Approche matricielle de la résolution d'équations polynomiales

B. Mourrain

INRIA, SAGA
2004 route des Lucioles, BP 93
06902 Sophia-Antipolis Cedex
mourrain@sophia.inria.fr
http://www.inria.fr/saga/mourrain/

Résoudre des équations polynomiales

Input: Les équations $f_1 = \cdots = f_m = 0$, $f_i \in R = \mathbb{C}[x_1, \ldots, x_n]$.

Problème : On cherche les solutions $\zeta \in \mathbb{C}^n$ telles que $f_1(\zeta) = \cdots = f_n(\zeta) = 0$.

Objectifs :

$\Rightarrow$ Compter

- □ toutes les solutions.
- □ toutes les solutions dans une boîte.
- □ toutes les solutions réelles (dans une boîte).

$\Rightarrow$ Calculer une approximation de

- □ toutes les racines.
- □ toutes les racines (réelles) dans une boîte.
- □ une racine (spécifique).

Approche algébrique :

Calculer en nommant les inconnues et en combinant les équations qui les relient.

On calcule modulo l'idéal $I = (f_1, \ldots, f_m)$.

Étude du quotient $\mathcal{A} = \mathbb{C}[\mathbf{x}]/I$ pour analyser $\mathcal{Z}(I) = \{\zeta \in \mathbb{C}^n \; ; \; f_i(\zeta) = 0\}$.

Théorème : *L'algèbre $\mathcal{A}$ est de dimension finie sur $\mathbb{C}$ ssi $\mathcal{Z}(I) =$ est fini.*

Exemple

Soit I l'idéal de $\mathbb{K}[x_1, x_2]$ engendré par

$$\begin{aligned} f_1 &= 13\,{x_1}^2 + 8\,x_1x_2 + 4\,{x_2}^2 - 8\,x_1 - 8\,x_2 + 2 \\ f_2 &= {x_1}^2 + x_1x_2 - x_1 - 1/6 \end{aligned}$$

Le quotient $\mathcal{A} = \mathbb{K}[x_1, x_2]/I$ est de dimension 4, de base $1, x_1, x_2, x_1x_2$.

```
expand(x[1]*x[1] -f2);
```

$$x_1^2 \equiv -x_1x_2 + x_1 + \frac{1}{6}$$

```
expand(x[1]*(x[1]*x[2])+1/9*x[1]*f1-(5/9+13/9*x[1]+4/9*x[2])*f2);
```

$$x_1^2x_2 \equiv -x_1x_2 + \frac{55}{54}\,x_1 + \frac{2}{27}\,x_2 + \frac{5}{54}.$$

Dualité

Le dual de R est $\widehat{R} = \{\Lambda : R \rightarrow \mathbb{C}, \text{linaire}\}$.

On note $(\mathtt{d}^{\alpha})_{\alpha\in\mathbb{N}^n}$ la base duale de $(\mathbf{x}^{\alpha})_{\alpha\in\mathbb{N}^n}$.

$$\Lambda = \sum_{\alpha\in\mathbb{N}^n} \Lambda(\mathbf{x}^{\alpha})\mathtt{d}^{\alpha} \in \mathbb{C}[[\mathtt{d}_1, \ldots, \mathtt{d}_n]].$$

Exemple : $\mathbf{1}_{\zeta} : p \mapsto p(\zeta)$ s'écrit dans la base $(\mathtt{d}^{\alpha})$ est $\mathbf{1}_{\alpha} = \sum_{\alpha\in\mathbb{N}^n} \zeta^{\alpha}\, \mathtt{d}^{\alpha} = \frac{1}{\prod_{i=1}^{n}(1-\zeta_i \mathtt{d}_i)}$.

Une structure de R-module : $\forall a \in R, \forall \Lambda \in \widehat{R}$, $a \cdot \Lambda : b \mapsto a \cdot \Lambda(b) = \Lambda(ab)$.

Exemple : $x_1 \cdot \mathtt{d}_1^{\alpha_1}\mathtt{d}^{\alpha_2}\cdots\mathtt{d}^{\alpha_n} = \mathtt{d}_1^{\alpha_1-1}\mathtt{d}^{\alpha_2}\cdots\mathtt{d}^{\alpha_n}$ si $\alpha_1 > 0$ et 0 sinon.

Le dual de $\mathcal{A}$ est $\widehat{\mathcal{A}} = \{\Lambda : R \rightarrow \mathbb{C} \text{ st. } \Lambda(I) = 0\}$.

Exemple :

- Pour $\zeta \in \mathcal{Z}(I)$, $\mathbf{1}_{\zeta} : a \mapsto a(\zeta)$.
- $a \mapsto$ le coefficient de $\mathbf{x}^{\alpha}$ dans la forme normale de a.

La structure du quotient

Solutions dans $\mathbb{C}^n$: $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\}$.

