Singularités et complexité dans les algorithmes de la géométrie algébrique réelle

Étude du calcul d'un point par composante connexe sur une variété algébrique réelle définie par une équation

M. Safey El Din

Mohab.Safey@lip6.fr

http://www-calfor.lip6.fr/~safey

LIP6 (CalFor), Projet INRIA/LIP6 SALSA

Université Pierre et Marie Curie

Problématique

$\mathbb{Q}$ le corps des rationnels

$\mathbb{R}$ le corps des réels

$\mathbb{C}$ le corps des complexes

$f_1, \ldots, f_s$ une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D.

$\mathcal{V} \subset \mathbb{C}^n$ une **variété algébrique** définie par :

$$f_1 = \cdots = f_s = 0$$

Calculer au moins un point par composante connexe sur $\mathcal{V} \cap \mathbb{R}^n$

- Borne sur le nombre de composantes connexes (Thom-Milnor) : $(2D)^n$
- Amélioration (S./Trébuchet 2004) : $D^s(D-1)^{n-s}\binom{n}{n-s}$

Obtenir un algorithme de complexité asymptotiquement optimale ($D^{\mathcal{O}(n)}$)
et efficace en pratique

Motivations

Décider du vide d'un semi-algébrique

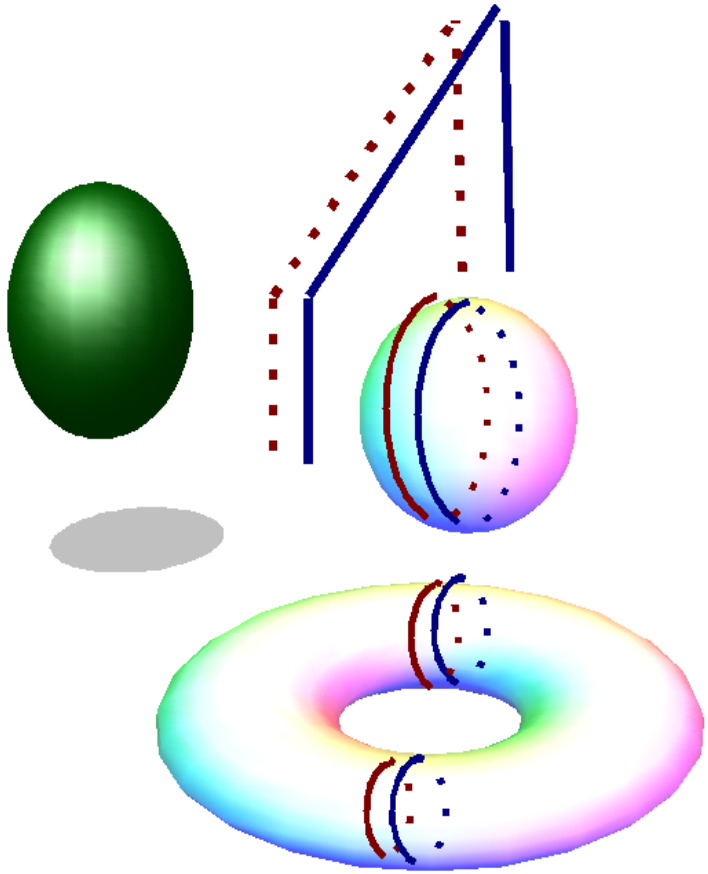
$$f_1 = \cdots = f_s = 0, g_1 > 0, \ldots, g_k > 0$$

(ou en calculer au moins un point par composante connexe)

Calcul d'au moins un point par composante connexe des variétés définies par :

$$f_1 = \cdots = f_s = g_{i_1} - \varepsilon = \cdots = g_{i_\ell} - \varepsilon = 0$$

pour tout $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, k\}$



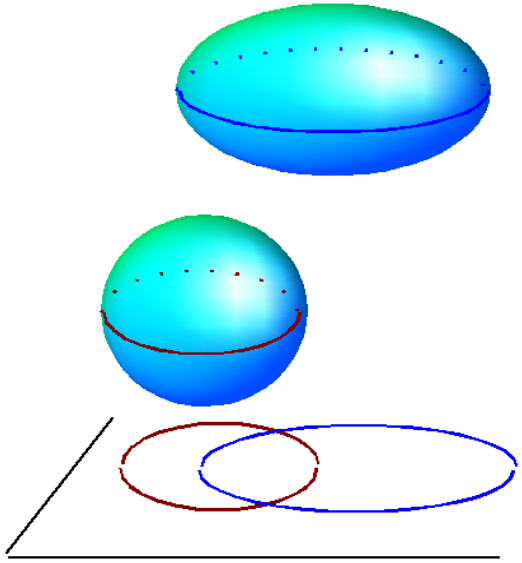
Applications : robotique, mécanique céleste, théorie du signal, etc.

