Aspects conceptuels dans la résolution du probléme 17-ième de Smale: complexité, probabilité, équations polynomiales et géométrie intégrale. *

Luis M. Pardo
Universidad de Cantabria

March 18, 2007

*ALGO, Mars 2007

La Liste de Smale

Une liste avec 18 problèmes pour le XXIe siècle, dont....

Problem 1: The Riemann Hypothesis

Problem 2: The Poincaré Conjecture (Perelman)

Problem 3: Does P = NP ?

Problem 4: Integer Zeros of a Polynomial.

Problem 5: Height Bounds for diophantine curves.

...

Problem 9: The Linear Programming Problem.

...

Problem 14: The Lorentz Attractor Problem. (Tucker, 02)

Le Problème 17.

Can a zero of n complex polynomial equations in n unknowns be found approximately on the average, in polynomial time with a uniform algorithm?.

(Beltrán-P. , 06)

Historique du sujet

19-ième siècle: La Théorie de l'Élimination moderne
Bézout, Cayley, Hilbert † *Kronecker, Sturm, Sylvester*

1900–1930: *Macaulay, König,...*

1930–1965: Evanouissement

1965–: Les ordres monomiales et les bases standard–Gröbner *Hironaka, Buchberger,...,...*

1995–: Les méthodes intrinsèques adaptables aux structures des données *TERA, KRONECKER ....Pour citer seulement les locaux: Bostan, Durvye, Giusti, Lecerf, Salvy, Schost,....*

†Malgré lui même.

Une version simplifiée du sujet

But: *Algorithmique Efficace des Problèmes donnés par des équations polynomiales*

Applications (Potentielles): ‡ Information Theory (Codes, Cryptographie,...), Théorie des Jeux, Graphic and Mechanical Design, Chimie, Robotique, ...

Le Problème: Efficacité

Rk. *La plûpart des algorithmes de Théorie de l'Élimination necessitent un temps exponentiel dans le nombres des variables:*

Intractable pour les Applications.

‡Many of them Casual but not Causal

Résoudre?

Input: Une liste de polynômes multivariés: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$.

Output: Une description de la variété des solutions:
$V(f_1, \ldots, f_s) := \{x \in \mathbb{C}^n \ : \ f_i(x) = 0 \ldots\}$.

Description: Le type de description qu'on a choisi est determiné (et determine) le type des questions sur $V(f_1, \ldots, f_s)$ qu'on peut répondre.

Exemple:
Calcul Formel $\longrightarrow$ questions autour des quantificateurs

Hilbert's Nulltellensatz (HN) *Étant donnée une liste* $f_1, \ldots, f_s$ *decider si:*

$$\exists x \in \mathbb{C}^n \ \ f_i(x) = 0, \ \ 1 \leq i \leq s.$$

Differents Écoles

Syntactiques Bases standard, de Gröbner, rewriting et assimilés...La liste est trop longue

Structurels:Encadrement des problèmes dans des classes de complexité structurelle: P,NP, PSPACE,...

Semi–sémantiques: Ils utilisent des objets combinatoires (dont semi-sémantiques) pour controler la complexité: l'école creuse (sparse): L'usage de l'environement de Sturmfels des idées de Bernstein. Kouchnirenko...

Sémantiques: Surtout le groupe TERA: *Cantabria (P., Morais, Montaña, Hägele,...); Polytechnique (Giusti, Bostan, Lecerf, Schost, Salvy...); * Buenos Aires (Heintz, Krick, Matera, Solerno, ...); Humboldt (Bank, Mbakop,Lehmann)*

Quelques Concepts sous-jaçantes

- Polynômes vus comme programs.

- Les objets sémantiques (variétés algèbriques) ont des valeurs "intrinsèques" que dominent (sûrement) la complexité.

Degré de V *([Heintz,83], [Vogel, 83], [Fulton, 81]) :♯ points d'intersection avec une variété affine linéaire générique.*

Hauteur de V:
Taille binaire des coefficients de la forme de Chow

* *Geometric Degree d'une suite de variétés:*

$$\delta(V_1, \ldots, V_r) := max\{deg(V_i) \ : \ 1 \leq i \leq r\}.$$

Un Énoncé

Theorem 1 *Il y a une machine de Turing avec probabilité d'erreur bornée et temps borné par un polynôme dans les quantités suivantes que réponds* **HN**

$$L\ \delta\ H,$$

où

L *la taille de l'entrée (pour n'importe quel structure des données usuelle),*

δ *est le degré géométrique d'une suite de deformations (Kronecker's deformation) and*

H *la hauteur de la derniére variété résolue.*

Exemples

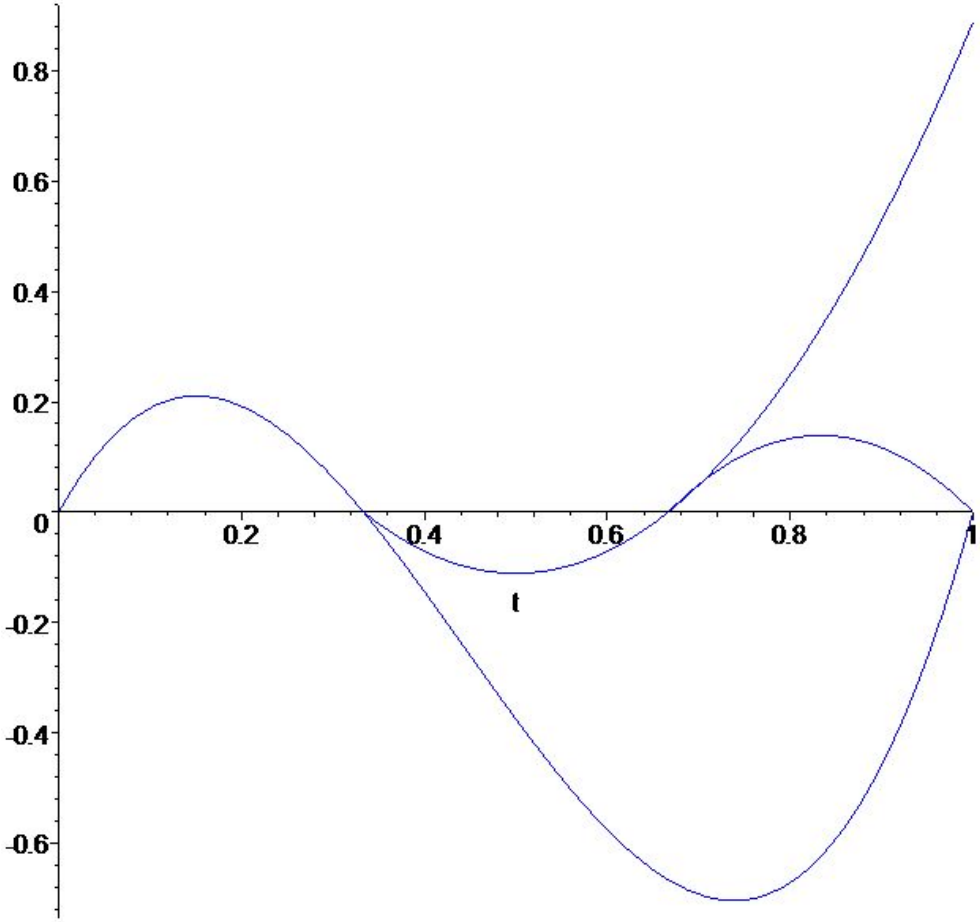
$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, k - \sum_{i=1}^{n} m_i X_i = 0.$$

$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, k - \sum_{i=1}^{n} 2^{i-1} X_i = 0.$$

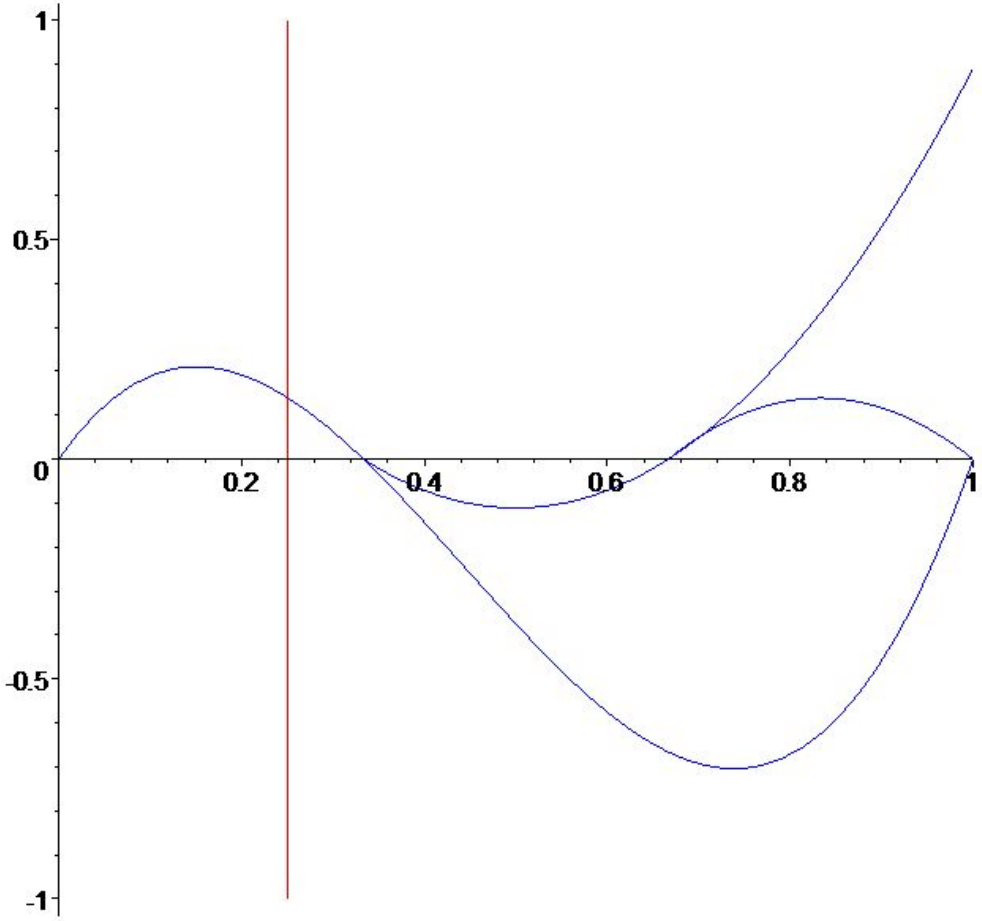
$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, 512 - \sum_{i=1}^{n} 2^{i-1} X_i = 0.$$

