Conceptual Aspects to solve Smale's 17–th Problem: complexity, probability, polynomial equations and Integral Geometry. *

Luis M. Pardo
Universidad de Cantabria

April 11, 2007

*IMA, April 2007

Smale's List

18 Problems, as....

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.

$\cdots$

Problem 9: The Linear Programming Problem.

$\cdots$

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

$\boxed{\textbf{17-th Problem.}}$

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

(Beltrán-**P.** , 06)

Historical Scketch

XIX-th century: Modern Elimination Theory
Bézout, Cayley, Hilbert, Kronecker, Sturm, Sylvester

1900–1930: *Macaulay, König,...*

1930–1965: Vanished on the air?

1965–: Monomial orders and standard–Gröbner Basis *Hironaka, Buchberger,...,Rewriting Techniques*

Sparse Approach... *Bernstein, Kouchnirenko, Sturmfels....*

Complexity Classes Approach... *Cook [* $\mathbf{P} = \mathbf{NP}$ *?]*

1995–: Intrinsical Methods adapted to data structures
TERA, KRONECKER ....

A Simplified version

Goal: *Efficient Algorithmics for Problems Given by Polynomial Equations*

Potential Applications : † Information Theory (Coding, Crypto,...), Game Theory, Graphic and Mechanical Design, Chemist, Robotics, ...

The Problem: Efficiency

Rk. *Most algorithms for Elimination Problems run in worse than exponential time in the number of variables:*

Intractable for Practical Applications.

†Many of them Casual but not Causal

SOLVING

INPUT: A list of multivariate polynomial equations: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$.

OUTPUT: A description of the solution variety
$V(f_1, \ldots, f_s) := \{x \in \mathbb{C}^n \ : \ f_i(x) = 0 ...\}$.

Description: The kind of description determines the kind of problems/questions you may answer about $V(f_1, \ldots, f_s)$

Example: Symbolic/Algebraic Computing $\longrightarrow$ questions involving quantifiers

Hilbert's Nulltellensatz (HN) *Given $f_1, \ldots, f_s$ decide whether the following holds:*

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

DIFFERENT SCHOOLS

Syntactic Standard, Gröbner Basis, Rewriting...a Long List

Structural :Find the suitable complexity class for the problem NP-hard, PSPACE,...

Semi–Semantics: Using combinatorial objects (hence semi-semantic) to control complexity: Sparse School: using Newton polytopes Bernstein. Kouchnirenko, Sturmfels...

Semantic/Intrinsic: Mostly the TERA group: *Cantabria (P., Morais, Montaña, Hägele,...); Polytechnique (Giusti, Bostan, Lecerf, Schost, Salvy...); * Buenos Aires (Heintz, Krick, Matera, Solerno, ...); * Humboldt (Bank, Mbakop,Lehmann)*

- Polynomials viewed as programs.

- Parameters of Semantical Objects (algebraic varieties) dominate complexity.

Degree of V *([Heintz,83], [Vogel, 83], [Fulton, 81]) :♯ of intersection points with generic linear varieties.*

Height of V:
Bit length of the coefficients CHOW FORM

* *Geometric Degree of a Sequence:*

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

Theorem 1 *There is a bounded error probability Turing machine that answers* **HN** *in time polynomial in*

$$L\ \delta\ H,$$

where

L *is the input length (whatever usual data structure),*

δ *is the geometric degree of a deformation sequence (Kronecker's deformation) and*

H *is the height of the last equi-dimensional variety computed.*

Examples

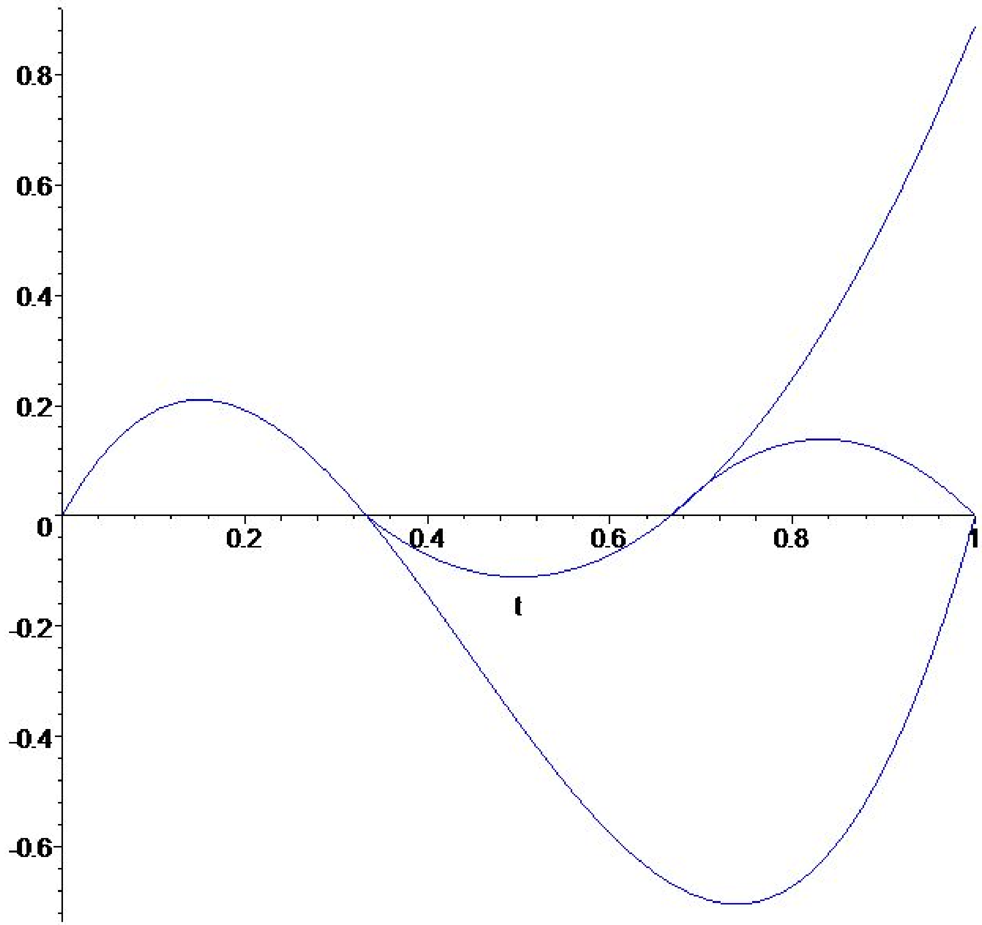
$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, k - \sum_{i=1}^{n} m_i X_i = 0.$$