Motivations

Résolution réelle de systèmes à paramètres (Lazard, Rouillier)

Étude du complémentaire d'une hypersurface

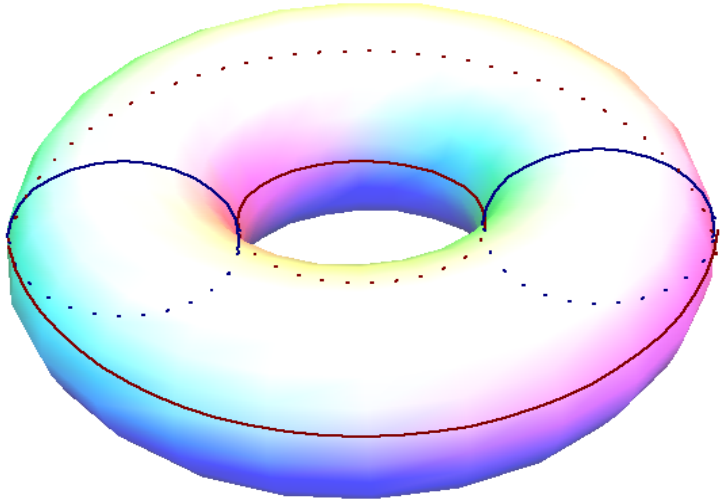
Applications : robotique, statistique



Calcul de cartes routières sur une variété algébrique réelle

Une courbe connexe dans chaque composante connexe

Applications : planification, topologie d'une variété



Optimisation algébrique

$\mathcal{V}$ définie par $f_1 = \cdots = f_s = 0$.
$\phi : \mathcal{V} \cap \mathbb{R}^n \to \mathbb{R}$ atteignant ses extrema sur chaque composante connexe de $\mathcal{V} \cap \mathbb{R}^n$.

Calculer les points extremaux de ϕ restreinte à $\mathcal{V}$
Engendrer un nouveau système polynomial dont ils sont solutions
et n'ayant qu'un nombre fini de solutions complexes

Paramétrisations rationnelles
Isolation des racines d'un polynôme univarié
(Sturm-Habicht, Uspensky)

$$\begin{cases} X_n = \frac{q_n(T)}{q_0(T)}, \\ \vdots \\ X_1 = \frac{q_1(T)}{q_0(T)} \\ q(T) = 0 \end{cases}$$

Outils algébriques : Nombre fini de solutions complexes

Entrée : Une famille de polynômes $(f_1, \ldots, f_s)$ ayant un nombre fini de solutions communes

Sortie : Une paramétrisation rationnelle de l'ensemble des solutions.

Bases de Gröbner (Buchberger, Algorithmes F4 et F5 de Faugère) puis **Représentation Univariée Rationnelle** (Rouillier)

- Complexité (Gröbner): $D^{\mathcal{O}(n)}$ Lakshman (90), Lazard et Hashemi (05)
  Systèmes surdéterminés : Thèse de M. Bardet (Bardet, Faugère, Salvy)
- RUR (Rouillier) : polynomiale en le nombre de solutions complexes
- Implantations[a] : Gröbner (`Gb`, `FGb`), RUR (`RS`)

Voir aussi Formes normales généralisées (Trébuchet)

[a] `http://fgbrs.lip6.fr`

Outils algébriques : Nombre fini de solutions complexes

Entrée : $f_1 = \ldots = f_s = 0,\ g \neq 0$

- $\mathcal{L}$ est la complexité d'évaluation du système.
- La jacobienne est de rang plein en chacun des points de $f_1 = \cdots = f_i = 0, g \neq 0$

Sortie : Une paramétrisation rationnelle de l'ensemble des solutions du système.

