Un Résumé autour du Problème 17-ième de Smale (avant l'Armistice 2014) (Les quatre pattes de SUMO)

Luis M. Pardo

Univ. Cantabria

23 décembre 2014

Genèse : Au commencement, j'allait organiser l'exposé autour de SUMO (le chat de Marc Giusti)...Je l'ai connu il y a sept ans...

Genèse : Au commencement, j'allait organiser l'exposé autour de SUMO (le chat de Marc Giusti)...Je l'ai connu il y a sept ans...

Exode : De même que le Problème 17-ième ; ça fait dèja 7 ans que je n'était pas vénu vous visiter (sauf TERA'2008...)...et il a beacoup changé.

Genèse : Au commencement, j'allait organiser l'exposé autour de SUMO (le chat de Marc Giusti)...Je l'ai connu il y a sept ans...

Exode : De même que le Problème 17-ième ; ça fait dèja 7 ans que je n'était pas vénu vous visiter (sauf TERA'2008...)...et il a beacoup changé.

Lévitique : Plus tard, je me suis rendu compte que la "distance" entre le calcul formel et les idées sous-jaçantes au Problème 17-ième produisse des confusions...j'avait dèja detecté au CIRM il y a deux semaines...

Genèse : Au commencement, j'allait organiser l'exposé autour de SUMO (le chat de Marc Giusti)...Je l'ai connu il y a sept ans...

Exode : De même que le Problème 17-ième ; ça fait dèja 7 ans que je n'était pas vénu vous visiter (sauf TERA'2008...)...et il a beacoup changé.

Lévitique : Plus tard, je me suis rendu compte que la "distance" entre le calcul formel et les idées sous-jaçantes au Problème 17-ième produisse des confusions...j'avait dèja detecté au CIRM il y a deux semaines...

Nombres : Deux positions tout à fait respectables : D'un côté, le développement d'un logiciel qui fonctione pour l'analyse numérique (basé sur n'importe quoi...), sans s'occuper ni de sa complexité ni de la certification de la sortie, ni, même, de savoir pourquoi ça fonctione quand il fonctione (on est dèja habitué à la "complexité experimentale" (?)...). L'autre option (la mienne) est celle de développer un algorithme efficace, basé sur des vrai mathématiques, avec un jistification de son comportement et de sa complexité. Ceci dit, mes "nombres" ne sont jamais "flottants".

Et, surtout, excusez-moi d'être un "Opéra-Tuer" : je suis un peu dislexique et disgraphique avec le clavier.

Proposé par S. Smale dans sa list des Problèmes pour le XXI-ème siècle.

Proposé par S. Smale dans sa list des Problèmes pour le XXI-ème siècle.

Smale's 17-th Problem

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

Proposé par S. Smale dans sa list des Problèmes pour le XXI-ème siècle.

Smale's 17-th Problem

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

Rq.- Il n'est que une re-édition d'un problème ennoncé par tout le monde depuis longtemps (sans avoir eu un medaille).

Proposé par S. Smale dans sa list des Problèmes pour le XXI-ème siècle.

Smale's 17-th Problem

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

Rq.- Il n'est que une re-édition d'un problème ennoncé par tout le monde depuis longtemps (sans avoir eu un medaille). À ma connaisance, Évariste Galois c'était historiquement le premier : **En un mot, les calculs sont impraticables ! !.**

Proposé par S. Smale dans sa list des Problèmes pour le XXI-ème siècle.

Smale's 17-th Problem

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

Rq.- Il n'est que une re-édition d'un problème ennoncé par tout le monde depuis longtemps (sans avoir eu un medaille). À ma connaisance, Évariste Galois c'était historiquement le premier : **En un mot, les calculs sont impraticables ! !.**

Rq Historique.-Le problème a été résolu dans [**Beltrán-P., 2009**], le plus efficace algorithme connu est montré dans [**Beltrán-P., 2011**].
Une version détérministe sous-exponentielle (?) (et des fois, polynomiale (?)) est montrée dans [**Bürgisser-Cucker, 2011**].

Proposé par S. Smale dans sa list des Problèmes pour le XXI-ème siècle.

Smale's 17-th Problem

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

Rq.- Il n'est que une re-édition d'un problème ennoncé par tout le monde depuis longtemps (sans avoir eu un medaille). À ma connaisance, Évariste Galois c'était historiquement le premier : **En un mot, les calculs sont impraticables ! !.**

Rq Historique.-Le problème a été résolu dans [**Beltrán-P., 2009**], le plus efficace algorithme connu est montré dans [**Beltrán-P., 2011**].
Une version détérministe sous-exponentielle (?) (et des fois, polynomiale (?)) est montrée dans [**Bürgisser-Cucker, 2011**].

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.Il ne s'agit pas de la résolution universelle (Calcul Formel...). Mais il y a des liens (à travers de l'approximation diophantienne....).

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.Il ne s'agit pas de la résolution universelle (Calcul Formel...). Mais il y a des liens (à travers de l'approximation diophantienne....).
- Algorithme uniforme : [Shub-Smale, 94] : Algorithme "non-uniform" en temps polynomial en moyenne. Ils montrent qu'il éxistait un système "miraculeux", mais ils n'avaient pas moyen de le trouver.

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.Il ne s'agit pas de la résolution universelle (Calcul Formel...). Mais il y a des liens (à travers de l'approximation diophantienne....).
- Algorithme uniforme : [Shub-Smale, 94] : Algorithme "non-uniform" en temps polynomial en moyenne. Ils montrent qu'il éxistait un système "miraculeux", mais ils n'avaient pas moyen de le trouver.
  Uniforme veut dire modèlisable sur un modèle de machine (Turing ou BSS). À partir de [Beltrá-**P.** 09, 11], quelques veulent changer "uniforme" par "déterministe". Pas moi. D'une part, ce n'est pas important (...anecdote sur Smale, AKS en 2002...) et d'autre part parce que tu ne peux pas changer les règles une fois le jeu a commencé.

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.Il ne s'agit pas de la résolution universelle (Calcul Formel...). Mais il y a des liens (à travers de l'approximation diophantienne....).
- Algorithme uniforme : [Shub-Smale, 94] : Algorithme "non-uniform" en temps polynomial en moyenne. Ils montrent qu'il éxistait un système "miraculeux", mais ils n'avaient pas moyen de le trouver.
  Uniforme veut dire modèlisable sur un modèle de machine (Turing ou BSS). À partir de [Beltrá-**P.** 09, 11], quelques veulent changer "uniforme" par "déterministe". Pas moi. D'une part, ce n'est pas important (...anecdote sur Smale, AKS en 2002...) et d'autre part parce que tu ne peux pas changer les règles une fois le jeu a commencé.
- Complexité en moyenne : Complexité en moyenne par rapport à une distribution de probabilité raisonnable dans l'espace des entrées.

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.Il ne s'agit pas de la résolution universelle (Calcul Formel...). Mais il y a des liens (à travers de l'approximation diophantienne....).
- Algorithme uniforme : [Shub-Smale, 94] : Algorithme "non-uniform" en temps polynomial en moyenne. Ils montrent qu'il éxistait un système "miraculeux", mais ils n'avaient pas moyen de le trouver.
  Uniforme veut dire modèlisable sur un modèle de machine (Turing ou BSS). À partir de [Beltrá-**P.** 09, 11], quelques veulent changer "uniforme" par "déterministe". Pas moi. D'une part, ce n'est pas important (...anecdote sur Smale, AKS en 2002...) et d'autre part parce que tu ne peux pas changer les règles une fois le jeu a commencé.
- Complexité en moyenne : Complexité en moyenne par rapport à une distribution de probabilité raisonnable dans l'espace des entrées.
- Polynomial : Dans la "tête" de Smale "polynomial"= polynomial dans le nombre des coeffcients en codification dense.

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.Il ne s'agit pas de la résolution universelle (Calcul Formel...). Mais il y a des liens (à travers de l'approximation diophantienne....).
- Algorithme uniforme : [Shub-Smale, 94] : Algorithme "non-uniform" en temps polynomial en moyenne. Ils montrent qu'il éxistait un système "miraculeux", mais ils n'avaient pas moyen de le trouver.
  Uniforme veut dire modèlisable sur un modèle de machine (Turing ou BSS). À partir de [Beltrá-**P.** 09, 11], quelques veulent changer "uniforme" par "déterministe". Pas moi. D'une part, ce n'est pas important (...anecdote sur Smale, AKS en 2002...) et d'autre part parce que tu ne peux pas changer les règles une fois le jeu a commencé.
- Complexité en moyenne : Complexité en moyenne par rapport à une distribution de probabilité raisonnable dans l'espace des entrées.
- Polynomial : Dans la "tête" de Smale "polynomial"= polynomial dans le nombre des coeffcients en codification dense.Dans ma tête : Polynomial dans la dimension de l'espace de paramètres...

- Résoudre : Résolution numérique : une solution est un point initiale pour l'opérateur de Newton.Il ne s'agit pas de la résolution universelle (Calcul Formel...). Mais il y a des liens (à travers de l'approximation diophantienne....).
- Algorithme uniforme : [Shub-Smale, 94] : Algorithme "non-uniform" en temps polynomial en moyenne. Ils montrent qu'il éxistait un système "miraculeux", mais ils n'avaient pas moyen de le trouver.
  Uniforme veut dire modèlisable sur un modèle de machine (Turing ou BSS). À partir de [Beltrá-**P.** 09, 11], quelques veulent changer "uniforme" par "déterministe". Pas moi. D'une part, ce n'est pas important (...anecdote sur Smale, AKS en 2002...) et d'autre part parce que tu ne peux pas changer les règles une fois le jeu a commencé.
- Complexité en moyenne : Complexité en moyenne par rapport à une distribution de probabilité raisonnable dans l'espace des entrées.
- Polynomial : Dans la "tête" de Smale "polynomial"= polynomial dans le nombre des coeffcients en codification dense.Dans ma tête : Polynomial dans la dimension de l'espace de paramètres...
  Dans ce dernier sense le problème reste encore ouvert.

- **Le conditionnement :** Malgré les opinions généralisées, ce n'est pas l'inverse de la distance à une variété des problèmes mal posés :

- **Le conditionnement :** Malgré les opinions généralisées, ce n'est pas l'inverse de la distance à une variété des problèmes mal posés :il faut la voir comme la quantité que détermine (borne) la complexité.

- **Le conditionnement :** Malgré les opinions généralisées, ce n'est pas l'inverse de la distance à une variété des problèmes mal posés :il faut la voir comme la quantité que détermine (borne) la complexité.
- **L'opérateur :** On a choisi l'opérateur de Newton " à la Shub" (c.à d., projectif) mais il peut avoir d'autres options et généralisations.

- **Le conditionnement :** Malgré les opinions généralisées, ce n'est pas l'inverse de la distance à une variété des problèmes mal posés :il faut la voir comme la quantité que détermine (borne) la complexité.
- **L'opérateur :** On a choisi l'opérateur de Newton " à la Shub" (c.à d., projectif) mais il peut avoir d'autres options et généralisations.
- **L'homotopie :** L'existence d'un relèvement (lift) d'une courbe localement connexe à travers d'un revêtement est bien connu ([García-Zangwill], p. ex.), la manière de suivre algorithmiquement cet relèvement fait la différence.

- **Le conditionnement :** Malgré les opinions généralisées, ce n'est pas l'inverse de la distance à une variété des problèmes mal posés :il faut la voir comme la quantité que détermine (borne) la complexité.
- **L'opérateur :** On a choisi l'opérateur de Newton " à la Shub" (c.à d., projectif) mais il peut avoir d'autres options et généralisations.
- **L'homotopie :** L'existence d'un relèvement (lift) d'une courbe localement connexe à travers d'un revêtement est bien connu ([García-Zangwill], p. ex.), la manière de suivre algorithmiquement cet relèvement fait la différence.
- **Complexité en moyenne (basée sur la géométrie intégrale (voir probabilité)) :** Puisque on s'intéresse à la complexité en moyenne, la probabilité joue un rôle. En plus, on veut un "algorithme uniforme", ce qui ne veut pas dire déterministe (sauf interpretations intéressées).

Il faut atribuer à M. Shub et S. Smale l'initiative autour des objets sous-jaçantes aux trois premières pattes. La quatrième ?...

Le Conditionement

- Une liste de degrés $(d) = (d_1, \ldots, d_n)$,
- L'espace vectoriel complex des systèmes d'équations polynomiales homogènes $\mathcal{H}_{(d)}$ de dimension $N + 1 = \sum_{i=1}^{n} \binom{d_i+n}{n}$. $f_i \in \mathbb{C}[X_0, \ldots, X_n]$.

$$f = (f_1, \ldots, f_s) : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^s, \quad deg(f_i) \leq d_i,$$

- Une liste de degrés $(d) = (d_1, \ldots, d_n)$,
- L'espace vectoriel complex des systèmes d'équations polynomiales homogènes $\mathcal{H}_{(d)}$ de dimension $N+1 = \sum_{i=1}^{n} \binom{d_i+n}{n}$. $f_i \in \mathbb{C}[X_0, \ldots, X_n]$.

$$f = (f_1, \ldots, f_s) : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^s, \quad deg(f_i) \leq d_i,$$

- L'espace tangent $T_\zeta \mathbb{P}_n(\mathbb{C}) := \{\dot{\zeta} \ : \ \langle \dot{\zeta}, \zeta \rangle = 0\} = \zeta^\perp$ et la derivée $T_\zeta f : T_\zeta \mathbb{P}_n(\mathbb{C}) \longrightarrow \mathbb{C}^n$ donnée par

$$T_\zeta f := Df(\zeta) \mid_{\zeta^\perp}$$

- Parfois $\Omega \subseteq \mathbb{P}(\mathcal{H}_{(d)})$ est une sous-variété (réelle ou complexe ou diophantienne) des systèmes d'équations interéssants. Dans la plupart de cet exposé $\Omega = \mathbb{P}(\mathcal{H}_{(d)})$.

- Une liste de degrés $(d) = (d_1, \ldots, d_n)$,
- L'espace vectoriel complex des systèmes d'équations polynomiales homogènes $\mathcal{H}_{(d)}$ de dimension $N+1 = \sum_{i=1}^{n} \binom{d_i+n}{n}$. $f_i \in \mathbb{C}[X_0, \ldots, X_n]$.

$$f = (f_1, \ldots, f_s) : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^s, \ \ deg(f_i) \leq d_i,$$

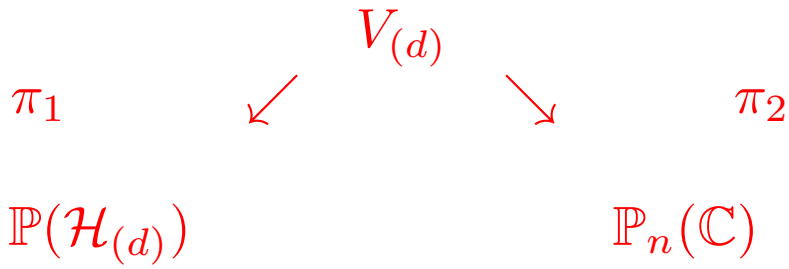
- L'espace tangent $T_\zeta \mathbb{P}_n(\mathbb{C}) := \{\dot{\zeta} \ : \ \langle \dot{\zeta}, \zeta \rangle = 0\} = \zeta^\perp$ et la derivée $T_\zeta f : T_\zeta \mathbb{P}_n(\mathbb{C}) \longrightarrow \mathbb{C}^n$ donnée par

$$T_\zeta f := Df(\zeta) \mid_{\zeta^\perp}$$

- Parfois $\Omega \subseteq \mathbb{P}(\mathcal{H}_{(d)})$ est une sous-variété (réelle ou complexe ou diophantienne) des systèmes d'équations interéssants. Dans la plupart de cet exposé $\Omega = \mathbb{P}(\mathcal{H}_{(d)})$.
- **La "variété" d'incidence (dépendante de M) associé à Ω :**

$$V_{(d)}(\Omega) := \{(f, \zeta) \in M \times \mathbb{P}_n(\mathbb{C}) \ : \ f(\zeta) = 0\} \subseteq \mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C}).$$

Les projections cannoniques :



Les projections cannoniques :

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

L'espace tangent :

$$T_{(f,\zeta)}V_{(d)} := \{(\dot{f},\dot{\zeta}) \ : \ \dot{f}(\zeta) + T_\zeta f\dot{\zeta} = 0\}.$$

Les projections cannoniques :

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

L'espace tangent :

$$T_{(f,\zeta)}V_{(d)} := \{(\dot{f},\dot{\zeta}) \ : \ \dot{f}(\zeta) + T_\zeta f\dot{\zeta} = 0\}.$$

- L'application π_2 est une submersion en tout point et l'image inverse $\pi_2^{-1}(z)$ est un sous-variété projective linéaire de codimension n dans $\mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C})$.
- L'application π_1 a des points et valeurs critiques. L'ensemble des valeurs critiques forment la variété discriminante $\Sigma_{(d)}$ (voir [Busé-Jouanolou, 2012] pour une belle description).

$$f \in \Sigma_{(d)} \text{ sii } \exists\, \zeta V_{\mathbb{P}}(f),\ rank(T_\zeta f) < n.$$

Hors de la variété discriminante (i.e. $f \notin \Sigma_{(d)}$), les fibres de π_1 sont les variétés projectives, intersection complète, lisses et de dimension zéro données par des équations dans $\mathcal{H}_{(d)}$:

$$V_{\mathbb{P}}(f) := \pi_1^{-1}(f) := \{\zeta \in \mathbb{P}_n(\mathbb{C}) \ : \ f(\zeta) = 0\}.$$

En plus, π_1 est un revêtement localement trivial hors de $\Sigma_{(d)}$, où les fibres $\pi_1^{-1}(f)$ ont toutes la même cardinalité, connu comme **nombre de Bézout :**

$$\mathcal{D} := \prod_{i=1}^{n} d_i.$$

Il y a, alors, des sections localement définies $\sigma : (\mathbb{P}(\mathcal{H}_{(d)}), f) \longrightarrow (V_{(d)}, (f, \zeta))$.

