $\mathbf{D}[X]$. Il existe U et V dans $\mathbf{D}[X]$ tels que $\deg(U) < q$, $\deg(V) < p$ et $\mathrm{Res}(A,B) = UA + VB$.
Soit $A = a_p \prod_{i=1}^{p}(X - x_i)$ et $B = b_q \prod_{j=1}^{q}(X - y_j)$, alors

$$\mathrm{Res}(A,B) = a_p^q b_q^p \prod_{i=1}^{p}\prod_{j=1}^{q}(x_i - y_j)$$

Corollaire : $\mathrm{Res}(A,BC) = \mathrm{Res}(A,B)\,\mathrm{Res}(A,C)$

Propriétés du résultant (suite)

Si $A = a_p \prod_{i=1}^{p}(X - x_i)$

$$\mathrm{Res}(A,B) = a_p^q \prod_{i=1}^{p} B(x_i)$$

Soit R tel que $A = BQ + R$ (avec $\deg(R) < \deg(B)$),

$$\mathrm{Res}(A,B) = (-1)^{\deg(A)\deg(B)}\mathrm{LeadCoeff}(B)^{\deg(A)-\deg(R)}\,\mathrm{Res}(B,R)$$

Relation forte entre résultant et suite des restes euclidiens

Propriétés du résultant (suite)

Soit $\mathbf{D}$ et $\mathbf{D}'$ deux anneaux. Un morphisme d'anneau $h : \mathbf{D} \to \mathbf{D}'$ vérifie

$$h(1) = 1, \quad h(a+b) = h(a) + h(b), \quad h(ab) = h(a)h(b)$$

$A \in \mathbf{D}[X]$ et $B \in \mathbf{D}[X]$ et $h : \mathbf{D} \to \mathbf{D}'$ un morphisme d'anneau tel que $h(a_p)h(b_q) \neq 0$ ou $h(b_q) \neq 0$. Alors

$$\mathrm{Res}(h(A), h(B)) = h(\mathrm{Res}(A, B))$$

Exemple : $\mathbf{D} = \mathbb{Z}$ et $h(z) = z \mod p$ avec p premier.
$\mathbf{D} = \mathbb{Q}[Y]$ et $h(P(Y)) = P(y)$ pour $y \in \mathbb{Q}$.

Euclide et PGCD

Entrée : A et B dans $\mathbb{Q}[X]$ de degrés $p > q$

- $A_1 \leftarrow A$
- $A_2 \leftarrow B$
- $i \leftarrow 2$
- Tant que $A_i \neq 0$ Faire
  - $A_{i+1} \leftarrow A_{i-1} \mod A_i$
  - $i++$
- return A_{i-1}

- Division euclidienne en degrés n et m (avec $n > m$) en $\mathcal{O}((n-m)m)$
- Complexité : $\mathcal{O}(p^2)$ (si $d_i = \deg(A_i)$ on a $\sum_i (d_{i-1} - d_i)d_i$)
- Croissance des coefficients anormale (en particulier si A et B sont dans $\mathbb{Z}[X]$ on se retrouve avec des coefficients rationnels).

De l'algorithme d'Euclide au calcul du résultant

Entrée : A et B dans $K[Y]$ de degrés $p > q$

- $A_1 \leftarrow A$, $A_2 \leftarrow B$
- $i \leftarrow 2$, $R_1 \leftarrow 1$
- Tant que $A_i \neq 0$ Faire
  - $A_{i+1} \leftarrow A_{i-1} \mod A_i$
  - $R_i \leftarrow (-1)^{d_i d_{i-1}} \mathrm{LeadCoeff}(A_i)^{d_{i-1}-d_i} R_{i-1}$
  - $i++$
- Si $A_i \neq 0$ return $R_{i-1}\mathrm{LeadCoeff}(A_i)^{\deg(A_{i-1})}$ Sinon return 0
- **Correction** : Si $\deg(A_i) > 0$, $\mathrm{Res}(A, B) = R_i \,\mathrm{Res}(A_i, A_{i+1})$
  Si $\deg(A_i) \leq 0$,
  - Si $A_i = 0$ $\mathrm{Res}(A_{i-1}, A_i) = 0$
  - Sinon $\mathrm{Res}(A_i, A_{i-1}) = \mathrm{LeadCoeff}(A_i)^{\deg(A_{i-1})}$
- **Complexité :** $\mathcal{O}(p^2)$

Méthode de Newton

Équations non linéaires

- Étant donné une fonction f, on cherche une valeur x pour laquelle

$$f(x) = 0$$

- Une solution x est une racine de l'équation ou un zéro de la fonction f.