Résolution Géométrique (initiée par Giusti, Heintz, Pardo),

- Complexité (Giusti, Lecerf, Salvy 2001, Lecerf 2002, thèse de Lecerf)

$$\mathcal{O}(n(n\mathcal{L} + n^3)\mathtt{M}(D\delta)^2)$$

$\delta \leq D^n$ est le max des degrés des variétés $f_1 = \cdots = f_i = 0, g \neq 0, i = 1, \ldots, s$

- Implantations : Paquetage Magma `Kronecker`[a]

Généralisation au calcul de décomposition équi-dimensionnelle
avec un *léger* surcoût, Lecerf, 2003.

[a] `http://www.math.uvsq.fr/~lecerf/software/`

Points critiques

Soit d la dimension de $\mathcal{V} \subset \mathbb{C}^n$ définie par $f_1 = \cdots = f_s = 0$ et $y \in \mathcal{V}$

Hypothèse (R): $\mathbf{grad}_y(f_1), \ldots, \mathbf{grad}_y(f_s)$ est de dimension $n - d$

Points réguliers de $\mathcal{V}$ ($\mathrm{Reg}(\mathcal{V})$) : ensemble des points de $\mathcal{V}$ vérifiant **(R)**.
Points singuliers de $\mathcal{V}$ ($\mathrm{Sing}(\mathcal{V})$) : les points de $\mathcal{V}$ ne vérifiant pas **(R)**.

Soit $\phi : y \in \mathbb{C}^n \to (\phi_1(y), \ldots, \phi_p(y)) \in \mathbb{C}^p$

$y \in \mathrm{Reg}(\mathcal{V})$ est un point critique de ϕ restreinte à $\mathcal{V}$ ssi
$\dim(\mathbf{grad}_y(\phi_1), \ldots, \mathbf{grad}_y(\phi_p)) + \dim(\mathbf{grad}_y(f_1), \ldots, \mathbf{grad}_y(f_s)) < n - d + p$

Notation $K(\phi, \mathcal{V}) \subset \mathrm{Reg}(\mathcal{V})$ est l'ensemble des points critiques de ϕ restreinte à $\mathcal{V}$.

Méthode des points critiques : Les problèmes

Que se passe-t-il lorsque $\dim(\mathbf{grad}_y(f_1), \ldots, \mathbf{grad}_y(f_s)) \neq n - d$?

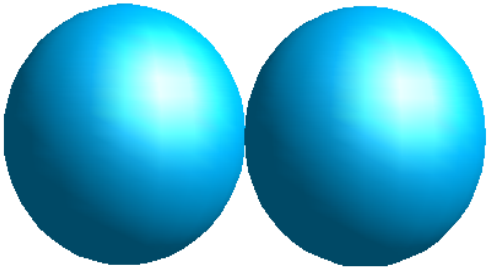
$(X^2 + Y^2 + Z^2 - 1)^2 = 0$

La jacobienne est de rang nul partout

$((X-1)^2 + Y^2 + Z^2 - 1)$

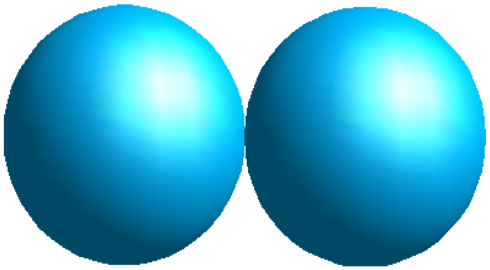
$((X+1)^2 + Y^2 + Z^2 - 1) = 0$

La jacobienne est de rang nul en l'origine



$P(X,Y,Z)(X-3) = P(X,Y,Z)Z = 0$

La jacobienne est de rang 2 en $X - 3 = Y = 0$, de rang nul en l'origine, de rang 1 ailleurs.