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

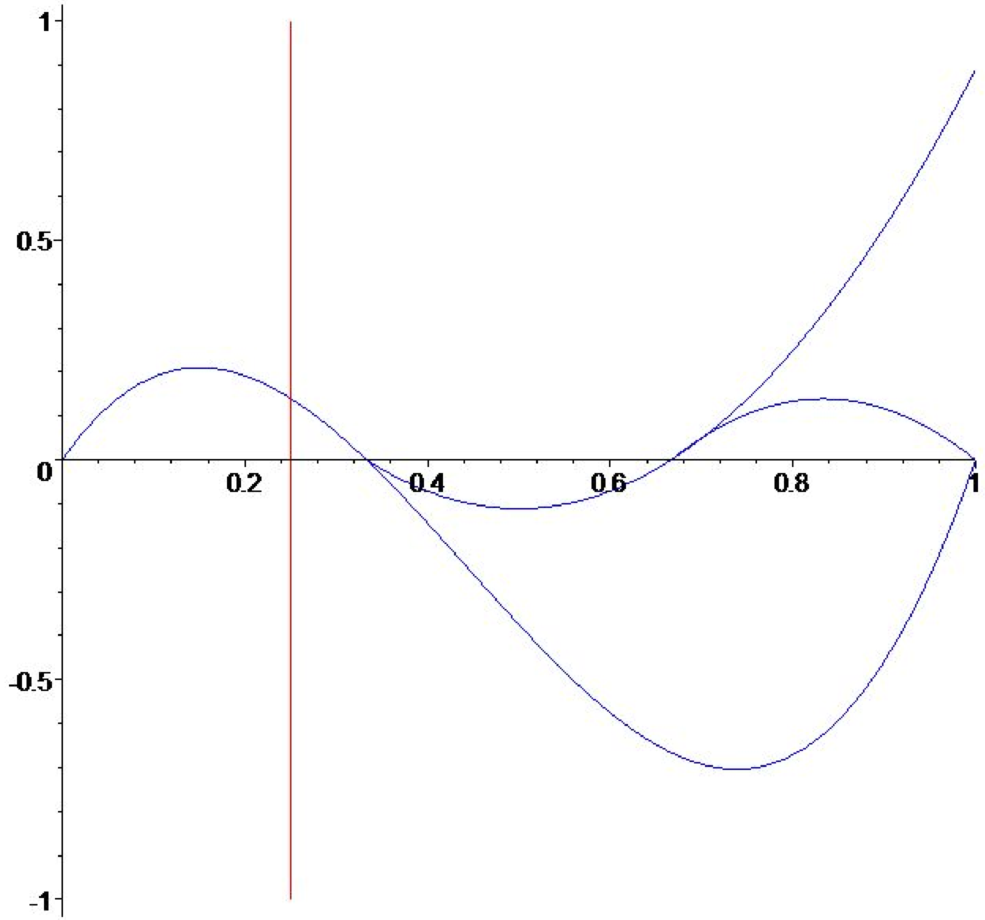
$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, 512 - \sum_{i=1}^{n} 2^{i-1} X_i = 0.$$