Équations non linéaires (suite)

Deux cas importants :

- Une seule équation avec une seule inconnue, où $f : \mathbb{R} \to \mathbb{R}$
  Une solution est un scalaire x vérifiant $f(x) = 0$
- Un système de n équations à n inconnues, où $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$
  Une solution est un vecteur x tel que $\mathbf{f}(x) = 0$

Exemples d'équations non linéaires

- Exemple d'équations non linéaire en dimension 1

$$x^2 - 4\sin(x) = 0$$

  pour laquelle $x = 1.9$ est une solution approchée

- Exemple d'un système d'équations non linéaires en dimension 2

$$\begin{aligned} x_1^2 - x_2 + 0.25 &= 0 \\ -x_1 + x_2^2 + 0.25 &= 0 \end{aligned}$$

  pour lequel $x = [0.5\ ;\ 0.5]^T$ est une solution

Existence et unicité des solutions

- L'existence et l'unicité de solution sont plus compliquées dans le cas non linéaire que dans le cas linéaire
- Si $f : \mathbb{R} \to \mathbb{R}$ est continue et si signe$(f(a)) \neq$ signe$(f(b))$ alors le Théorème des Valeurs Intermédiaires nous dit qu'il existe $x^* \in [a, b]$ tel que $f(x^*) = 0$
- Il n'y a pas d'analogue en dimension supérieure.

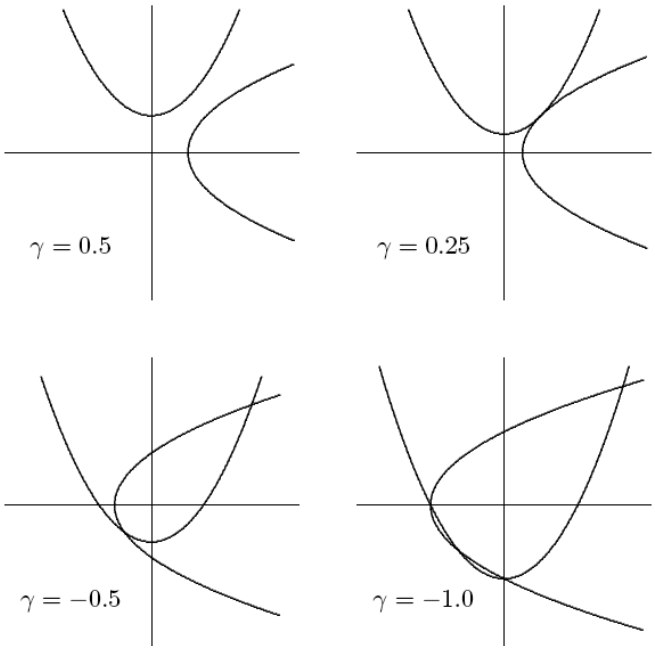
Exemple en dimension 1

Les équations non linéaires peuvent avoir un nombre quelconque de solutions :

- $e^x + 1 = 0$ n'a pas de solution
- $e^{-x} - x = 0$ a une solution
- $x^2 - 4\sin(x) = 0$ a deux solutions
- $x^3 + 6x^2 + 11 - 6 = 0$ a trois solutions
- $\sin(x) = 0$ a une infinité de solutions

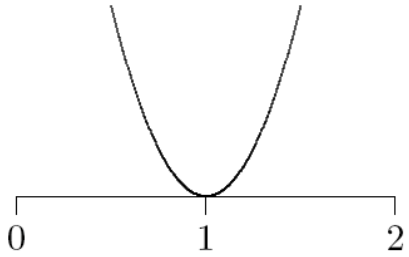
Exemple en dimension 2

$$\begin{aligned} x_1^2 - x_2 + \gamma &= 0 \\ -x_1 + x_2^2 + \gamma &= 0 \end{aligned}$$

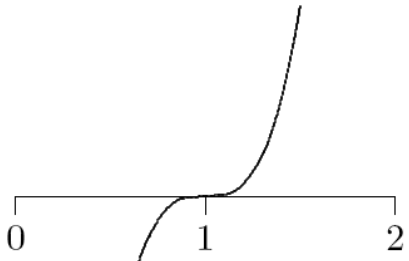


Multiplicité

- Si $f(x^*) = f'(x^*) = f''(x^*) = \cdots = f^{(m-1)}(x^*) = 0$ mais $f^{(m)}(x^*) \neq 0$, alors on dit que x^* est une racine de multiplicité m