Hors de la variété discriminante (i.e. $f \notin \Sigma_{(d)}$), les fibres de π_1 sont les variétés projectives, intersection complète, lisses et de dimension zéro données par des équations dans $\mathcal{H}_{(d)}$:

$$V_{\mathbb{P}}(f) := \pi_1^{-1}(f) := \{\zeta \in \mathbb{P}_n(\mathbb{C}) \ : \ f(\zeta) = 0\}.$$

En plus, π_1 est un revêtement localement trivial hors de $\Sigma_{(d)}$, où les fibres $\pi_1^{-1}(f)$ ont toutes la même cardinalité, connu comme **nombre de Bézout :**

$$\mathcal{D} := \prod_{i=1}^{n} d_i.$$

Il y a, alors, des sections localement définies $\sigma : (\mathbb{P}(\mathcal{H}_{(d)}), f) \longrightarrow (V_{(d)}, (f, \zeta))$. **Résoudre** consiste a composer $\pi_2 \circ \sigma$ localement autour de f.

Hors de la variété discriminante (i.e. $f \notin \Sigma_{(d)}$), les fibres de π_1 sont les variétés projectives, intersection complète, lisses et de dimension zéro données par des équations dans $\mathcal{H}_{(d)}$:

$$V_{\mathbb{P}}(f) := \pi_1^{-1}(f) := \{\zeta \in \mathbb{P}_n(\mathbb{C}) \ : \ f(\zeta) = 0\}.$$

En plus, π_1 est un revêtement localement trivial hors de $\Sigma_{(d)}$, où les fibres $\pi_1^{-1}(f)$ ont toutes la même cardinalité, connu comme **nombre de Bézout :**

$$\mathcal{D} := \prod_{i=1}^{n} d_i.$$

Il y a, alors, des sections localement définies $\sigma : (\mathbb{P}(\mathcal{H}_{(d)}), f) \longrightarrow (V_{(d)}, (f, \zeta))$.
Résoudre consiste a composer $\pi_2 \circ \sigma$ localement autour de f.

Conditionnement

Conditionnement est la norme (comme opérateur linéaire) de la derivée de la résolution (comme fonction localement définie et différentiable) :

$$||T_f(\pi_2 \circ \sigma)||.$$

$$
\begin{array}{ccccc}
 & & V_{(d)} & & \\
\pi_1 & \swarrow & & \searrow & \pi_2 \\
\mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma & & \longrightarrow & & \mathbb{P}_n(\mathbb{C}) \\
 & & \pi_2 \circ \sigma & & \\
f & & \longmapsto & & \zeta
\end{array}
$$

Le conditionnement linéaire est une idée du à Alan Turing.

Le conditionnement linéaire est une idée du à Alan Turing. Une histoire raconte que, dans une voyage en train, Turing a raconté ses idées à von Neumann. Alors, von Neumann a travaillé vite pour devenir de “patron” intelectuel du conditionnement.

Le conditionnement linéaire est une idée du à Alan Turing. Une histoire raconte que, dans une voyage en train, Turing a raconté ses idées à von Neumann. Alors, von Neumann a travaillé vite pour devenir de “patron” intelectuel du conditionnement. Hereusement, il existe an article (pas trop connu jusqu’à très récemment)...[Turing, 47].

Le conditionnement linéaire est une idée du à Alan Turing. Une histoire raconte que, dans une voyage en train, Turing a raconté ses idées à von Neumann. Alors, von Neumann a travaillé vite pour devenir de “patron” intelectuel du conditionnement. Hereusement, il existe an article (pas trop connu jusqu'à très récemment)...[Turing, 47].

Pour tout $\dot{f} \in T_f\mathbb{P}(\mathcal{H}_{(d)})$ on a :

$$T_f(\pi_2 \circ \sigma)(\dot{f}) = T_{(f,\zeta)}\pi_2 \left(T_f\sigma(\dot{f})\right)$$

Le conditionnement linéaire est une idée du à Alan Turing. Une histoire raconte que, dans une voyage en train, Turing a raconté ses idées à von Neumann. Alors, von Neumann a travaillé vite pour devenir de "patron" intelectuel du conditionnement. Hereusement, il existe an article (pas trop connu jusqu'à très récemment)...[Turing, 47].

Pour tout $\dot{f} \in T_f\mathbb{P}(\mathcal{H}_{(d)})$ on a :

$$T_f(\pi_2 \circ \sigma)(\dot{f}) = T_{(f,\zeta)}\pi_2 \left(T_f\sigma(\dot{f})\right)$$

Si $T_f\sigma(\dot{f}) = (\dot{f}, \dot{\zeta})$, alors $\dot{\zeta} = -\left(T_\zeta f\right)^{-1} \dot{f}(\zeta)$. Si on assume que $||f|| = ||\zeta|| = 1$, sont representés par des points dans la sphère, on voit que

$$||T_f(\pi_2 \circ \sigma)|| = || - T_{(f,\zeta)}\pi_2 \circ \left(Df(\zeta) \mid_{\zeta^\perp}\right)^{-1} || = ||T_\zeta f^{-1}|| = \|Df(\zeta)^\dagger\|.$$

C'est à dire, le conditionnement n'est que la norme de la pseudo-inverse de Moore-Penrose de la matrice Jacobienne $Df(\zeta)$.

Le conditionnement linéaire est une idée du à Alan Turing. Une histoire raconte que, dans une voyage en train, Turing a raconté ses idées à von Neumann. Alors, von Neumann a travaillé vite pour devenir de “patron” intelectuel du conditionnement. Hereusement, il existe an article (pas trop connu jusqu'à très récemment)...[Turing, 47].

Pour tout $\dot{f} \in T_f\mathbb{P}(\mathcal{H}_{(d)})$ on a :

$$T_f(\pi_2 \circ \sigma)(\dot{f}) = T_{(f,\zeta)}\pi_2 \left(T_f\sigma(\dot{f})\right)$$

Si $T_f\sigma(\dot{f}) = (\dot{f}, \dot{\zeta})$, alors $\dot{\zeta} = -\left(T_\zeta f\right)^{-1} \dot{f}(\zeta)$. Si on assume que $||f|| = ||\zeta|| = 1$, sont representés par des points dans la sphère, on voit que

$$||T_f(\pi_2 \circ \sigma)|| = || - T_{(f,\zeta)}\pi_2 \circ \left(Df(\zeta) \mid_{\zeta^\perp}\right)^{-1} || = ||T_\zeta f^{-1}|| = \|Df(\zeta)^\dagger\|.$$

C'est à dire, le conditionnement n'est que la norme de la pseudo-inverse de Moore-Penrose de la matrice Jacobienne $Df(\zeta)$. Après il faudra normaliser....

On assume sur $\mathcal{H}_{(d)}$ la metrique hermitienne de Bombieri-Weyl (i.e. le seul produit hermitien invariant par l'action du group unitaire $\mathcal{U}(n+1)$:

$$f \longmapsto f \circ U^*.$$

La norme qui vérifie :

$$||f||_d^2 = \binom{d+n}{n} \frac{1}{\nu_S[S^{2n+1}]} \int_{S^{2n+1}} |f(z)|^2 d\nu_S(z),$$

On normalise le contiditionnement de la façon suivante :

$$\mu_{\text{norm}}(f,\zeta) := \|f\|_\Delta \|T_z f^{-1} \Delta(d_i^{1/2})\|,$$

où $\|\zeta\| = 1$. C'est une notion projective (définie sur $\mathbb{P}(\mathcal{H}_{(d)}) \times \mathbb{P}_n(\mathbb{C})$)

Le conditionnement satsifait un Théorème du nombre de conditionnement. Mais ce n'est pas la distance à la variété discriminante, sinon une dsitance dans la fibre.

Le conditionnement satsifait un Théorème du nombre de conditionnement. Mais ce n'est pas la distance à la variété discriminante, sinon une dsitance dans la fibre.

Rq.- Parfois il y a des gens qui confondent les deux choses par ce mauvais apprentissage : conditionnement comme inverse de la distance à la variété des problèmes mal posés...

Le conditionnement satsifait un Théorème du nombre de conditionnement. Mais ce n'est pas la distance à la variété discriminante, sinon une dsitance dans la fibre.

Rq.- Parfois il y a des gens qui confondent les deux choses par ce mauvais apprentissage : conditionnement comme inverse de la distance à la variété des problèmes mal posés...Ça se passe dans le cas linéaire (Eckart & Young, 1936)

Les distances : Riemannienne (Fubini-Study) :

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

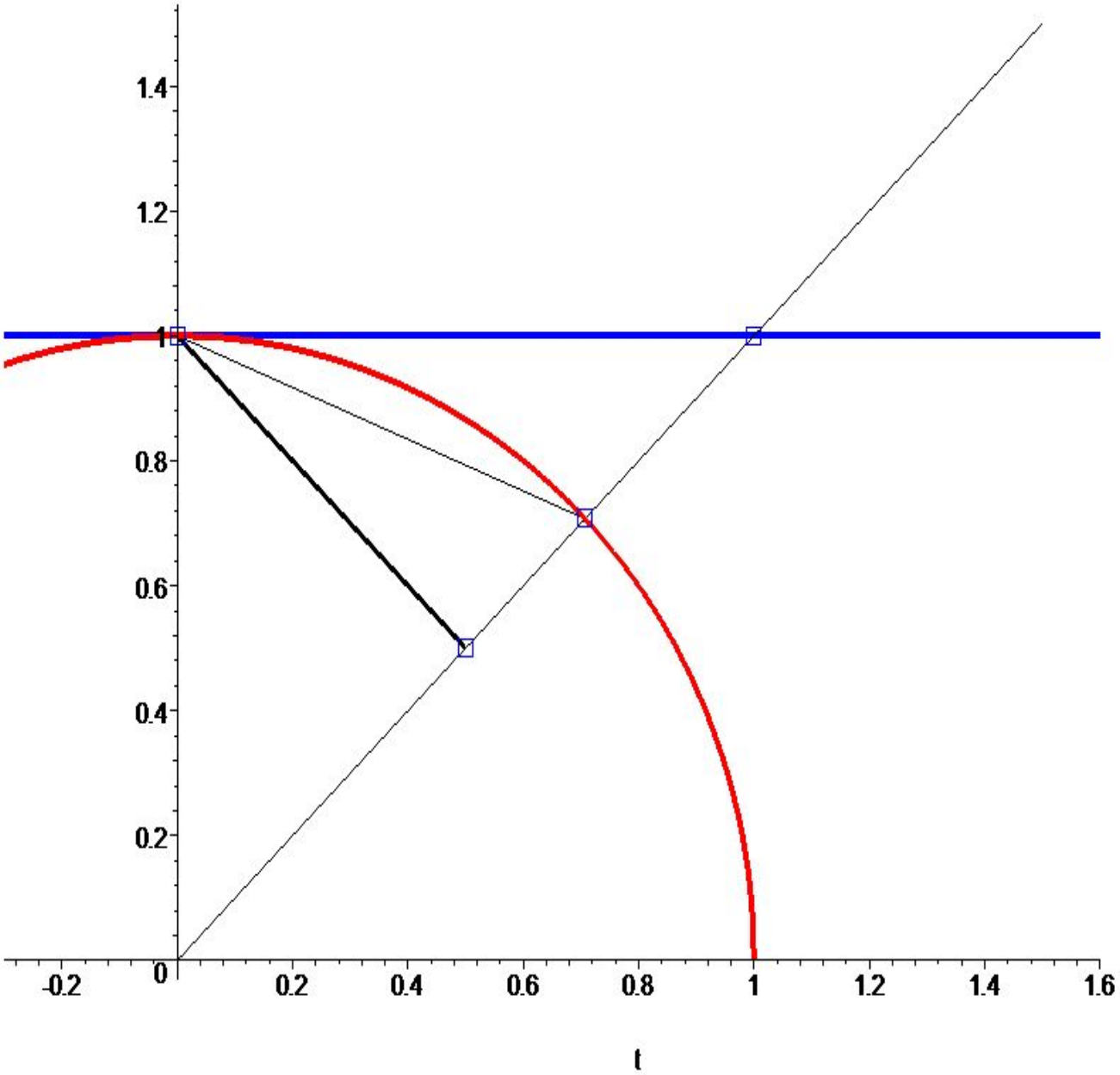
Projective (aussi sin-distance) :

$$d_{\mathbb{P}}(\pi(x), \pi(x')) := sin\ d_R(\pi(x), \pi(x')).$$

"Distance" tangente :

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

Les distances



Pour $z \in \mathbb{P}_n(\mathbb{C})$, soit :

$$\Sigma_z = \pi_2^{-1}(z) := \{f \in \mathbb{P}(\mathcal{H}_{(d)}) \ : \ f(z) = 0\}.$$

Soit *dist* la distance induite sur Σ_z par $d_{\mathbb{P}}$

Theorem (Shub-Smale)

Pour tout $f \in \mathcal{H}_{(d)}$, $\|f\| = 1$, *par rapport à la metrique de Bombieri-Weyl :*

$$\mu_{\text{norm}}(f, z) = \frac{1}{\text{dist}(f, \Sigma_z)}.$$

L'Opérateur de Newton Projectif [Shub]

Souvenez-vous du espace tangent $T_z\mathbb{P}_n(\mathbb{C}) = z^\perp$ et la restriction $T_z f := Df(z)\mid_{z^\perp}$.

La pseudo-inverse, si z n'est pas critique la tangente est donnée par :

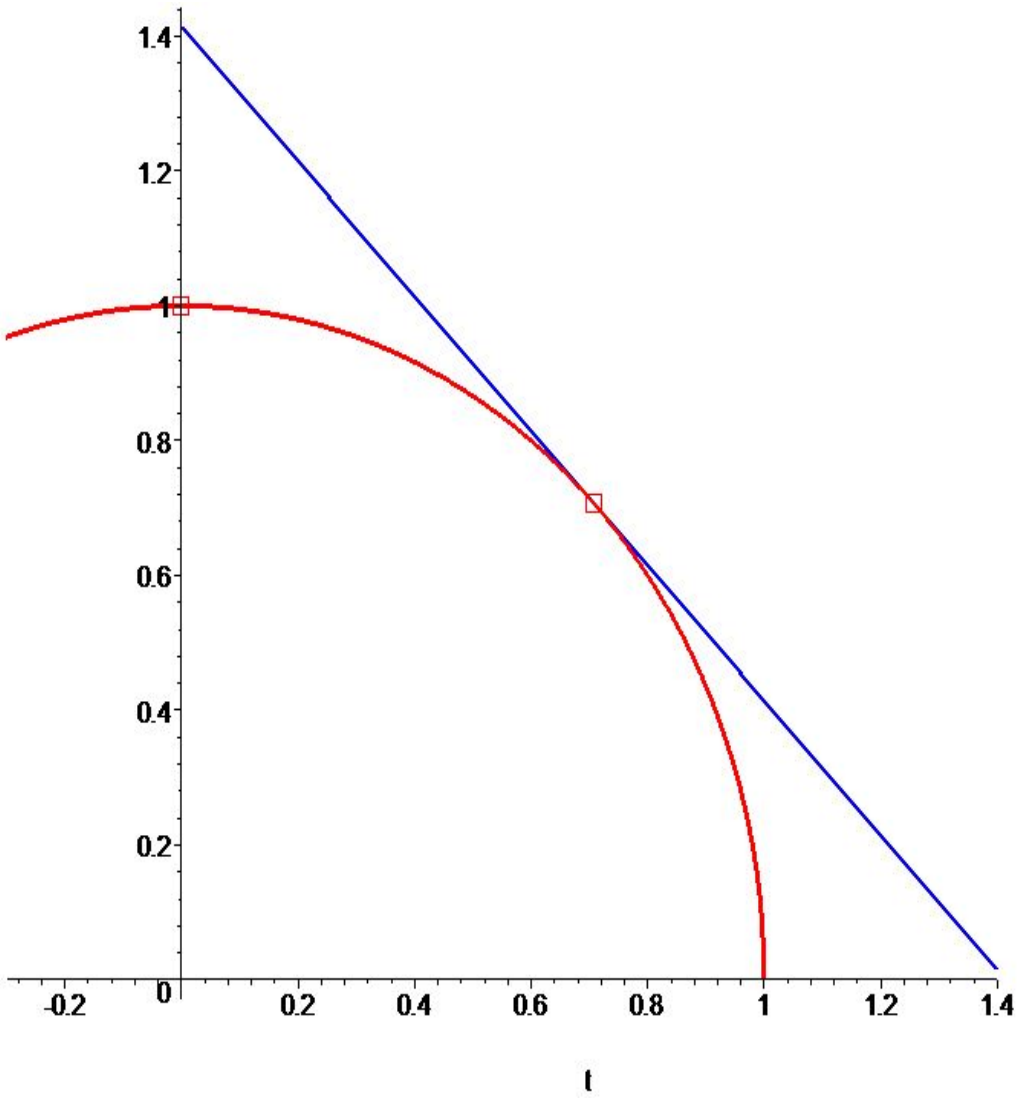
$$T_z f^{-1} := Df(z)^\dagger := (Df(z)\mid_{T_z})^{-1} \ : \mathbb{C}^n \longrightarrow T_z\mathbb{P}_n(\mathbb{C}) \subseteq \mathbb{C}^{n+1}.$$

