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

Cours n°9 : Résolution de systèmes polynomiaux

Stef Graillat

Université Pierre et Marie Curie (Paris 6)

Résumé du cours précédent

- Introduction à la cryptographie
- Chiffrement symétrique (DES, AES)

Objectifs

1. Étude des systèmes polynomiaux : idéaux, variétés
2. Systèmes à 2 équations à 2 variables : PGCD, résultants

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

Exemples d'applications

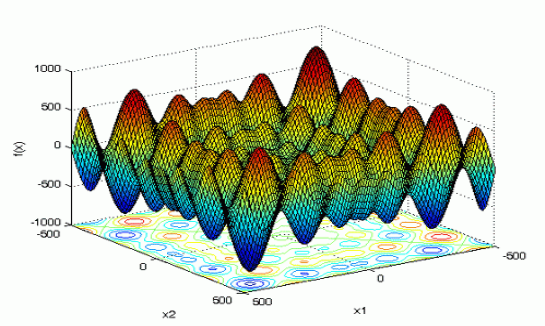


Figure: Optimisation

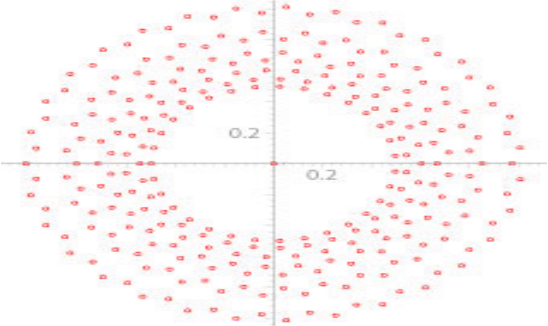


Figure: Protéines et cellules

Figure: Robotique

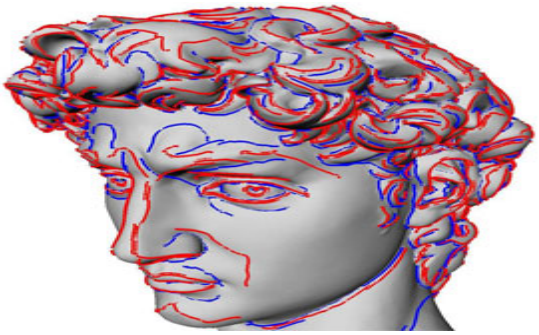


Figure: Vision 3D

Systèmes linéaires versus systèmes polynomiaux

- **Existence de solutions :** Soit $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et $u = (\sum_{i=1}^{n} a_i X_i) + a_0$ avec $a_i \in \mathbb{Q}$
  $u = 0$ a toujours au moins une solution dans $\mathbb{Q}$ si $\exists a_i \neq 0$
  $f = 0$ n'a pas toujours de solutions dans $\mathbb{Q}^n$
  $f = 0$ n'a pas toujours de solutions dans $\mathbb{R}^n$
  $f = 0$ a toujours des solutions dans $\mathbb{C}^n$ (si $f \notin \mathbb{Q}$)
- **Nombre de solutions :** $u_1 = \cdots = u_n = 0$ (n formes linéaires en n variables), $f_1 = \cdots = f_n = 0$ n polynômes en n variables.
  Cas linéaire : une infinité de solutions ou une unique solution rationnelle
  Cas polynomial : une infinité de solutions ou un nombre fini de solutions dans $\mathbb{C}^n$ ou aucune solution
  Exemples : $XY - 1 = X = 0$ (aucune solution),
  $X^2 + Y^2 - 1 = X - Y = 0$ (2 solutions)

Besoin d'algorithmes et d'implantations

Représentation informatique des données :

- Polynôme en une variable : $P = a_0 + a_1 X + \cdots + a_n X^d$, $a_i \in \mathbf{K}$
  Tableau de $d+1$ coefficients, d est le degré P
- Polynômes en plusieurs variables : $X_1, \ldots, X_n$ les variables,
  $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ est un monôme
  L'ensemble des monômes est isomorphe à $\mathbb{N}^n$
  Un terme est de la forme $\mathrm{coeff} \times \mathrm{monome}$
  $P = \sum_{j=1}^{M} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$, $a_i \in \mathbf{K}$
  Degré total de P $= \max(\sum_{j=1}^{n} \alpha_{i,j}, i = 1, \ldots, M)$
  Degré de P en X_i $= \max(\alpha_{j,i}, j = 1, \ldots, M)$