Décomposition primaire : $I = Q_1 \cap \cdots \cap Q_d$ avec $\sqrt{Q_i} = \mathbf{m}_{\zeta_i}$ (Q_i $\mathbf{m}_{\zeta_i}$-primaire).

$$\mathcal{A} = \mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_m) = R/I = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_d,$$

avec

- $\mathcal{A}_i = \mathbf{e}_i\, \mathcal{A}$,
- $\mathbf{e}_i^2 = \mathbf{e}_i$, $\mathbf{e}_i\, \mathbf{e}_j = 0$ if $i \neq j$,
- $\mathbf{e}_1 + \cdots + \mathbf{e}_d = 1$.

Le cas simple en une variable

On prend $f = f_d\, x^d + \cdots + f_1 x + f_0$ ($f_d \neq 0$), avec des racines simples $\zeta_1, \ldots, \zeta_d$.

Les idempotents sont les polynômes d'interpolation de Lagrange :

$$\mathbf{e}_i(x) = \prod_{j=1, j\neq i}^{d} \frac{x - \zeta_j}{\zeta_i - \zeta_j},$$

et on a

$$\mathcal{A} = \mathbb{C}[x]/(f) = \mathbb{K}\,\mathbf{e}_1 \oplus \cdots \oplus \mathbb{K}\,\mathbf{e}_d; \quad \forall a \in \mathcal{A}, a \equiv a(\zeta_1)\,\mathbf{e}_1 + \ldots + a(\zeta_d)\,\mathbf{e}_d.$$

La base duale de $(\mathbf{e}_i)$ est $(\mathbf{1}_{\zeta_i})$.

Une autre base de $\mathcal{A}$ est $(1, x, \ldots, x^{d-1})$. La matrice de multiplication par x dans cette base est

$$\mathtt{M}_x = \begin{pmatrix} 0 & \cdots & 0 & -\frac{f_0}{f_d} \\ 1 & \ddots & \vdots & \vdots \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -\frac{f_{d-1}}{f_d} \end{pmatrix}.$$

Opérateurs de multiplication

$$\begin{array}{rcl} M_a : \mathcal{A} & \to & \mathcal{A} \\ u & \mapsto & a\,u \end{array} \qquad \begin{array}{rcl} M_a^{\mathtt{t}} : \widehat{\mathcal{A}} & \to & \widehat{\mathcal{A}} \\ \Lambda & \mapsto & a \cdot \Lambda : u \mapsto \Lambda(au) \end{array}$$

Théorème :

1. *Les valeurs propres de M_a sont $\{a(\zeta_1), \ldots, a(\zeta_d)\}$.*
2. *Les vecteurs communs à tous les $(M_a^{\mathtt{t}})_{a \in \mathcal{A}}$ sont les $\mathbf{1}_{\zeta_i} : p \mapsto p(\zeta_i)$ (à un scalaire près).*

Théorème : *Il existe une base de $\mathcal{A}$ tq. $\forall a \in R$, la matrice de M_a dans cette base est de la forme*

$$\mathtt{M}_a = \begin{bmatrix} \mathtt{N}_a^1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \mathtt{N}_a^d \end{bmatrix} \text{ avec } \mathtt{N}_a^i = \begin{bmatrix} a(\zeta_i) & & \star \\ & \ddots & \\ \mathbf{0} & & a(\zeta_i) \end{bmatrix}$$

Calcul des racines par les vecteurs propres.

Soit $a \in R$ et $\mathtt{M}_a$ la matrice de la multiplication par a dans une base $(1, x_1, \ldots, x_n, \ldots)$ de $\mathcal{A}$.

1. Calculer les vecteurs propres $\Lambda = [\Lambda_1, \Lambda_{x_1}, \ldots, \Lambda_{x_n}, \ldots]$ de $\mathtt{M}_a^{\mathtt{t}}$.
2. Pour tout vecteur propre Λ avec $\Lambda_1 \neq 0$, calculer $\zeta = \left(\frac{\Lambda_{x_1}}{\Lambda_1}, \ldots, \frac{\Lambda_{x_n}}{\Lambda_1}\right)$.

Les points ζ ainsi calculés contiennent les racines simples de I.

Calcul des racines par triangulation simultanée.

1. Calculer une décomposition (de Schur) triangulaire $\mathtt{T}_{x_1} = \mathtt{P}\mathtt{M}_{x_1}\mathtt{P}^{-1}$.
2. Calculer $\mathtt{T}_{x_i} = \mathtt{P}\mathtt{M}_{x_i}\mathtt{P}^{-1}$, $i = 2, \ldots, n$ qui sont aussi triangulaires.

Les racines sont les vecteurs diagonaux $\mathbf{t}_i = (t_{i,i}^1, \ldots, t_{i,i}^n)$ des matrices $\mathtt{T}_{x_i}$, $i = 1, \ldots, n$.