Obtenir une bonne complexité (Basu, Pollack, Roy)

Voir aussi **Grigoriev**, **Vorobjov** (1988), **Renegar** (1992), **Heintz**, **Roy** et **Solerno** (1993)

Réduire l'étude au cas d'une hypersurface lisse dont le lieu réel est compact

- $F \leftarrow (f_1^2 + \cdots + f_s^2) + (X_1^2 + \cdots + X_n^2 + X_{n+1}^2 - 1/\varepsilon)^2$
  (ε est un infinitésimal)
- $G \leftarrow \zeta F^2 + (1-\zeta)(X_1^{2D_1+2} + \cdots + X_1^{2D_n+2} + X_{n+1}^6 - (n+1)/\varepsilon^{2D+2}$
  (ζ est un infinitésimal et $D_i = \deg(F, X_i)$)
- $G, \frac{\partial G}{\partial X_2}, \ldots, \frac{\partial G}{\partial X_{n+1}}$ est une base de Gröbner.

Nombre de solutions (complexes) du système produit :	$5(2(D+1))^n$
Taille maximale des données intermédiaires :	$\tau 5(2(D+1))^{4n}$
Complexité :	$\mathcal{O}(n^2(2D)^{6n}\tau)$

Quelques améliorations (Rouillier, Roy, S.)

Étudier l'hypersurface $\mathcal{H}_\varepsilon \subset \mathbb{C}\langle\varepsilon\rangle^n$ définie par $f - \varepsilon = 0$ (ε est un infinitésimal).

Soit $A = (a_1, \ldots, a_n) \in \mathbb{Q}^n$ et $\phi_A : (x_1, \ldots, x_n) \to (x_1 - a_1)^2 + \cdots + (x_n - a_n)^2$

Il existe un fermé algébrique $\mathcal{A} \subset \mathbb{C}^n$ tel que pour tout $A \in \mathbb{Q}^n \setminus \mathcal{A}$ l'ensemble des limites de $K(\phi_A, \mathcal{H}_\varepsilon)$ (quand ε tend vers 0) est zéro-dimensionnel et intersecte chaque composante connexe de $\mathcal{H}_0 \cap \mathbb{R}^n$.

Analyse en utilisant la thèse de É. Schost

Nombre de solutions (complexes) du système produit :	D^n
Taille maximale des données intermédiaires :	τD^{3n}
Complexité :	$\mathcal{O}(\tau . n^2 D^{4n})$

Quelques améliorations (Aubry, Rouillier, S.)

Soit $\mathcal{V} \subset \mathbb{C}^n$ équidimensionnelle de dimension d définie par $f_1 = \cdots = f_s = 0$.
Hypothèse : Pour un point *générique* de $\mathcal{V}$ le rang de $\mathrm{Jac}(f_1, \ldots, f_s)$ est $n-d$
$\phi_A : (x_1, \ldots, x_n) \in \mathbb{C}^n \to (x_1 - a_1)^2 + \cdots + (x_n - a_n)^2 \in \mathbb{C}$

S_A le système annulant les f_i et tous les mineurs $(n-d+1, n-d+1)$ de $\mathrm{Jac}(f_1, \ldots, f_s, \phi_A)$. L'ensemble des solutions de S_A est constitué de :

- L'ensemble des points ne vérifiant pas (R) est de dimension strictement inférieure à celle de $\mathcal{V}$;
- et des points critiques de ϕ_A qui pour un choix générique de A sont en nombre fini.