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

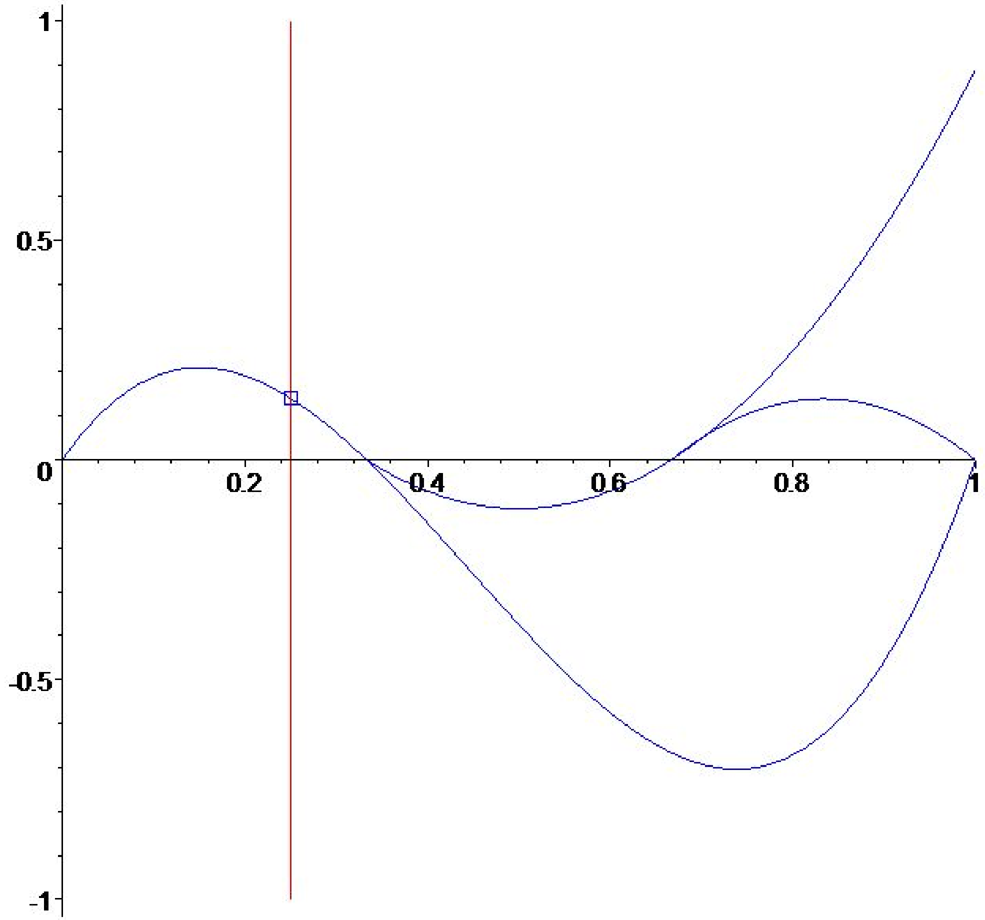
Kronecker's Deformation



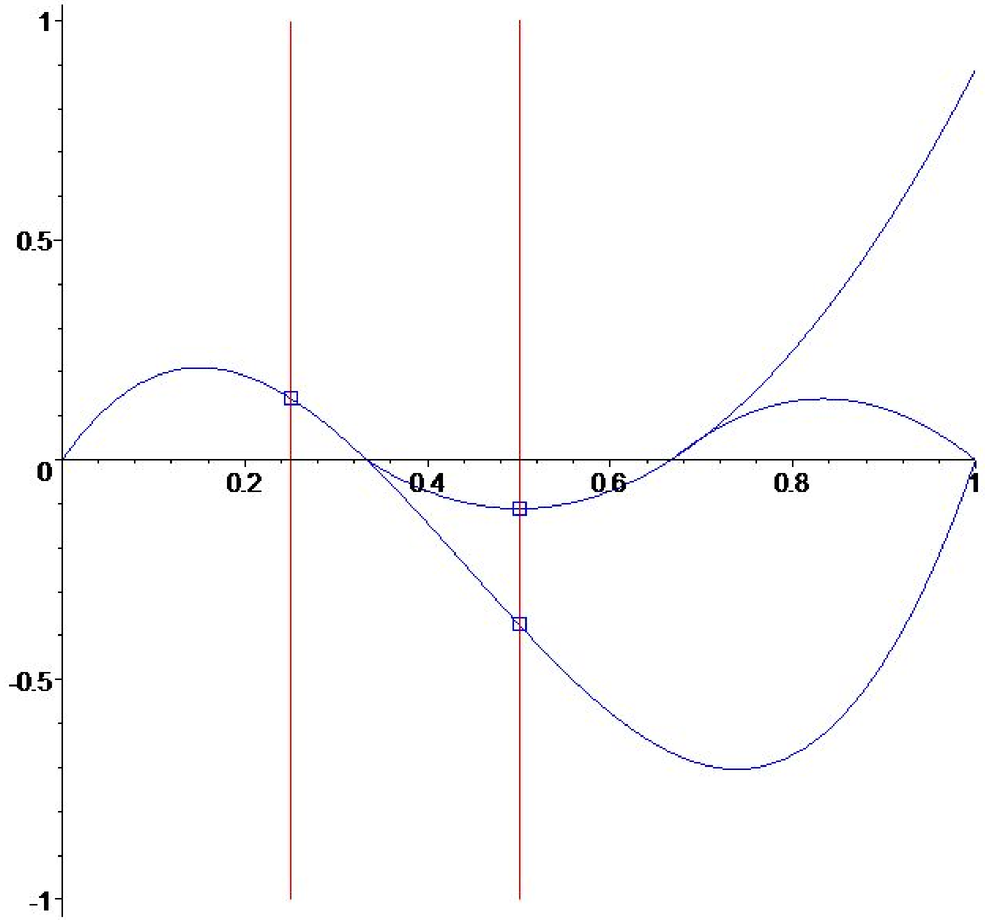