$$X_2^2 - X_1 = 0, X_3^2 - X_2 = 0 \ldots, X_n^2 - X_{n-1} = 0, k - X_n = 0.$$

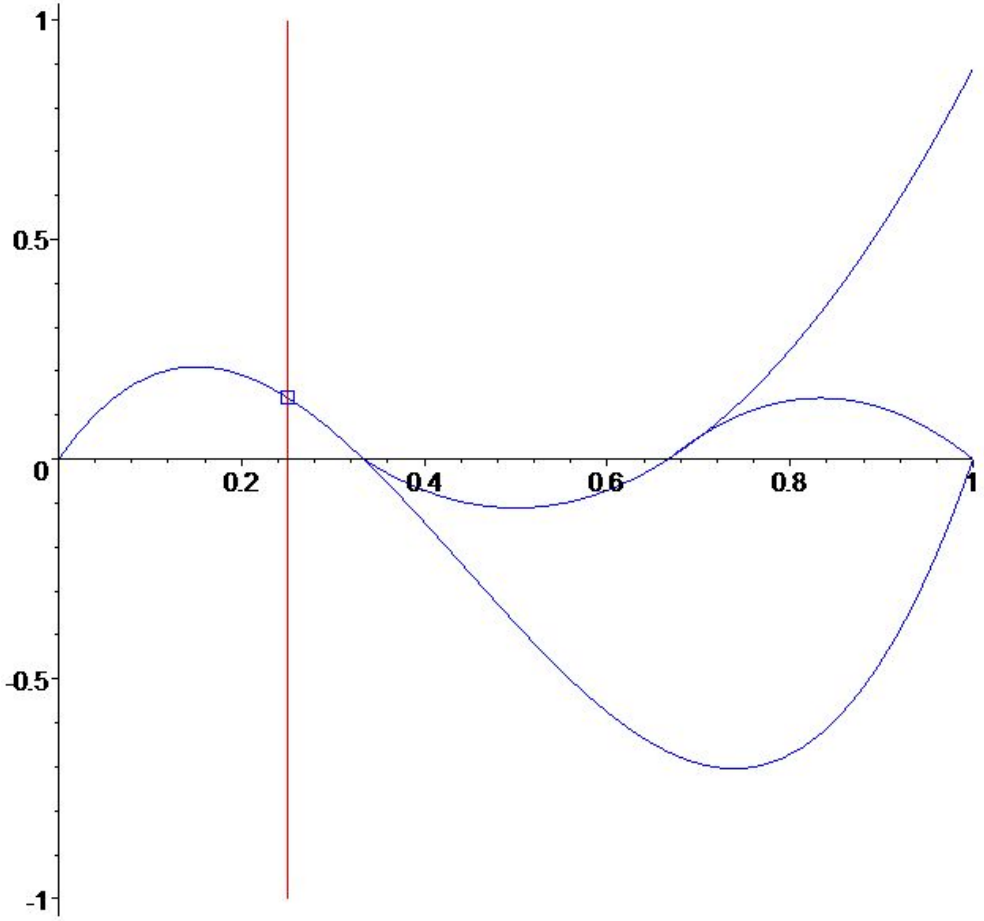
Kronecker's Deformation



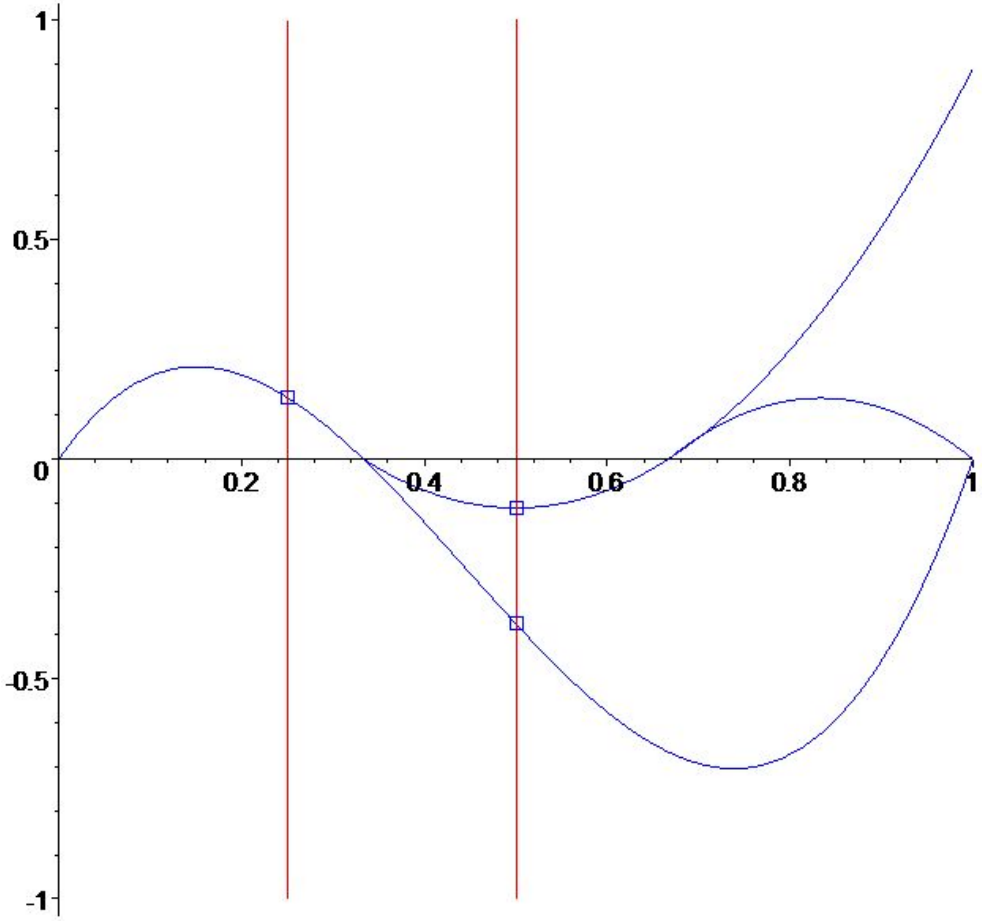
On commence à avancer



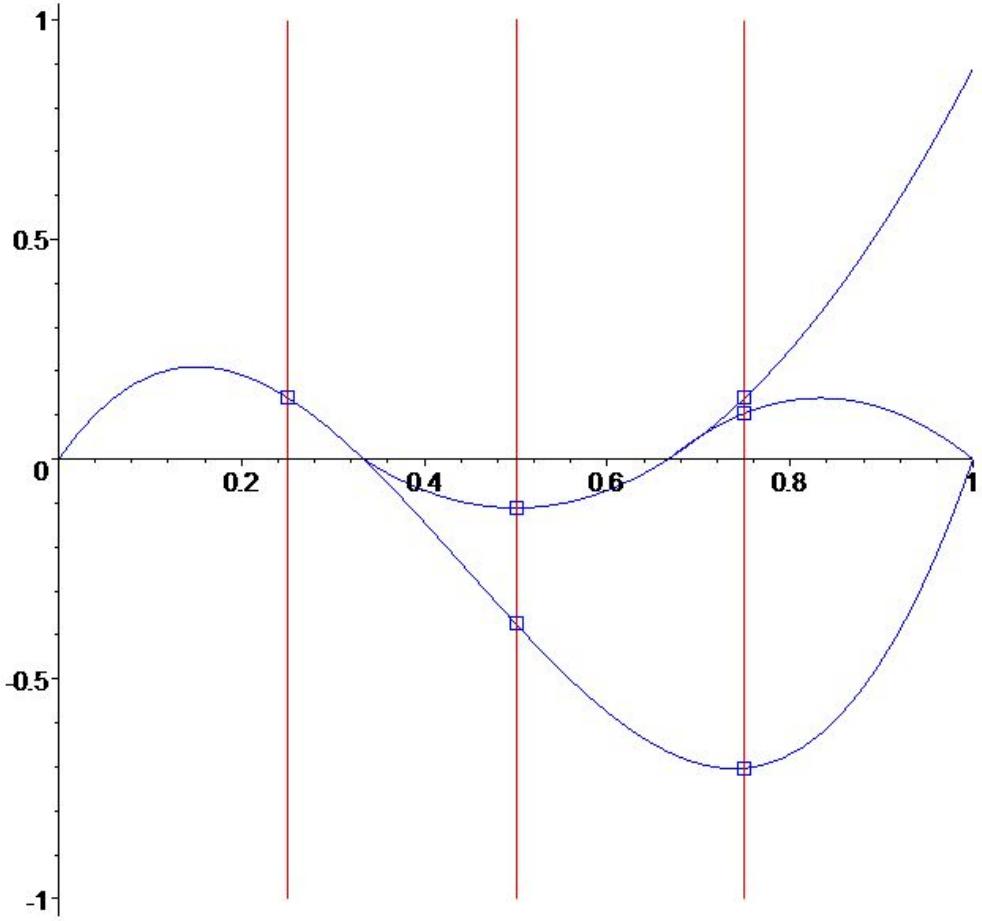
Une Lifting Fiber



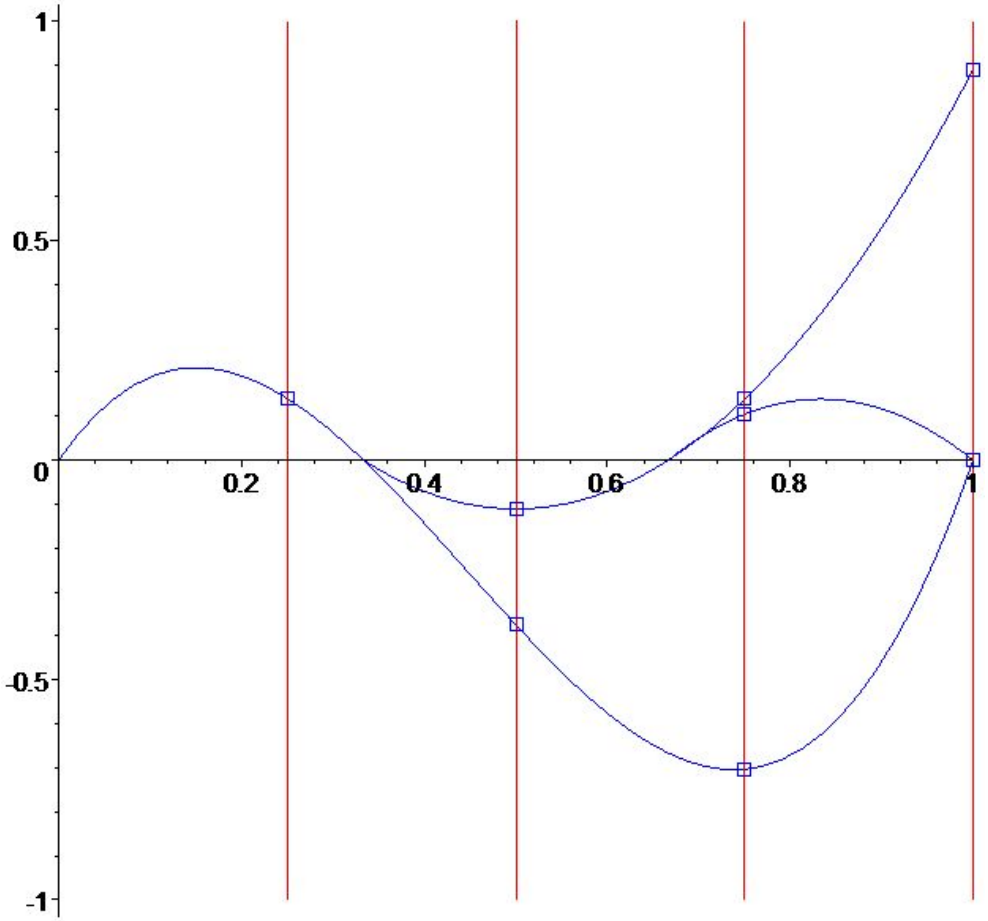
D'une fibre non–ramifiée à la suivante



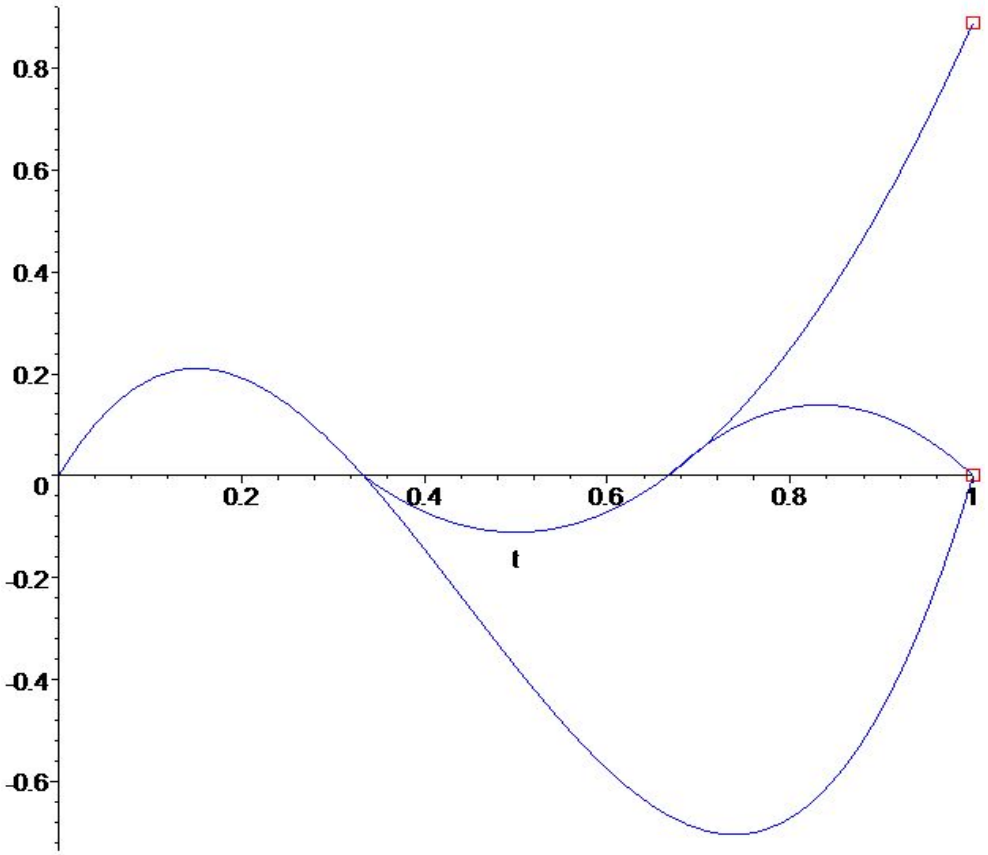
Et à la suivante



Jusqu'à Finir le chemin



Le résultat



Le résultat (II)

Comme ça on obtient:

Une description de la variété des solutions par un isomorphisme birationel, même biregulier dans le cas zero–dimensionel, qui suffit pour répondre aux questions d'élimination.