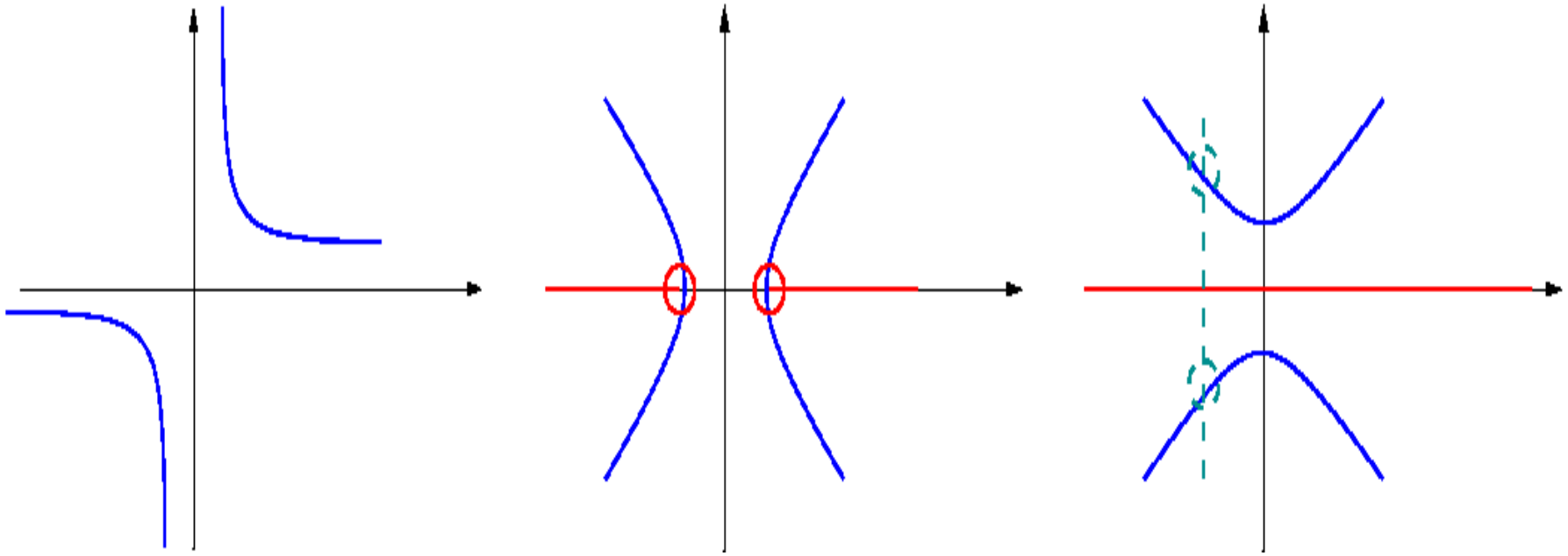
Le cas lisse et équi-dimensionnel

- Peut-on **améliorer la complexité** des algorithmes généraux ?
- Peut-on substituer des **fonctions de projection** aux fonctions distances?
- Si oui, peut-on **quantifier** le gain ?
- Peut-on avoir des **informations géométriques** sur les lieux critiques ?

- Bank, Giusti, Heintz, M'Bakop et Pardo : Cas lisses et équi-dimensionnels étude des variétés polaires, complexité dans le cas de la fonction distance
- S. Schost 03, S. Trébuchet 04 (levée de l'hypothèse d'équidimensionnalité) algorithmes utilisant des fonctions de projection, introduction du système de Lagrange, bornes de complexité fines

Le cas lisse (S., Schost)

Utiliser des fonctions de projections



Faire des changements de variables pour rendre les projections propres
Calculer des lieux critiques et des fibres au-dessus d'un point arbitraire de l'espace sur lequel on projette.

Le cas lisse (S., Schost)

$\mathcal{V} \subset \mathbb{C}^n$ équi-dimensionnelle, de dimension d définie par $f_1 = \cdots = f_s = 0$.

$\mathbf{A} \in GL_n(\mathbb{Q})$, $f_i^{\mathbf{A}} \leftarrow f_i(\mathbf{X})$ (pour $i = 1, \ldots, s$), et $\mathcal{V}^{\mathbf{A}}$

$$\Pi_i : (x_1, \ldots, x_n) \in \mathbb{C}^n \to (x_1, \ldots, x_i) \in \mathbb{C}^i, \quad i = 1, \ldots, d$$

Soit $p = (p_1, \ldots, p_d)$ un point arbitrairement choisi dans $\mathbb{Q}^d$.

Soit $\mathcal{K}_p^{\mathbf{A}}$ la réunion des :

- $K(\Pi_i, \mathcal{V}^{\mathbf{A}}) \cap \Pi_{i-1}^{-1}(p_1, \ldots, p_i)$ (pour $i = 2, \ldots, d-2$)
- de $K(\Pi_1, \mathcal{V}^{\mathbf{A}})$ et de $\mathcal{V}^{\mathbf{A}} \cap \Pi_d^{-1}(p_1, \ldots, p_d)$

Le cas lisse (S., Schost)

$$\mathcal{K}_p^{\mathbf{A}} = \left(\bigcup_{i=2}^{d-1} K(\Pi_i, \mathcal{V}^{\mathbf{A}}) \cap \Pi_{i-1}^{-1}(p_1, \ldots, p_i)\right) \cup K(\Pi_1, \mathcal{V}^{\mathbf{A}}) \cup \mathcal{V}^{\mathbf{A}} \cap \Pi_d^{-1}(p_1, \ldots, p_d)$$

Il existe un fermé algébrique $\mathcal{A} \subset GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$,

- $\mathcal{K}_p^{\mathbf{A}}$ est zéro-dimensionnel,
- $\mathcal{K}_p^{\mathbf{A}}$ intersecte chaque composante connexe de $\mathcal{V}^{\mathbf{A}} \cap \mathbb{R}^n$.