Initialize



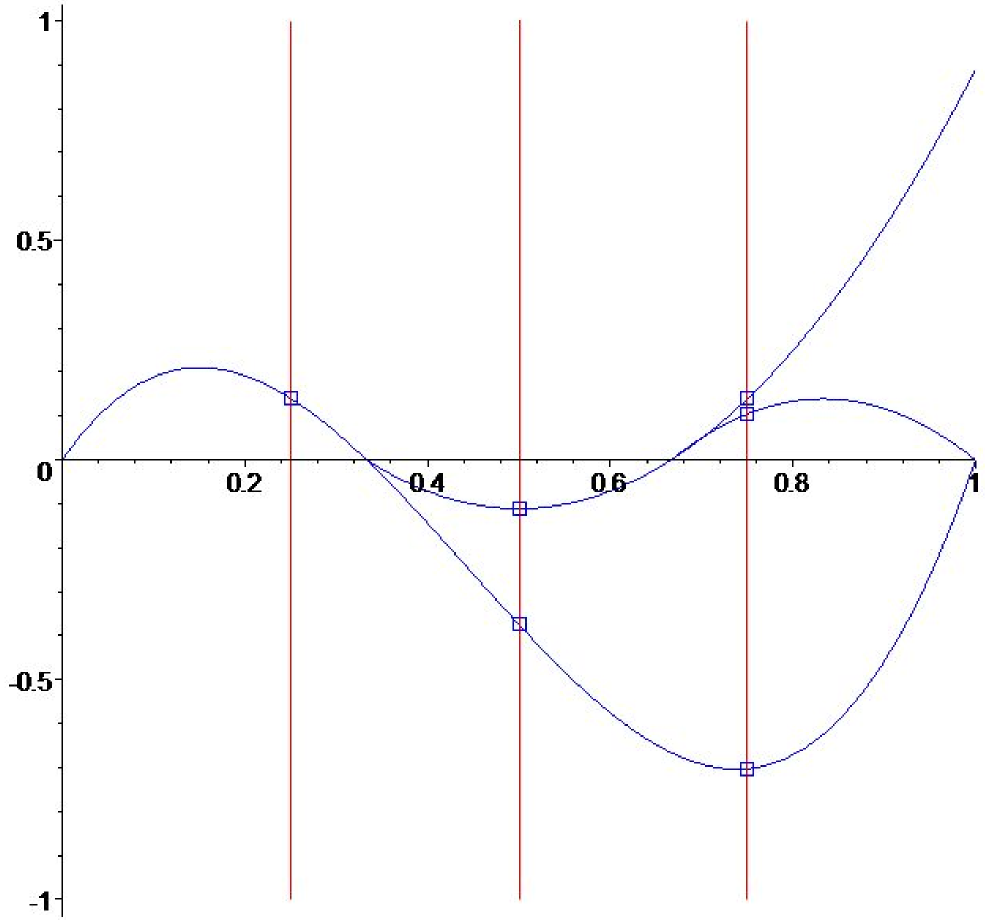
Lifting Fibers



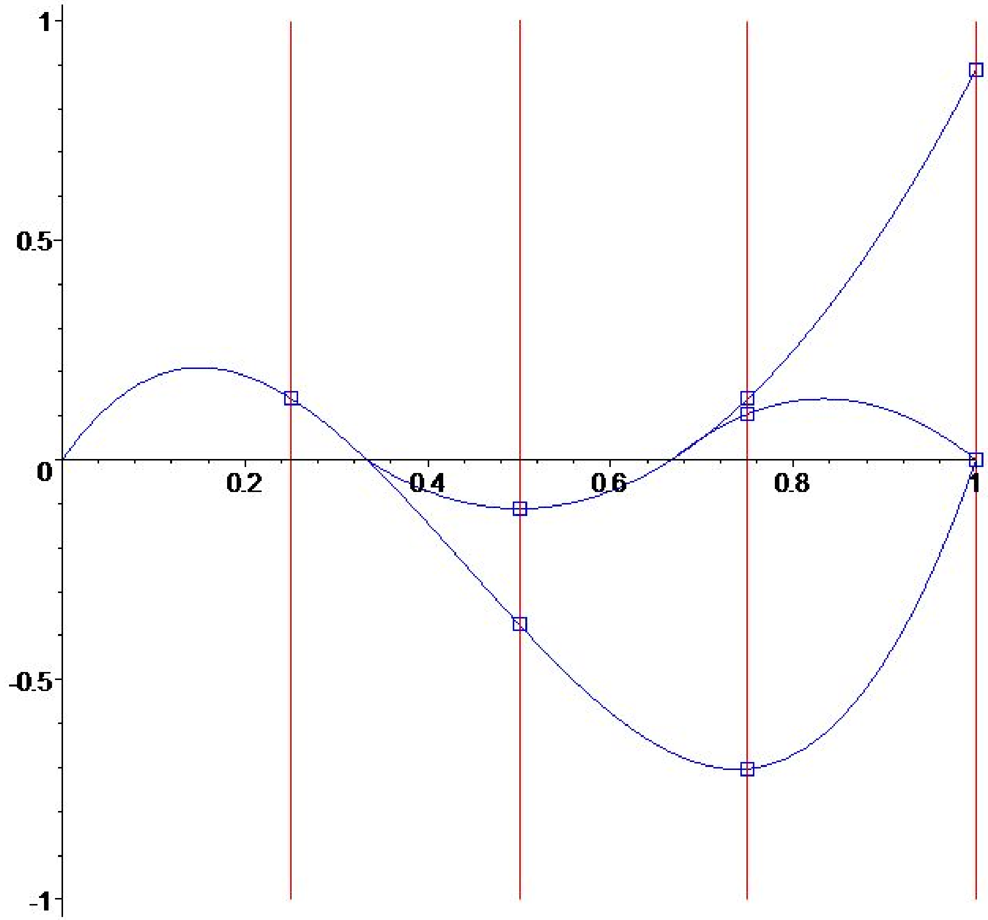
Jumping from a Lifting Fiber to a new one