Exemple

$f_1 = 13\,{x_1}^2 + 8\,x_1x_2 + 4\,{x_2}^2 - 8\,x_1 - 8\,x_2 + 2,\ f_2 = {x_1}^2 + x_1x_2 - x_1 - 1/6$

$$
\begin{aligned}
1 \times x_1 &\equiv x_1, \\
x_1 \times x_1 &\equiv -x_1x_2 + x_1 + \frac{1}{6}, \\
x_2 \times x_1 &\equiv x_1x_2, \\
x_1x_2 \times x_1 &\equiv x_1x_2 + \frac{55}{54}x_1 + \frac{2}{27}x_2 + \frac{5}{54}.
\end{aligned}
$$

$$
M_{x_1} = \begin{bmatrix} 0 & \frac{1}{6} & 0 & \frac{5}{54} \\ 1 & 1 & 0 & \frac{55}{54} \\ 0 & 0 & 0 & \frac{2}{27} \\ 0 & -1 & 1 & -1 \end{bmatrix}.
$$

```
neigenvects(transpose(M1),1);
```

$$
[-\frac{1}{3}, 2, \left\{[1, -\frac{1}{3}, \frac{5}{6}, -\frac{5}{18}]\right\}], [\frac{1}{3}, 2, \left\{[1, \frac{1}{3}, \frac{7}{6}, \frac{7}{18}]\right\}].
$$

Forme de Chow et représentation rationnelle

Théorème : $\Delta(\mathbf{u}) = \det(u_0 + u_1\,\mathtt{M}_{x_1} + \cdots + u_n\,\mathtt{M}_{x_n}) = \prod_{\zeta\in\mathcal{Z}(I)}(u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{\mu_\zeta}$.

Dessin : image de racines en une variable (extension rationelle)

Représentation univariée rationnelle

1. Calculer un *multiple* de $\Delta(\mathbf{u})$ et $d(\mathbf{u})$ sa partie sans carré.
2. Choisir $t \in \mathbb{K}^{n+1}$ générique et calculer les premiers coefficients de
$$d(t+u) = d_0(u_0) + u_1\,d_1(u_0) + \cdots + u_n\,d_n(u_0) + \cdots$$
3. La représentation rationnelle est $\zeta_1 = \frac{d_1(u_0)}{d_0'(u_0)}, \ \ldots, \ \zeta_n = \frac{d_n(u_0)}{d_0'(u_0)}, \ d_0(u_0) = 0$.
4. Factoriser $d_0(u_0)$ et ne garder que les bons facteurs premiers pour une *repésentation minimale*.

Exemple : $\xi_1 = -\frac{1}{6\,(1+u_0)}, \ \xi_2 = \frac{11+12\,u_0}{12\,(1+u_0)}, \ \left(u_0+\frac{3}{2}\right)\left(u_0+\frac{1}{2}\right) = 0.$

Racines réelles

On suppose que $f_i \in \mathbb{R}[\mathbf{x}]$.

Considèrons la *forme linéaire* $Tr : a \mapsto trace(M_a) = \sum_{\zeta \in \mathcal{Z}(I)} \mu_\zeta \, a(\zeta)$.

Exemple :

$$Tr(x_1) = trace\left(\begin{bmatrix} 0 & \frac{1}{6} & 0 & \frac{5}{54} \\ 1 & 1 & 0 & \frac{55}{54} \\ 0 & 0 & 0 & \frac{2}{27} \\ 0 & -1 & 1 & -1 \end{bmatrix}\right) = 0$$

On lui associe la *forme quadratique* $Q_h : (a, b) \mapsto Tr(hab)$.

Théorème : (Hermite) *Soit* $h \in \mathbb{R}[\mathbf{x}]$.

1. *Le rang de la forme quadratique* Q_h *est le nombre de racines complexes* ζ *tq.* $h(\zeta) \neq 0$.
2. *La signature de* Q_h *est*

   $\#\{\ \zeta$ *réelles telles que* $h(\zeta) > 0\ \} - \#\{\ \zeta$ *réelles telles que* $h(\zeta) < 0\ \}$

On calcule $Tr(1) = 4,\ Tr(x_1) = 0,\ Tr(x_2) = 4, Tr(x_1 x_2) = \frac{2}{9}$

```
T0   := evalm([4,0,4,2/9]):
T1   := evalm(transpose(M1)&*T0):  T2:= evalm(transpose(M2)&*T0):
T11  := evalm(transpose(M1)&*T1): T12:= evalm(transpose(M2)&*T1):
T112:= evalm(transpose(M2)&*T11):
Q1   := matrix(4,4,[T0,T1,T2,T12]);
Qx1  := matrix(4,4,[T1,T11,T12,T112]);
```

$$Q_1 = \begin{pmatrix} 4 & 0 & 4 & \frac{2}{9} \\ 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ 4 & \frac{2}{9} & \frac{37}{9} & \frac{4}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \end{pmatrix}, \quad Q_{x_1} = \begin{pmatrix} 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ \frac{4}{9} & 0 & \frac{4}{9} & \frac{2}{81} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \\ \frac{4}{9} & \frac{2}{81} & \frac{37}{81} & \frac{4}{81} \end{pmatrix}$$

Le rang et la signature des formes quadratiques Q_1, Q_{x_1} sont

```
rank(Q1), signature(Q1), rank(Qx1), signature(Qx1);
```

$$2, \quad [2, 0], \quad 2, \quad [1, 1]$$

Comment calculer la structure du quotient ?

Objectifs

- □ Rapidité, efficacité.
- □ Continuité, stabilité des calculs.