Nombre de solutions (complexes) des systèmes :	$D\left(\sum_{i=0}^{n-1}(D-1)^i\right)$
Taille maximale des données intermédiaires :	$\tau D^2\left(\sum_{i=0}^{n-1}(D-1)^{2i}\right)$
Complexité :	$\mathcal{O}(\tau n^2 D^{3n})$

Récapitulatif des complexités

	Taille	**Sortie**	**Complexité**
B.P.R.	$\tau 5(2(D+1))^{4n}$	$(2D)^n$	$\mathcal{O}(\tau n^2(2D)^{6n})$
Rou.Roy.S.	τD^{3n}	D^n	$\mathcal{O}(\tau n^2 D^{4n})$
	$\tau D\left(\sum_{i=0}^{n-1}(D-1)^{3i}\right)$	$D\left(\sum_{i=0}^{n-1}(D-1)^{i}\right)$	$\mathcal{O}(\tau n^2 D^{4n}))$
A.Rou.S.	**??**	**??**	**??**
Sa.Sc.	$\tau D\left(\sum_{i=0}^{n-1}(D-1)^{2i}\right)$	$D\left(\sum_{i=0}^{n-1}(D-1)^{i}\right)$	$\mathcal{O}(\tau n^2 D^{3n}))$

Le surcoût calculatoire induit par la présence de singularités est-il justifié ?

Retour sur la déformation infinitésimale

$f \in \mathbb{Q}[X_1, \ldots, X_n]$ de degré D et $\mathcal{H}_t \subset \mathbb{C}^n$ définie par $f - t = 0$

$\phi : \mathbb{C}^n \to \mathbb{C}$ une application polynomiale, $K(\phi, \mathcal{H}_t)$

- Que veut-on vraiment calculer ?
  Les limites des points critiques quand t tend vers 0

- Qu'est-ce qui pose problème ?
  La taille des paramétrisations rationnelles à coefficients dans $\mathbb{Q}(t)$.

- Utiliser le système de Lagrange $\mathcal{L}_t$ défini par $L.\mathbf{grad}(f) = \mathbf{grad}(\phi), f - t = 0$

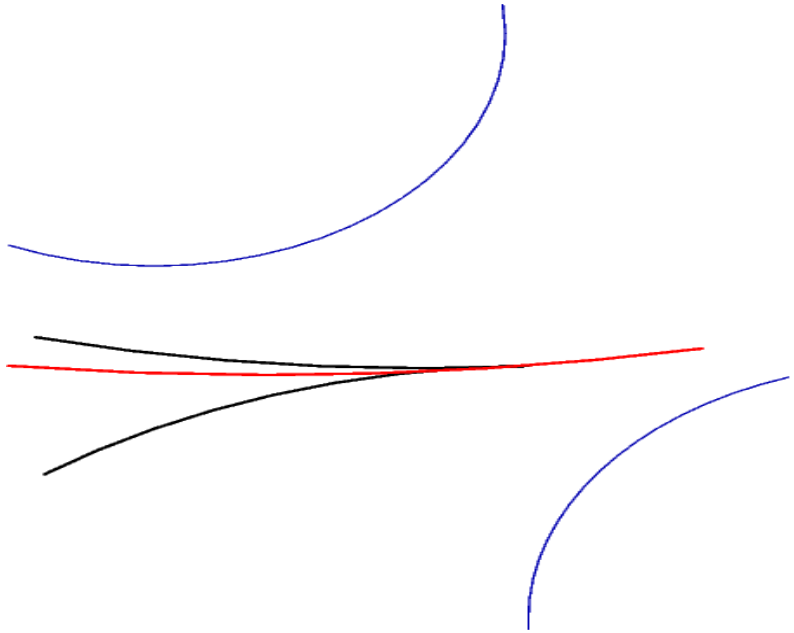
- **Remarque** : Soit y_t la projection dans $X_1, \ldots, X_n$ d'une solution de $\mathcal{L}_t$ convergeant vers un point de $\mathrm{Sing}(\mathcal{H}_0)$. Alors $L(y_t)$ tend vers l'infini.