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

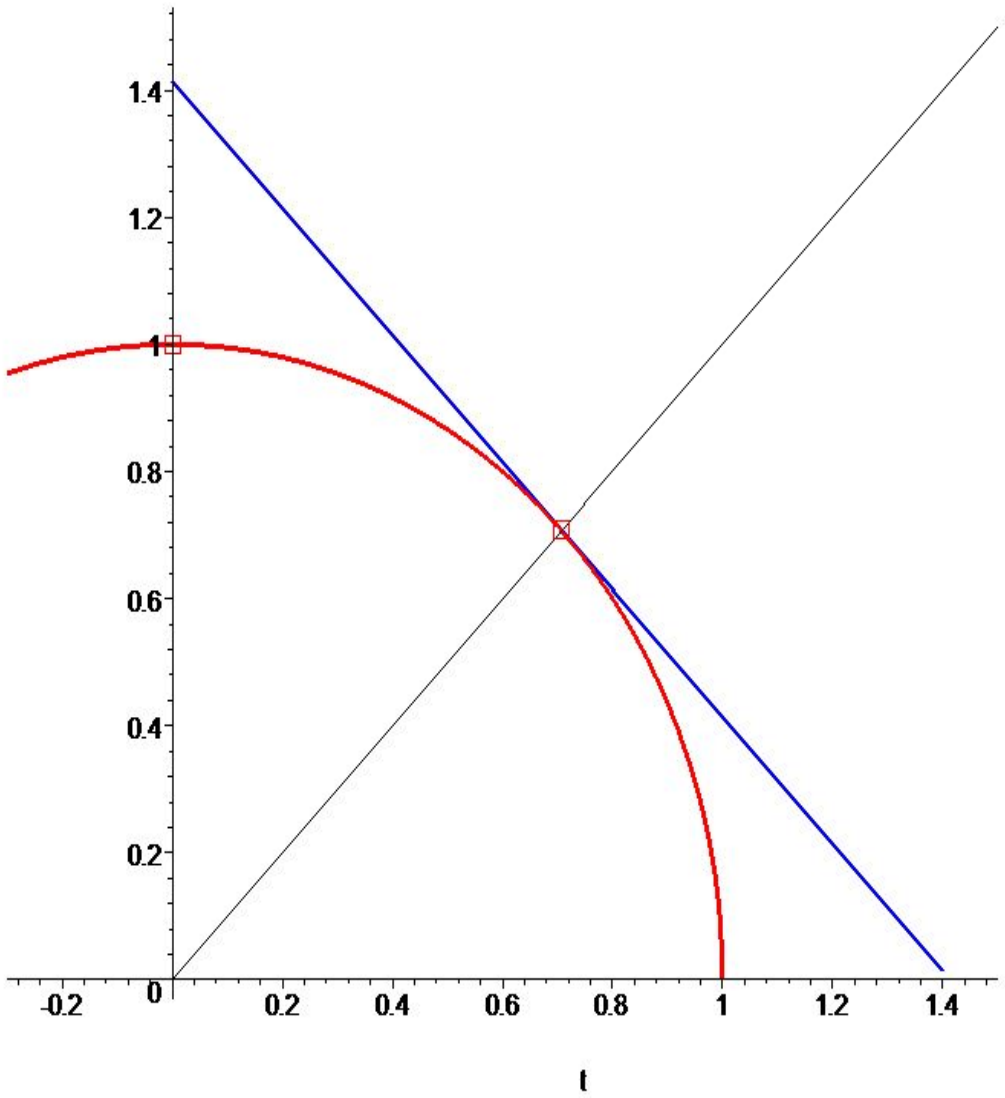
Definition

Opérateur de Newton

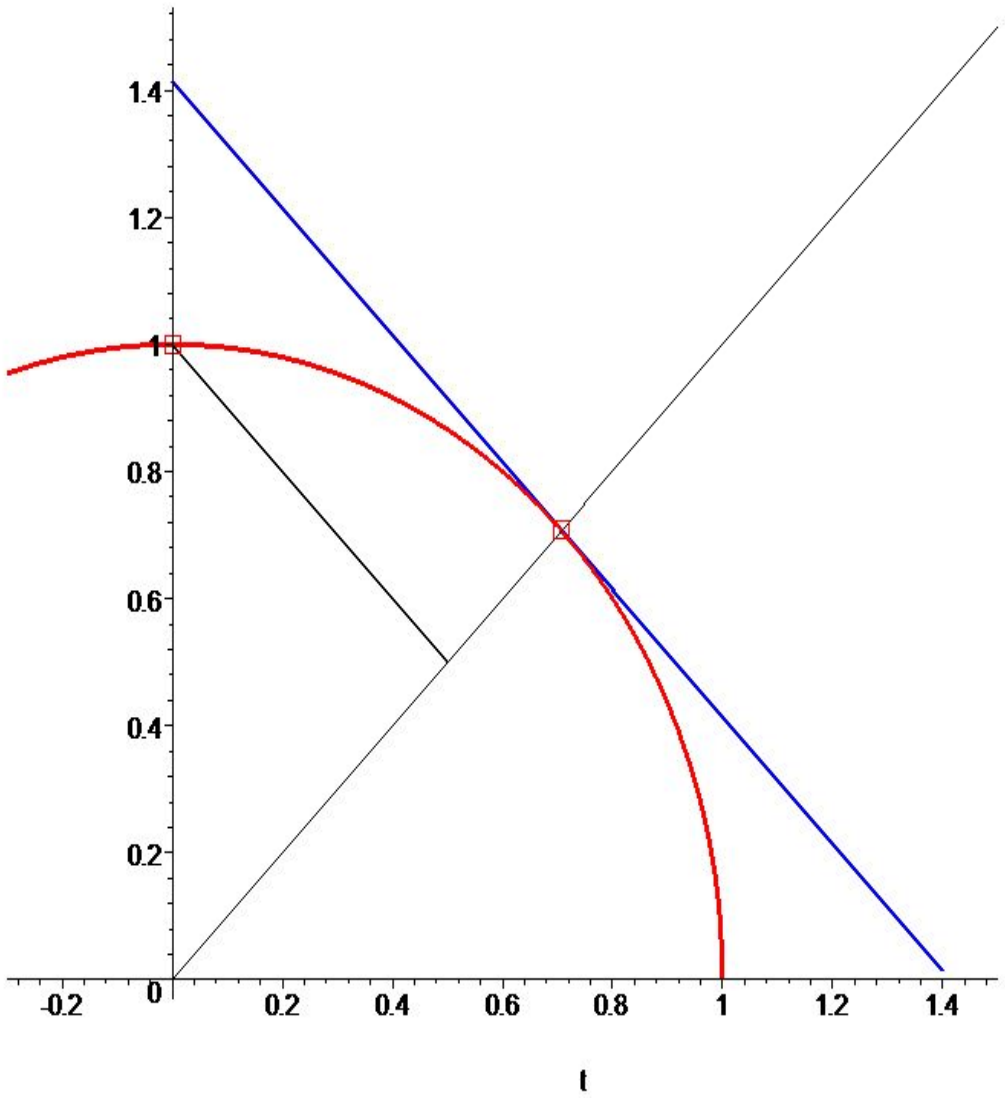
$$N_f(\pi(z)) := \pi\left(z - (Df(z)\mid_{T_z})^{-1} f(z)\right),$$



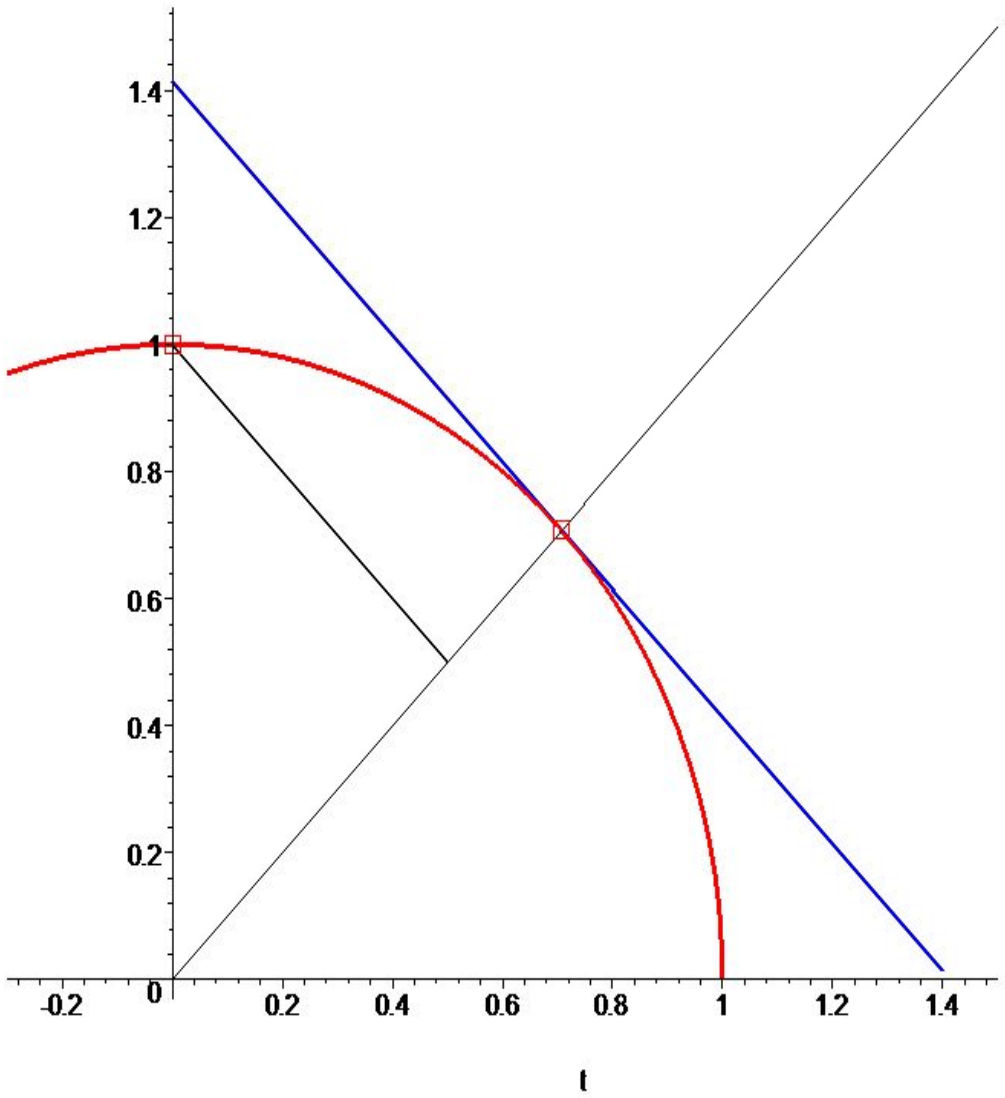
$T_z\mathbb{P}_n(\mathbb{C})$



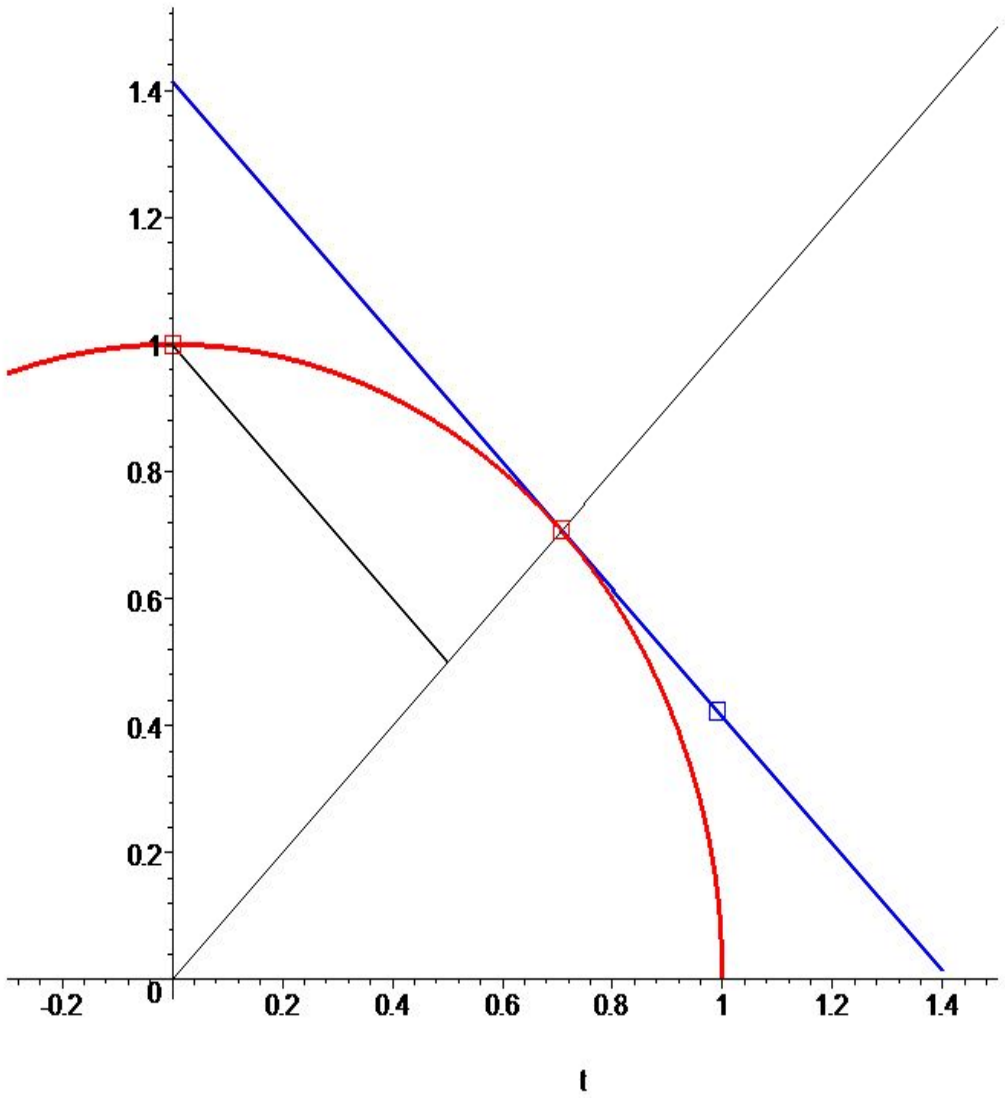
$T_z\mathbb{P}_n(\mathbb{C})$



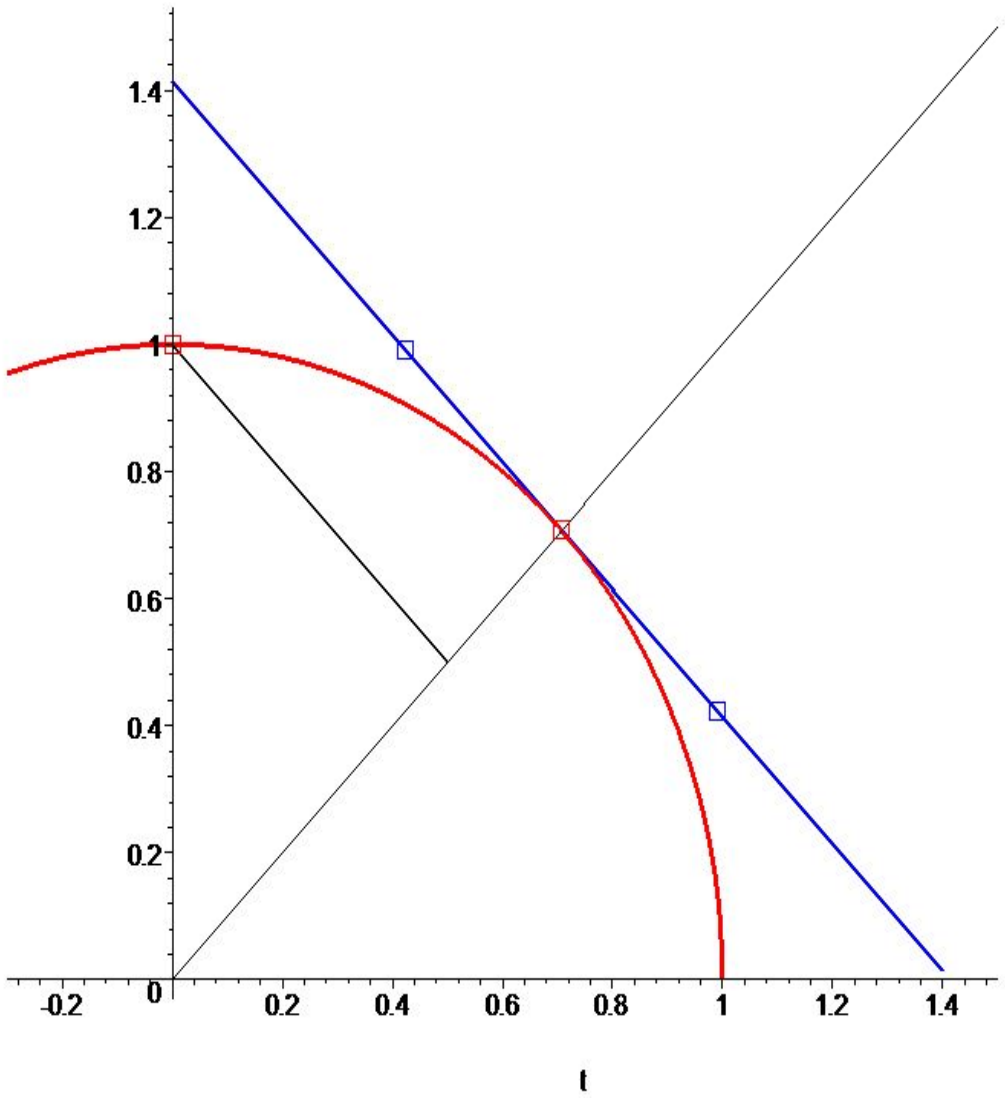
$T_z\mathbb{P}_n(\mathbb{C})$



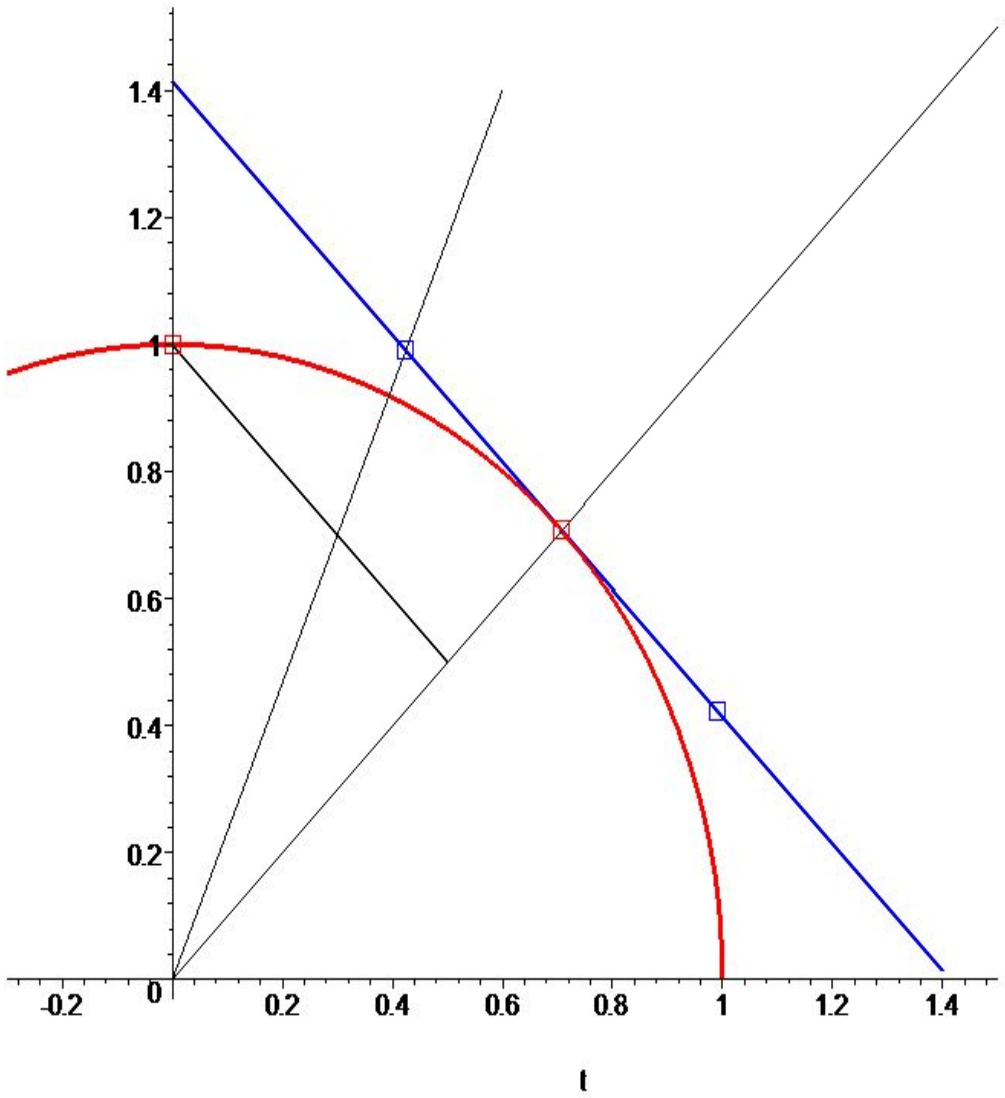
$f(z) \in \mathbb{C}^n$ $T_z\mathbb{P}_n(\mathbb{C})$