Codage possible des polynômes en plusieurs variables : vecteurs de coefficients (si on **ordonne** les monômes)
Question naturelle : à degré et nombre de variables fixés, quel est le nombre de monômes dans le pire cas (**représentation dense**) $\rightarrow$ Occupation mémoire

Besoin d'algorithmes et d'implantations (suite)

- Systèmes polynomiaux de petite taille (petit nombre de solutions, peu de variables, etc.) mais un très grand nombre à résoudre.
  On s'intéressera au cas des systèmes de 2 variables
- Systèmes polynomiaux de grande taille (grand nombre de solutions et/ou nombre de variables > 3).
  On va utiliser les algorithmes de l'algèbre linéaire pour résoudre
- Fiabilité du résultat produit : les méthodes purement numériques ne sont pas fiables sur ces problèmes.

  On utilise le Calcul Formel/Calcul Exact pour garantir les résultats (nombre de solutions, localisation/approximation garantie)
- Champs applicatifs : cryptanalyse algébrique, géométrie algorithmique, robotique

Plan du cours

- **Généralités** – Notion d'idéal – Relations avec l'ensemble des solutions – Du non-linéaire au linéaire.
- **Polynômes en deux variables** – Retour sur l'algorithme d'euclide – Lien entre Gauss et Euclide – Sous-résultants
  Application : tracé de courbes – courbes implicites
- Polynômes multivariés, Représentations, opérations de base, extension de la division euclidienne, notion de réduction.
- **Calcul dans les algèbres-quotient et algèbre linéaire** – Résolution symbolique
  Application : optimisation de fonctions polynomiales

Notion d'idéal – Motivation

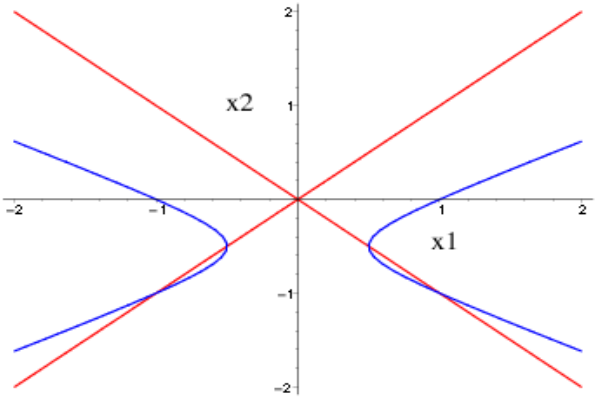
Solutions de $X^3 - X = 0$ et $X^2 - 3X + 2 = 0 \Longrightarrow$ PGCD $\rightarrow X - 1 = 0$

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

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

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



Notion d'idéal

Définition 1

Soit A un anneau. Un **idéal** *I de A est un sous-ensemble de A tel que :*

- $0 \in I$
- $\forall (f, g) \in I \times I,\ f + g \in I$
- $\forall f \in I,\ et\ \forall g \in A,\ fg \in I$

Notion d'idéal

Définition 2

Soit $\{f_1, \ldots, f_k\} \subset A$, $\{p_1 f_1 + \ldots + p_k f_k \mid (p_1, \ldots, p_k) \in A^k\}$ est **le plus petit idéal contenant** *$\{f_1, \ldots, f_k\}$. On le note $\langle f_1, \ldots, f_k \rangle$.*

Définition 3

Un idéal $I \subset A$ est **radical** *ssi pour tout $f \in A$ tel que $f^k \in I$* **(pour** *$k \in \mathbb{N}$***) implique** *$f \in I$.*

Générateur d'un idéal

Pour faire des calculs : une représentation finie des idéaux est nécessaire

Théorème 1

Soit I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$. Il existe **une famille finie** *$\{f_1, \ldots, f_k\} \subset \mathbb{Q}[X_1, \ldots, X_n]$ telle que $I = \langle f_1, \ldots, f_k \rangle$.*

Définition 4

Soit $I \subset A$ un idéal. On dit que I est **principal** *ssi il existe $f \in A$ tel que $I = \langle f \rangle$.*

Théorème 2

Tout idéal de $A[X]$ est principal $\Longleftrightarrow$ A est un corps.

Attention : des idéaux de $\mathbb{Z}[X]$ et $\mathbb{Q}[X, Y]$ ne sont pas principaux.