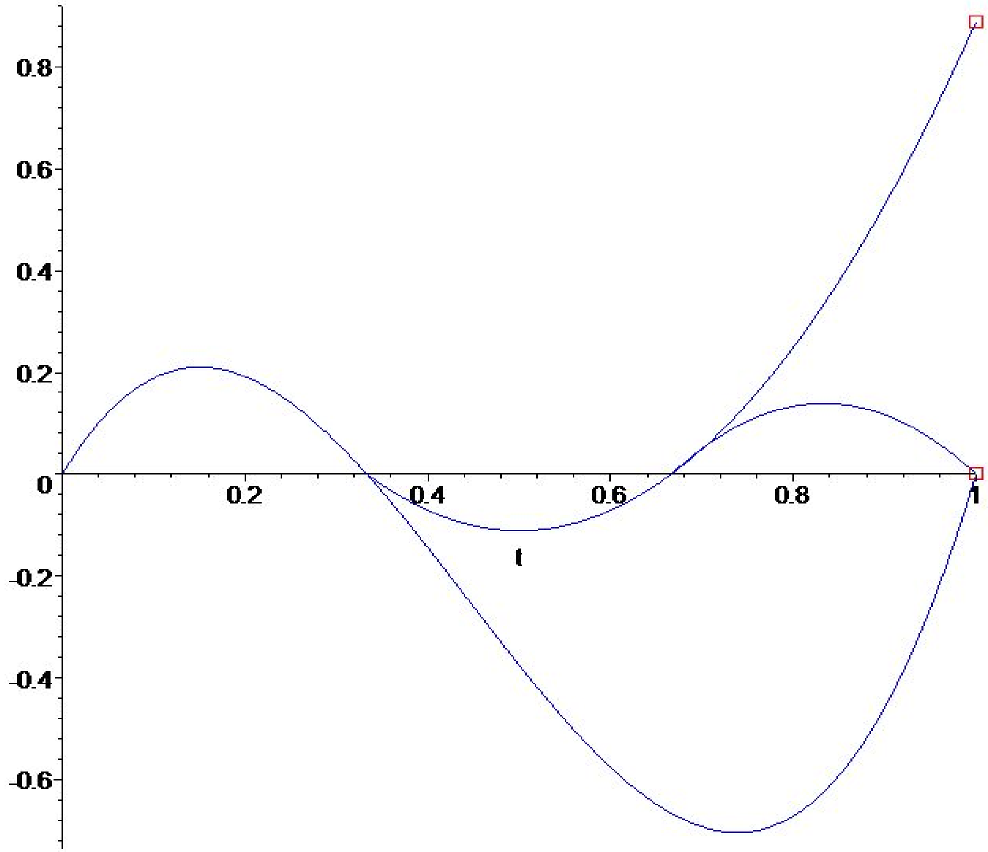
And so on...



Until the End



The target



We got:

A description of the target variety through a birational isomorphism, even biregular in the zero–dimensional case, that contains information that suffices to answer elimination questions.

But...

Is that optimal in terms of complexity ?

Algorithms based on **a deformation***:*
A sequence suite $V_1, \ldots, V_n$ of intermediate varieties to solve before "eliminating"

Universal Solving
An algorithm is called **Universal** *if its output contains information enough about the variety of solutions to answer* **all** *elimination questions.*

Remark 2 *Most Computer Algebra/Symbolic Computation procedures are Universal.*

Lower Complexity Bounds

Theorem [Castro-Giusti-Heintz-Matera-P.,2003]
Any universal solving procedure requires exponential running time.