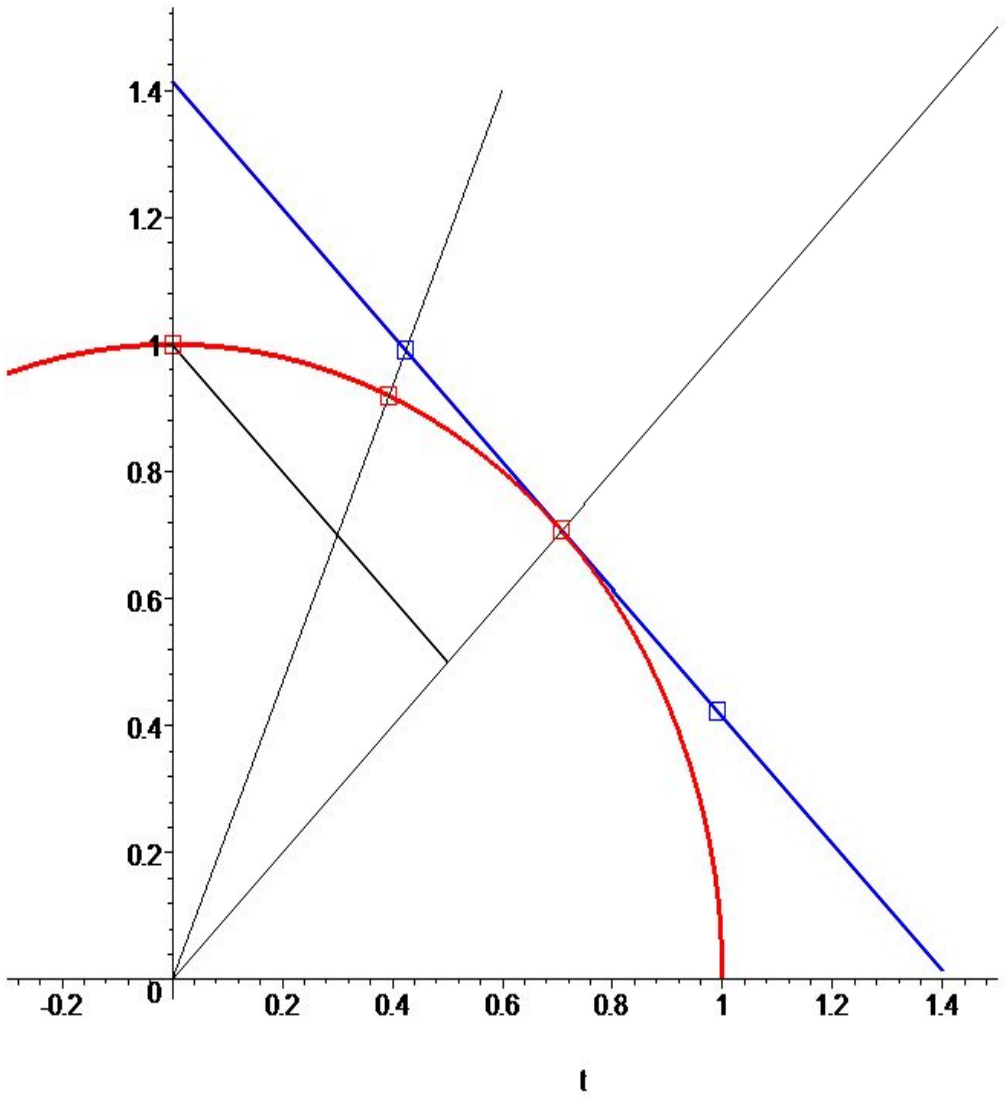
$$T_z f^{-1} f(z) \in T_z \mathbb{P}_n(\mathbb{C})$$



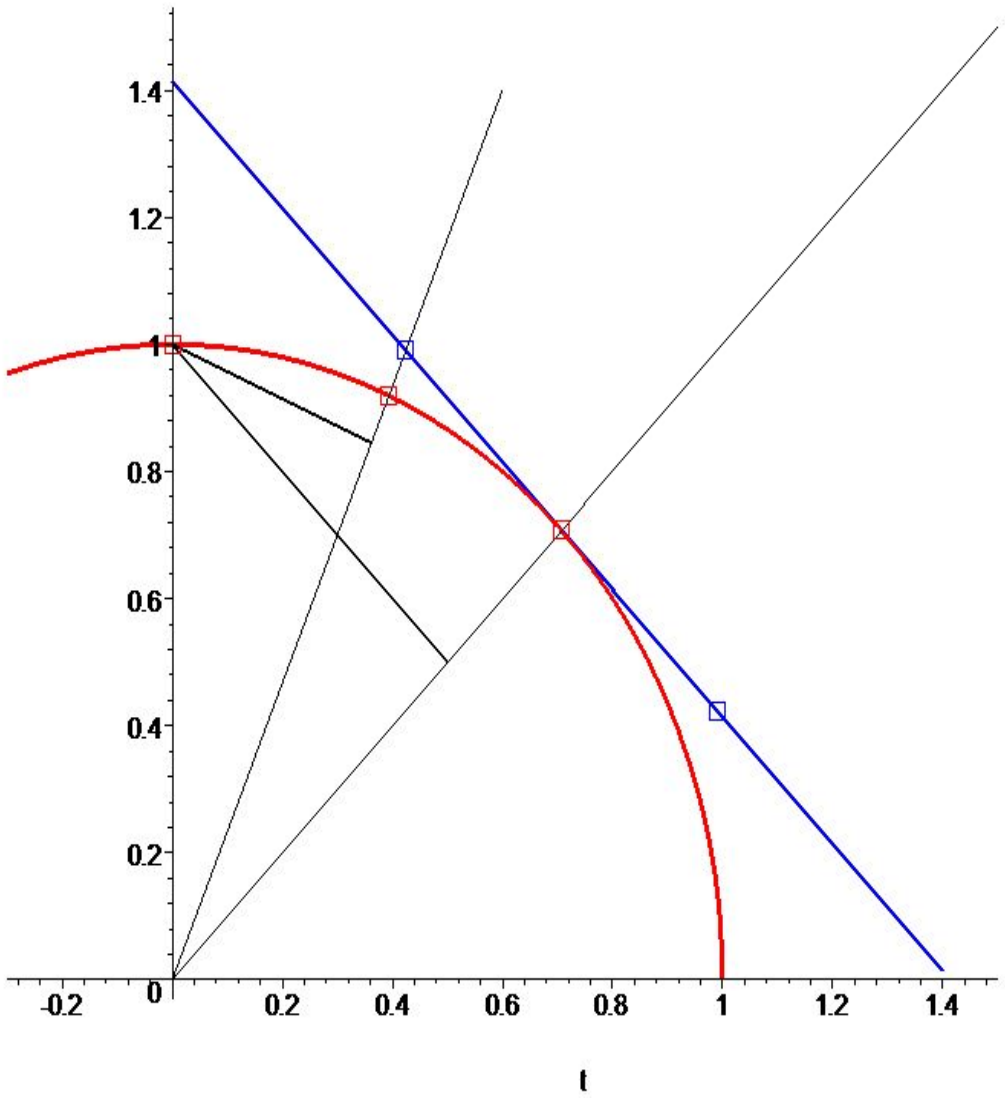
$$-T_z f^{-1} f(z) \in T_z \mathbb{P}_n(\mathbb{C})$$



$$z - T_z f^{-1} f(z) \in \mathbb{C}^{n+1}$$



$$\pi(z - T_z f^{-1} f(z)) \in \mathbb{P}_n(\mathbb{C})$$



$$\pi(z - T_z f^{-1} f(z)) \in \mathbb{P}_n(\mathbb{C})$$

Definition

Zéro approché [Smale'81] : Un point $z \in \mathbb{P}_n(\mathbb{C})$ est un zéro approché de f avec zéro approché $\zeta \in V_{\mathbb{P}}(f)$ si :

$$d_{\mathbb{P}}(N_f^k(z), \zeta) \leq \frac{1}{2^{2^{k-1}}}.$$

Une longe liste de contributeurs dans les années : 90 : Shub, Smale, Dedieu, Kim, Hubbard, Kostlan, Malajovich, Yakoubsohn...

Definition

Zéro approché [Smale'81] : Un point $z \in \mathbb{P}_n(\mathbb{C})$ est un zéro approché de f avec zéro approché $\zeta \in V_{\mathbb{P}}(f)$ si :

$$d_{\mathbb{P}}(N_f^k(z), \zeta) \leq \frac{1}{2^{2^{k-1}}}.$$

Une longe liste de contributeurs dans les années : 90 : Shub, Smale, Dedieu, Kim, Hubbard, Kostlan, Malajovich, Yakoubsohn...

Résoudre (non–universel) : Étant donné un système f, trouver un zéro approché associé à une des solutions dans $V_{\mathbb{P}}(f)$.

Theorem ($\gamma-$Theorem, Béz I)

Pour chaque $f \in \mathcal{H}_{(d)}$ *et* $\zeta \in V_{\mathbb{P}}(f)$, *si :*

$$d_{\mathbb{P}}(z,\zeta) \leq \frac{3-\sqrt{7}}{d^{\frac{3}{2}}\,\mu_{\text{norm}}(f,\zeta)},$$

alors, z *est un zéro approché de* f *avec zéro associé* ζ.

Theorem ($\gamma-$Theorem, Béz I)

Pour chaque $f \in \mathcal{H}_{(d)}$ *et* $\zeta \in V_{\mathbb{P}}(f)$, *si :*

$$d_{\mathbb{P}}(z,\zeta) \leq \frac{3-\sqrt{7}}{d^{\frac{3}{2}}\,\mu_{\mathrm{norm}}(f,\zeta)},$$

alors, z *est un zéro approché de* f *avec zéro associé* ζ.

Theorem ($\alpha-$Theorem)

Avec les notations precédentes, $\|f\|_{\Delta} = 1$, *soient :*

$$\alpha^*(f,z) := \frac{d^{3/2}}{2}\beta(f,z)\mu_{\mathrm{norm}}(f,z),$$

où $d := \max\{d_1,\ldots,d_n\}$, *et* $\beta(f,z) := d_{\mathbb{P}}(z, N_f(z))$. *Il éxiste une constante* α_0, *telle que si*

$$\alpha^*(f,z) \leq \alpha_0,$$

alors, z *est un zéro approché de* f *avec some zéro associé* $\zeta \in V_{\mathbb{P}}(f)$.

L'homotopie

La projection $\pi_1 : V_{(d)} \setminus \pi_1^{-1}(\Sigma_{(d)}) \longrightarrow \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma_{(d)}$ est un relévement (hors de la variété discriminante).

Les fibres sur chaque $f \in \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma_{(d)}$ ont cardinal constant égal au nombre de Bézout $\mathcal{D}$.

La projection $\pi_1 : V_{(d)} \setminus \pi_1^{-1}(\Sigma_{(d)}) \longrightarrow \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma_{(d)}$ est un relévement (hors de la variété discriminante).

Les fibres sur chaque $f \in \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma_{(d)}$ ont cardinal constant égal au nombre de Bézout $\mathcal{D}$.

Propiété de relèvement : Pour chaque $g \in \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma_{(d)}$ and chaque zéro $\zeta_0 \in V_{\mathbb{P}}(g)$ and chaque courbe $\gamma \subseteq \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma_{(d)}$, telle que $g \in \gamma$, il existe une courbe $\Gamma \subseteq V_{(d)}$, contennant $(g, \zeta_0) \in \Gamma$, que se projette sur γ.

$$\begin{array}{ccc} & & V \setminus \pi_1^{-1}(\Sigma) \\ \Gamma & \nearrow & \downarrow \quad \pi_1 \\ [0,1] & \underset{\gamma}{\longrightarrow} & \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma \end{array}$$

- [Bez I–II] L'Opérateur de Newton suit de très près le chemin Γ avec la seule connaissance du point initial (g, ζ_0).

- [Bez I–II] L'Opérateur de Newton suit de très près le chemin Γ avec la seule connaissance du point initial (g, ζ_0).
- Le chemin le plus simple (segment entre deux points) peut servir (après on peut projeter sur la sphère (si on le veut)) :

$$[f, g] := \{tf + (1-t)g \in \mathbb{P}(\mathcal{H}_{(d)}) \ : \ t \in [0,1]\}.$$

- Pour chaque zéro $\zeta_0 \in V_{\mathbb{P}}(g)$ le rélevement $\Gamma(f, g, \zeta_0)$ attrappe un seul zéro $\zeta_1 \in V_{\mathbb{P}}(f)$.

- [Bez I–II] L'Opérateur de Newton suit de très près le chemin Γ avec la seule connaissance du point initial (g, ζ_0).
- Le chemin le plus simple (segment entre deux points) peut servir (après on peut projeter sur la sphère (si on le veut)) :

$$[f, g] := \{tf + (1-t)g \in \mathbb{P}(\mathcal{H}_{(d)}) \ : \ t \in [0,1]\}.$$

- Pour chaque zéro $\zeta_0 \in V_{\mathbb{P}}(g)$ le rélevement $\Gamma(f, g, \zeta_0)$ attrappe un seul zéro $\zeta_1 \in V_{\mathbb{P}}(f)$.
- Comme la co-dimension (reèlle) de $\Sigma_{(d)}$ est deux, un segment $[f, g]$ vérifie $[f, g] \cap \Sigma = \emptyset$ avec probabilité 1. De même pour le grand circle $\mathcal{L}(f, g)$ determiné par $[f, g]$ sur la sphère unité dans $\mathcal{H}_{(d)}$.
- Travailler sur l'affine $[f, g]$ ou le projectif $\mathcal{L}(f, g)$ est un peu au choix...plus tard

Pour un segment $\Gamma := [f, g]$ et un zéro $\zeta_0 \in V_{\mathbb{P}}(g)$.
Définissons une partition de l'interval $[0, 1]$:

$$0 = t_0 < t_1 < \ldots < t_k = 1$$

Intialize $z_0 = \zeta_0$

Pour un segment $\Gamma := [f, g]$ et un zéro $\zeta_0 \in V_{\mathbb{P}}(g)$.
Définissons une partition de l'interval $[0, 1]$:

$$0 = t_0 < t_1 < \ldots < t_k = 1$$

Intialize $z_0 = \zeta_0$
Itérations :

$$z_{i+1} = N_{f_{t_{i+1}}}(z_i)$$

Output : z_k.

Pour un segment $\Gamma := [f, g]$ et un zéro $\zeta_0 \in V_{\mathbb{P}}(g)$.
Définissons une partition de l'interval $[0, 1]$:

$$0 = t_0 < t_1 < \ldots < t_k = 1$$

Intialize $z_0 = \zeta_0$
Itérations :

$$z_{i+1} = N_{f_{t_{i+1}}}(z_i)$$

Output : z_k.
Rq.- Les différentes algorithmes dépendent de la façon de choisir les "pas" t_i, mais il faut tenir en compte que :
t_i est construit de telle façon que z_i est dans le "strong basin of attraction" dus suivant systme $f_{t_{i+1}}$.