Idéal et ensemble de solutions

Soit $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[X_1, \ldots, X_n]$ et $I = \langle f_1, \ldots, f_k \rangle$
On note $V(f_1, \ldots, f_k) = \{x \in \mathbb{C}^n \mid f_1(x) = \cdots = f_k(x) = 0\}$

Pour tout $x \in V$ et pour tout $f \in I$, $f(x) = 0$, $V(f_1, \ldots, f_k) = V(I)$

Définition 5

Soit $\mathbb{K}$ un corps et $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$. $V \subset \overline{\mathbb{K}}^n$ est une **$\mathbb{K}$-variété algébrique** *ssi il existe $\{f_1, \ldots, f_k\} \subset \mathbb{K}[X_1, \ldots, X_n]$ tel que*

$$V = \{x \in \overline{\mathbb{K}}^n \mid f_1(x) = \cdots = f_k(x) = 0\}$$

- L'intersection de $\mathbb{K}$-variétés algébriques est une $\mathbb{K}$-variété algébrique.
- Une union **finie** de $\mathbb{K}$-variétés algébriques est une $\mathbb{K}$-variété algébrique. Attention : si l'union n'est pas finie, l'assertion ci-dessus n'est pas toujours vraie.

Idéal et ensemble de solutions

Définition 6

Soit I un idéal de $\mathbb{K}[X_1, \ldots, X_n]$. L'ensemble des points en lesquels tous les polynômes de I s'annulent est la $\mathbb{K}$-variété algébrique associée à I.

Définition 7

Soit $V \subset \mathbb{C}^n$ une $\mathbb{Q}$-variété algébrique.
$\{f \in \mathbb{Q}[X_1, \ldots, X_n] \mid \forall x \in V f(x) = 0\}$ *est un* **idéal** *de $\mathbb{Q}[X_1, \ldots, X_n]$. On l'appelle* **idéal associé à** V *et* **on le note** $\mathcal{I}(V)$.

Question : quel est l'idéal associé à la variété algébrique définie par l'idéal $\langle X^2, Y \rangle$?

Idéal et ensemble de solutions (suite)

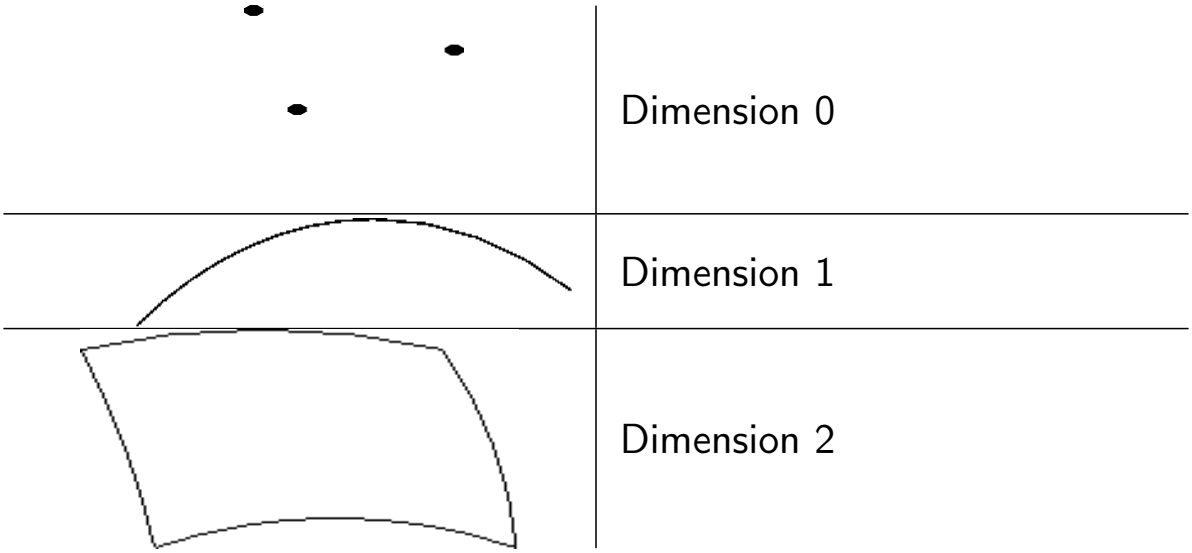
Nulltstellensatz : Soit $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[X_1, \ldots, X_n]$. $V(f_1, \ldots, f_k) = \emptyset$ ssi il existe $A_1, \ldots, A_k$ dans $\mathbb{Q}[X_1, \ldots, X_n]$ tel que $1 = A_1 f_1 + \cdots + A_k f_k$

Propriété 1

Soit I un idéal, $\mathcal{I}(V(I)) = I \iff \sqrt{I} = I$.