Démarche

- ∘ Algèbre linéaire, contrôl des calculs.
- ∘ Exploiter la structure des objets.

I Controler les calculs

Résultant en une variable

Soient $f_0 = c_{0,0} + \cdots + c_{0,d_0}\, x^{d_0}$, $f_1 = c_{1,0} + \ldots + c_{1,d_1}\, x^{d_1}$ (avec $d_0 \leq d_1$).

Sylvester (1840)

$$
\begin{array}{c}
\overbrace{\begin{array}{cccccc} f_0 & \cdots & x^{d_1-1} f_0 & f_1 & \cdots & x^{d_0-1} f_1 \end{array}}^{d_0+d_1} \\
\left[\begin{array}{ccc|ccc}
c_{0,0} & & \mathbf{0} & c_{1,0} & & \mathbf{0} \\
\vdots & \ddots & & \vdots & \ddots & \\
\vdots & & c_{0,0} & \vdots & & c_{1,0} \\
c_{0,d_0} & & \vdots & c_{1,d_1} & & \vdots \\
& \ddots & \vdots & & \ddots & \vdots \\
\mathbf{0} & & c_{0,d_0} & \mathbf{0} & & c_{1,d_1}
\end{array}\right]
\end{array}
\quad
\left.\begin{array}{l}
1 \\
x \\
. \\
x^{d_1-1} \\
. \\
x^{d_0+d_1-1}
\end{array}\right\} d_0 + d_1
$$

Bézout (1779)

$$\Theta_{f_0,f_1}(x,y) := \frac{f_1(x)\, f_0(y) - f_1(y)\, f_0(x)}{y - x} = \sum_{i=0}^{d_1-1} \theta_{f_0,f_1,i}(x)\, y^i = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_1-1} \theta_{i,j}\, x^i\, y^j.$$

La matrice de Bézout est

$$\mathsf{B}_{f_0,f_1} = (\theta_{i,j})_{0 \leq i,i \leq d_1}.$$

Généralisation en plusieurs variables

Condition sur $(c_{i,j})$ pour que le système ait une solution :

$$\begin{cases} f_0 = \sum_{\alpha \in A_0} c_{0,\alpha}\, x_0^{\alpha_0} \cdots x_n^{\alpha_n}, \\ \vdots \\ f_n = \sum_{\alpha \in A_n} c_{n,\alpha}\, x_0^{\alpha_0} \cdots x_n^{\alpha_n}, \end{cases}$$

On s'intéresse aux matrices d'applications de la forme

$$\begin{aligned} \mathcal{S} : \langle \mathbf{x}^{E_0} \rangle \times \cdots \langle \mathbf{x}^{E_n} \rangle &\rightarrow \langle \mathbf{x}^{F} \rangle \\ (q_0, \ldots, q_n) &\mapsto \sum_{i=0}^{n} q_i\, f_i \end{aligned}$$

Macaulay (1902)

$A_i = \{\alpha \;;\; |\alpha| \le d_i\}$, $\nu = \sum_{i=0}^{n} (d_i - 1) + 1$,
$F = \{\beta \;;\; |\beta| \le \nu\}$, $E_n = \{\ldots\}$, …, $E_0 = \{\alpha \;;\; 0 \le \alpha_i \le d_i - 1\}$

Torique (1975)

A_i **polytope fixé (suport).** $F = A_0^{\delta} \oplus \cdots \oplus A_n^{\delta}$, $E_i = \oplus_{j \neq i} A_j^{\delta}$.

$$F\left\{\begin{array}{l}\mathbf{x}^{\alpha_1}\\ \cdot\\ \cdot\\ \cdot\\ \mathbf{x}^{\alpha_N}\end{array}\right.\quad\left[\begin{array}{c|c|c|c}\overbrace{\begin{array}{c}\cdot\\ \cdot\\ \mathbf{x}^{\beta_{0,1}}f_0\ \cdots\\ \cdot\\ \cdot\end{array}}^{E_0} & \overbrace{\begin{array}{c}\cdot\\ \cdot\\ \mathbf{x}^{\beta_{1,1}}f_1\ \cdots\\ \cdot\\ \cdot\end{array}}^{E_1} & \cdots\cdots\cdots & \overbrace{\begin{array}{c}\cdot\\ \cdot\\ \mathbf{x}^{\beta_{n,1}}f_n\ \cdots\\ \cdot\\ \cdot\end{array}}^{E_n}\end{array}\right].$$

```
S := mresultant([u[0]+u[1]*x[1]+u[2]*x[2],f1,f2],[x[1],x[2]]);
```

$$S := \left[\begin{array}{cccc|cccccc}
u_0 & 0 & 0 & 0 & 2 & 0 & 0 & -\frac{1}{6} & 0 & 0\\
u_2 & u_0 & 0 & 0 & -8 & 2 & 0 & 0 & -\frac{1}{6} & 0\\
u_1 & 0 & u_0 & 0 & -8 & 0 & 2 & -1 & 0 & -\frac{1}{6}\\
0 & u_1 & u_2 & u_0 & 8 & -8 & -8 & 1 & -1 & 0\\
\hline
0 & 0 & 0 & u_2 & 0 & 8 & 4 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 13 & 0 & 0 & 1\\
0 & 0 & 0 & u_1 & 0 & 13 & 8 & 0 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0\\
0 & 0 & u_1 & 0 & 13 & 0 & -8 & 1 & 0 & -1\\
0 & u_2 & 0 & 0 & 4 & -8 & 0 & 0 & 0 & 0
\end{array}\right]$$

```
det(S);
```

$$\frac{1}{36}\left(u_0+\frac{1}{3}u_1+\frac{7}{6}u_2\right)^2\left(u_0-\frac{1}{3}u_1+\frac{5}{6}u_2\right)^2$$