Pour un segment $\Gamma := [f, g]$ et un zéro $\zeta_0 \in V_{\mathbb{P}}(g)$.
Définissons une partition de l'interval $[0, 1]$:

$$0 = t_0 < t_1 < \ldots < t_k = 1$$

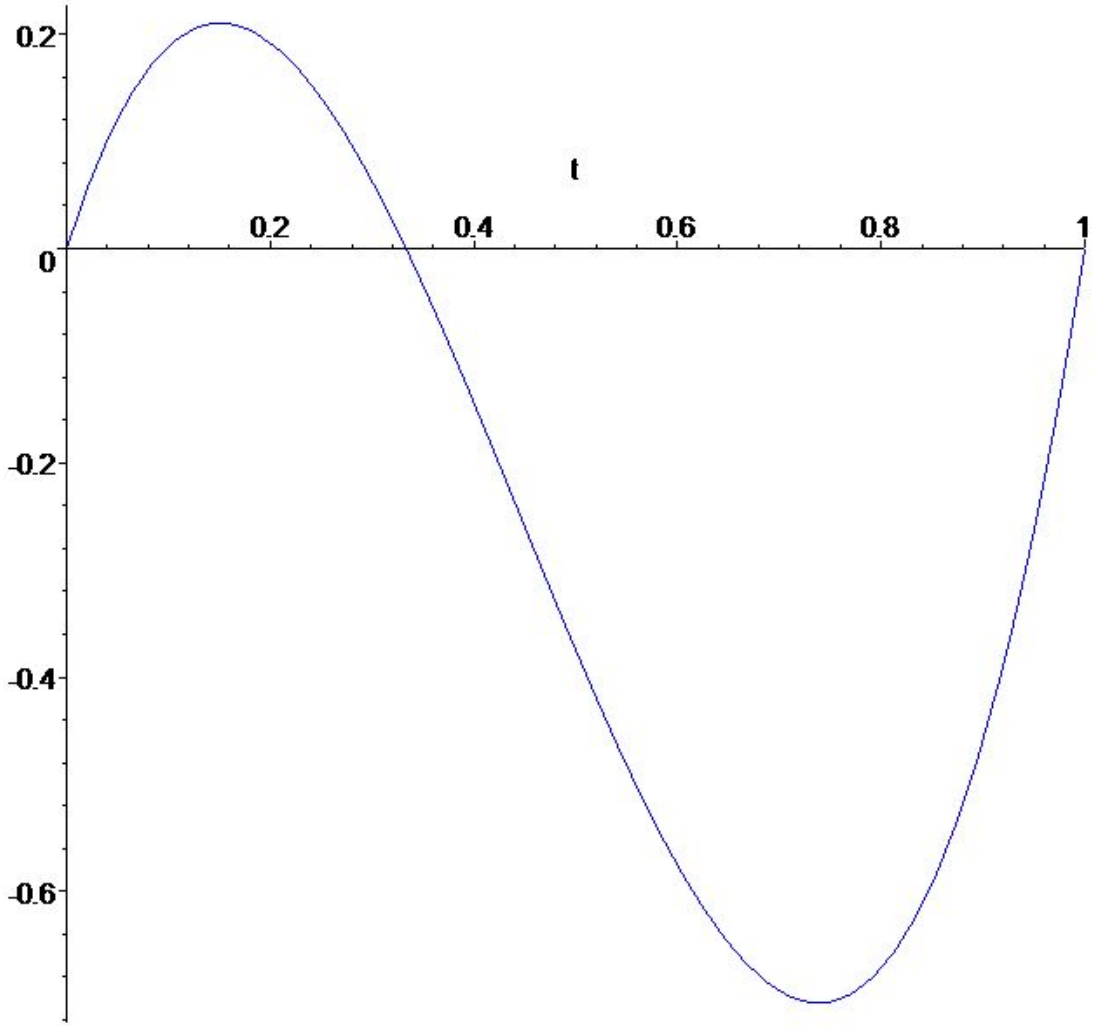
Intialize $z_0 = \zeta_0$
Itérations :

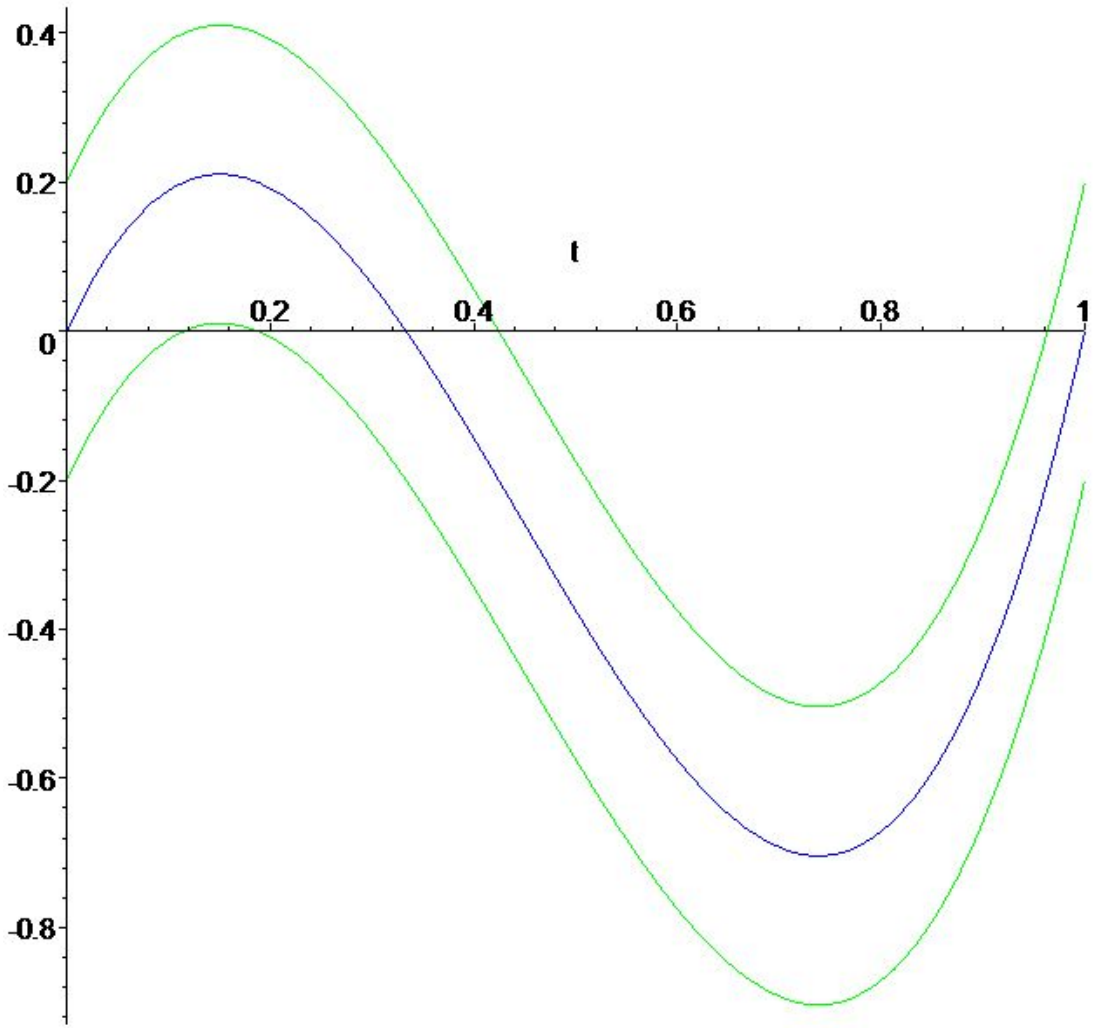
$$z_{i+1} = N_{f_{t_{i+1}}}(z_i)$$

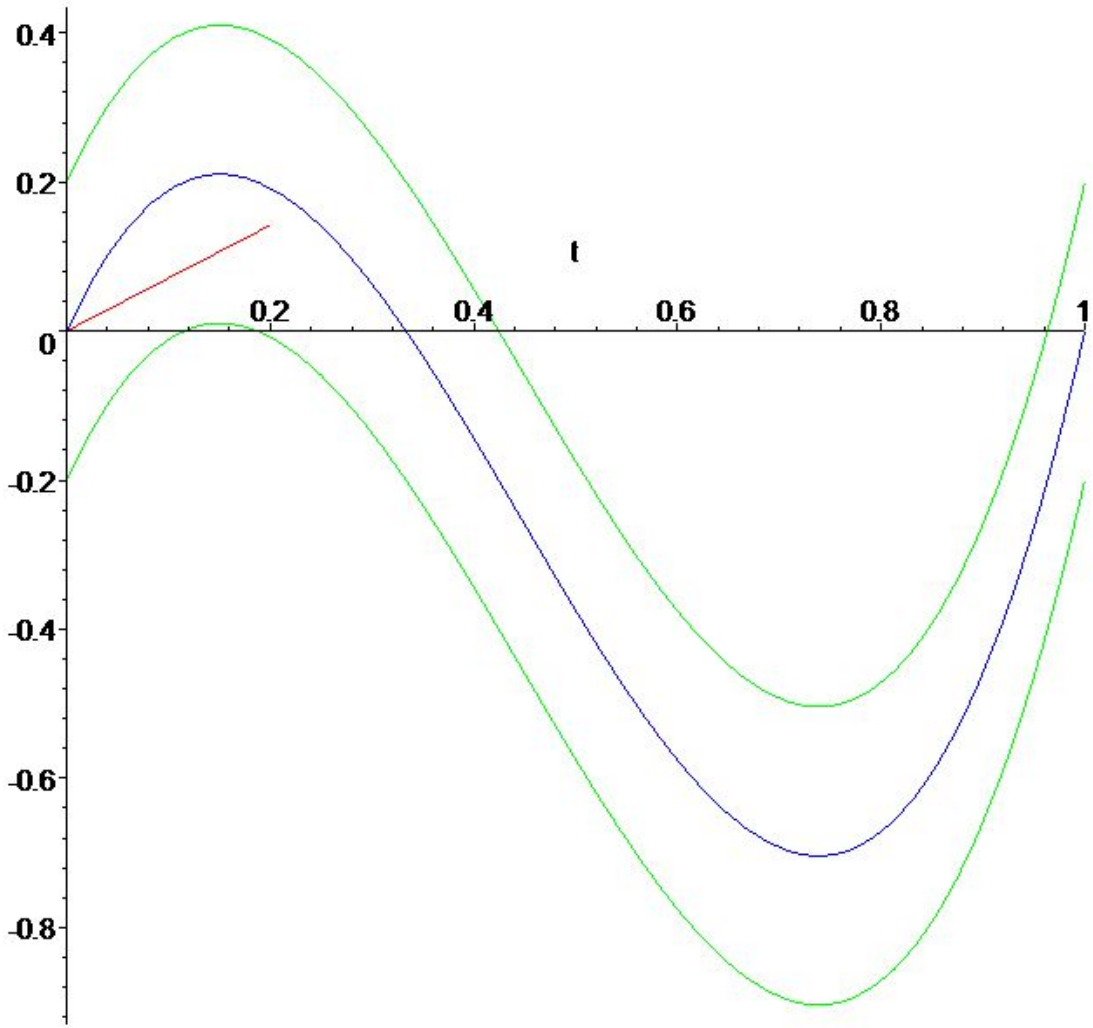
Output : z_k.
Rq.- Les différentes algorithmes dépendent de la façon de choisir les "pas" t_i, mais il faut tenir en compte que :
t_i est construit de telle façon que z_i est dans le "strong basin of attraction" dus suivant systme $f_{t_{i+1}}$. Le plus comfortable est choisir les points t_i de telle façon qu'ils satisfait la condition du $\alpha-$Théorème :

$$\alpha(f_{t_{i+1}}, z_i) < \alpha_0$$

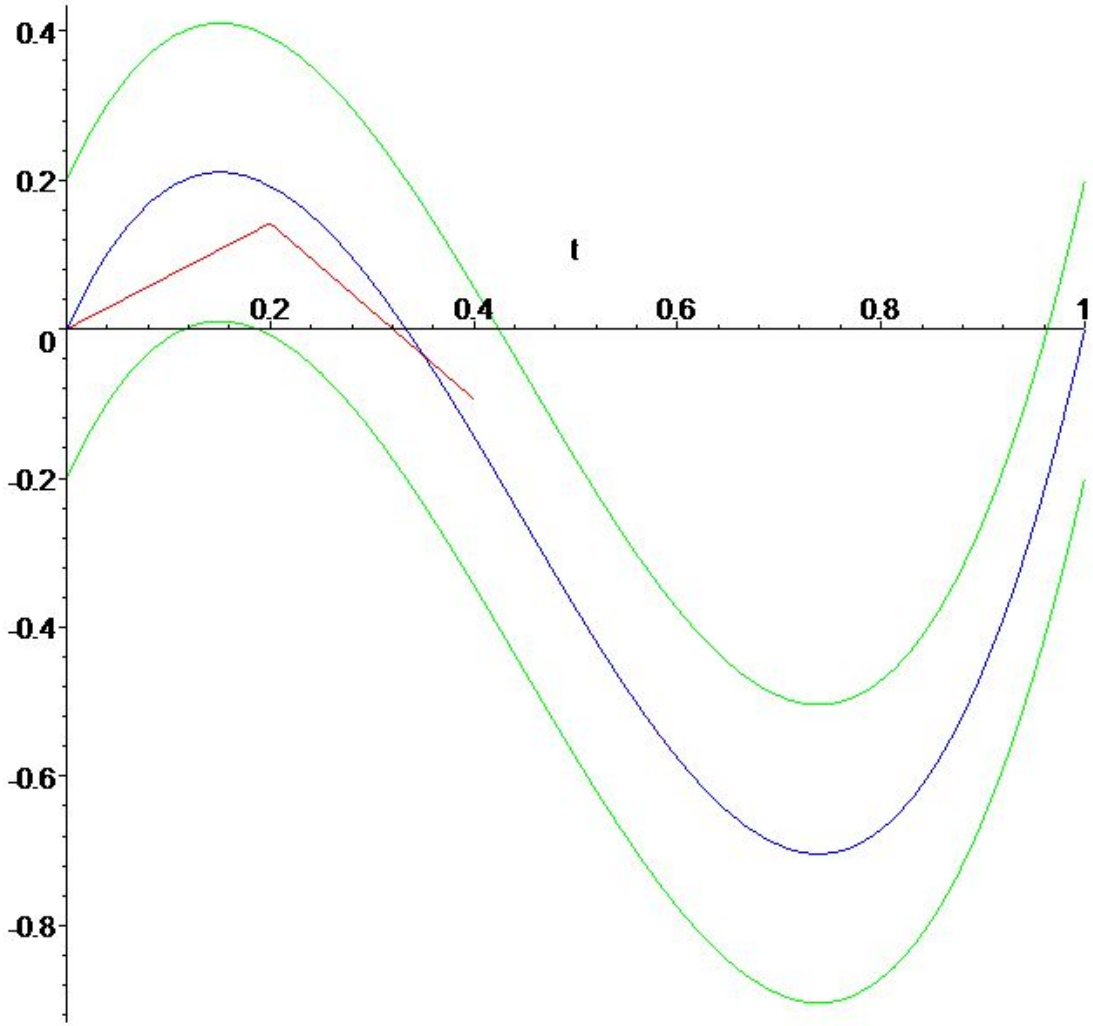
Des dessins : relévement



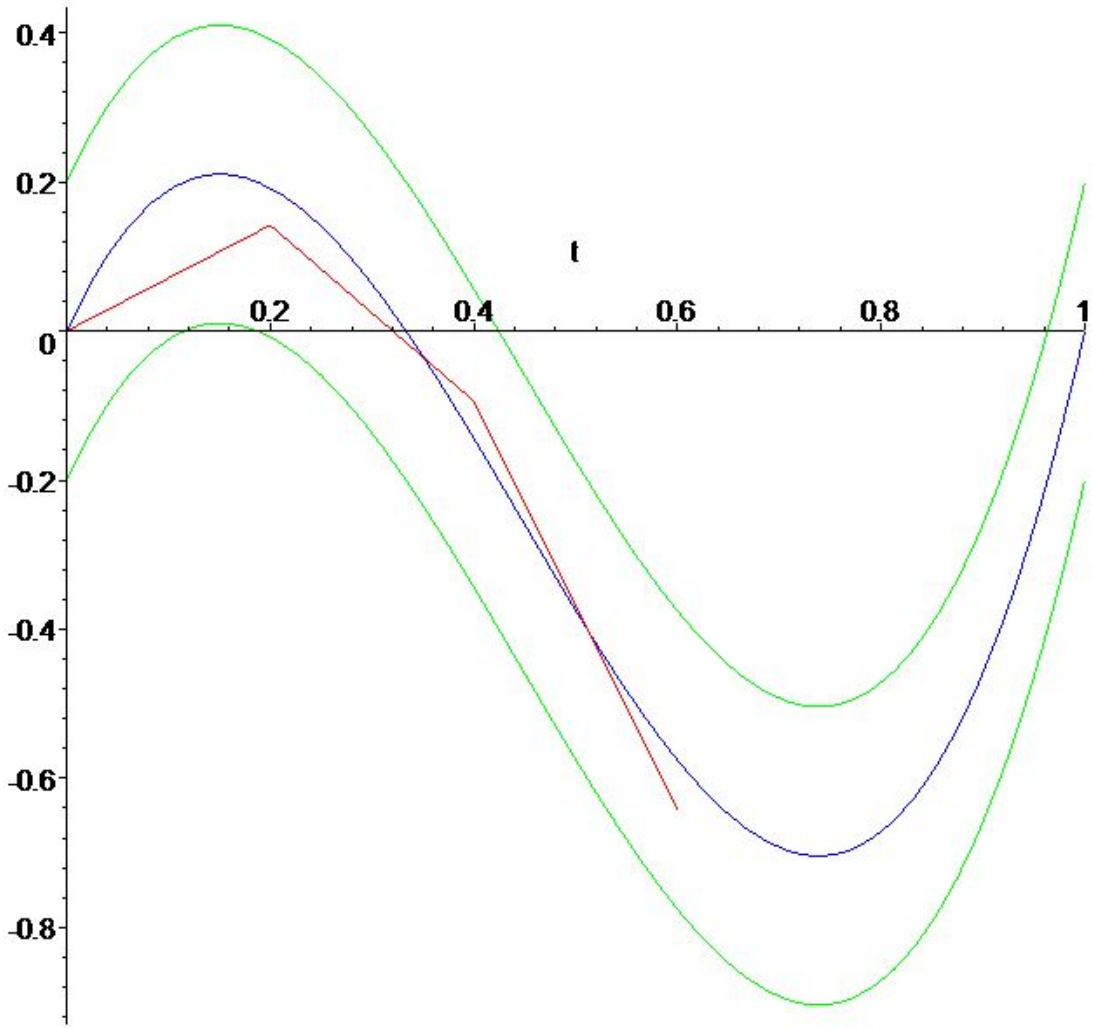

0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
t
0.2
0.4
0.6
0.8
1

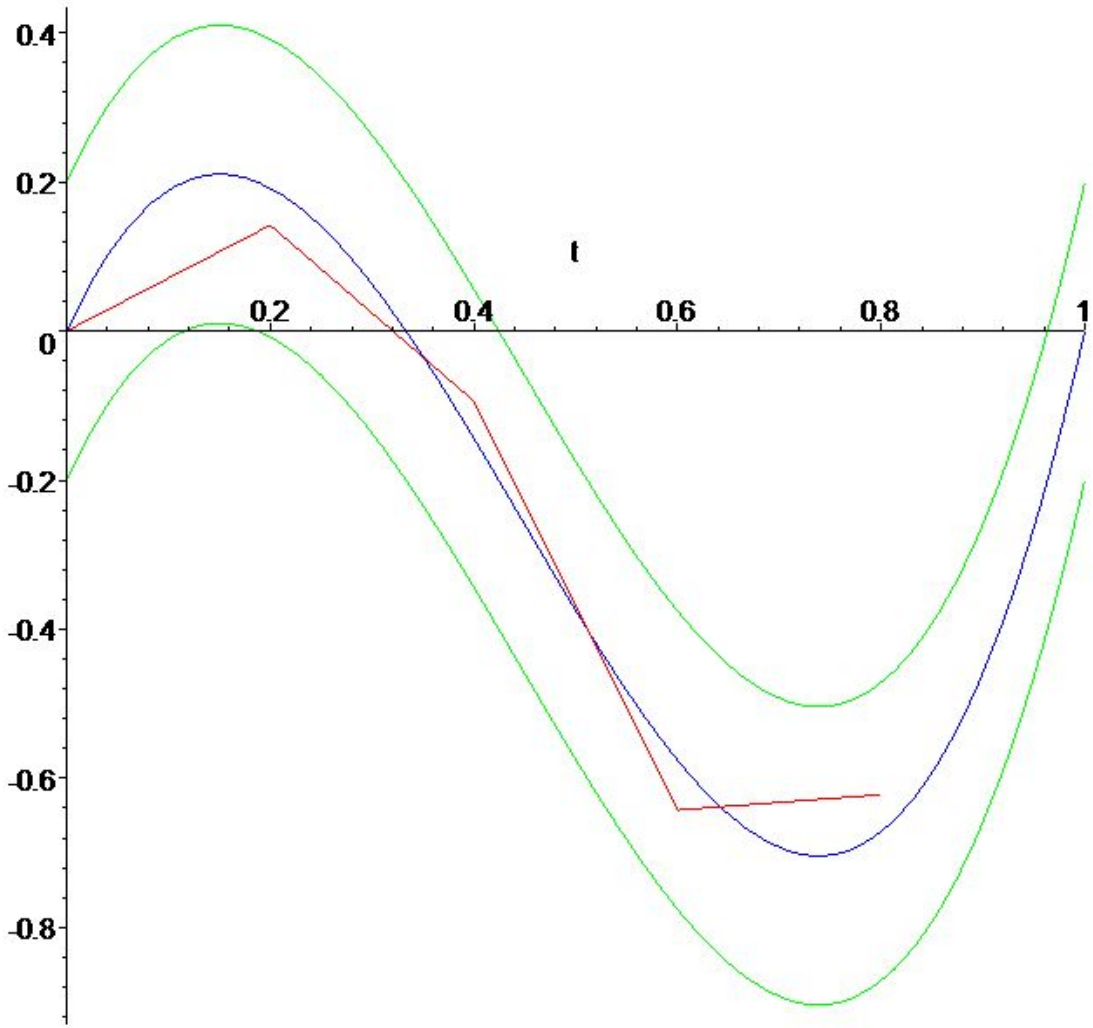

0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
t
0.2
0.4
0.6
0.8
1

Itérations...