* *TERA algorithm is* **essentially optimal.**

* *Running time is greater than the* **Bézout Number:**

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

* *No Universal solving procedure may improve this lower complexity bound.*

Searching Non–Universal Solving Procedures.

Searching for procedures that compute partial (non–universal) information about the solution variety in polynomial running time.

Smale's 17th Problem

What is "Partial Information"?

What is "Partial Information"?

For instance, a "good approximation" to some of the solutions

What is "Partial Information"?

For instance, a "good approximation" to some of the solutions

Example

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: $z \in \mathbb{Q}[i]^n$ such that there exists $\zeta \in V(f_1, \ldots, f_n)$ satisfying

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

for som $\varepsilon > 0$.

Some Multivariate Elimination and some lattice reduction algorithms (under KLL approach) yield

Theorem 3 (Castro-Hagele-Morais-P., 01) *There is a computational equivalence between:*

- *Approimations* $z \in \mathbb{Q}[i]^n$ *of some of the zeros*$\zeta \in V(f_1, \ldots, f_n)$,
- *A description "á la Kronecker–TERA" of the residual class field of* $\mathbb{Q}_\zeta$.

Theorem (cont.)

The running time of this computational equivalence is polynomial in:

- $D_\zeta =$ *degree of the residual class field* $\mathbb{Q}_\zeta$.
- $L =$ *input size.*
- $H_\zeta =$ *height of the residual class field* $\mathbb{Q}_\zeta$.

Namely, **a "good" approximation contains information that suffices for elimination**(although it is not clear whether you should compute it)

Immediate Application

Theorem 4 *There is an algorithm that performs the following taks:*

- Input: *A univariate polynomial $f \in \mathbb{Q}[T]$.*

- Output: *A primitive element description of the normal closure of f.*

THe running time of this procedure is polynomial in the following quatities:

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

where d is the degree of f and h is the bit length of the coefficients of f.

Remark: A geometric algorithm such that the complexity is not of order $d!$ except when unavoidable.

Good Approximation?

For simplicity we work on the projective space

Systems of homogeneous polynomials:

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

$deg(f_i) = d_i$, $(d) := (d_1, \ldots, d_n)$,
$\mathcal{H}_{(d)} :=$ Complex vector space of all equations of given degree.

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

The incidence variety (Room-Kempf, Shub-Smale)

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

PROJECTIVE NEWTON'S OPERATOR

(M. Shub amd S. Smale 1986–1996)

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

Notations: *Projective Metrics :*

Riemannian :

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

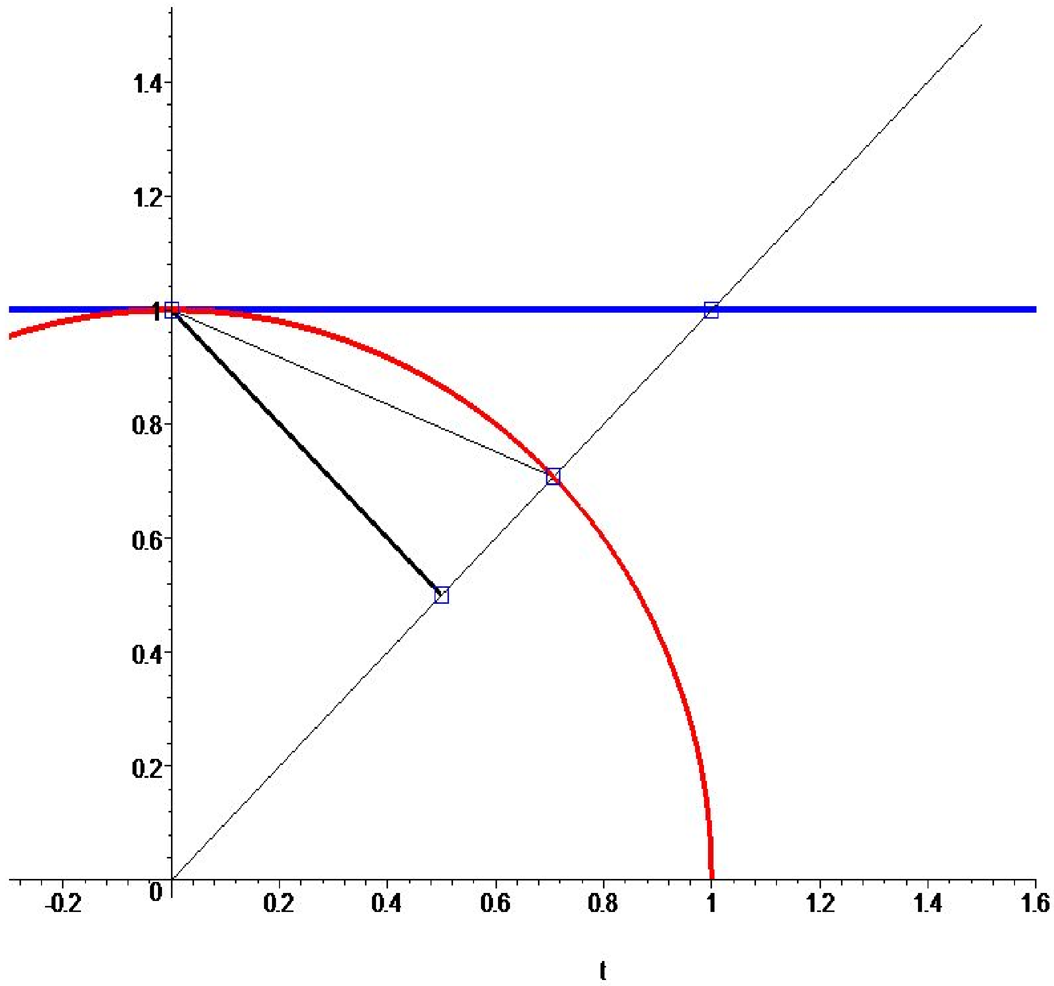
Fubini–Study :