En d'autres termes, $\mathcal{I}(V(I)) = \sqrt{I}$

Notion de dimension



Une variété algébrique de dimension 0 est un **ensemble fini de points dans $\mathbb{C}^n$**, une variété de dimension $n-1$ dans $\mathbb{C}^n$ est appelée **hypersurface**.

Notion de dimension (suite)

Soit $V \subset \mathbb{C}^n$ une variété algébrique. La **dimension de V** est le plus grand entier r tel que :
il existe $X_{i_1}, \ldots, X_{i_r}$ et une variété algébrique H de $\mathbb{C}^r$ tel que la projection

$$\begin{array}{ccc} V \subset \mathbb{C}^n & \longrightarrow & \mathbb{C}^r \setminus H \\ (x_1, \ldots, x_n) & \mapsto & (x_{i_1}, \ldots, x_{i_r}) \end{array}$$

est surjective.

Soit I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$. La **dimension de I** est égale à celle de $V(I)$.

Le cas zéro-dimensionnel : du non-linéaire au linéaire

Relation d'équivalence(réflexive, symétrique et transitive) Soit $I \subset A$ un idéal et $(f, g) \in A \times A$. $f \sim_I g$ **ssi** $f - g \in I$
Pour $f \in \mathbb{Q}[X_1, \ldots, X_n]$, on note $\overline{f} = \{g \in \mathbb{Q}[X_1, \ldots, X_n] \mid f \sim_I g\}$.

Anneau-quotient : $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ est l'ensemble des classes d'équivalence muni d'une structure d'algèbre.

$$\overline{f+g} = \overline{f} + \overline{g},\ \overline{fg} = \overline{f}\,\overline{g} \text{ et } \forall \lambda \in \mathbb{Q},\ \overline{\lambda f} = \lambda \overline{f}.$$

Exemples

- Classes d'équivalences dans $\mathbb{Q}[X, Y]/\langle X, Y\rangle \sim \mathbb{Q}$ (coefficients constants des polynômes).
- Classes d'équivalences dans $\mathbb{Q}[X, Y]/\langle X, Y^2\rangle$.

Le cas zéro-dimensionnel : du non-linéaire au linéaire (suite)

Théorème 3

Soit I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$ de **dimension 0**. *Alors* $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ **est un $\mathbb{Q}$-espace vectoriel de dimension finie**.

Définition 8

Le **degré d'un idéal zéro-dimensionnel** *I est la dimension de l'espace vectoriel* $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$.

Il est égal au nombre de solutions dans $\mathbb{C}^n$ dans le cas où I est radical.
Lorsque I n'est pas radical, son degré borne le nombre de solutions.

Le degré d'une variété V de dimension 0 est le degré de $\mathcal{I}(V)$
Notion d'élément séparant u : $\forall (x, y) \in V(I),\ \ u(x) \neq u(y) \Leftrightarrow x \neq y$
Il existe un élément séparant parmi $X_1 + iX_2 + \cdots + i^{n-1}X_n$ pour $0 \leq i \leq (n-1)\binom{D}{2}$ avec $D = \sharp V(I)$

Le cas zéro-dimensionnel : du non-linéaire au linéaire (suite)

Représenter cette algèbre-quotient pour y faire des calculs d'algèbre linéaire ?
Chercher une base de l'algèbre-quotient en tant que $\mathbb{Q}$-e.v.
Objectif : fournir une représentation des solutions pour en déduire des approximations numériques

- Systèmes linéaires : Gauss/LU $\longrightarrow$ **Mise sous forme triangulaire**
- Systèmes polynomiaux :
$$\begin{cases} q_0(T)X_n &= q_n(T) \\ & \vdots \\ q_0(T)X_1 &= q_1(T) \\ q(T) &= 0 \end{cases}$$

Paramétrisation rationnelle
T doit alors être un élément séparant

Conclusion

Au prochain cours :

- résolution d'un système de 2 polynômes à 2 variables
- méthode de Newton en calcul scientifique