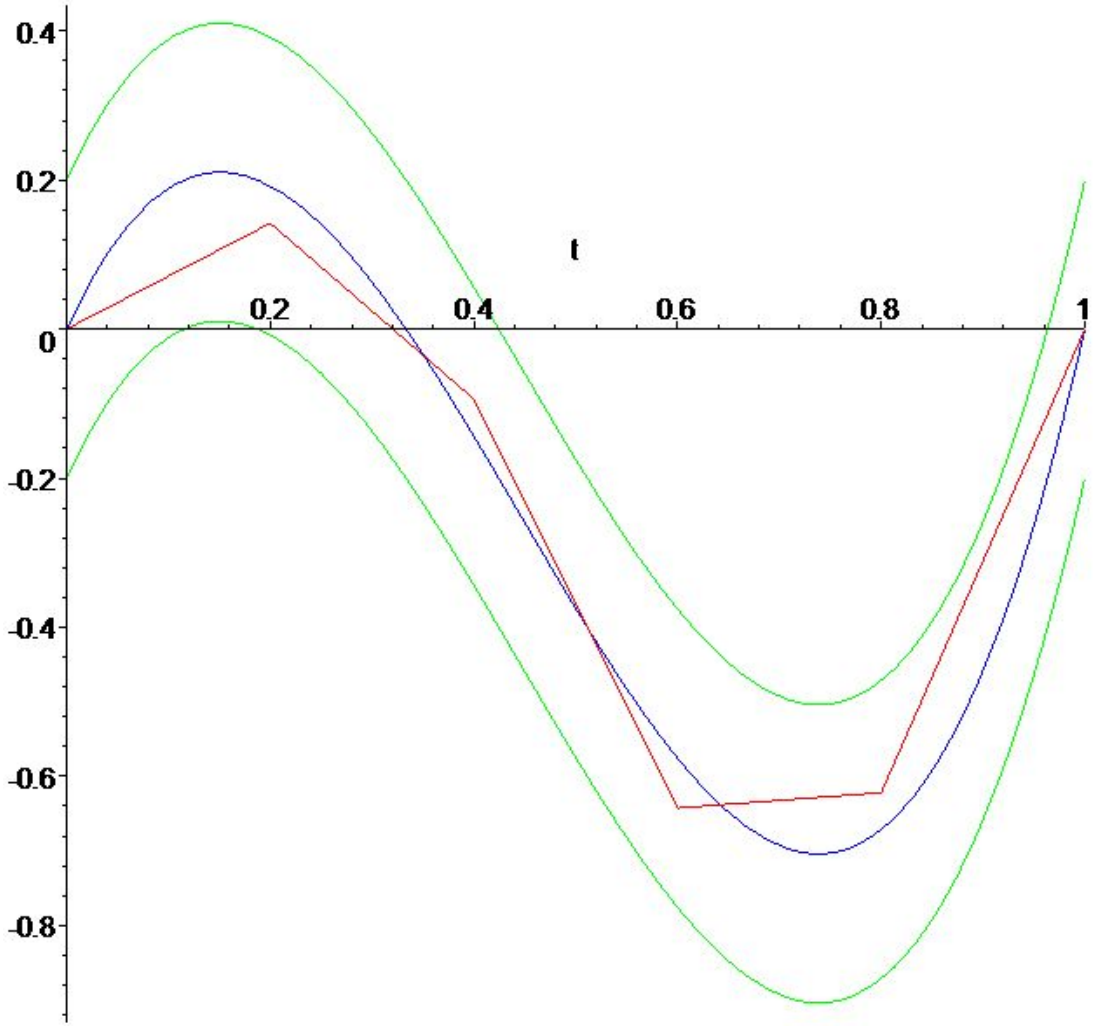


Itérations...




0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
t
0.2
0.4
0.6
0.8
1

Itérations : un zéro approché du système à résoudre...



La Complexité/Probabilité

L'option plus efficace serait celle des "géodesiques par rapport au conditionnement"...

L'option plus efficace serait celle des "géodesiques par rapport au conditionnement"...Malhereusement, on sait pas les calculer....même dans le cas linéaire....et la complexité augmente...

L'option plus efficace serait celle des "géodesiques par rapport au conditionnement"...Malhereusement, on sait pas les calculer....même dans le cas linéaire....et la complexité augmente...
L'option dominante est celle de checher des chemins $[f, g]$ les plus simples posibles. Cette idée était déja dans Shub-Smale (années 90) et elle se mantiens :

- Bien dans l'espace affine $[f, g] \subseteq \mathcal{H}_{(d)}$ (voir, par exemple, [Bürgisser-Cucker, 11]).
- Bien comme un grand circle $L(f, g) \subseteq \mathbb{S}(\mathcal{H}_{(d)})$ dans la sphère de rayon 1 par rapport à la métrique de Bombieri-Weyl. En projettant depuis le segment $[f, g]$
- Ou sur l'espace projectif (courbe enlèvée à la sphère....)

L'option plus efficace serait celle des "géodesiques par rapport au conditionnement"...Malhereusement, on sait pas les calculer....même dans le cas linéaire....et la complexité augmente...
L'option dominante est celle de checher des chemins $[f, g]$ les plus simples posibles. Cette idée était déja dans Shub-Smale (années 90) et elle se mantiens :

- Bien dans l'espace affine $[f, g] \subseteq \mathcal{H}_{(d)}$ (voir, par exemple, [Bürgisser-Cucker, 11]).
- Bien comme un grand circle $L(f, g) \subseteq \mathbb{S}(\mathcal{H}_{(d)})$ dans la sphère de rayon 1 par rapport à la métrique de Bombieri-Weyl. En projettant depuis le segment $[f, g]$
- Ou sur l'espace projectif (courbe enlèvée à la sphère....)

Rq.- Le projectif suffira : parce que (selon [Beltrán-**P.**, 09]) tout peut se faire en projectif et aprés le cas affine est assez accesible : La raison est que la taille/norme des zéros d'un système affine est très petite en moyenne [Pardo-**P.**, 14].

$$E_{f \in \mathcal{H}_{(d)}}[\log_{av} || \cdot ||_1] = \psi(n+1) - \psi(1) = H_n,$$

- Dans les version implementées de Verschelde- Bates- Sommesse- Wampler etc. (Bertini), je ne suis pas même capable de deviner comme est-ce qu'ils choisissent la longeur des pas...ni s'ils on jamais demontré pourquoi ces pas là sont bien choisis...

- Dans les version implementées de Verschelde- Bates- Sommesse- Wampler etc. (Bertini), je ne suis pas même capable de deviner comme est-ce qu'ils choisissent la longeur des pas...ni s'ils on jamais demontré pourquoi ces pas là sont bien choisis...
- Dans les premières version de Shub- Smale : l'idée était celle de contrôler la moyenne du conditionnement (en gros)...alors ils ont decidé choisir le **pas de longueur constante** : la distance entre $t_i - t_{i+1} = 1/H$.

- Dans les version implementées de Verschelde- Bates- Sommesse- Wampler etc. (Bertini), je ne suis pas même capable de deviner comme est-ce qu'ils choisissent la longeur des pas...ni s'ils on jamais demontré pourquoi ces pas là sont bien choisis...
- Dans les premières version de Shub- Smale : l'idée était celle de contrôler la moyenne du conditionnement (en gros)...alors ils ont decidé choisir le **pas de longueur constante** : la distance entre $t_i - t_{i+1} = 1/H$.
- Plus récentement, dèja dans Shub-Smale, Bezout V, et aussi dans [Shub, 07] et ses adaptations : **le pas de longuer adaptée au conditionnement (stisfaisant le $\alpha-$Théorème)**.

Une fois qu'on a fixé un chemin "en bas" $[f, g] \subseteq \mathbb{P}(\mathcal{H}_{(d)})$ et une solution $\zeta_0 \in V_{\mathbb{P}}(g)$ on a un relèvement $\Gamma(f, g, \zeta_0) \subseteq V_{(d)}$ dans la variété solution.

Theorem (Shub-Smale, 93-4)

Soit

$$\mu_{\max}(\Gamma) := \max\{\mu_{\text{norm}}(f_t, \zeta_t) \ : \ (f_t, \zeta_t) \in \Gamma(f, g, \zeta_0)\}.$$

Soit

$$k \geq 18 D^{3/2} \mu_{\max}(\Gamma)^2$$

, *où* $D := \max\{d_1, \ldots, d_n\}$. *Alors, l'homotopie à pas constant, avec* k *pas, permet d'obtenir un zéro approché de* f *à partir d'un zéro approché de* g *associé à* ζ_0. *La complexité est alors, de l'ordre :*

$$O(D^{3/2} \mu_{\max}(\Gamma)^2)$$

Leur problème deviens, alors, trouver un bon système initial g et un bon zéro tel que pour la plupart des systèmes cette méthode se comporte “bien”, en moyenne.

Leur problème deviens, alors, trouver un bon système initial g et un bon zéro tel que pour la plupart des systèmes cette méthode se comporte "bien", en moyenne. Ils proposent :

Conjecture[Shub-Smale, Bez V] Le système initial :

$$G(z) = \begin{cases} d_1^{1/2} z_0^{d_1-1} z_1, \\ \vdots \\ d_n^{1/2} z_0^{d_n-1} z_n \end{cases},$$

avec zéro intial $e_0 = (1, 0, \ldots, 0)$ doit être un bon système initial a.e.

Leur problème deviens, alors, trouver un bon système initial g et un bon zéro tel que pour la plupart des systèmes cette méthode se comporte "bien", en moyenne. Ils proposent :

Conjecture[Shub-Smale, Bez V] Le système initial :

$$G(z) = \begin{cases} d_1^{1/2} z_0^{d_1-1} z_1, \\ \vdots \\ d_n^{1/2} z_0^{d_n-1} z_n \end{cases},$$

avec zéro intial $e_0 = (1, 0, \ldots, 0)$ doit être un bon système initial a.e.
Ce qu'ils attendait est que la moyenne :

$$E_{f \in \mathbb{P}(\mathcal{H}_{(d)})} \left[\mu_{\max}(\Gamma(f, G, e_0))^2 \right] \leq N^{O(1)},$$

où $N := \dim(\mathcal{H}_{(d)})$.

Leur problème deviens, alors, trouver un bon système initial g et un bon zéro tel que pour la plupart des systèmes cette méthode se comporte "bien", en moyenne. Ils proposent :

Conjecture[Shub-Smale, Bez V] Le système initial :

$$G(z) = \begin{cases} d_1^{1/2} z_0^{d_1-1} z_1, \\ \vdots \\ d_n^{1/2} z_0^{d_n-1} z_n \end{cases},$$

avec zéro intial $e_0 = (1, 0, \ldots, 0)$ doit être un bon système initial a.e.
Ce qu'ils attendait est que la moyenne :

$$E_{f \in \mathbb{P}(\mathcal{H}_{(d)})} \left[\mu_{\max}(\Gamma(f, G, e_0))^2 \right] \leq N^{O(1)},$$

où $N := \dim(\mathcal{H}_{(d)})$.La question reste ouverte, même aujourd'hui.

- Au lieu de chercher un système initial "miraculeux", cherchons une méthode probabiliste : un ensemble questeur $\mathcal{G}_{(d)}$. Il s'agit des systèmes qui s'annulent sur le point projectif $e_0 := (1 : 0 : \ldots : 0)$. Et ils sont faciles à construire.

- Au lieu de chercher un système initial "miraculeux", cherchons une méthode probabiliste : un ensemble questeur $\mathcal{G}_{(d)}$. Il s'agit des systèmes qui s'annulent sur le point projectif $e_0 := (1 : 0 : \ldots : 0)$. Et ils sont faciles à construire.
- Au lieu de fixer le nombre des pas dans l'absolu, chercher un nombre de pas que depends d'aun paramètre ε.

$$p(n, N, D, \varepsilon) := 18 * 10^4 n^5 N^2 D^3 \varepsilon^{-2}.$$

- Au lieu de chercher un système initial "miraculeux", cherchons une méthode probabiliste : un ensemble questeur $\mathcal{G}_{(d)}$. Il s'agit des systèmes qui s'annulent sur le point projectif $e_0 := (1 : 0 : \ldots : 0)$. Et ils sont faciles à construire.
- Au lieu de fixer le nombre des pas dans l'absolu, chercher un nombre de pas que depends d'aun paramètre ε.

$$p(n, N, D, \varepsilon) := 18 * 10^4 n^5 N^2 D^3 \varepsilon^{-2}.$$

- Un système initial (g, ζ_0) est appelé $\varepsilon-$efficient si la probabilité de qu'un système f soit résolu dans $p(n, N, D, \varepsilon)$ pas es plus grande que :

$$1 - \varepsilon$$

Theorem (Beltrán-**P.**, 08)

L'ensemble $\mathcal{G}_{(d)}$ *vérifie :*

- *La pobabilité qu'un pair* $(g, \zeta_0) \in \mathcal{G}_{(d)}$ *choisi au hasard, soit un pair* $\varepsilon-$*efficient est plus grande que* $1 - \varepsilon$.
- *La pobabilité qu'un pair* $(g, \zeta_0) \in \mathcal{G}_{(d)}$ $\varepsilon-$*efficient, permet résoudre un système* $f \in \mathbb{P}(\mathcal{H}_{(d)}$ *dans moins de* $O(n^5 N^2 D^3 \varepsilon^{-2})$ *pas d'homotopie à pas constant es plus grande que :*

$$1 - \varepsilon$$

Theorem (Beltrán-**P.**, 08)

L'ensemble $\mathcal{G}_{(d)}$ *vérifie :*

- *La pobabilité qu'un pair* $(g, \zeta_0) \in \mathcal{G}_{(d)}$ *choisi au hasard, soit un pair* $\varepsilon-$*efficient est plus grande que* $1 - \varepsilon$.
- *La pobabilité qu'un pair* $(g, \zeta_0) \in \mathcal{G}_{(d)}$ $\varepsilon-$*efficient, permet résoudre un système* $f \in \mathbb{P}(\mathcal{H}_{(d)}$ *dans moins de* $O(n^5 N^2 D^3 \varepsilon^{-2})$ *pas d'homotopie à pas constant es plus grande que :*

$$1 - \varepsilon$$

Ex. : Cas cubique $(d) = (3, 3, \ldots, 3)$,il existe un algorithme probabiliste (Monte Carlo) en temps $O((N)^{4.1})$ capable de résoudre (certifiée) avec une probabilité plus grande que :

$$1 - 1/N^{1/2}.$$

- C'était une méthode MonteCarlo et pas Las Vegas.
- Il ne sert que pour résoudre des systèmes avec une grande probabilité se succés. Mais, la probabilité de succés est liée au temps de calcul : plus de succés, plus grande complexité.
- L'ensemble questeur $\mathcal{G}_{(d)}$ qu'on a introduit est calculable, mais pas élégant...Ils sont tous des systémes que s'annulent sur $e_0 := (1 : 0 : \cdots : 0)$. On les construit avec trois paramètres :
  1. Une matrice carrée qui determine un système d'équations $h_1 = (h_{1,1}, \ldots, h_{1,n})$ dans l'espace vectoriel L_{e_0}, donnée par des listes de polynômes :
  $$h_{1,i} := d_1^{1/2} X_0^{d_i - 1} \ell_i(\underline{X}) = \ell_i(X_1, \ldots, X_n),$$
  ℓ_i étant linéaire.
  2. Un système h_2 dans l'espace vectoriel $L_{e_0}^{\perp}$ des systèmes qui ont e_0 comme racine avec ordre au moins 2.
  3. Un nombre $t \in [0, 1]$
  4. Une quantité τ pour équilibrer.