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

Tangent Distance :

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

A Picture



Newton's Operator II

Tangent Space at a point $z \in \mathbb{P}_n(\mathbb{C})$:

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

A system of polynomial equations $F := [f_1, \ldots, f_n]$, Jacobian matrix :

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

If z is not a critical point, the restriction to the tangent space:

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

The inverse:

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

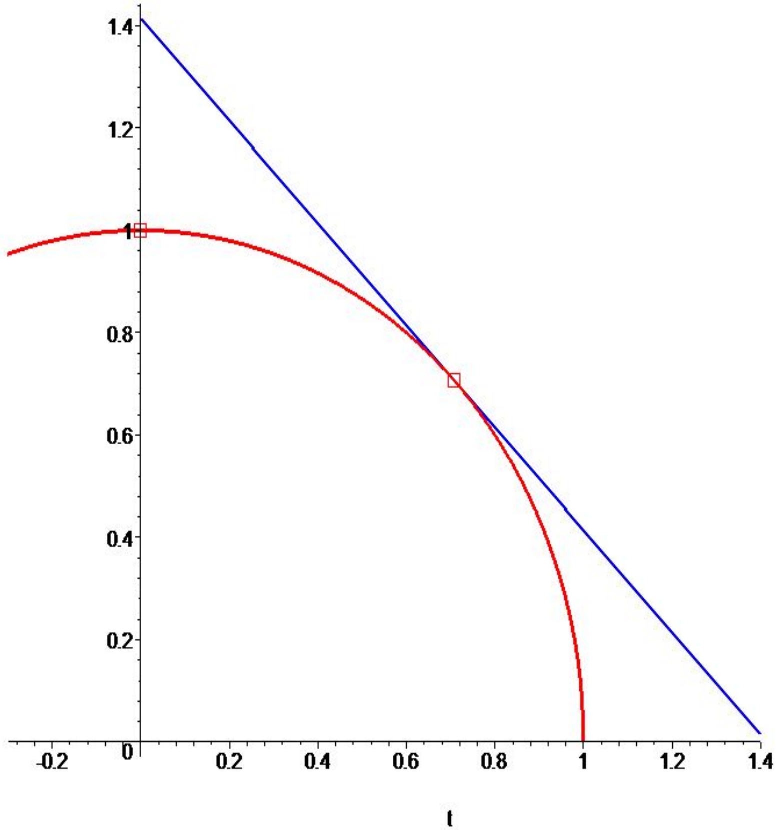
Projective Newton's Operator III

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

For every non-critical $\pi(z) \in \mathbb{P}_n(\mathbb{C})$ Newton's operator is given by:

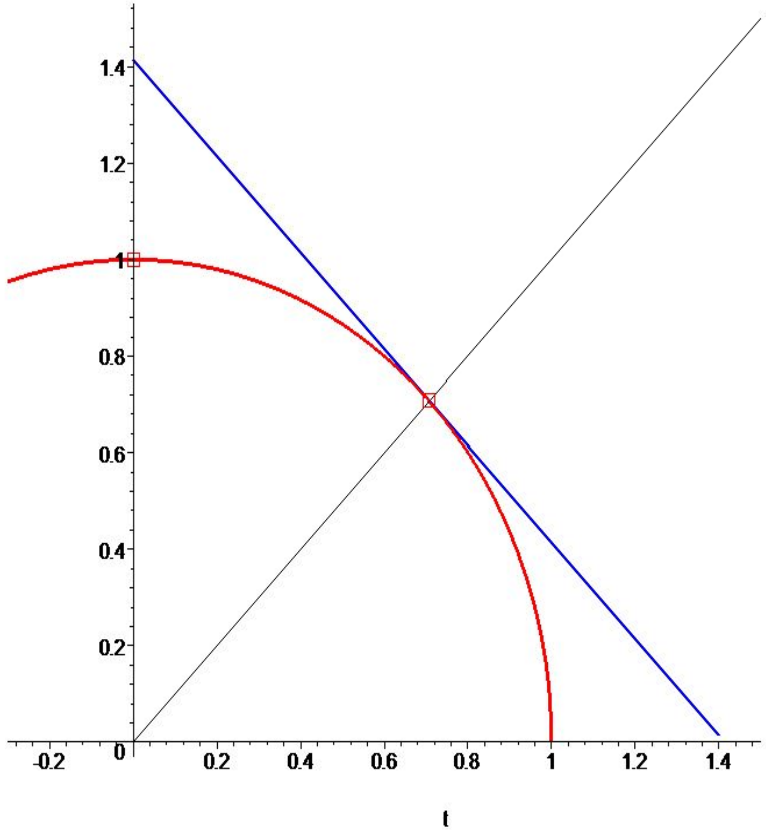
$$N_F(\pi(z)) := \pi\left(z - \left(DF(z)\mid_{T_z}\right)^{-1} F(z)\right),$$