  Phénomène de non-propreté pour la projection
  $\Pi : (x_1, \ldots, x_n, \ell) \in \mathbb{C}^{n+1} \to (x_1, \ldots, x_n) \in \mathbb{C}^n$
  restreinte aux solutions de $L.\mathbf{grad}(f) = \mathbf{grad}(\phi)$.

Calcul des limites de points critiques

$\mathcal{H}_t$ définie par $f = t$ (pour $t \in \mathbb{Q}$),
$\phi : \mathbb{C}^n \to \mathbb{C}$ une application polynomiale
$\Pi : (x_1, \ldots, x_n, \ell) \in \mathbb{C}^{n+1} \to (x_1, \ldots, x_n) \in \mathbb{C}^n$

On suppose que l'ensemble des solutions de : $L.\mathbf{grad}(f) = \mathbf{grad}(\phi)$
est une courbe (dimension 1) que l'on note $\mathfrak{C}$.
Les limites de $K(\phi, \mathcal{H}_t)$ (quand $t \to 0$) sont contenues dans $\mathfrak{C} \cap \mathcal{H}_0$.



Solutions algorithmiques

- **Bases de Gröbner**
  - Utiliser un ordre monomial éliminant L et calculer une base de Gröbner du système $L.\mathbf{grad}(f) = \mathbf{grad}(\phi)$.
    On obtient une famille de polynômes G définissant $\overline{\Pi(\mathfrak{C})}$
    Il suffit maintenant de calculer une base de Gröbner de $G \cup \{f\}$

- **Résolution géométrique**
  - Calculer tous les mineurs $(2,2)$ de $\mathrm{Jac}(f,\phi)$
    Résoudre le système constitué de l'annulation de ces mineurs et l'inéquation $\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}^2 \neq 0$
    (représenter la courbe par une paramétrisation rationnelle à coefficients dans le corps des fractions rationnelles d'un paramètre).
    Intersecter la courbe avec l'hypersurface définie par $f = 0$.

Application à la fonction distance

$A = (a_1, \ldots, a_n) \in \mathbb{Q}^n$
$\phi_A : (x_1, \ldots, x_n) \in \mathbb{C}^n \to (x_1 - a_1)^2 + \cdots + (x_n - a_n)^2 \in \mathbb{C}$
$\Pi : (x_1, \ldots, x_n, \ell) \subset \mathbb{C}^{n+1} \to (x_1, \ldots, x_n) \in \mathbb{C}$

$\mathfrak{C}_A \subset \mathbb{C}^{n+1}$ l'ensemble des solutions de $L.\mathbf{grad}(f) = \mathbf{grad}(\phi_A)$.
$\overline{\Pi(\mathfrak{C}_A)}$ la clôture de Zariski de $\Pi(\mathfrak{C}_A)$.

Il existe un fermé algébrique $\mathcal{A} \subset \mathbb{C}^n$ tel que pour tout $A \in \mathbb{Q}^n \setminus \mathcal{A}$:

- $\overline{\Pi(\mathfrak{C}_A)} \cap \mathcal{H}_0$ est zéro-dimensionnel,
- $\overline{\Pi(\mathfrak{C}_A)} \cap \mathcal{H}_0$ intersecte chaque composante connexe de $\mathcal{H}_0 \cap \mathbb{R}^n$.