Le produit finale est un pair initial (g, e_0), donné par un système polynomiale :

$$g := \tau t^{1/(2n^2+n)} \frac{h_1}{\|h_1\|} + (1 - \tau^2 t^{1/(n^2+n)})^{1/2} \frac{h_2}{\|h_2\|}.$$

Le produit finale est un pair initial (g, e_0), donné par un système polynomiale :

$$g := \tau t^{1/(2n^2+n)} \frac{h_1}{\|h_1\|} + (1 - \tau^2 t^{1/(n^2+n)})^{1/2} \frac{h_2}{\|h_2\|}.$$

La partie dure de la preuve était celle de demontrer que $\mathcal{G}_{(d)}$ est un ensemble questeur.

Le produit finale est un pair initial (g, e_0), donné par un système polynomiale :

$$g := \tau t^{1/(2n^2+n)} \frac{h_1}{\|h_1\|} + (1 - \tau^2 t^{1/(n^2+n)})^{1/2} \frac{h_2}{\|h_2\|}.$$

La partie dure de la preuve était celle de demontrer que $\mathcal{G}_{(d)}$ est un ensemble questeur. Mais ce n'est pas qu'un "peu" de Géométrie Intégrale sur des variétés projectives...Exercise...

Le produit finale est un pair initial (g, e_0), donné par un système polynomiale :

$$g := \tau t^{1/(2n^2+n)} \frac{h_1}{\|h_1\|} + (1 - \tau^2 t^{1/(n^2+n)})^{1/2} \frac{h_2}{\|h_2\|}.$$

La partie dure de la preuve était celle de demontrer que $\mathcal{G}_{(d)}$ est un ensemble questeur. Mais ce n'est pas qu'un "peu" de Géométrie Intégrale sur des variétés projectives...Exercise...45 pages dans FoCM

Le produit finale est un pair initial (g, e_0), donné par un système polynomiale :

$$g := \tau t^{1/(2n^2+n)} \frac{h_1}{\|h_1\|} + (1 - \tau^2 t^{1/(n^2+n)})^{1/2} \frac{h_2}{\|h_2\|}.$$

La partie dure de la preuve était celle de demontrer que $\mathcal{G}_{(d)}$ est un ensemble questeur. Mais ce n'est pas qu'un "peu" de Géométrie Intégrale sur des variétés projectives...Exercise...45 pages dans FoCM

En tout cas, ce type de méthodes ne sert que pour obtenir une suele solution et, peut être, toujours la même... ?

Le produit finale est un pair initial (g, e_0), donné par un système polynomiale :

$$g := \tau t^{1/(2n^2+n)} \frac{h_1}{\|h_1\|} + (1 - \tau^2 t^{1/(n^2+n)})^{1/2} \frac{h_2}{\|h_2\|}.$$

La partie dure de la preuve était celle de demontrer que $\mathcal{G}_{(d)}$ est un ensemble questeur. Mais ce n'est pas qu'un "peu" de Géométrie Intégrale sur des variétés projectives...Exercise...45 pages dans FoCM

En tout cas, ce type de méthodes ne sert que pour obtenir une suele solution et, peut être, toujours la même... ?
La solution viendrait des homotopies de pas adapté.

Il était deja presente dans [Shub-Smale, 94].

Il était deja presente dans [Shub-Smale, 94].
Au lieu d'un pas constant (passage de t_i à t_{i+1}), on peut utiliser una pas adapté.

Il était deja presente dans [Shub-Smale, 94].
Au lieu d'un pas constant (passage de t_i à t_{i+1}), on peut utiliser una pas adapté.
Par exemple,

$$\triangle t := \frac{\lambda}{d_R(f,g)D^{3/2}\mu_{\text{norm}}(f_t,z_t)^2}.$$

et

$$t_{i+1} := t_i + \triangle t_i.$$

Il était deja presente dans [Shub-Smale, 94].
Au lieu d'un pas constant (passage de t_i à t_{i+1}), on peut utiliser una pas adapté.
Par exemple,

$$\triangle t := \frac{\lambda}{d_R(f,g)D^{3/2}\mu_{\text{norm}}(f_t,z_t)^2}.$$

et

$$t_{i+1} := t_i + \triangle t_i.$$

Theorem (Shub-Smale, 94)

Le nombre des pas suffisants por l'homotopie “adaptée” est borné par :

$$\mu_{\max}(\Gamma(f,g,\zeta_0))L,$$

où L est la longueur du relèvement $L := Length(\Gamma(f,g,\zeta_0)) \subseteq V_{(d)}$.

Un truc :

- $L \leq \mu_{\max}(\Gamma(f, g, \zeta_0))$,

Un truc :

- $L \leq \mu_{\max}(\Gamma(f, g, \zeta_0))$,
- $L \leq \mathcal{D}_{(d)} := \prod_{i=1}^{n} d_i$.

Alors, le nombre des pas d'homotopie est borné par

$$\mu_{\max}(\Gamma(f, g, \zeta_0))^{2-\frac{1}{\log(\mathcal{D}_{(d)})}} \mathcal{D}_{(d)}^{\frac{1}{\log(\mathcal{D}_{(d)})}} \leq cte\mu_{\max}(\Gamma(f, g, \zeta_0))^{2-\frac{1}{\log(\mathcal{D}_{(d)})}}.$$

Un truc :

- $L \leq \mu_{\max}(\Gamma(f, g, \zeta_0))$,
- $L \leq \mathcal{D}_{(d)} := \prod_{i=1}^{n} d_i$.

Alors, le nombre des pas d'homotopie est borné par

$$\mu_{\max}(\Gamma(f, g, \zeta_0))^{2-\frac{1}{\log(\mathcal{D}_{(d)})}} \mathcal{D}_{(d)}^{\frac{1}{\log(\mathcal{D}_{(d)})}} \leq cte\mu_{\max}(\Gamma(f, g, \zeta_0))^{2-\frac{1}{\log(\mathcal{D}_{(d)})}}.$$

Avec ces elements on peut deja donner une réponse positive au problème 17-ième de Smale dans
[Beltrán- **P.**, J AMS (2009)]

Theorem

Il existe un algorithme Las Vegas pour la résolution du problème 17-ième de Smale en temps polynomial.

1. *Le caractère Las Vegas viens de l'utilisation de l'ensemble "questeur"* $\mathcal{G}_{(d)}$ *de [Beltrán-**P.**, 08].*
2. *Il sert tant pour les solutions projectives comme pour les solutions affines.*
3. *Le temps moyenne de calcul est de l'ordre* $O(n^6 N^3 D^3 \log \mathcal{D}_{(d)})$*, où* N *est la taille de l'entrée en codification dense,* D *est le maximum des degrés.*

Theorem

Il existe un algorithme Las Vegas pour la résolution du problème 17-ième de Smale en temps polynomial.

1. *Le caractère Las Vegas viens de l'utilisation de l'ensemble "questeur"* $\mathcal{G}_{(d)}$ *de [Beltrán-**P.**, 08].*
2. *Il sert tant pour les solutions projectives comme pour les solutions affines.*
3. *Le temps moyenne de calcul est de l'ordre* $O(n^6 N^3 D^3 \log \mathcal{D}_{(d)})$*, où* N *est la taille de l'entrée en codification dense,* D *est le maximum des degrés.Le cas affine donne une complexité moyenne de l'ordre* $O(N^5)$*.*
4. *Le nombre des pas d'homotopie est de l'ordre* $O(n^3 N^2 D^3)$*.*

La problème 17-ième est résolu sous ça forme originale...

- Ce fois-ci, ça commence à faire du bruit. Les gens commencent a s'énérver...

La problème 17-ième est résolu sous ça forme originale...

- Ce fois-ci, ça commence à faire du bruit. Les gens commencent a s'énérver...
- L'algorithm est Las Vegas, mais pas déterministe...à mon avis, ça change pas grande chose...Non-plus dans la tête de Smale (au moins en 2002..anecdote sur AKS...).

La problème 17-ième est résolu sous ça forme originale...

- Ce fois-ci, ça commence à faire du bruit. Les gens commencent a s'énérver...
- L'algorithm est Las Vegas, mais pas déterministe...à mon avis, ça change pas grande chose...Non-plus dans la tête de Smale (au moins en 2002..anecdote sur AKS...).
- Il y a deux problèmes encore :
  1. La méthode semble résoudre q'une solution pour chanque système donné : l'homotopie à partir de $\mathcal{G}_{(d)}$ commence toujours dans $e_0 := (1 : 0 : \cdots : 0)$. Ça va à arriver toujours à la même solution...paraît-il.

La problème 17-ième est résolu sous ça forme originale...

- Ce fois-ci, ça commence à faire du bruit. Les gens commencent a s'énérver...
- L'algorithm est Las Vegas, mais pas déterministe...à mon avis, ça change pas grande chose...Non-plus dans la tête de Smale (au moins en 2002..anecdote sur AKS...).
- Il y a deux problèmes encore :
  1. La méthode semble résoudre q'une solution pour chanque système donné : l'homotopie à partir de $\mathcal{G}_{(d)}$ commence toujours dans $e_0 := (1 : 0 : \cdots : 0)$. Ça va à arriver toujours à la même solution...paraît-il.
  2. L'ensemble questeur $\mathcal{G}_{(d)}$ n'est pas chic. Et les gens n'arrivent pas à comprendre très bien la preuve : ce n'est qu'un "peu" de Géométrie Intégrale, mais.....

La problème 17-ième est résolu sous ça forme originale...

- Ce fois-ci, ça commence à faire du bruit. Les gens commencent a s'énérver...
- L'algorithm est Las Vegas, mais pas déterministe...à mon avis, ça change pas grande chose...Non-plus dans la tête de Smale (au moins en 2002..anecdote sur AKS...).
- Il y a deux problèmes encore :
  1. La méthode semble résoudre q'une solution pour chanque système donné : l'homotopie à partir de $\mathcal{G}_{(d)}$ commence toujours dans $e_0 := (1 : 0 : \cdots : 0)$. Ça va à arriver toujours à la même solution...paraît-il.
  2. L'ensemble questeur $\mathcal{G}_{(d)}$ n'est pas chic. Et les gens n'arrivent pas à comprendre très bien la preuve : ce n'est qu'un "peu" de Géométrie Intégrale, mais.....
- En plus, la borne $O(N^2)$ des pas d'homotopie...peut-on l'améliorer ?.

On avait dit que le nombre des pas dans le cas adaptatif sont bornés par

$$\mu_{\max}(\Gamma)L(\Gamma) = \mu_{\max}(\Gamma)\int_0^1 \left(\|\dot{f}\|^2 + \|\dot{\zeta}\|^2\right)^{1/2} dt.$$

On avait dit que le nombre des pas dans le cas adaptatif sont bornés par

$$\mu_{\max}(\Gamma)L(\Gamma) = \mu_{\max}(\Gamma)\int_0^1 \left(\|\dot{f}\|^2 + \|\dot{\zeta}\|^2\right)^{1/2} dt.$$

Shub se rends compte qu'on peut être plus fin :

Proposition (Shub, 09)

Le nombre des pas dans une méthode adataptive dominé par le $\alpha-$Théorème est borné par

$$C\int_0^1 \mu_{\text{norm}}(f(t,\zeta_t)) \left(\|\dot{f}\|^2 + \|\dot{\zeta}\|^2\right)^{1/2} dt.$$

Trouver la constante C...pas trop important.

Souvenez-vous de l'espace tangent :

$$T_{(f,\zeta)}V_{(d)} := \{(\dot{f},\dot{\zeta}) \ : \ \dot{f}(\zeta) + T_\zeta f(\dot{\zeta}) = 0\}.$$

Souvenez-vous de l'espace tangent :

$$T_{(f,\zeta)}V_{(d)} := \{(\dot{f},\dot{\zeta}) \ : \ \dot{f}(\zeta) + T_\zeta f(\dot{\zeta}) = 0\}.$$

Alors, $\|\dot{\zeta}\| \leq \|(T_\zeta f)^{-1}\|\|\dot{f}\|$.

Souvenez-vous de l'espace tangent :

$$T_{(f,\zeta)}V_{(d)} := \{(\dot{f},\dot{\zeta}) \ : \ \dot{f}(\zeta) + T_\zeta f(\dot{\zeta}) = 0\}.$$

Alors, $\|\dot{\zeta}\| \leq \|(T_\zeta f)^{-1}\|\|\dot{f}\|$.
En conclusion, la borne deviens (et elle peut être utilisée comme ça) :

$$C\int_0^1 \mu_{\text{norm}}(f(t,\zeta_t))\left(\|\dot{f}\|^2 + \|\dot{\zeta}\|^2\right)^{1/2} dt \leq C\int_{\gamma(f,g)} \mu_{\text{norm}}(f(t,\zeta_t))^2 d\gamma.$$

Souvenez-vous de l'espace tangent :

$$T_{(f,\zeta)}V_{(d)} := \{(\dot{f},\dot{\zeta}) \ : \ \dot{f}(\zeta) + T_\zeta f(\dot{\zeta}) = 0\}.$$

Alors, $\|\dot{\zeta}\| \leq \|(T_\zeta f)^{-1}\|\|\dot{f}\|$.
En conclusion, la borne deviens (et elle peut être utilisée comme ça) :

$$C\int_0^1 \mu_{\text{norm}}(f(t,\zeta_t))\left(\|\dot{f}\|^2 + \|\dot{\zeta}\|^2\right)^{1/2} dt \leq C\int_{\gamma(f,g)} \mu_{\text{norm}}(f(t,\zeta_t))^2 d\gamma.$$

On peut tout recommencer et nous obtenons [Beltrán-**P.**, 11] (écrit et diffusé vers 2008-09)

On construit un nouveau ensemble questeur $\mathcal{U}_{(d)}$:

- Choix aléatoire d'une matrice $M \in \mathcal{M}_{n\times(n+1)}(\mathbb{C})$.

On construit un nouveau ensemble questeur $\mathcal{U}_{(d)}$:

- Choix aléatoire d'une matrice $M \in \mathcal{M}_{n\times(n+1)}(\mathbb{C})$.
- Calcul d'un point ζ dans $\ker(M)$.

On construit un nouveau ensemble questeur $\mathcal{U}_{(d)}$:

- Choix aléatoire d'une matrice $M \in \mathcal{M}_{n\times(n+1)}(\mathbb{C})$.
- Calcul d'un point ζ dans $\ker(M)$.
- Choix aléatoire d'un système $h_2 := (h_{2,1}, \ldots, h_{2,n})$ tel que chaque $h_{2,i}$ a un ordre au moins 2 sur ζ.

On construit un nouveau ensemble questeur $\mathcal{U}_{(d)}$:

- Choix aléatoire d'une matrice $M \in \mathcal{M}_{n\times(n+1)}(\mathbb{C})$.
- Calcul d'un point ζ dans $\ker(M)$.
- Choix aléatoire d'un système $h_2 := (h_{2,1}, \ldots, h_{2,n})$ tel que chaque $h_{2,i}$ a un ordre au moins 2 sur ζ.
- Le système $h_1 = (h_{1,1}, \ldots, h_{1,n})$ associé à la matrice M

$$Diag(d_i^{1/2}\langle \underline{X}, \zeta\rangle^{d_i-1})M \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

On construit un nouveau ensemble questeur $\mathcal{U}_{(d)}$:

- Choix aléatoire d'une matrice $M \in \mathcal{M}_{n\times(n+1)}(\mathbb{C})$.
- Calcul d'un point ζ dans $\ker(M)$.
- Choix aléatoire d'un système $h_2 := (h_{2,1}, \ldots, h_{2,n})$ tel que chaque $h_{2,i}$ a un ordre au moins 2 sur ζ.
- Le système $h_1 = (h_{1,1}, \ldots, h_{1,n})$ associé à la matrice M

$$Diag(d_i^{1/2}\langle \underline{X}, \zeta\rangle^{d_i-1})M \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

- Finalement, on commence l'homotopie á :

$$(h_1 + (\sqrt{1 - \|M\|_F^2})h_2, \zeta).$$

Theorem

Il existe an algorithme Las Vegas pour résoudre des systèmes d'équations polynomiales.

1. *Le caractère Las Vegas viens de l'utilisation de l'ensemble "questeur"* $\mathcal{U}_{(d)}$.
2. *Il sert tant pour les solutions projectives comme pour les solutions affines.*
3. *Le temps moyenne de calcul est de l'ordre* $O(nD^{3/2}N(N+n))$, *où* N *est la taille de l'entrée en codification dense,* D *est le maximum des degrés.*

Theorem

Il existe an algorithme Las Vegas pour résoudre des systèmes d'équations polynomiales.

1. *Le caractère Las Vegas viens de l'utilisation de l'ensemble "questeur"* $\mathcal{U}_{(d)}$.
2. *Il sert tant pour les solutions projectives comme pour les solutions affines.*
3. *Le temps moyenne de calcul est de l'ordre* $O(nD^{3/2}N(N+n))$, *où* N *est la taille de l'entrée en codification dense,* D *est le maximum des degrés.Le cas affine donne une complexité moyenne similaire.*
4. *Le nombre des pas d'homotopie est de l'ordre* $O(nD^{3/2}N)$ *(c.à d., linéaire dans la taille de l'entrée).*

Theorem

L'algorithme Las Vegas precédant, satisfait :

1. *L'entropie est maximale, c. à d., on peut calculer n'importe quelle solution du système donné comme entrée.*
2. *Si on le veut, il peut devenir universl, c. à d., On peu calculer K solution différentes en temps*

$$O(KnD^{3/2}N(N+n))$$

Theorem

L'algorithme Las Vegas precédant, satisfait :

1. *L'entropie est maximale, c. à d., on peut calculer n'importe quelle solution du système donné comme entrée.*
2. *Si on le veut, il peut devenir universl, c. à d., On peu calculer K solution différentes en temps*
$$O(KnD^{3/2}N(N+n))$$
3. *Il cacule toutes les solutions en temps*
$$\mathcal{D}_{(d)}O(nD^{3/2}N(N+n))$$
, c. à d., **linéaire dans le nombre de Bézout**.