Le quotient par $f_1, \ldots, f_n$

$$
\mathtt{S} = \begin{array}{c} \\ E_0 \\ \\ F' \\ \\ \end{array}
\begin{array}{c}
\begin{array}{cc} E_0 & E_1 \cdots E_n \end{array} \\
\left[\begin{array}{c|c} \mathtt{A} & \mathtt{B} \\ \hline & \\ \mathtt{C} & \mathtt{D} \\ & \end{array}\right]
\end{array}.
$$

Proposition : *Si* $\det(\mathtt{D}) \neq 0$*, alors la matrice de multiplication par* f_0 *dans la base* $\mathbf{x}^{E_0}$ *de* $\mathcal{A}$ *est*

$$\mathtt{M}_{f_0} = \mathtt{A} - \mathtt{B}\,\mathtt{D}^{-1}\mathtt{C}.$$

```
Mu := uschur(S,4);
```

$$
\begin{bmatrix}
u_0 & -\frac{25}{24}\,u_2 & \frac{1}{6}\,u_1 & \frac{5}{54}\,u_1 - \frac{5}{54}\,u_2 \\
u_2 & u_0 + 2\,u_2 & 0 & \frac{2}{27}\,u_1 + \frac{5}{54}\,u_2 \\
u_1 & -\frac{5}{4}\,u_2 & u_0 + u_1 & \frac{55}{54}\,u_1 - \frac{55}{54}\,u_2 \\
0 & u_1 + \frac{5}{4}\,u_2 & u_2 - u_1 & u_0 - u_1 + 2\,u_2
\end{bmatrix}
$$

Méthode itérative controlée

Calculer la limite de $\mathbf{w}_n = \frac{1}{\|\mathbf{w}_{n-1}\|}(\mathtt{M}_{f_0}^{\mathtt{t}})^{-1}\mathbf{w}_{n-1}$, $\mathbf{w}_0$ étant générique.

Sélectionner une racine qui minimize f_0

Prendre $\mathbf{w}_0$ au hazard. Résoudre

$$S^t \begin{bmatrix} \mathbf{w}_{n+1} \\ \mathbf{v}_{n+1} \end{bmatrix} = \begin{bmatrix} \mathbf{w}_n \\ \mathbf{0} \end{bmatrix}$$

jusqu'à $\|\mathbf{w}_{n+1} - \mathbf{w}_n\| < \epsilon$. La racine est $\zeta = (\frac{w_{x_1}}{w_1}, \ldots, \frac{w_{x_n}}{w_1})$.

Implémentation en C++ (ALP):

	N	S	D	n	k	T
`s44`	36	138	16	2	7	0.050s
`s442`	165	821	32	3	6	0.151s
`s4422`	715	3704	64	4	8	1.179s
`s455`	364	1664	100	3	6	2.331s
`s2445`	1820	8795	160	4	8	4.323s
`s22445`	8568	41942	320	5	8	28.213s
`sq4`	126	585	16	4	5	0.313s
`sq5`	462	2175	32	5	44	2.135s
`sing`	210	4998	21	2	14	0.438s
`kruppa`	792	15822	1	5	1	0.698s

Le Bézoutien en plusieurs variables

$$\Theta(f_0, f_1, \ldots, f_n) = \begin{vmatrix} f_0(X_{(0)}) & \theta_1(f_0) & \cdots & \theta_n(f_0) \\ \vdots & \vdots & & \vdots \\ f_n(X_{(0)}) & \theta_1(f_n) & \cdots & \theta_n(f_n) \end{vmatrix} = \sum_{\alpha \in E, \beta \in F} t_{\alpha,\beta}\, \mathbf{x}^{\alpha}\, \mathbf{y}^{\beta}, \text{ où}$$