Mais...

C'est assez Optimal en termes d'éfficacité ?

Algorithms basés sur **une déformation**:
Une suite $V_1, \ldots, V_n$ *de variétés intermédiaires qu'il faut résoudre avant "éliminer"*

Résolution Universelle
Un algorithme est dit **Universel** *si son output contient assez d'information sur la variété des solutions pour répondre* **tous** *les questions d'élimination.*

Remark 2 *La plûpart des algorithmes d'élimination du calcul formel sont Universelles.*

Theorem [Castro-Giusti-Heintz-Matera-P.,2003]
Tous les méthodes d'élimination universels ont besoin d'un temps exponentiel pour finir ses calculs..

* *L'algorithme TERA est* **essentielement optimale.**
* *Le temps de calcul est plus grand que le* **Nombre de Bézout:**

$$\prod_{i=1}^{n} deg(f_i) \geq 2^n.$$

* *Aucun algorithme universel peut ameliorer cette borne exponentielle.*

À la recherche des algorithmes non–universels.

À la recherche des algorithmes capables d'obtenir information partielle de la variété des solutions en temps polynomial dans la taille de l'entrée.

Smale's 17th Problem

Quelques Idées Initiales

Qu'est-ce que c'est "Information Partielle"?

Qu'est-ce que c'est "Information Partielle"?

Par exemple, une "bonne approximation" à une des solutions

Qu'est-ce que c'est "Information Partielle"?

Par exemple, une "bonne approximation" á une des solutions

Exemple

INPUT: $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$ t.q. $\sharp V(f_1, \ldots, f_n) < \infty$.

OUPUT: $z \in \mathbb{Q}[i]^n$ tel qu'il existe $\zeta \in V(f_1, \ldots, f_n)$ vérif.

$$||\zeta - z|| < \varepsilon,$$

pour un bon ε.

Approximations?

Un peu d'élimination multivariée et un peu des algorithmes de réduction des reseaux (philosohie KLL) donnent

Theorem 3 (Castro-Hagele-Morais-P., 01) *Il existe une equivalence entre les informations suivantes:*

- *Une bonne approximation* $z \in \mathbb{Q}[i]^n$ *d'une des solutions* $\zeta \in V(f_1, \ldots, f_n)$,

- *Une description "á la Kronecker–TERA" du corps de classes residuelles de la solution* $\mathbb{Q}_\zeta$.

Theorem (cont.)

Le temps de calcul de cet algorithm (et la taille binaire de l'approximation) sont bornés par un quantité polynomial dans:

- D_ζ= *degré du corps de classes residuelles* $\mathbb{Q}_\zeta$.
- L= *taille de la descriptions des polynômes donnés.*
- H_ζ= *hauteur du corps de classes residuelles* $\mathbb{Q}_\zeta$.

Autremet dit, **une "bonne" approximation contient information utile et valable pour l'élimination**(quoique il n'est pas du tout claire s'il vaut la peine de l'utiliser de la manière habituelle)

Une Application Immediate

Theorem 4 *Il existe un algorithm que fait les calculs suivants:*

- Input: *Un polnôme univarié* $f \in \mathbb{Q}[T]$.

- Output: *Une description par un élement primitif du corps de décomposition de* f.

Tel que le temps de calcul est polynomiale dans les quantités suivantes:

$$d, h, \sharp Gal_{\mathbb{Q}}(f),$$

où d *est le degré de* f *et* h *la longueure binaire des coefficients de* f.

Remarque: Il s'agit d'un algorithme géometrique dont l complexité n'est pas de l'rodre $d!$ que quand c'est inévitable.

Une Bonne Approximation?

Pour simplicité des calculs, on travaille sur l'espace projective

Systémes d'équations données par des polynômes homogénes:

$$F := [f_1, \ldots, f_n] \in \mathcal{H}_{(d)},$$

$deg(f_i) = d_i$, $(d) := (d_1, \ldots, d_n)$,
$\mathcal{H}_{(d)} :=$ l'espace vectoriel de tous ces listes d'équations.

$$V_{\mathbb{IP}}(F) := \{x \in \mathbb{IP}_n(\mathbb{C}) \ : \ F(x) = 0\}.$$

L'Opérateur de Newton Projectif

(M. Shub amd S. Smale 1986–1996)

$$\pi \ : \mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_n(\mathbb{C})$$

Notations: *Metriques projetives :*

Riemannienne :

$$d_R(\pi(x), \pi(x')) := arccos\left(\frac{|\langle x, x'\rangle|}{\|x\|\|x'\|}\right).$$

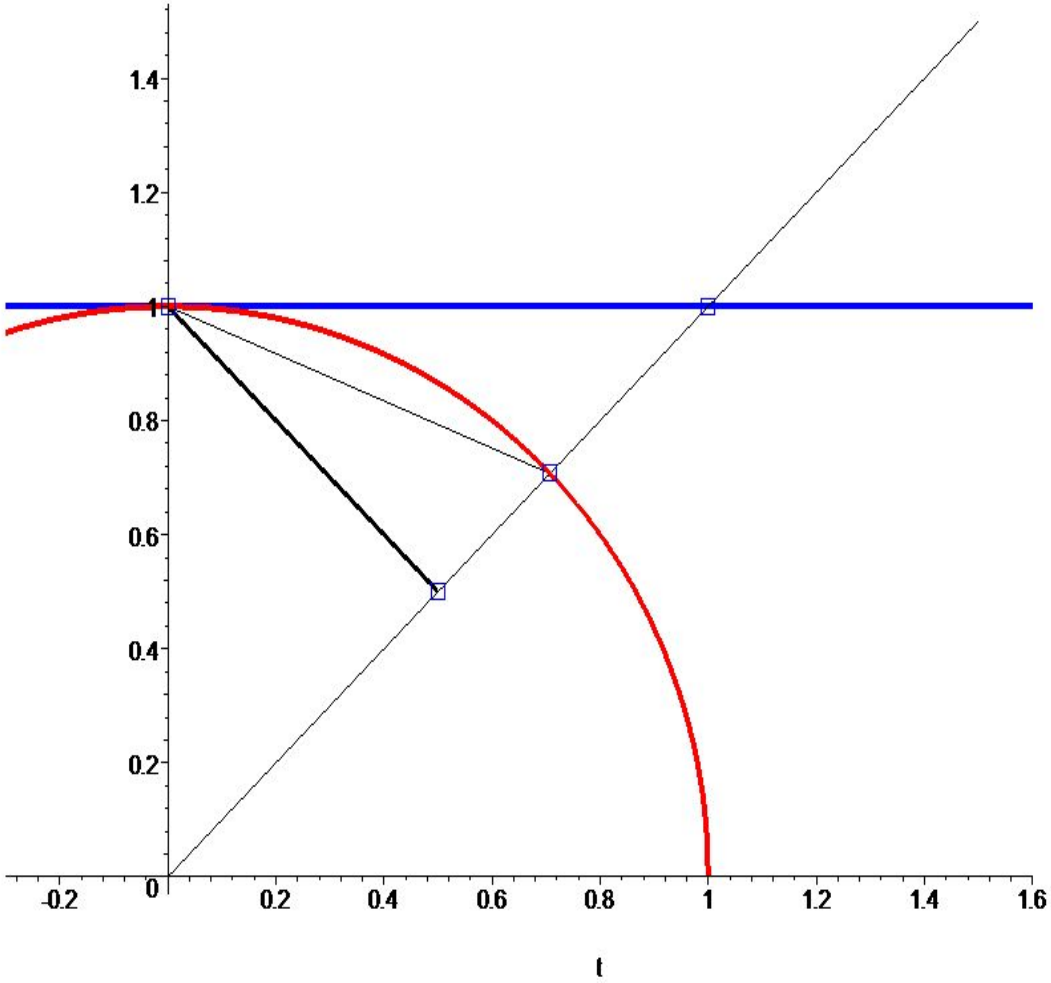
Fubini–Study :

$$d_P(\pi(x), \pi(x')) := sin\ d_R(\pi(x), \pi(x')).$$

Tangent Distance :

$$d_T(\pi(x), \pi(x')) := tand_R(\pi(x), \pi(x')).$$

Un Petit Dessin



L'Opérateur de Newton II

L'espace tangent á un point $z \in \mathbb{IP}_n(\mathbb{C})$:

$$T_z\mathbb{IP}_n(\mathbb{C}) := \{w \in \mathbb{C}^{n+1} \ : \ \langle w, z\rangle = 0\}.$$

Un système d'équations polynomiales $F := [f_1, \ldots, f_n]$, la matrix jacobienne :

$$DF(z) \ : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n.$$

Si z n'est pas un point critique, restriction á l'espace tangent:

$$T_z f := DF(z) \mid_{T_z} \ : T_z\mathbb{IP}_n(\mathbb{C}) \longrightarrow \mathbb{C}^n.$$

Dans ce cas là, l'inverse:

$$(T_z f)^{-1} \ : \mathbb{C}^n \longrightarrow \mathbb{C}^{n+1}.$$

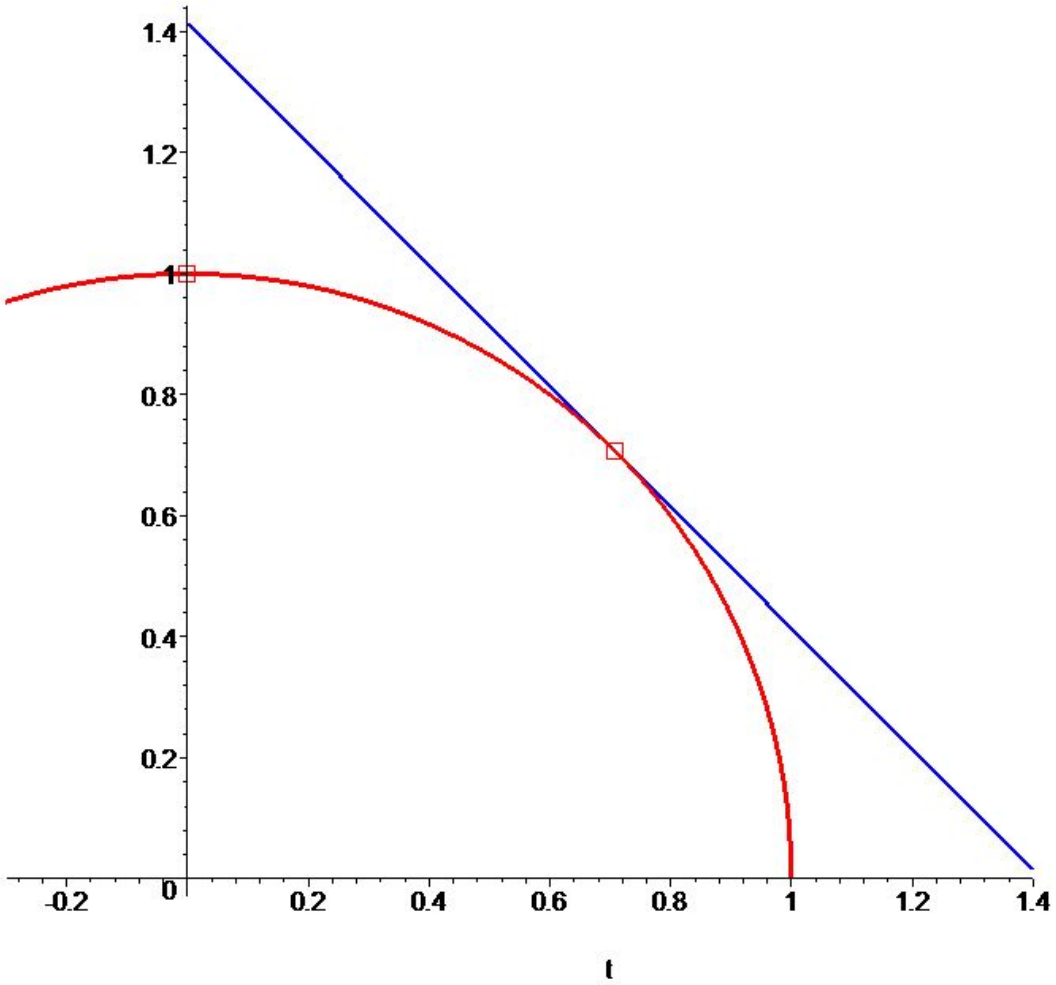
L'Opérateur de Newton III

La projection canonique $\pi : \mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_n(\mathbb{C})$.