$x^2 - 2x + 1$



$x^3 - 3x^2 + 3x - 1$

- Si $m = 0$, on dit que x^* est une racine simple

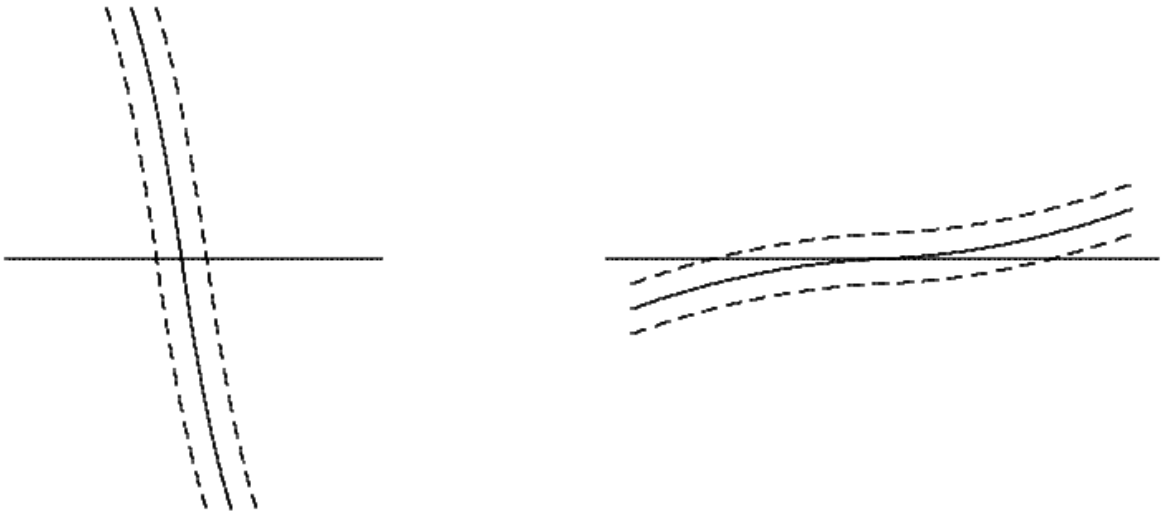
Sensibilité et conditionnement

- le conditionnement du calcul de racines est l'opposé de celui de l'évaluation de fonction
- Le conditionnement absolu du calcul d'une racine x^* de $f : \mathbb{R} \to \mathbb{R}$ est $1/|f'(x^*)|$
- Le calcul est mal conditionné quand la tangente est proche de l'horizontale
- En particulier, les racines multiples sont mal conditionnées
- Le conditionnement absolu du calcul d'une racine x^* de $f : \mathbb{R}^n \to \mathbb{R}^n$ est $\|J_f^{-1}(x^*)\|$ où J_f est la matrice jacobienne de f,

$$J_f(x) = \{\partial f_i(x)/\partial x_j\}$$

- Une racine est mal conditionnée si la matrice jacobienne est presque singulière

Sensibilité et conditionnement (suite)



Sensibilité et conditionnement (suite)

- Que signifie une solution approchée $\widehat{x}$ de l'équation ?

$$\|f(\widehat{x})\| \approx 0 \qquad \text{ou} \qquad \|\widehat{x} - x^*\| \approx 0?$$

- La première correspond à un "petit résidu", la seconde mesure la distance à la vraie solution
- Un petit résidu implique une solution approchée précision seulement si le problème est bien conditionné

Taux de convergence

- Pour une méthode itérative générale, on définit l'erreur à l'itération k par

$$e_k = x_k - x^*$$

où x_k l'approximation de la solution et x^* est la solution

- On dit que la suite (x_k) converge avec un taux r si

$$\lim_{x \to \infty} \frac{\|e_{k+1}\|}{\|e_k\|^r} = C$$

pour une constance C

Taux de convergence (suite)

Quelques cas particuliers intéressants

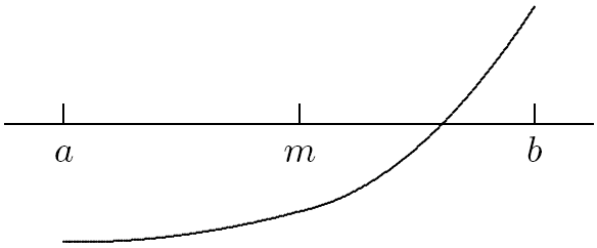
- $r = 1$: linéaire
- $r > 1$: superlinéaire
- $r = 2$: quadratique