$X_{(0)} = (x_1, \ldots, x_n)$, $X_{(1)} = (y_1, x_2 \ldots, x_n)$, ..., $X_{(n)} = (y_1, \ldots, y_n)$, $\theta_i(P) = \frac{P(X_{(i)}) - P(X_{(i-1)})}{y_i - x_i}$.
La matrice du Bézoutien : $B_{f_0,\ldots,f_n} = [t_{\alpha,\beta}]_{\alpha \in E, \beta \in F}$.

```
Theta([u[0]+u[1]*x[1]+u[2]*x[2],f1,f2],[x[1],x[2]]);
```

$$-10/3\,u_1\xi_1 + 8\,u_0\xi_1 + 5\,u_0{\xi_1}^2 - 8\,u_0 - 4\,u_0\xi_1\xi_2 + \frac{25}{6}\,u_2\xi_1 + 4/3\,u_1 - 10/3\,u_2 - 2/3\,u_1\xi_2 + 4\,u_0\xi_2 - 4\,x_1x_2u_2\xi_2 + (-4\,u_1\xi_1 - 4\,u_0)\,x_1x_2 + \cdots$$

```
mbezout([u[0]+u[1]*x[1]+u[2]*x[2],f1,f2],[x[1],x[2]]);
```

$$\begin{bmatrix} -4\,u_2 & 5\,u_2 & -2/3\,u_1 + 10/3\,u_2 + 12\,u_0 & 8\,u_1 - 4\,u_0 & -4\,u_0 + 4\,u_2 \\ -4\,u_1 & 5\,u_1 & 8\,u_0 + \frac{25}{6}\,u_2 & 8\,u_1 + 5\,u_2 + 5\,u_0 & -4\,u_0 \\ -4\,u_0 & 5\,u_0 & 4/3\,u_1 - 8\,u_0 - 10/3\,u_2 & 8\,u_0 - 10/3\,u_1 + \frac{25}{6}\,u_2 & -2/3\,u_1 + 4\,u_0 \\ 0 & 0 & -4\,u_0 & -4\,u_1 & -4\,u_2 \\ 0 & 0 & -4\,u_0 & -4\,u_1 & -4\,u_2 \end{bmatrix}$$

Bézoutien et résultant

Condition pour que le système ait une solution :

$$\left\{ \begin{array}{rcl} f_0(\mathtt{t}) & = & \sum_{j=0}^{k_0} c_{0,j}\, \kappa_{0,j}(\mathtt{t}) \\ & \vdots & \\ f_n(\mathtt{t}) & = & \sum_{j=0}^{k_n} c_{n,j}\, \kappa_{n,j}(\mathtt{t}) \end{array} \right.$$

où $\mathtt{t} = (t_1, \ldots, t_n)$ et les $\kappa_{i,j}(\mathtt{t})$ sont des polynômes en $\mathtt{t}$.

Sous les bonnes hypothèses, il existe X et un polynôme Res_X des coefficients $c_{i,j}$ tel que $\mathrm{Res}_X(f_0, \ldots, f_n) = 0$ ssi il exite une « solution » sur X.

Théorème : *Tout mineur maximal de $B_{f_0,\ldots,f_n}$ est divisible par le résultant* $\mathrm{Res}_X(f_0, \ldots, f_n)$.

Applications

- **Pour résoudre $f_1, \ldots, f_n$:**

  1. Construire une matrice de résultant M_u
     – en prenant $f_0 = l(\mathbf{x}) - u$.
     – ou en cachant une variable $u = x_n$ ($n-1$ variables).
  2. Calculer les valeurs de u pour lesquelles M_u chute de rang
     – en résolvant un polynôme en une variable,
     – ou en se ramenant à un problème de valeurs/vecteurs propres.

- **Pour résoudre des problèmes surdéterminés approchés.**

- **Pour éliminer des variables :** Projection de variétés sur des sous-espaces. Passage d'une équation paramétré à une équation implicite.

- **Pour décomposer géométriquement d'une variété :**

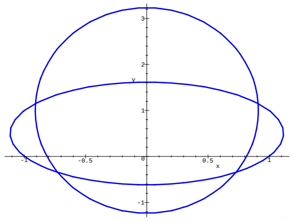
  1. Calculer la représentation univariée rationnelle des points isolés.
  2. Cacher une variable, prendre $n-1$ combinaisons génériques des équations et recommencer l'étape 1 avec $n-1$ variables.

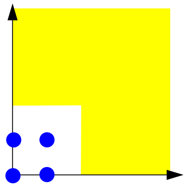
- **Pour mettre en place des prédicats géométriques certifiés.**

Peut-on envisager des calculs stables de GB ?

Base de $\mathcal{A} = \mathbb{K}[x_1, x_2]/(p_1, p_2)$:

$$\begin{cases} p_1 := a\,x_1^2 + b\,x_2^2 + l_1(x_1, x_2) \\ p_2 := c\,x_1^2 + d\,x_2^2 + l_2(x_1, x_2) \end{cases}$$

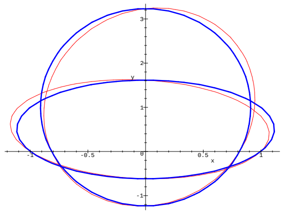


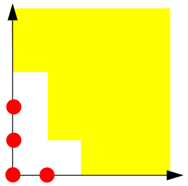


Une petite perturbation :

Base de $\tilde{\mathcal{A}} = \mathbb{K}[x_1, x_2]/(\tilde{p}_1, \tilde{p}_2)$:

$$\begin{cases} \tilde{p}_1 := p_1 + \epsilon_1\, x_1 x_2 \\ \tilde{p}_2 := p_2 + \epsilon_2\, x_1 x_2 \end{cases}$$





Catastrophe !