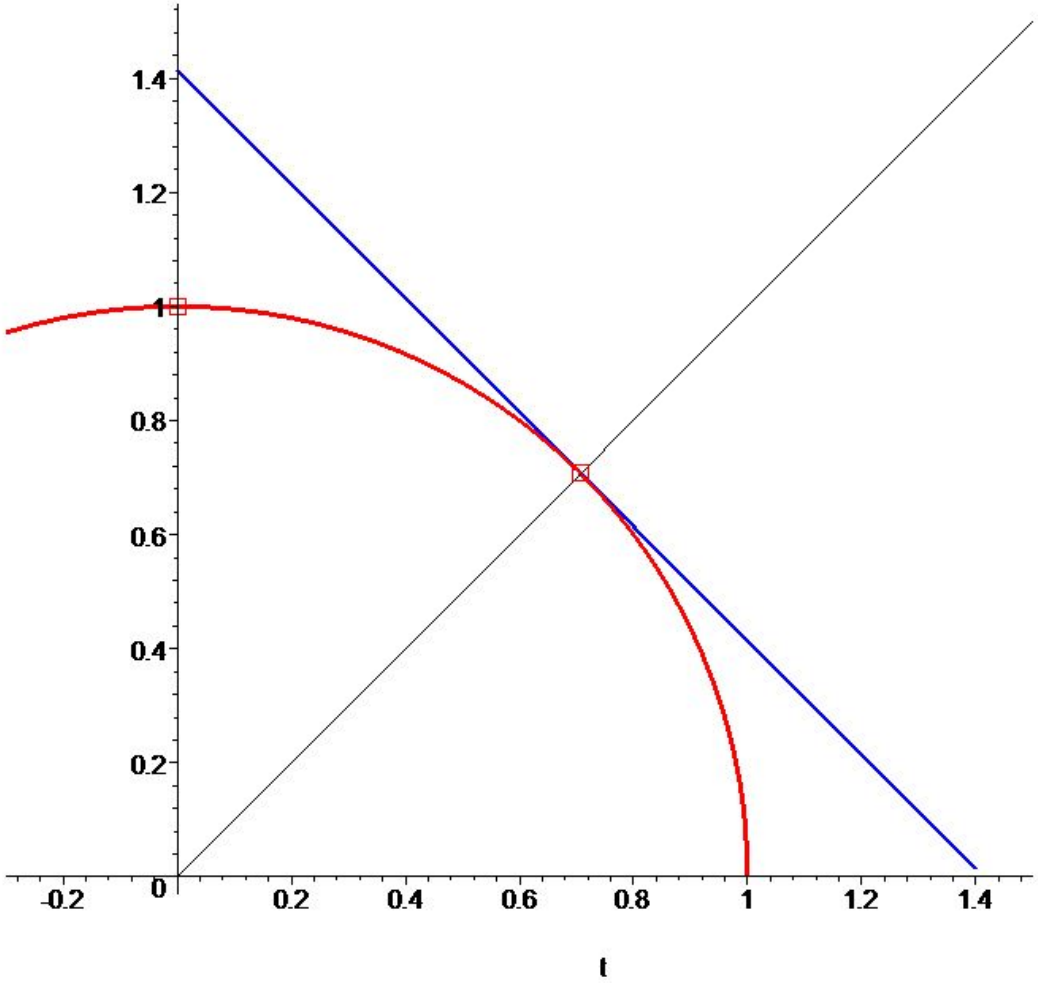
Pour chaque $\pi(z) \in \mathbb{P}_n(\mathbb{C})$ non critique l'opératuer de Newton par:

$$N_F(\pi(z)) := \pi\left(z - \left(DF(z)\mid_{T_z}\right)^{-1} F(z)\right),$$

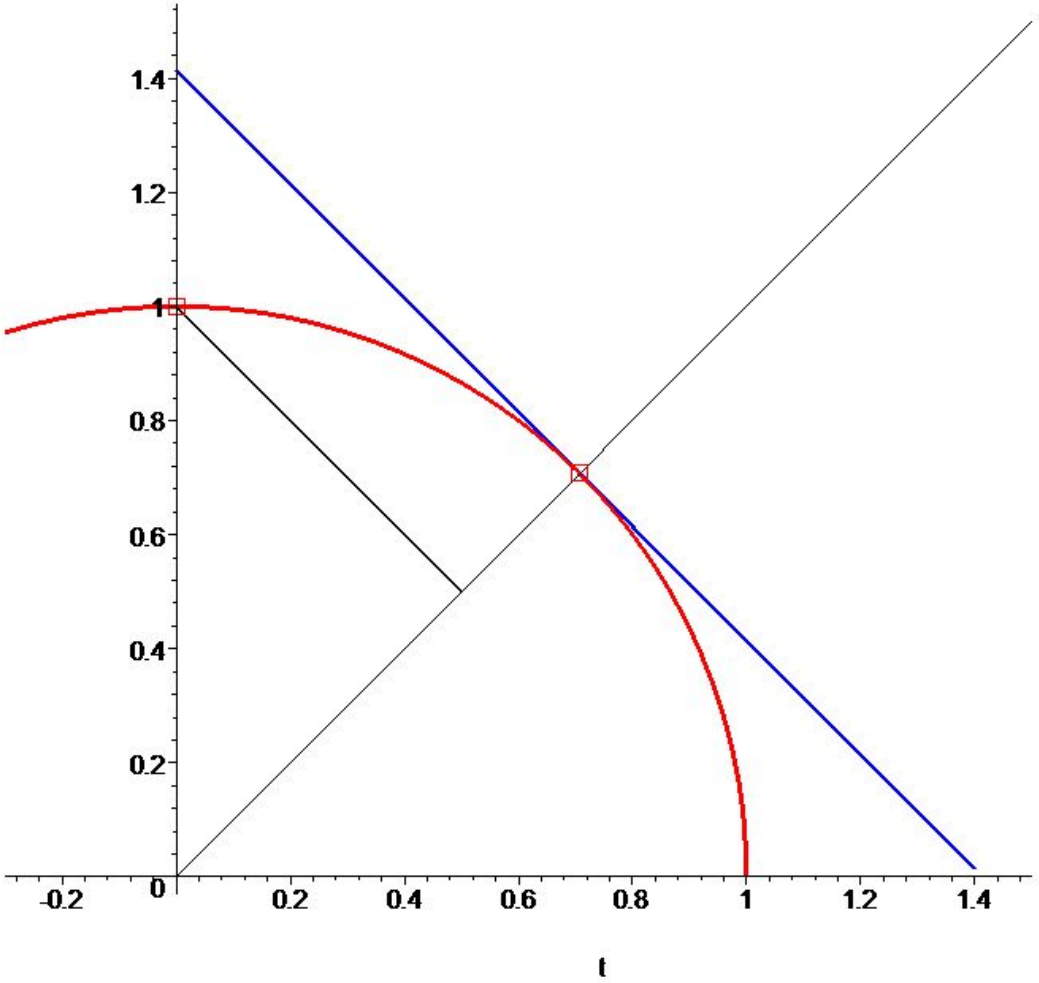
Dessiné



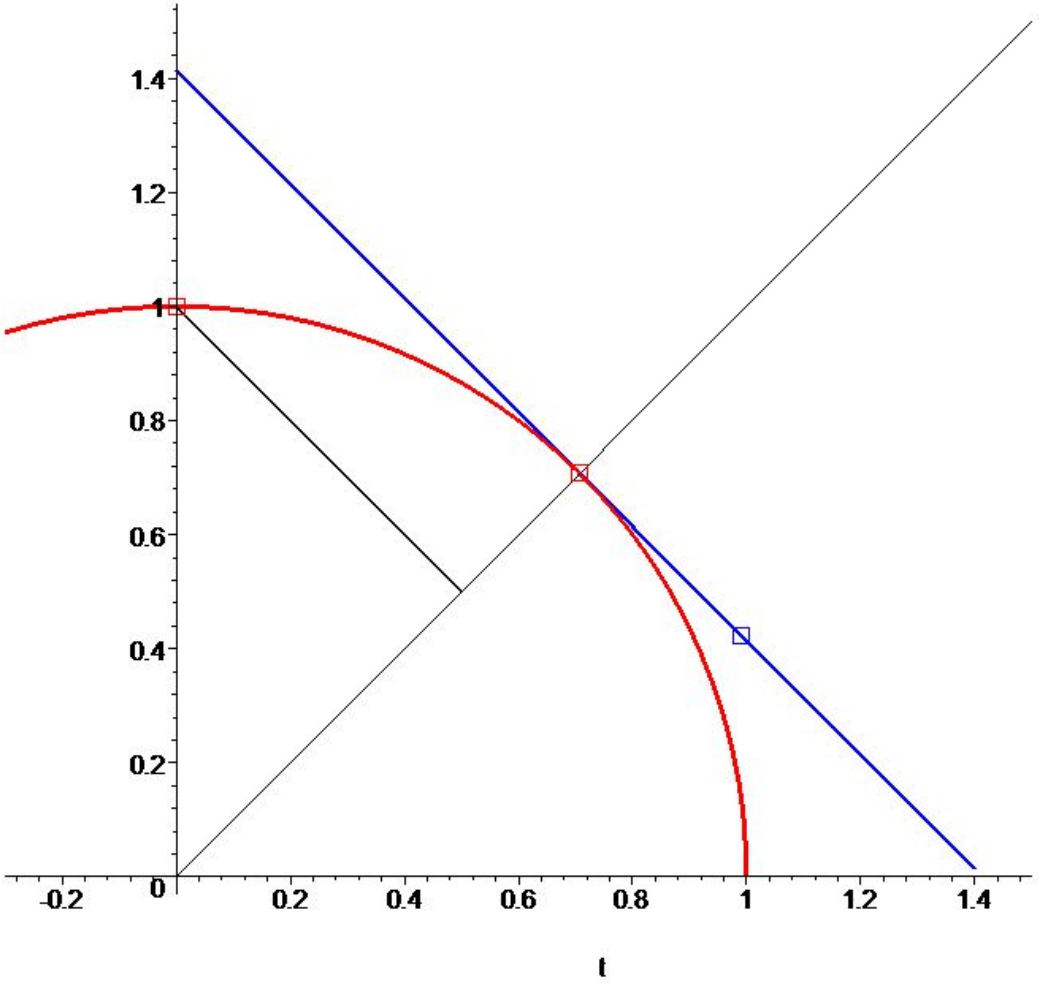
DESSINÉ



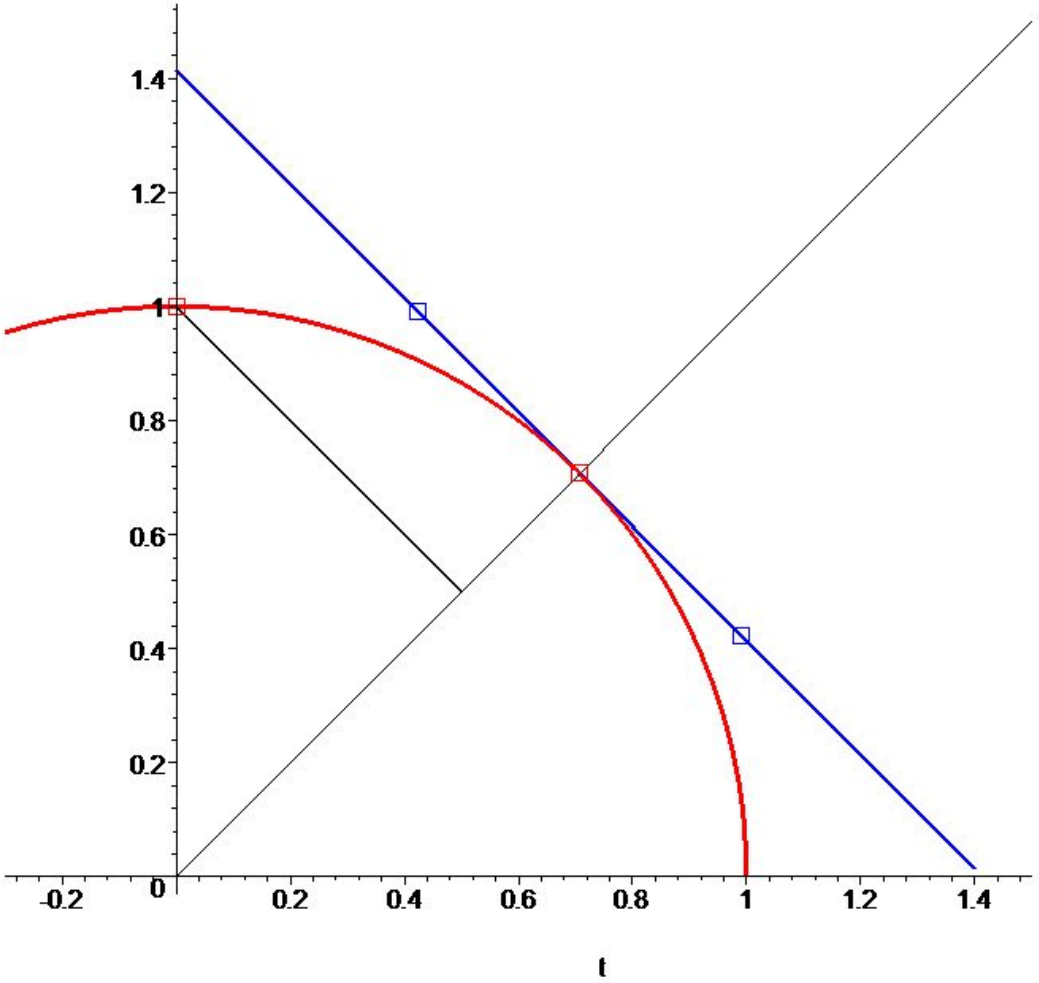
Dessiné



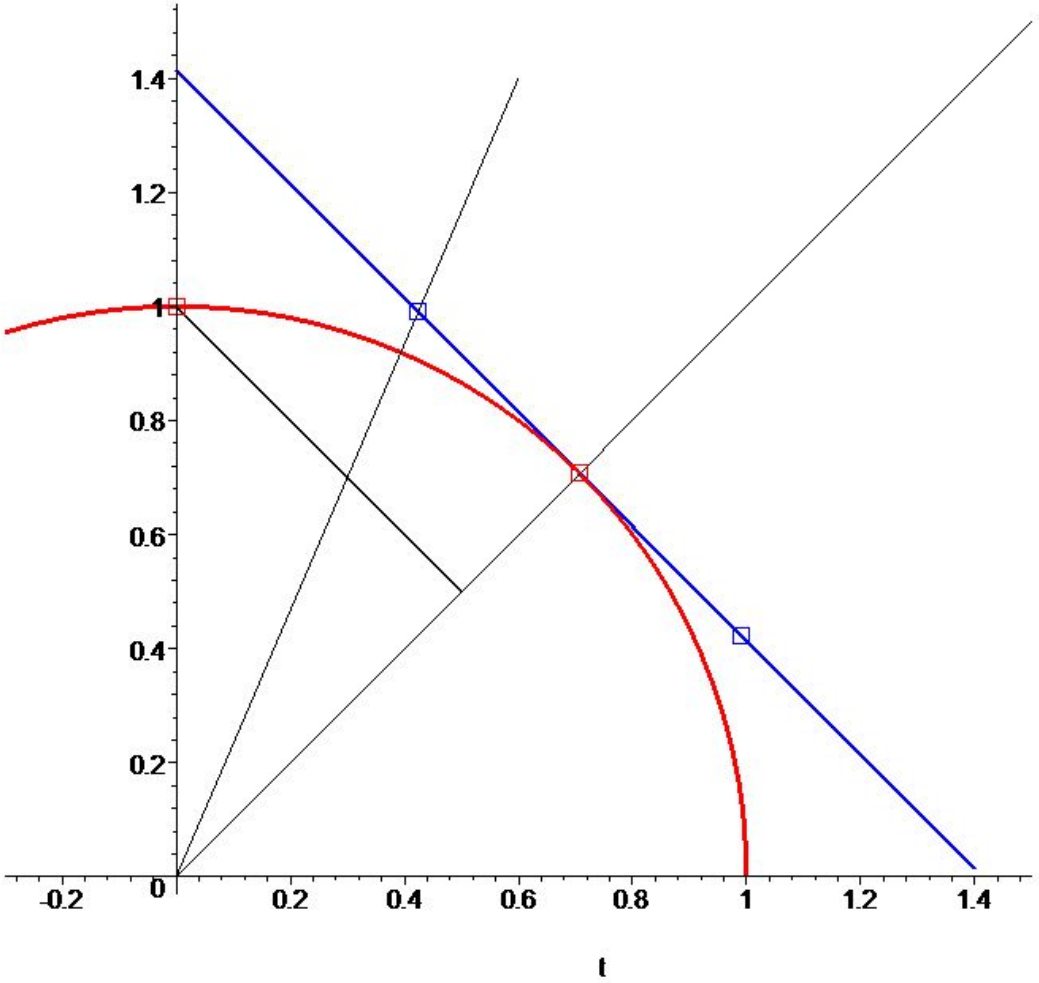
Dessiné



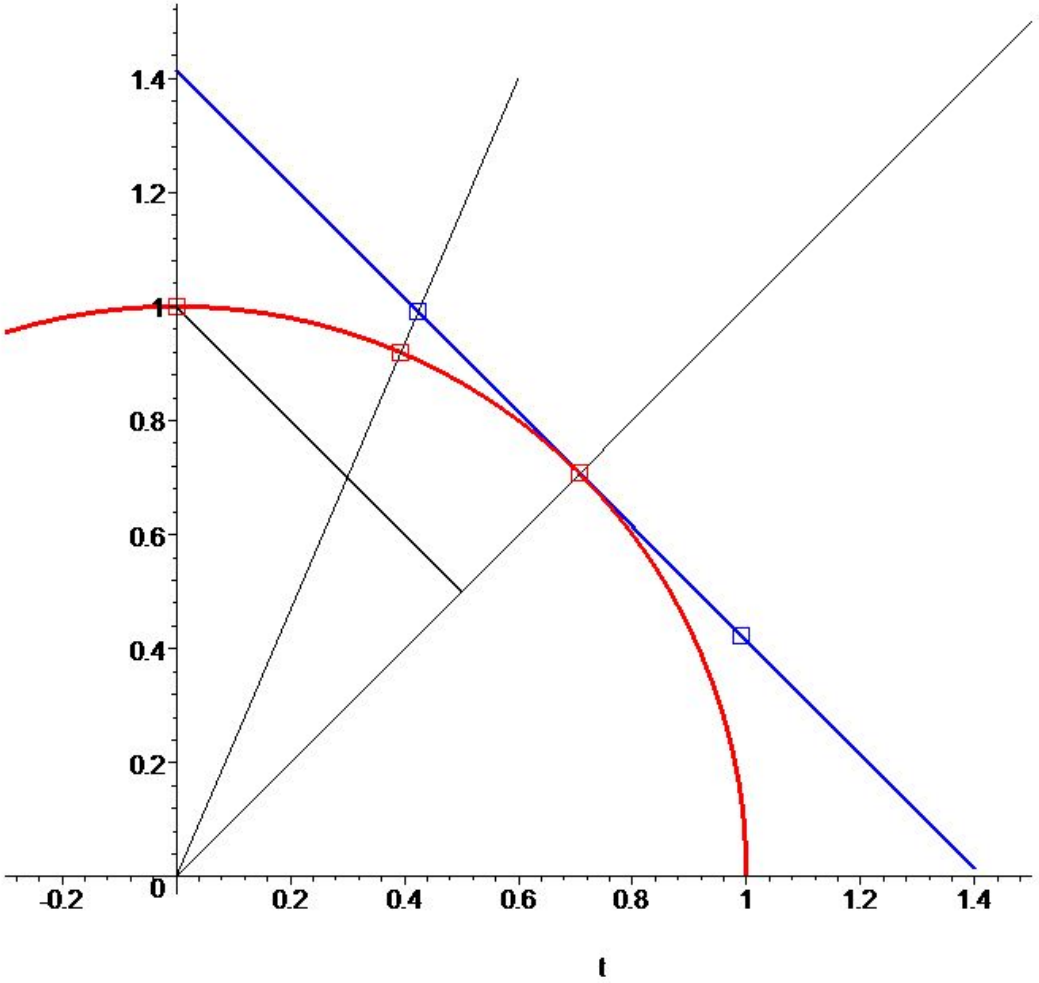
Dessiné



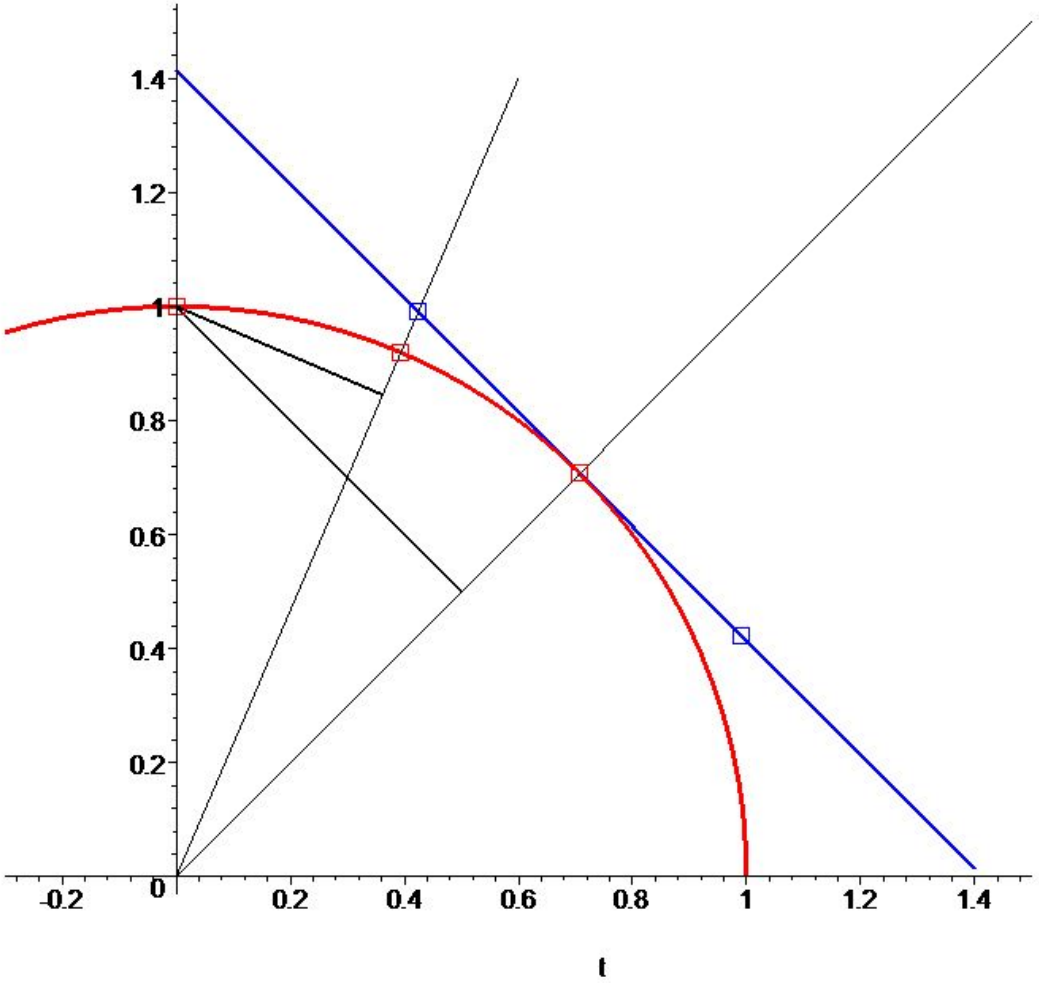
Dessiné



Dessiné



Dessiné



Les Zéros Approchés

* Input: *Un systéme d'équations homogénes*

$$F := [f_1, \ldots, f_n] \in \mathcal{H}_{(d)},$$

$deg(f_i) = d_i$, $(d) := (d_1, \ldots, d_n)$.

Un zéro $\zeta \in V(F)$

Un zéro approché(Smale'81) a point $z\mathbb{P}_n(\mathbb{C})$ tel que l'opérateur de Newton N_F appliqué a z converges trés rapidement vers le zéro.

$$d_T(N_F^k(z), \zeta) \leq \frac{1}{2^{2^{k-1}}}.$$

$d_T :=$ "distance" tangente.

Le Nombre de conditionement ([Shub–Smale, 86–96])

$$\mu_{norm}(F,\zeta) := \|F\|\|T_zF^{-1}\Delta(\|\zeta^{d_i-1}\|d_i^{1/2})\|.$$

Condition Number Theorem : *Variété discriminant dans* $\mathbb{IP}(\mathcal{H}_{(d)})$.

$$\Sigma_\zeta := \{F \in \mathbb{IP}(\mathcal{H}_{(d)}) \ : \ \zeta \in V(F), T_\zeta F \notin GL(n,\mathbb{C})\}.$$

$$\Sigma := \bigcup_{\zeta \in \mathbb{IP}_n(\mathbb{C})} \Sigma_\zeta. \quad \text{(Systèmes avec un zéro singulier).}$$

Distance dans la fibre : $\rho(F,\zeta) := d_P(F,\Sigma_\zeta)$.