Taux de convergence	Gain en chiffre par itération
linéaire	constant
superlinéaire	augmente
quadratique	double

Dichotomie

Le principe de la méthode par dichotomie est de partir un intervalle qui contient une solution et l'on divise ensuite par deux sa longueur jusqu'à ce qu'on ait isolé la solution avec une précision suffisante

```
while (b − a) > tol do
    m=a +(b-a)/2
    if signe(f(a)) = signe(f(m)) then
        a=m
    else
        b=m
    end
end
```



Dichotomie (suite)

- L'algorithme de dichotomie converge tout le temps mais lentement
- Le taux de convergence est $r = 1$ et $C = 0.5$
- On gagne 1 bit de précision à chaque itération

Méthode de Newton

- Développement de Taylor à l'ordre 1

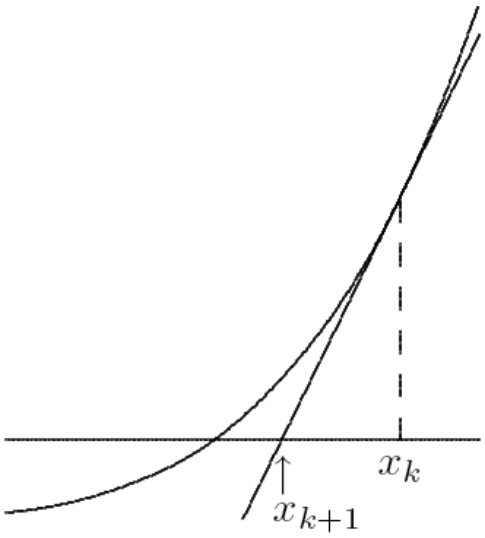
$$f(x+h) \approx f(x) + hf'(x)$$

  Il s'agit d'une fonction linéaire en h approximant f au voisinage de x
- On remplace la fonction non linéaire f par cette fonction linéaire dont la racine est $h = -f(x)/f'(x)$
- Les racines de la fonction f et de l'approximation linéaire ne sont en général pas identique donc on itère le processus

$$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}$$

Méthode de Newton (suite)

La méthode de Newton approxime une fonction non linéaire f près de x_k par sa tangente en $f(x_k)$



Convergence de la méthode de Newton

- Si la racine x^* est simple alors la convergence est quadratique ($r = 2$)
- Mais l'itération doit commencer suffisament près de la racine pour qu'il y ait convergence

Racines de polynômes

- Étant donné un polynôme $p(x)$ de degré n, on veut trouver ses n racines.
- Plusieurs approches existent
  - Utiliser la méthode de Newton pour trouver une racine puis faire de la déflation et continuer
  - Fabriquer la matrice compagnon et calculer ses valeurs propres
  - Utiliser des méthodes spécifiques pour calculer toutes les racines d'un polynôme (Jenkins-Traub, Durand-Kerner, etc.)

Système d'équations non linéaires

Le cas des systèmes d'équations non linéaires est beaucoup plus complexe

- une large variété de comportement possible (déterminer l'existence, le nombre de solutions ou un bon point de départ est plus complexe)
- Le temps de calcul augmente rapidement en fonction de la dimension du problème

Méthode de Newton

- En dimension n, la méthode de Newton est de la forme

$$x_{x+1} = x_k - J(x_k)^{-1} f(x_k)$$

où $J(x)$ est la matrice jacobienne de f

- En pratique, on ne calcule pas explicitement l'inverse de $J(x_k)$ mais on résout le système linéaire

$$J(x_k)s_k = -f(x_k)$$

et on choisit

$$x_{k+1} = x_k + s_k$$

Convergence de la méthode de Newton

- Le taux de convergence de la méthode de Newton est quadratique, à condition que la matrice jacobienne soit inversible
- Mais il faut commencer les itérations assez proche de la solution pour converger

Coût de la méthode de Newton

Le coût par itération de la méthode de Newton pour un problème dense en dimension n est important

- Calculer la matrice jacobienne nécessite n^2 évaluations de fonctions
- Résoudre un système linéaire coûte $\mathcal{O}(n^3)$ opérations

Conclusion

Méthode de Newton

- Méthode pour calculer les racines d'équations non linéaires
- Utiliser en calcul numérique mais aussi en calcul formel