- Plus de base carrée, mais une base monomiale moins naturelle.
- Gros coefficients (in $\frac{1}{\epsilon_i}$).

Un nouveau critère de forme normale

On se donne

- **un ensemble de monômes B (connecté à 1),**
- **une projection du bord de B sur B suivant un esp. vectoriel K :** $N : \langle B^{+} \rangle \to \langle B \rangle$, avec $N^2 = N$ **suivant un idéal I.**

où $B^{+} = B \cup x_1 B \cup \cdots \cup x_n B$

Problème:

Est-ce que N est une forme normal modulo $I = (K)$?

Théorème : *Soient $M_i : \langle B \rangle \to \langle B \rangle$ tp. $M_i(b) = N(x_i b)$.*

$M_i \circ M_j = M_j \circ M_i, i, j = 1, \ldots, n \Leftrightarrow$ B base de $\mathcal{A}$ et N normalisation pour $\mathcal{A} = R/I$.

La structure du quotient

Soient $f_1, \dots, f_m \in R = \mathbb{K}[x_1, \dots, x_n]$ tels que $\mathcal{A} = R/(f_1, \dots, f_m)$ avec $\dim_{\mathbb{K}}(\mathcal{A}) = D$.
On se donne $V \subset R$ un espace vectoriel de dimension finie connecté à 1.

Calcul de la forme normale

1. $K_0 = \langle f_1, \dots, f_m \rangle \cap V$; $K_1 = K_0^+ \cap V$; $i := 1$;
2. Tant que $K_i \neq K_{i-1}$ faire $K_{i+1} := K_i^+ \cap V$; $i := i + 1$;
3. Choisir un supplémentaire B de K^* dans V, connecté à 1.
4. – Si $B^+ \not\subset V$, remplacer V par V^+ et recommencer (1).
   – Sinon, la projection sur B suivant K_* est une forme normale pour $R/(f_1, \dots, f_m)$.

Exemple pour $f_1, \dots, f_n$ une intersection complete : $V = R_{\leq \nu}$ avec $\nu = \sum_{i=1}^{n} (\deg(f_i) - 1)$

Le construction de Macaulay revisitée

On suppose ici que $f_1, \ldots, f_n$ sont de degré d, et générique pour la construction de Macaulay: une base de $\mathcal{A}$ est

$$B := \mathbf{x}^{E_0} = \{x_1^{a_1} \cdots x_n^{a_n} \ ; \ 0 \leq a_i \leq d-1\}.$$

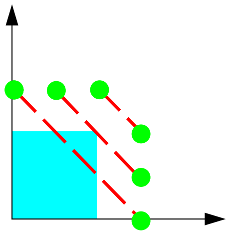
Soit $p^\star = \{x_i\, p; i = 1, \ldots, n \text{ and } x_i\, p \in B^+\}$.

Macaulay revisited

$\mathtt{S}_d = (f_i | x_j^d)$; $\mathtt{F} := \mathtt{S}_d^{-1}[f_1, \ldots, f_n]$; $\mathtt{M} = [x_1^d, \ldots, x_n^d]$;

while $r \leq n(d-1)$ do

- $\mathtt{M} := \mathtt{M}^\star$; $\mathtt{F} := \mathtt{F}^\star$; $r := r + 1$;
- $S_r := (F_i | M_j)$; $F := S_r^{-1}\, F$;



n	D	Mc	$\sum s_i$												$d=2$
7	128	6307	448	7	42	105	140	105	42	7					
8	256	24 054	1 024	8	56	168	280	280	168	56	8				
9	512	91 866	2 304	9	72	252	504	630	504	252	72	9			
10	1024	351 692	5 120	10	90	360	840	1260	1260	840	360	90	10		
11	2048	1 350 030	11 264	11	110	495	1320	2310	2772	2310	1320	495	110	11	
12	4096	5 196 204	24 576	12	132	660	1980	3960	5544	5544	3960	1980	660	132	12

II Exploiter la structure des objets

Dualité algébrique

Hypothèse : Le système $f_1, \dots, f_n$ a un nombre fini de solutions (intersection complète).

Théorème : *Le dual $\widehat{\mathcal{A}}$ est un $\mathcal{A}$-module libre de rang 1 : $\widehat{\mathcal{A}} = \mathcal{A} \cdot \tau$.*

Le polynôme $\Delta(\mathbf{x}, \mathbf{y}) = \Theta_{1,f_1,\dots,f_n} \equiv \sum_{\alpha \in E} \mathbf{x}^\alpha, \mathbf{w}_\alpha(y) = \sum_{\alpha \in E} \mathbf{w}_\alpha(\mathbf{x})\, \mathbf{y}^\alpha$ définit l'isomorphisme de $\mathcal{A}$-modules

$$\Delta^\triangleright : \Lambda \mapsto \sum_{\alpha \in E} \mathbf{x}^\alpha \Lambda(\mathbf{w}_\alpha).$$

Formule de projection : $\forall a \in \mathcal{A}, \quad a = \sum_{\alpha \in E} \mathbf{x}^\alpha \tau(a\, \mathbf{w}_\alpha) = \sum_{\alpha \in E} \mathbf{w}^\alpha(\mathbf{x}) \tau(a\, \mathbf{x}^\alpha).$

Base duale de $(\mathbf{x}^\alpha)$ pour $(a, b) \mapsto (a|b) = \tau(a\, b)$: $(\mathbf{w}_\alpha)$.