Theorem 5 (Shub-Smale, 91)

$$\mu_{norm}(F,\zeta) := \frac{1}{\rho(F,\zeta)}.$$

$$d := \max\{d_i \ : \ 1 \leq i \leq n\}.$$

La Quantité :

$$\gamma_0(F,\zeta) \leq d^{\frac{3}{2}}\mu_{norm}(F,\zeta).$$

Theorem 6 (Smale,81) *Si :*

$$d_T(z,\zeta) \leq \frac{3-\sqrt{7}}{\gamma_0(F,\zeta)},$$

alors, z est un zéro approché du zéro ζ du système F.

Algorithme Non–Universel

* Input:
Un Systéme $F \in \mathbb{IP}(\mathcal{H}_{(d)})$,

* Output:
Solution Universelle: **Un *Zéro Approché* z pour chaque zéro** $\zeta \in V(F)$.

Borne Inférieure Inévitable: Nombre de Bézout ($\mathcal{D} := \prod_{i=1}^{n} d_i$) **$\Rightarrow$ Intractable**

Ou bien:
Solution Non-Universelle : **Un *Zéro Approché* z pour quelqu'un des zéros** $\zeta \in V(F)$.

Complexité du calcul d'une Solution Non–Universelle? (= Problème 17 de Smale)

Déformation Homotopique (HD)

Variété d'Incidence:

$$V := \{(F, \zeta) \in \mathbb{IP}(\mathcal{H}_{(d)} \times \mathbb{IP}_n(\mathbb{C}) \ : \ f(\zeta) = 0\}.$$

Deux Projections Canoniques:

$$\begin{array}{ccccc} & & V & & \\ & \swarrow^{\pi_1} & & \searrow^{\pi_2} & \\ \mathbb{IP}(\mathcal{H}_{(d)}) & & & & \mathbb{IP}_n(\mathbb{C}) \end{array}$$

L'Ensemble des valeurs critiques de π_1=Σ.

En particulier, la suivante est une "covering map":

$$\pi_1 : V \setminus \Sigma' \longrightarrow \mathbb{IP}(\mathcal{H}_{(d)}) \setminus \Sigma.$$

Et la codimension réelle: $codim_{\mathbb{IP}(\mathcal{H}_{(d)})}(\Sigma) \geq 2$.

Autrement Dit

Sauf un emsemble de mesure nulle, étant donnés $F, G \in \mathbb{IP}(\mathcal{H}_{(d)}) \setminus \Sigma$, :

$$[F, G] \cap \Sigma = \emptyset,$$

où

$$[F, G] := \{(1-t)F + tG, \quad t \in [0, 1]\}.$$

et le suivant est aussi un "covering space":

$$\pi_1 : \pi_1^{-1}([F, G]) \longrightarrow [F, G].$$

Autrement dit, pour chaque $\zeta \in V(G)$ on a une courbe:

$$\Gamma := \{(F_t, \zeta_t) \in V \ : \ \zeta_t \in V(F_t), t \in [0, 1]\}.$$

Une philosophie Algorithmique

L'idée est commencer par (G, ζ) $(t = 1)$et suivre (par des applications de l'opérateur de Newton projectif) un chemin polygonale proche de Γ jusqu'obtenir une zéro approché de F.

Input $F \in \mathcal{H}_{(d)}$

Avec pair initiel

$$(G, \zeta) \in \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C}), \;\; G(\zeta) = 0.$$

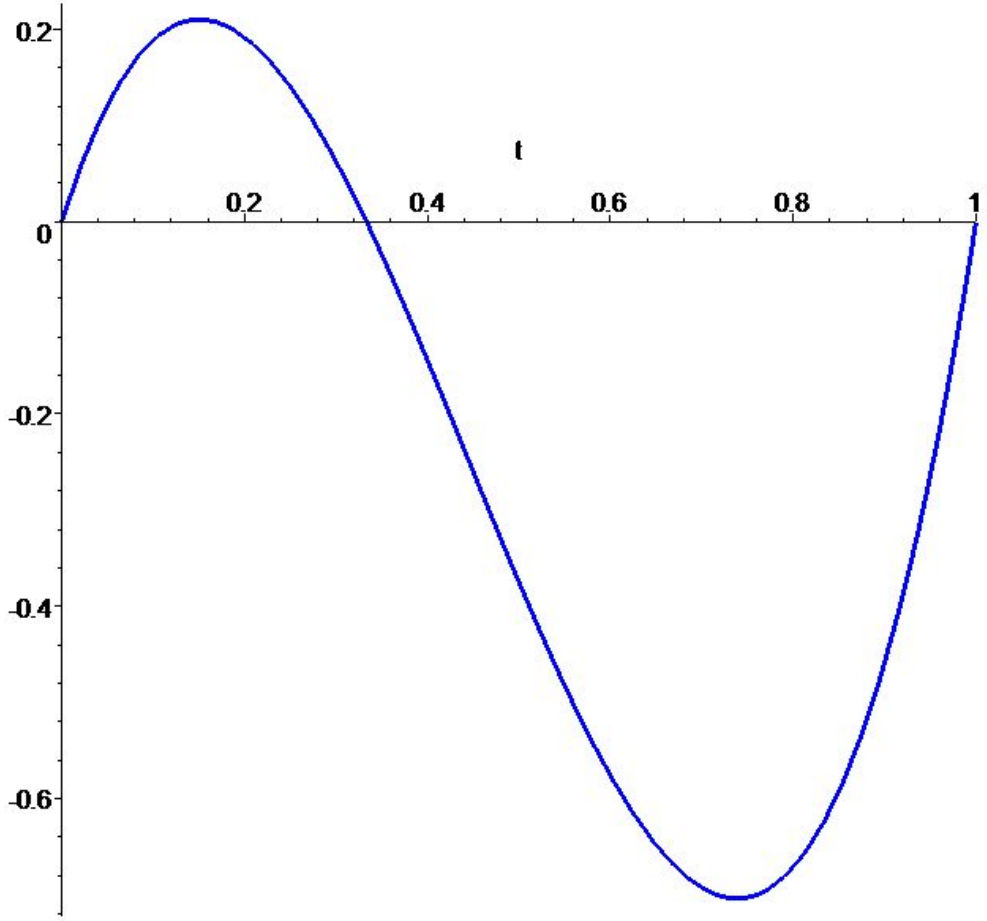
Suivant [F,G] et la courbe Γ

Output

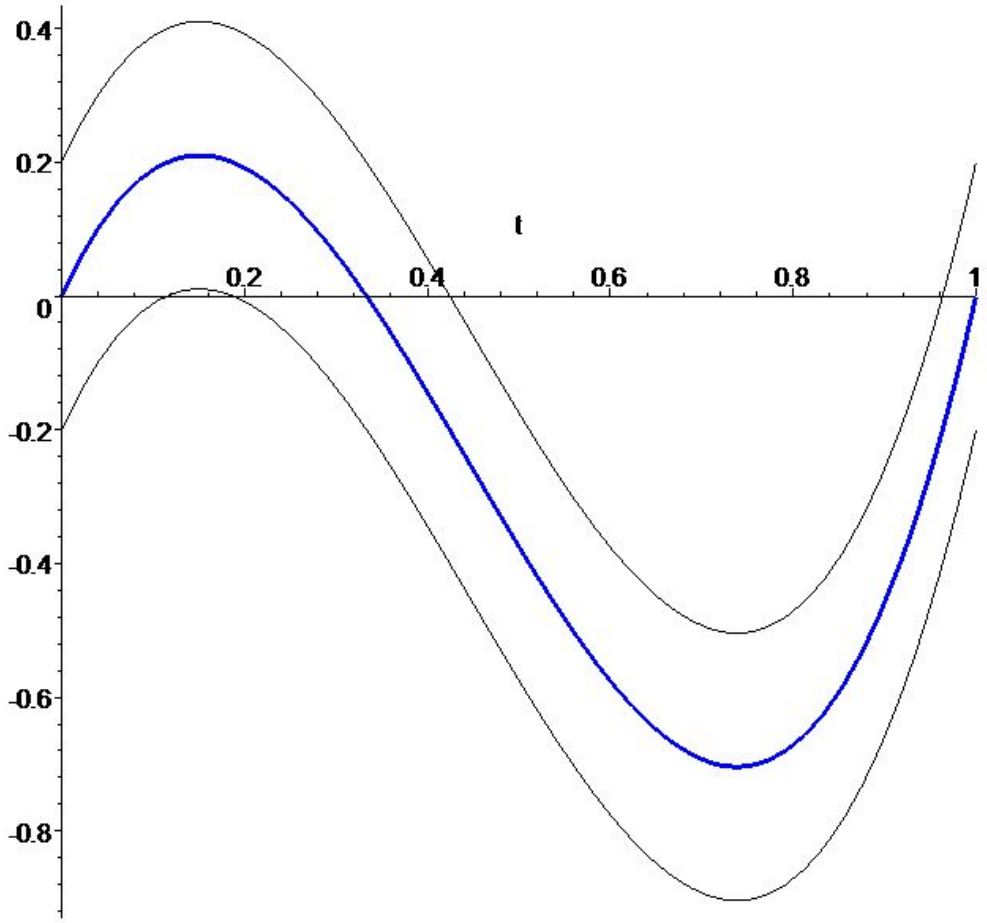
-- *Soit ERREUR*

-- *Soit un zéro approché* $z \in \mathbb{P}_n(\mathbb{C})$ *d'un zero* $\zeta \in \mathbb{P}_n(\mathbb{C})$ *de* $F \in \mathcal{H}_{(d)}$