Deux façons de comprendre le conditionement pour un systéme concret $f \in \mathcal{H}_{(d)}$:

$$\mu^2_{\mathrm{av}}(f) := \frac{1}{\mathcal{D}_{(d)}} \sum_{\zeta \in V_{\mathbb{P}}(f)} \mu^2_{\mathrm{norm}}(f, \zeta).$$

Deux façons de comprendre le conditionement pour un systéme concret $f \in \mathcal{H}_{(d)}$:

$$\mu^2_{\mathrm{av}}(f) := \frac{1}{\mathcal{D}_{(d)}} \sum_{\zeta \in V_{\mathbb{P}}(f)} \mu^2_{\mathrm{norm}}(f,\zeta).$$

$$\mu^2_{\max}(f) := \max\{\mu^2_{\mathrm{norm}}(f,\zeta) \ : \ \zeta \in V_{\mathbb{P}}(f)\}.$$

On connaît (voir [Beltrán-**P.**, 11] ou [Pardo-**P.**, 14]) tout son comportement en moyenne de μ_{av}.

$$E_{f \in \mathcal{H}_{(d)}}[\mu^2_{\mathrm{av}}] \leq nN.$$

Par contre, on ne connaît pas tellement de bonnes bornes pour la moyenne de $\mu_{\max}$

$$E_{f \in \mathcal{H}_{(d)}}[\mu^2_{\max}] \leq \mathcal{D}_{(d)} nN.$$

(c'est mieux que les anciens bornes dans [Shub-Smale], mais on a le $\mathcal{D}_{(d)}$....)

A Zeta Mahler function associated to $1/\mu_{\text{norm}}$:

$$\mathcal{Z}(t, 1/\mu_{\text{norm}}) := \frac{1}{\nu_{\mathbb{S}}[\mathbb{S}(\mathcal{H}_{(d)})]} \int_{f \in \mathbb{S}(\mathcal{H}_{(d)})} \left(\frac{1}{\mathcal{D}_{(d)}} \sum_{\zeta \in V_{\mathbb{P}}(f)} \mu_{\text{norm}}(f, \zeta)^{-t} \right) d\nu_{\mathbb{S}}(f).$$

Theorem ((Beltrán-**P.**, 11), (Pardo-**P.**, 14))

* $\mathcal{Z}(t, 1/\mu_{\text{norm}})$ *is defined and holomorphic in* $G := \{t \in \mathbb{C} \, : \, \Re(t) > -4\} \subseteq \mathbb{C}$.
* $\mathcal{Z}(t, 1/\mu_{\text{norm}})$ *admits analytic continuation to* $\mathbb{C} \setminus \{z \in \mathbb{Z} \, : \, z \leq -4\}$, *and*

$$\mathcal{Z}(t, 1/\mu_{\text{norm}}) = \frac{\Gamma(M_{(d)})}{\Gamma(M_{(d)} + t/2)} \sum_{k=0}^{n-1} \frac{\binom{n+1}{k} \Gamma(n + 1 - k + t/2)}{n^{n-k+1+t/2} \Gamma(n-k)}.$$

À la recherche d'un algorithme "deterministe". À mon avis, rien fascinant...Las Vegas est assez bon !.

À la recherche d'un algorithme "deterministe". À mon avis, rien fascinant...Las Vegas est assez bon !.
Nouveauté : Si on utilise une variation de l'inégalité d'Anderson (usuelle en statistique) avec des techniques de Géométrie Intégral (traduites au niveau probabilistique $N(q, \sigma^2 I)$, plus des méthodes de "smoothed analysis" (A. Edelman, D. Spielman et compagnie)....on obtiens

Theorem (Bürgisser-Cucker, 11)

$$E_{f \in \mathcal{H}_{(d)}}[\int_{\Gamma(f,g,\zeta)} \mu_{\text{norm}}(f_t, \zeta_t)^2 d\Gamma] \leq O(nN\mu^2_{\max}(g)).$$

La complexité moyenne deviens alors borné par :

$$O(DnN^2\mu^2_{\max}(g)).$$

Bürgisser et Cucker ils ont trouvé l'homogenisé du système des racines de l'unité :

$$U := \begin{cases} X_1^{d_1} - X_0^{d_1} \\ \vdots \\ X_n^{d_n} - X_0^{d_n} \end{cases}$$

Bürgisser et Cucker ils ont trouvé l'homogenisé du système des racines de l'unité :

$$U := \begin{cases} X_1^{d_1} - X_0^{d_1} \\ \vdots \\ X_n^{d_n} - X_0^{d_n} \end{cases}$$

Il vérifie :

$$\mu_{\max}(U) = \mu_{\text{av}}(U) \leq n^{D+1},$$

où $D := \max\{d_1, \ldots, d_n\}$.

La complexité de la méthode deviens avec une complexité :

$$O(DnN^2 n^{D+1}).$$

Bürgisser et Cucker ils ont trouvé l'homogenisé du système des racines de l'unité :

$$U := \begin{cases} X_1^{d_1} - X_0^{d_1} \\ \vdots \\ X_n^{d_n} - X_0^{d_n} \end{cases}$$

Il vérifie :

$$\mu_{\max}(U) = \mu_{\text{av}}(U) \leq n^{D+1},$$

où $D := \max\{d_1, \ldots, d_n\}$.
La complexité de la méthode deviens avec une complexité :

$$O(DnN^2 n^{D+1}).$$

Corollary (Bürgisser-Cucker, 14)

Il existe un algorithme deterministe pour résoudre des équations polynomiales en complexité moyenne :

$$N^{2\log(\log(N))+O(1)}.$$

La borne du $\mu_{\max}$ "en fleur" n^{D+1} ([Bürgisser-Cucker, 14]) :

- Si $D \leq n^{1-c}$,

$$n^{D+1} \leq \binom{d+n}{n}^{K},$$

Pour une constante K qui augmente avec c, n.

La borne du $\mu_{\max}$ "en fleur" n^{D+1} ([Bürgisser-Cucker, 14]) :

- Si $D \leq n^{1-c}$,

$$n^{D+1} \leq \binom{d+n}{n}^{K},$$

  Pour une constante K qui augmente avec c, n.

- Si $D \leq n$,

$$n^{D+1} \leq N^{2\log(\log(N))+O(1)}.$$

La borne du $\mu_{\max}$ "en fleur" n^{D+1} ([Bürgisser-Cucker, 14]) :

- Si $D \leq n^{1-c}$,

$$n^{D+1} \leq \binom{d+n}{n}^{K},$$

  Pour une constante K qui augmente avec c, n.

- Si $D \leq n$,

$$n^{D+1} \leq N^{2\log(\log(N))+O(1)}.$$

- La "borne" finale : Si $n \leq D$,

$$\mathcal{D}_{(d)} \leq D^n \leq N^{2\log(\log(N))+O(1)}.$$

La borne du $\mu_{\max}$ "en fleur" n^{D+1} ([Bürgisser-Cucker, 14]) :

- Si $D \leq n^{1-c}$,

$$n^{D+1} \leq \binom{d+n}{n}^{K},$$

  Pour une constante K qui augmente avec c, n.

- Si $D \leq n$,

$$n^{D+1} \leq N^{2\log(\log(N))+O(1)}.$$

- La "borne" finale : Si $n \leq D$,

$$\mathcal{D}_{(d)} \leq D^n \leq N^{2\log(\log(N))+O(1)}.$$

C'est à dire, cette algorithme numérique pour trouver une solution prends un temps plus grand que $\mathcal{D}_{(d)}N^{O(1)}...)$, pour tous les racines (si ont peu montrer que l'entropie se comporte bien (?)....) $\mathcal{D}^2_{(d)}N^{O(1)}...)$ **Pire que Kronecker...**

Tous ces méthodes ne servent pas grande chose : Ils ne s'appliquent qu'au cas générique (on pourrait aussi dire "mathématique", dans un sense péjoratif...). Et les problèmes de la vie courante sont donnés par des systèmes spéciaux.

Tous ces méthodes ne servent pas grande chose : Ils ne s'appliquent qu'au cas générique (on pourrait aussi dire "mathématique", dans un sense péjoratif...). Et les problèmes de la vie courante sont donnés par des systèmes spéciaux. Le vrai problème 17-ième doit être ennoncé de la façon suivante :

Smale's 17-th Problem

"Given a family Ω of systems of n polynomial equations in n unknowns, parameterized by a variety M. Can a zero of a system in Ω be found approximately, on the average, in polynomial time (in the dimension of Ω and the "size" of the parametrization) with a uniform (either deterministic, MonteCarlo or Las Vegas) algorithm ?"

Tous ces méthodes ne servent pas grande chose : Ils ne s'appliquent qu'au cas générique (on pourrait aussi dire "mathématique", dans un sense péjoratif...). Et les problèmes de la vie courante sont donnés par des systèmes spéciaux. Le vrai problème 17-ième doit être ennoncé de la façon suivante :

Smale's 17-th Problem

"Given a family Ω of systems of n polynomial equations in n unknowns, parameterized by a variety M. Can a zero of a system in Ω be found approximately, on the average, in polynomial time (in the dimension of Ω and the "size" of the parametrization) with a uniform (either deterministic, MonteCarlo or Las Vegas) algorithm ?"

Quelques exemples des systèmes spéciaux : systèmes génériques avec des coefficients réels, systèmes creux, systèmes "fewnomials", donnés par des calculs d'évaluation....

Presque rien n'est connu sur les cas spéciaux :

- Dans [Berthomieu-**P.**, 12] : Pour l'algorithme Las Vegas, la complexité moyenne dans le cas des systèmes réels génériques est bornée par la transformé de Radon sphérique de μ^2_{av}...

Presque rien n'est connu sur les cas spéciaux :

- Dans [Berthomieu-**P.**, 12] : Pour l'algorithme Las Vegas, la complexité moyenne dans le cas des systèmes réels génériques est bornée par la transformé de Radon sphérique de μ^2_{av}...La complexité moyenne de l'algorithme déterministe [Bü-Cu, 11] est $+\infty$

Presque rien n'est connu sur les cas spéciaux :

- Dans [Berthomieu-**P.**, 12] : Pour l'algorithme Las Vegas, la complexité moyenne dans le cas des systèmes réels génériques est bornée par la transformé de Radon sphérique de μ^2_{av}...La complexité moyenne de l'algorithme déterministe [Bü-Cu, 11] est $+\infty$
- Les systémes génériques avec des coefficients dans un corps des nombres ont la même complexité (grace a des anciens résultats d'approxiomation diophantienne et Géométrie des Nombres controlée dus à D. Castro, J.E. Morais, J. San Martín Corujo, **P.**....
- **Petit annoncé non-confirmé :** Je crois que je suis prêt à annoncer que la complexité moyenne de la méthode Las Vegas dans le "bon" ennoncé est

$$E_{f\in\Omega}[\mu^2_{\max}(f)].$$

Mais ça veut rien dire....

- **Sous-Problème 1 : À la recherche d'un $\mu_{\max}$ meilleur**. Tout le monde y est. Même Pierre Lairez s'est mis dans cette recherche : il m'annocé au CIRM (3-7 Nov. 2014) qu'il pense que dans très peu de temps il pourraît m'annocer quelque chose...J'espère qu'il aie un succés.

- **Sous-Problème 1 : À la recherche d'un $\mu_{\max}$ meilleur**. Tout le monde y est. Même Pierre Lairez s'est mis dans cette recherche : il m'annocé au CIRM (3-7 Nov. 2014) qu'il pense que dans très peu de temps il pourraît m'annocer quelque chose...J'espère qu'il aie un succés.
- **Sous-Problème 2 : Calculer exactement la moyenne $E[\mu_{\max}]$:** Et voir si elle depends (ou pas) du $\mathcal{D}_{(d)}$. Par contre, on connaît très bien $E[\mu_{\text{av}}]$. Dans [Pardo-**P.**, 14] on montre :

$$E_f[\mu_{\text{av}}^{-t}] = \frac{\Gamma(M_{(d)})}{\Gamma(M_{(d)}+t/2)} \sum_{k=0}^{n-1} \frac{\binom{n+1}{k}\Gamma(n+1-k+t/2)}{n^{n-k+1+t/2}\Gamma(n-k)}.$$

pour tout $t \in \mathbb{C}$, $\Re(t) > -4$ et, évidemment, elle admits prolongation analytique à $\mathbb{C} \setminus \{z \in \mathbb{Z} \ : \ z \leq -4\}$.

- **Sous-Problème 1 : À la recherche d'un $\mu_{\max}$ meilleur**. Tout le monde y est. Même Pierre Lairez s'est mis dans cette recherche : il m'annocé au CIRM (3-7 Nov. 2014) qu'il pense que dans très peu de temps il pourraît m'annocer quelque chose...J'espère qu'il aie un succés.
- **Sous-Problème 2 : Calculer exactement la moyenne $E[\mu_{\max}]$:** Et voir si elle depends (ou pas) du $\mathcal{D}_{(d)}$. Par contre, on connaît très bien $E[\mu_{\text{av}}]$. Dans [Pardo-**P.**, 14] on montre :

$$E_f[\mu_{\text{av}}^{-t}] = \frac{\Gamma(M_{(d)})}{\Gamma(M_{(d)}+t/2)} \sum_{k=0}^{n-1} \frac{\binom{n+1}{k}\Gamma(n+1-k+t/2)}{n^{n-k+1+t/2}\Gamma(n-k)}.$$

  pour tout $t \in \mathbb{C}$, $\Re(t) > -4$ et, évidemment, elle admits prolongation analytique à $\mathbb{C} \setminus \{z \in \mathbb{Z} \ : \ z \leq -4\}$.
- **Sous-Problème 3 : Pour des matrices, calculer exactement $E[\|A\|_{op}]$:** Voir blog par T. Tao. Par contre, on connaît (voir [Pardo-**P.**, 2014]), $t \in \mathbb{C}$, $\Re(t) > -4$:

$$E_{A\in\mathcal{M}}[\|A^{\dagger}\|^{-t}] := \sum_{k=0}^{n-1} \frac{\binom{n+1}{k}\Gamma(n-k+1+t/2)}{n^{n-k+1+t/2}\Gamma(n-k)}.$$

- **Sous-Problème 4 : Des agorithmes pour des solutions "spéciaux" :** Ce type d'algorithmes donnent tous les solutions dans $\mathbb{P}_n(\mathbb{C})$. Mais, parfois, on ne veut que des doslutions dans $\mathbb{P}_n(\mathbb{R})$ ou dans un corps des nombres $K \ : \ \mathbb{Q}] < \infty$...Quoi faire.... ? .

- **Sous-Problème 4 : Des agorithmes pour des solutions "spéciaux" :** Ce type d'algorithmes donnent tous les solutions dans $\mathbb{P}_n(\mathbb{C})$. Mais, parfois, on ne veut que des doslutions dans $\mathbb{P}_n(\mathbb{R})$ ou dans un corps des nombres $K : \mathbb{Q}] < \infty$...Quoi faire.... ? .
- **Sous-Problème 5 : Le cas singulier :** Mais on a assez d'experts dans la proximité : Giusti, Lecerf, Salvy Yakousohn....

- **Sous-Problème 4 : Des agorithmes pour des solutions "spéciaux" :** Ce type d'algorithmes donnent tous les solutions dans $\mathbb{P}_n(\mathbb{C})$. Mais, parfois, on ne veut que des doslutions dans $\mathbb{P}_n(\mathbb{R})$ ou dans un corps des nombres $K : \mathbb{Q}] < \infty$...Quoi faire.... ? .
- **Sous-Problème 5 : Le cas singulier :** Mais on a assez d'experts dans la proximité : Giusti, Lecerf, Salvy Yakousohn....
- **Sous-Problème 6 : Une méthode Las Vegas pour les ensembles questeurs :**Ça n'a rien à voir, mais ce dans le territoire....
- **Sous-Problème 7 : Liens formel numérique :** Si posible, sans passer par les approximation diophantiennes données en binaire...(Ça on connaît déjà depuis 15 ans). Alternatives ?

- **Sous-Problème 4 : Des agorithmes pour des solutions "spéciaux" :** Ce type d'algorithmes donnent tous les solutions dans $\mathbb{P}_n(\mathbb{C})$. Mais, parfois, on ne veut que des doslutions dans $\mathbb{P}_n(\mathbb{R})$ ou dans un corps des nombres $K : \mathbb{Q}] < \infty$...Quoi faire.... ? .
- **Sous-Problème 5 : Le cas singulier :** Mais on a assez d'experts dans la proximité : Giusti, Lecerf, Salvy Yakousohn....
- **Sous-Problème 6 : Une méthode Las Vegas pour les ensembles questeurs :**Ça n'a rien à voir, mais ce dans le territoire....
- **Sous-Problème 7 : Liens formel numérique :** Si posible, sans passer par les approximation diophantiennes données en binaire...(Ça on connaît déjà depuis 15 ans). Alternatives ?
- **Sous-Problème 8 : Un autre problème :** Je l'avais écrit quelque part,

- **Sous-Problème 4 : Des agorithmes pour des solutions "spéciaux" :** Ce type d'algorithmes donnent tous les solutions dans $\mathbb{P}_n(\mathbb{C})$. Mais, parfois, on ne veut que des doslutions dans $\mathbb{P}_n(\mathbb{R})$ ou dans un corps des nombres $K : \mathbb{Q}] < \infty$...Quoi faire.... ? .
- **Sous-Problème 5 : Le cas singulier :** Mais on a assez d'experts dans la proximité : Giusti, Lecerf, Salvy Yakousohn....
- **Sous-Problème 6 : Une méthode Las Vegas pour les ensembles questeurs :**Ça n'a rien à voir, mais ce dans le territoire....
- **Sous-Problème 7 : Liens formel numérique :** Si posible, sans passer par les approximation diophantiennes données en binaire...(Ça on connaît déjà depuis 15 ans). Alternatives ?
- **Sous-Problème 8 : Un autre problème :** Je l'avais écrit quelque part,mais je l'ai oublié...L'âge... ne pardonne jamais...

- **Sous-Problème 4 : Des agorithmes pour des solutions "spéciaux" :** Ce type d'algorithmes donnent tous les solutions dans $\mathbb{P}_n(\mathbb{C})$. Mais, parfois, on ne veut que des doslutions dans $\mathbb{P}_n(\mathbb{R})$ ou dans un corps des nombres $K : \mathbb{Q}] < \infty$...Quoi faire.... ? .
- **Sous-Problème 5 : Le cas singulier :** Mais on a assez d'experts dans la proximité : Giusti, Lecerf, Salvy Yakousohn....
- **Sous-Problème 6 : Une méthode Las Vegas pour les ensembles questeurs :**Ça n'a rien à voir, mais ce dans le territoire....
- **Sous-Problème 7 : Liens formel numérique :** Si posible, sans passer par les approximation diophantiennes données en binaire...(Ça on connaît déjà depuis 15 ans). Alternatives ?
- **Sous-Problème 8 : Un autre problème :** Je l'avais écrit quelque part,mais je l'ai oublié...L'âge... ne pardonne jamais...

Merci d'avoir supporté ce longue exposé !

Merci d'avoir supporté ce longue exposé !

Et excusez mon français.