Exemple : Si $\mathcal{A} = \mathbb{C}[x]/(f)$, $\Delta(\mathbf{x}, \mathbf{y}) = \sum_{i=0}^{d-1} x^i h_i(y)$ avec $h_i = f_d x^{d-i-1} + \cdots + f_i$ (polynôme de Hörner).

Matrices structurées

Type	Charact.	$M \cdot V$	$M\,X = W$	Exemple(s)
Toeplitz	$m_{i,j} = t_{i-j}$	$\mathcal{O}(d\log(d))$	$\mathcal{O}(d\log^2(d))$	$T_p : \mathbb{C}[x] \to \mathbb{C}[x]$,
Hankel	$m_{i,j} = h_{i+j}$	$\mathcal{O}(d\log(d))$	$\mathcal{O}(d\log^2(d))$	$H_\Lambda : \mathcal{A} \to \widehat{\mathcal{A}}$
U-Bezoutien	H^{-1}	$\mathcal{O}(d\log(d))$	$\mathcal{O}(d\log^2(d))$	$B_{u/v} : \widehat{\mathcal{A}} \to \mathcal{A}$
Quasi-Toeplitz	$m_{\alpha,\beta} = t_{\alpha-\beta}$	$\mathcal{O}(D\log(D))$	$\mathcal{O}(D^2\log(D))$	$T_{\mathbf{f}} : R \to R$
Quasi-Hankel	$m_{\alpha,\beta} = h_{\alpha+\beta}$	$\mathcal{O}(D\log(D))$	$\mathcal{O}(D^2\log(D))$	$H_\Lambda : \mathcal{A} \to \widehat{\mathcal{A}}$
M-Bezoutien	QH^{-1}			$B_\Delta : \widehat{\mathcal{A}} \to \mathcal{A}$

Matrice de multiplication : $M_{f_0} = A - BD^{-1}C$.

Matrice de la base duale : $[\mathbb{I}| - BD^{-1}]$.

Application : méthode itérative dans le quotient.

- $u_{n+1} = f_0 u_n$ (Bernoulli).
- $u_{n+1} \equiv u_n^2$ (Sebastio e Sylva).
- $u_{n+1} \equiv \frac{1}{2}(u_n \pm u_n^{-1})$ (Joukovski)

Convergence (rapide) vers une combinaison d'idempotents de $\mathcal{A}$.

Permet de séparer les racines ($|f_0(\zeta)|$ maximum, $Re(f_0(\zeta)) > 0, \ldots$).

Exemple : `http://www.inria.fr/saga/logiciels/ALP/`
implémentation de la méthode de Sebastio e Sylva, par H. Prieto.

	d	x0	k	T
`double`	10000	0.0	8	22.03s
`double`	100000	0.0	8	346.52s
`complex`	10000	(0.4,0.6)	6	16.86s
`complex`	100000	(0.4,0.6)	6	292.02s
`complex`	1000000	(0.4,0.6)	7	2520s
`exp`	100	(0.0,0.8)	6	45s
`exp`	150	(0.0,0.8)	6	59s
`exp`	200	(0.0,0.8)	6	101s

Généralisation au cas multivariable

Input:

– *Une forme linéaire* $\tau \in \widehat{\mathcal{A}} = I^{\perp}$, *telle que* $q : (a, b) \mapsto \tau(a\, b)$ *non-dégénée.*

– *une base de monomes* $(\mathbf{x}^{\alpha})_{\alpha \in E}$ *de* $\mathcal{A}$,

– *les coefficients* $(\tau(\mathbf{x}^{\alpha}))_{\alpha \in F}$ *pour* $F = E + E + E$.

Ingrédients :

Multiplication dans $\mathcal{A}$*:*

1. Calculer les coefficients $[f\, g]_{\mathbf{w}}$ de $(\mathbf{d}^{\alpha})_{\alpha \in E}$ dans le produit $f\, g \cdot \tau$.
2. Résoudre le système $\mathtt{H}_{\tau}\, \mathtt{X} = [f\, g]_{\mathbf{w}}$: $\mathtt{X} = [f\, g]_{\mathbf{x}}$.

Inversion dans $\mathcal{A}$*:*

1. Calculer $\wedge = \mathtt{H}_{\tau}\, [1]_{\mathbf{x}}$.
2. Résoudre le système $\mathtt{H}_{f \cdot \tau} \mathtt{X} = \wedge$: $\mathtt{X} = [f^{-1}]_{\mathbf{x}}$.

Applications:

– Selectionner une racine qui maximise (minimise) $|h|$.

– Calculer les racines presques réelles.

– Calculer les racines dans une boîte.