Application aux fonctions de projection

$\mathbf{A} \in GL_n(\mathbb{Q})$, $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$, $\Pi : (x_1, \ldots, x_n, \ell) \to (x_1, \ldots, x_n)$

$\overline{\Pi(\mathfrak{C}_i^{\mathbf{A}})}$ la **clôture de la projection** par Π des solutions de

$$L.\frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} = 1, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, X_1 = p_1, \ldots, X_i = p_i, \ i = 1, \ldots, n-2$$

$\overline{\Pi(\mathfrak{C}_0^{\mathbf{A}})}$ la **clôture de la projection** par Π des solutions de

$$L.\frac{\partial f^{\mathbf{A}}}{\partial X_1} = 1, \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0$$

$$\mathcal{K}_p^{\mathbf{A}} = \left(\bigcup_{i=0}^{n-2} \overline{\Pi(\mathfrak{C}_i^{\mathbf{A}})} \cap \mathcal{H}_0^{\mathbf{A}} \right) \cup \{ f = X_1 - p_1 = \cdots = X_{n-1} - p_{n-1} = 0 \}$$

Il existe un fermé algébrique $\mathcal{A} \subset GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$,

- $\mathcal{K}_p^{\mathbf{A}}$ est zéro-dimensionnel,
- $\mathcal{K}_p^{\mathbf{A}}$ intersecte chaque composante connexe de $\mathcal{V}^{\mathbf{A}} \cap \mathbb{R}^n$.

Complexités (fonctions distance et projection)

$f \in \mathbb{Q}[X_1, \ldots, X_n]$ de degré D
$\mathcal{L}$ la complexité de son évaluation.

Gröbner : en utilisant de l'interpolation $D^{\mathcal{O}(n)}$ mais
en pratique il est plus efficace d'utiliser un ordre d'élimination sur le système de Lagrange (éliminant L en l'occurence).

Résolution géométrique : $\mathcal{O}(n^2(\mathcal{L} + n^3)\mathtt{M}(D\delta)^3)$

- dans le cas de la fonction distance, δ est borné par D^n
- dans le cas des fonctions de projections, δ est borné par $D(D-1)^{n-1}$.

Amélioration des bornes dans les cas singuliers

Mieux évaluer le **degré** δ de l'ensemble des solutions de

$$L\frac{\partial f}{\partial X_1} = 1, \quad \frac{\partial f}{\partial X_2} = \cdots = \frac{\partial f}{\partial X_n} = 0$$

Lieu critique du polynôme f :

$$\{y \in \mathbb{C}^n \mid \mathbf{grad}_y(f) = \mathbf{0}\}$$

$\mathfrak{d}$ la **somme des degrés des composantes de dimension positive** de ce lieu critique.

$$\delta \leq D^n - \mathfrak{d}$$

Taille de la sortie (fonctions distance et projection)

- **Cas génériques :** Le lieu critique de f est zéro-dimensionnel.

  Fonction distance Ce qu'on sait prouver : D^n

  Constat expérimental $D + D(D-1) + D(D-1)^2 + \cdots + D(D-1)^{n-1}$

  Fonctions de projection

  $D + D(D-1) + D(D-1)^2 + \cdots + D(D-1)^{n-1}$

- **Cas non génériques :** Le lieu critique de f est de dimension positive

  Soit $\mathfrak{d}_i$ la somme des degrés des composantes de dimension positive du lieu critique de f intersecté avec i hyperplans.

  Fonction distance $D^n - \mathfrak{d}_0$

  Fonctions de projection

  $$D + (D(D-1) - \mathfrak{d}_{n-2}) + \big(D(D-1)^2 - \mathfrak{d}_{n-3}\big) + \cdots + \big(D(D-1)^{n-1} - \mathfrak{d}_0\big)$$

Perspectives

- **Généralisation au cas des systèmes polynomiaux**
  - Bornes sur le nombre de composantes connexes.
  - Stratégie récursive sur le lieu singulier : borner finement les degrés des variétés intermédiaires.
  - Structure du système de Lagrange à utiliser dans les algorithmes d'élimination (avec Bardet, Trébuchet, Schost).
- **Système d'équations et d'inégalités polynomiales**
  - Singularités à l'infini des applications polynomiales
  - Gestion d'une seule inégalité ou inéquation (S. 04)
  - Passage au cas général.
- **Cartes routières**
  - Algorithmes inspirés de la stratégie de Canny : $D^{\mathcal{O}(n^2)}$
  - Obtenir une complexité en $D^{\mathcal{O}(n)}$ (reséaux de silhouettes) ?
  - Gérer les singularités de manière similaire à ce que je viens d'exposer.