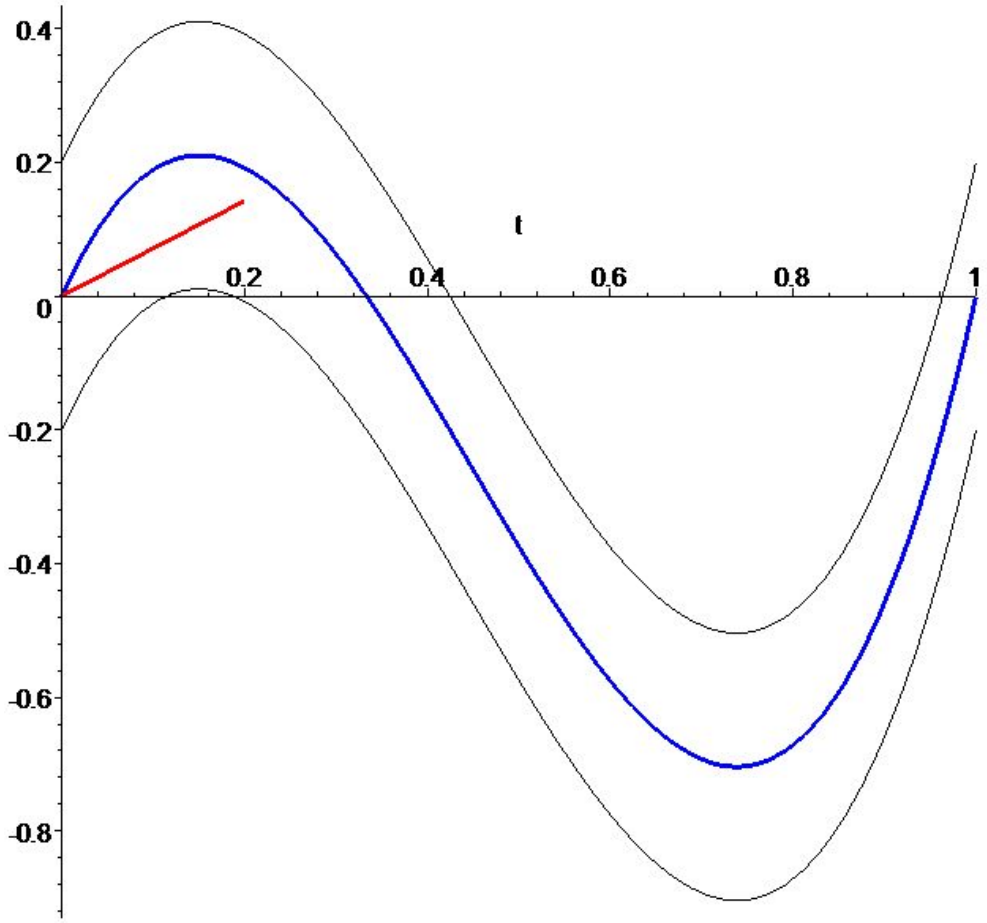
Dessins



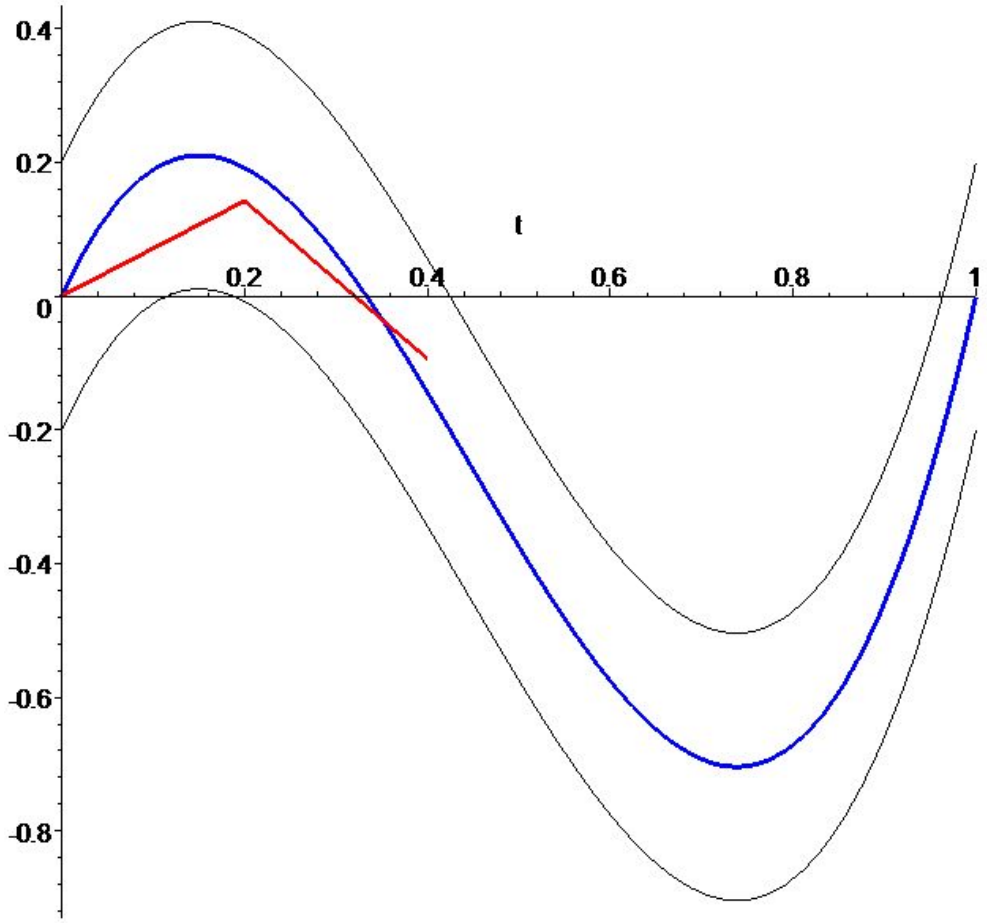
Dessins



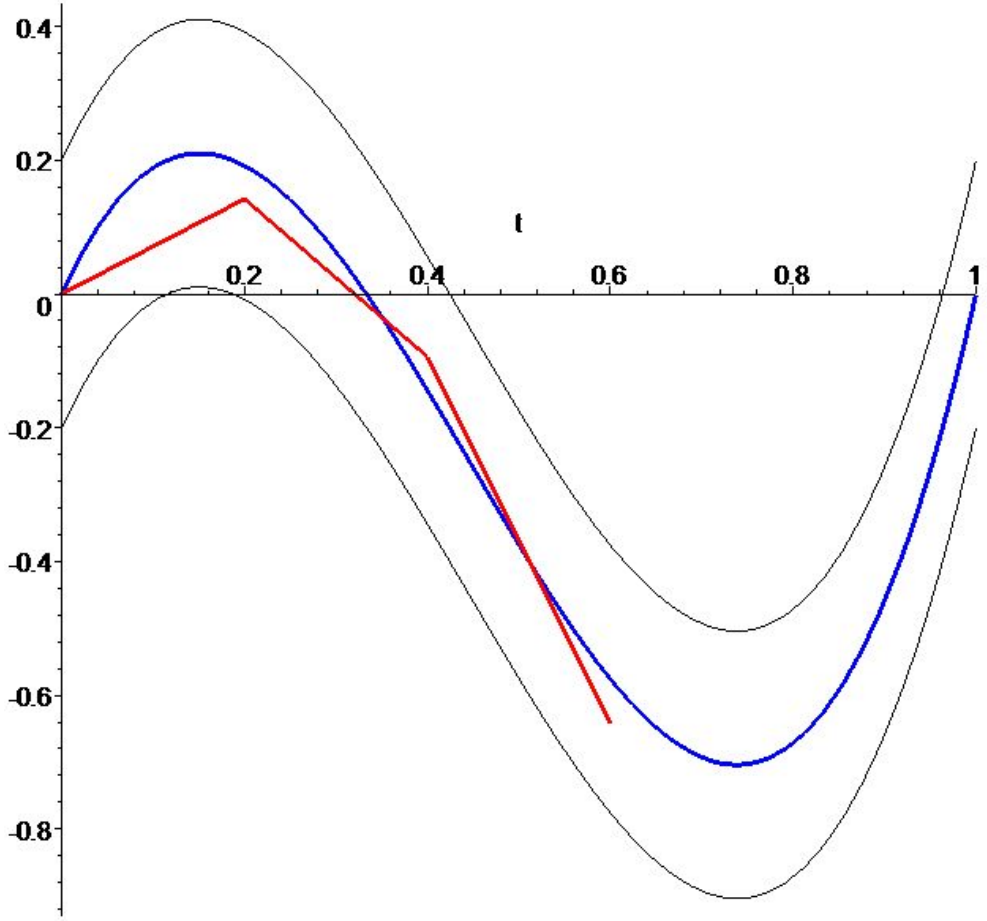
Dessins



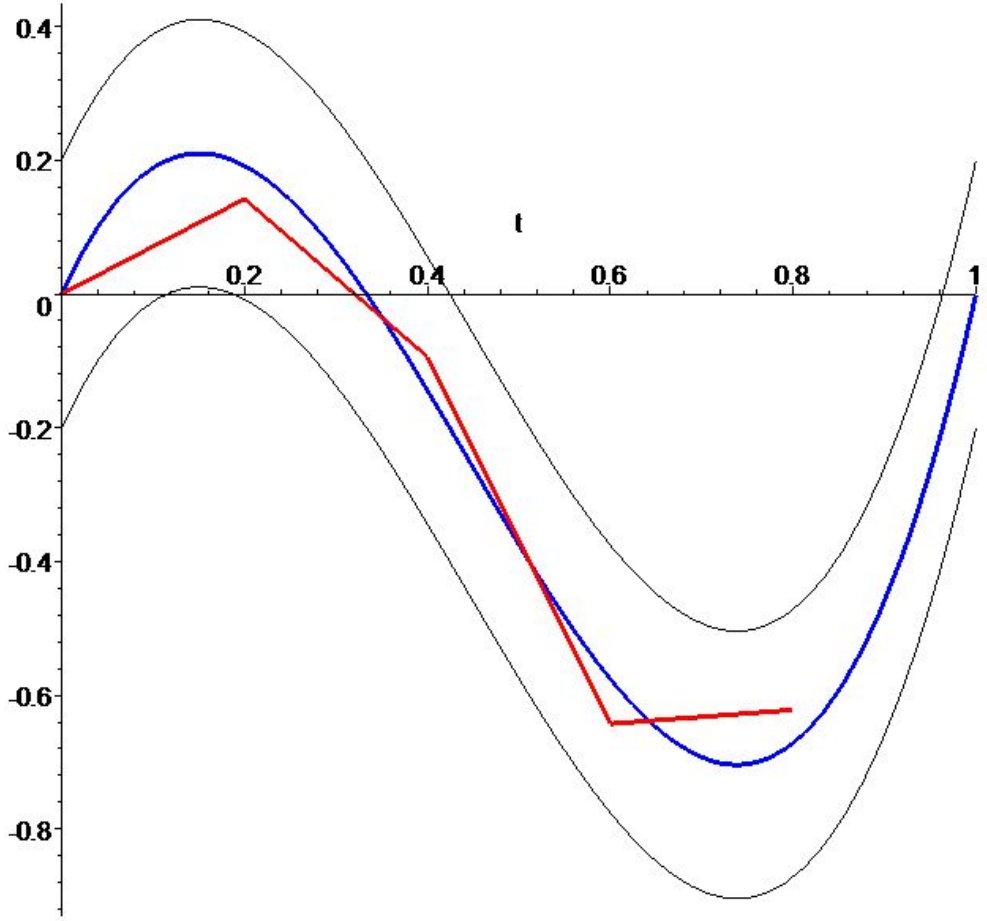
Dessins



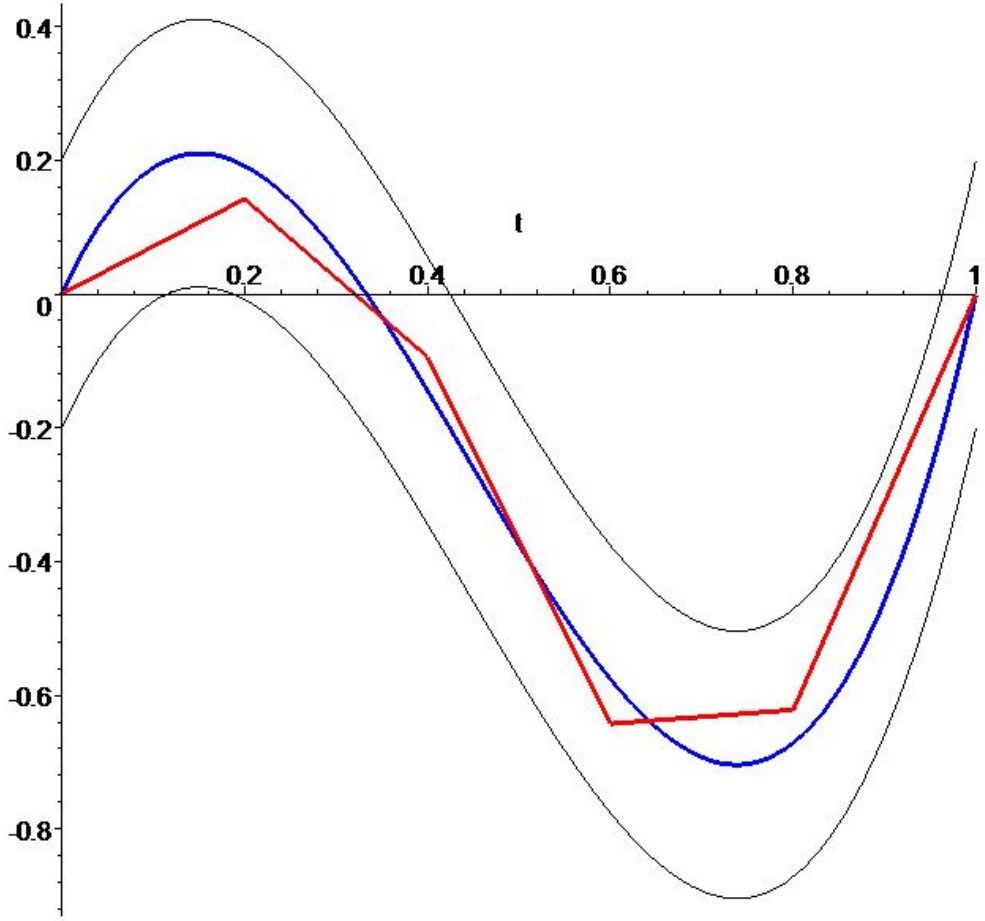
Dessins



Dessins



Dessins



Problème 1.- *Quelle est la complexité de ce méthode?*

Réponse.–

– La complexité d'un pas est polynomiale dans le nombre des variables et dans la complexité dévaluation des polynômes donnés. Donc, la complexité dépend plutôt du nombre des pas d'homotopie.

– Le nombre des "pas d'homotopie" (dans le cas projectif) est borné par $O(\mu_{norm}(\Gamma)^2)$ ([Shub-Smale, 91]), où

$$\mu_{norm}(\Gamma) := max\{\mu_{norm}(F_t, \zeta_t) \ : \ (F_t, \zeta_t) \in \Gamma\}.$$

Problème 2.- *La complexité du cas pire est doublement exponentielle dans le nombre des variables (voir exemple dans [castro–Hagele–Morais–P., 01]), alors que peut-on espérer?*

Réponse.–

– La complexité du cas pire ne suffit pas, il faut penser en complexité en moyenne.

– La moyenne oblige á avoir une distribution de probabilité dans l'espace des données. *Laquelle?.*

Réponse (Sous-problème 2b).–
– L'ensemble $\mathbb{IP}(\mathcal{H}_{(d)})$ est une veriété Riemannienne complexe et compacte. Donc, elle a une mesure associé (une forme de volume $d\nu_{\mathbb{IP}}$) telle que le volume $\nu_{\mathbb{IP}}[\mathbb{IP}(\mathcal{H}_{(d)}]$ est fini. On a donc une façon naturelle de definir une probabilité dans l'espace des entrées .

– La probabilité dans $\mathbb{IP}(\mathcal{H}_{(d)})$ est, essentiellement, equivalente á la distributione Guassienne dans l'espace affine $\mathcal{H}_{(d)}$.

Sous–problème 2c.–*Puis que la computation est discréte, cette probabilité a une interpretation naturelle quand les entrées sont des véritables entrées d'un algorithm (c. à d. coefficients dans un corps discret)?.*

Problème 3.–*En tout cas, cette philosophie n'est pas un algorithme. Est-ce qu'il existe un véritable algorithme et quelle est sa complexité en moyenne?.*

Réponses.–

1.– Oui.

2.- Polynomial dans la dimension de l'espace des entrées.

De nouveau HD

Input $F \in \mathcal{H}_{(d)}$

Appliquer la déformation homotopique (HD) *avec pair initial*

$$(G, \zeta) \in \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C})$$

suivant la composante Γ_z *de la courbe* $\Gamma = \pi_1^{-1}([F, g]))$ *qui contient* (G, z).

Output:

– *ERREUR*

– *où un zéro approché de* F.

HD avec resources bornés par une fonction $\varphi(f, \varepsilon)$.

INPUT $F \in \mathcal{H}_{(d)}$, $\varepsilon > 0$

Faire $\varphi(f, \varepsilon)$ étapes dans la déformation homotopique (HD) *avec pair initial*

$$(G, \zeta) \in \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C})$$

suivant la composante Γ_z *de la courbe* $\Gamma = \pi_1^{-1}([F, g]))$ *qui contient* (G, z).

OUTPUT:

– *ERREUR*

– *où un zéro approché de* F.

Pairs Initiales $\varepsilon-$efficients

Définition *Un pair $(G, \zeta) \in V$ est $\varepsilon-$efficient si avec la borne de ressources:*

$$\varphi(f, \varepsilon) := 10^5 n^5 N^2 d^3 \varepsilon^{-2}.$$

La probabilité de que pour un systéme $F \in \mathbb{IP}(\mathcal{H}_{(d)})$ aléatoirement choisi, l'algorithme HD avec pair initial (G, z) et borne de ressources φ produisse un zéro approché de F est plus grande que:

$$1 - \varepsilon.$$

HD avec un pair $\varepsilon-$efficient

Soit $(G_\varepsilon, \zeta_\varepsilon)$ un pair $\varepsilon-$efficient.

Input $F \in \mathcal{H}_{(d)}$, $\varepsilon > 0$

Faire $\varphi(f, \varepsilon)$ étapes dans la déformation homotopique (HD) *avec pair initial*

$$(G_\varepsilon, \zeta_\varepsilon) \in \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C})$$

suivant la composante Γ_z de la courbe $\Gamma = \pi_1^{-1}([F, G_\varepsilon]))$ qui contient $(G_\varepsilon, \zeta_\varepsilon)$.

Output:

– *ERREUR*

– *où un zéro approché de F.*

Theorem 7 *([Shub-Smale, BezV, Beltrán-P, 06] Il existent des pair $\varepsilon-$efficients.*

Remark 8 *Même avec $\zeta_\varepsilon = (1 : 0 : \cdots : 0)$.*

Problème 17 de Smale.– Comment construire ces pairs efficients?.

Ensembles Questeurs

[Beltrán- P., 2006]

Un sous-ensemble $\mathcal{G} \subseteq \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C})$ est *un ensemble questeur pour HD si:*

Pour chaque $\varepsilon > 0$ *la probabilité de qu'un pair* $(G, \zeta) \in \mathcal{G}$ *choisi au hasard soit* $\varepsilon-$*efficient pour HD est plus grand que*

$$1 - \varepsilon.$$

Input $F \in \mathcal{H}_{(d)}, \varepsilon > 0$

Choix aléatoire de $(G, \zeta) \in \mathcal{G}$

Appliquer $\varphi(f, \varepsilon)$ pas de la déformation HD entre G et F, commençant à (G, ζ).

Output:

– *ERREUR (avec probabilité plus petite que ε)*

– *ou un zéro approché de F (avec probabilité plus grande que $1 - \varepsilon$).*

Moindre: **C'est un algorithme probabilistique**

Relevant: **L'ensemble $\mathcal{G}$ doit être constructible et facile à manipuler .**

Theorem*[Beltrán, P. 2006]* *On est capable d'exhiber un ensemble questeur facile à construire et manipuler pour la résolution projective des équations polynomiales.*

Vers un Ensemble Questeur I

$e := (1 : 0 : \ldots : 0) \in \mathbb{IP}_n(\mathbb{C})$ *un "pole" dans l'esphere complexe.*

$V_e := \{F \in \mathcal{H}_{(d)} \ : \ F(e) = 0\}$. *Systémes qui s'annulent dans le "pole" e.*

$F \in V_e \longmapsto F : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^n$.

L'application "tangente" $T_eF := DF(e)$ *definie dans l'espace tangent* $T_e\mathbb{IP}_n(\mathbb{C}) = e^{\perp} = \mathbb{C}^n \subseteq \mathbb{C}^{n+1}$.:

$$T_eF := T_e\mathbb{IP}_n(\mathbb{C}) = \mathbb{C}^n \longrightarrow \mathbb{C}^n.$$

Une Idée Partielle

$L_e := \{F \in V_e \ : \ T_e F = F\}$. *"partie linéaire" des systémes dans* V_e.

$L_e^{\perp} :=$ *Systémes dans* V_e *d'ordre plus grand ou egal à 2 dans* e.

Remarque.- $V_e, L_e, L_e^{\perp}$ *sont des sous-espaces linéaires de* $\mathcal{H}_{(d)}$ *donné par les listes de ses coefficients.*

Idée Naïve: *Considerer*

$$\mathcal{G} := \{(G, e) \ : \ G \in V_e = L_e^{\perp} \bigoplus L_e\}.(?)$$

Vesr Ensembles Questeurs II (L_e)

$\mathcal{U}(n+1)$:= *matrices unitaires definies dans* $\mathbb{C}^{n+1}$.

$\mathcal{H}_{(1)} := \mathcal{M}_{n\times n+1}(\mathbb{C})$ **espace des matrices** $n\times(n+1)$ **complexes.**

$$X^{(d)} := \begin{pmatrix} X_0^{d_1-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & X_0^{d_n-1} \end{pmatrix}.$$

$$V_e^{(1)} := \{(M,U) \ : \ M \in \mathcal{H}_{(1)}, U \in \mathcal{U}, UKer(M) = e\}.$$

La Partie Lineaire L_e

$$\psi_e : V_e^{(1)} \longrightarrow L_e$$

$$\psi_e(M,U) := X^{(d)}(MU) \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

$$L_e := Im(\psi_e(M,U)).$$

Une constante outile

$$T := \left(\frac{n^2+n}{N}\right)^{n^2+n} \in \mathbb{R}, \qquad t \in [0,T].$$

Vers un ensemble questeur III

$$\mathbb{G} := [0, T] \times L_e^{\perp} \times V_e^{(1)}.$$

$$G : \mathbb{G} \longrightarrow V_e,$$

$$(t, L, M, U) \in \mathbb{G} \longmapsto G(t, L, M, U) \in V_e$$

$$G(t, L, M, U) := (1 - t^{\frac{1}{n^2+n}})^{1/2} L + t^{\frac{1}{n^2+n}} \psi_e(M, U) \in V_e,$$

Vers un Ensmeble Questeur IV $Bezout5\frac{1}{2}$

Theorem 9 (Beltrán-P., 2005a) *Pour toute liste de degrés* $(d) := (d_1, \ldots, d_n)$, *l'ensemble*

$$\mathcal{G}_{(d)} := IM(G).$$

est un ensemble questeur de pairs initiels pour HD. Autrement dit,

Un systéme $(G, e) \in \mathcal{G}_{(d)}$ **choisi aléatoirement est** $\varepsilon-$**efficient pour HD avec probabilité plus grande que**

$$1 - \varepsilon.$$

L'Algorithme

INPUT: $F \in \mathcal{H}_{(d)}$, $\varepsilon > 0$.

Choix aléatoire de $(G, e) \in \mathcal{G}_{(d)}$ *(Guess* (t, L, M)*...)*

Appliquer HD Deformation $\varphi(F, \varepsilon)$ **fois**

OUTPUT: soit "ERREUR" soit un zéro approché z de F.

Theorem 10 [Beltrn-P,06] *Il existe un algorithme probabiliste (bounded error probability) pour la résolution projective non–universelle pour des systémes d'équations homogénes tel que pour tout nombre réel positif* $\varepsilon > 0$*:*

- *Le temps de calcul de l'algorithm est au plus:*

$$O(n^5 N^2 \varepsilon^{-2})$$

- *La probabilité de que l'algorithme donne un zéro approché de l'input est au moins:*

$$1 - \varepsilon$$

Corollary 11 [Beltrn-P,06] *Il existe un algorithme probabiliste (bounded error probability) pour la résolution non–universelle des systémes d'équations homogénes cubiques tel que pour tout nombre réel positif* $\varepsilon > 0$*:*

- *Le temps de calcul de l'algorithm est au plus:*

$$O(n^{13}\varepsilon^{-2})$$

- *La probabilité de que l'algorithme donne un zéro approché de l'input est au moins:*

$$1 - \varepsilon$$

Remarque Pour $\varepsilon = 1/n^2$, L'algorithme est capable de calculer un zéro approché avec probabilité plus grande que

$$1 - 1/n^2.$$

En temps

$$O(n^{15}).$$

Complexité en moyenne (Projective version of Smale'2 17th)

Dans [Beltrán-P., 07] on a developpé une variante modifié de cet algorithme qui permet demontrer:

Theorem 12 *Il existe un algorithme que en complexité polynomial en moyenne calcule un zéro approché projectif des systémes d'équations polynomiales homogénes.*

Par complexité en moyenne on veut dire:

$$E_{\mathbb{IP}(\mathcal{H}_{(d)})}[T_{\mathcal{P}}] := \frac{1}{\nu_{\mathbb{IP}}[\mathbb{IP}(\mathcal{H}_{(d)})]} \int_{\mathbb{IP}(\mathcal{H}_{(d)})} T_{\mathcal{P}}(f) d\nu_{\mathbb{IP}} = O(n^5 N^3),$$

$T_{\mathcal{P}}(f) :=$ *temps de calcul sur l'input* f.

[Beltrán-P., 07] :

Theorem 13 *Il existe un algorithme que en complexité polynomial en moyenne calcule un zéro approché des solutions affines des systémes d'équations polynomiales multivarés.*

Par complexité en moyenne on veut dire:

$$E_{\mathbb{IP}(\mathcal{H}_{(d)})}[T_{\mathcal{P}}] := \frac{1}{\nu_{\mathbb{IP}}[\mathbb{IP}(\mathcal{H}_{(d)})]} \int_{\mathbb{IP}(\mathcal{H}_{(d)})} T_{\mathcal{P}}(f) d\nu_{\mathbb{IP}} = O(N^5),$$

$T_{\mathcal{P}}(f) :=$ *temps de calcul sur l'input* f.

[Beltrán-P., 07] : La clé du cas affine.

Theorem 14 *Soit $\delta > 0$ un nombre réel positive. Pour chaque $F \in \mathbb{IP}(\mathcal{H}_{(d)})$, soit*

$$V_A(F) := \{x \in \mathbb{C}^n \ : \ f(x) = 0\}.$$

Soit

$$||V_A(F)|| := sup\{||x|| \ : \ x \in V_A(F)\} \in [0, \infty].$$

Alors, la probability que pour un choix aléatroire d'un systéme $f \in \mathbb{IP}(\mathcal{H}_{(d)})$ on aie $||V_A(F)|| > \delta$ est au plus:

$$\mathcal{D}\sqrt{\pi n}\delta^{-1}$$

.

En fait, ce qu'on a montré est:

$$E_{\mathbb{P}(\mathcal{H}_{(d)})}[||V_A(f)||] = \mathcal{D}\frac{\Gamma(1/2)\Gamma(n+1/2)}{\Gamma(n)} \leq \mathcal{D}\sqrt{\pi n}.$$