Some pictures I



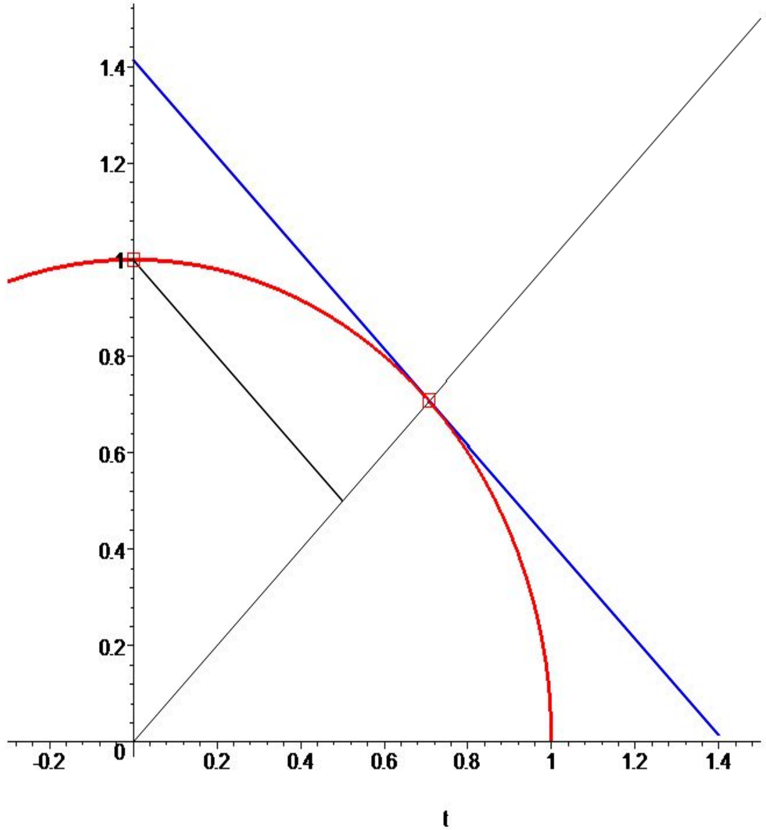
$$T_z\mathbb{P}_n(\mathbb{C})$$

N. Op. Picture II



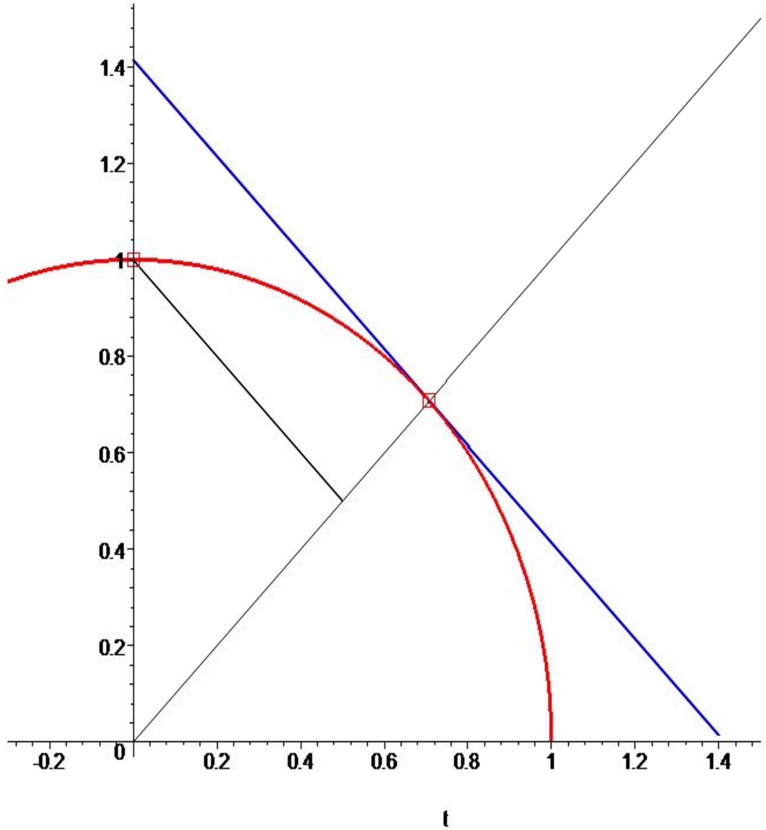
$$T_z\mathbb{P}_n(\mathbb{C})$$

N. Op. Picture III



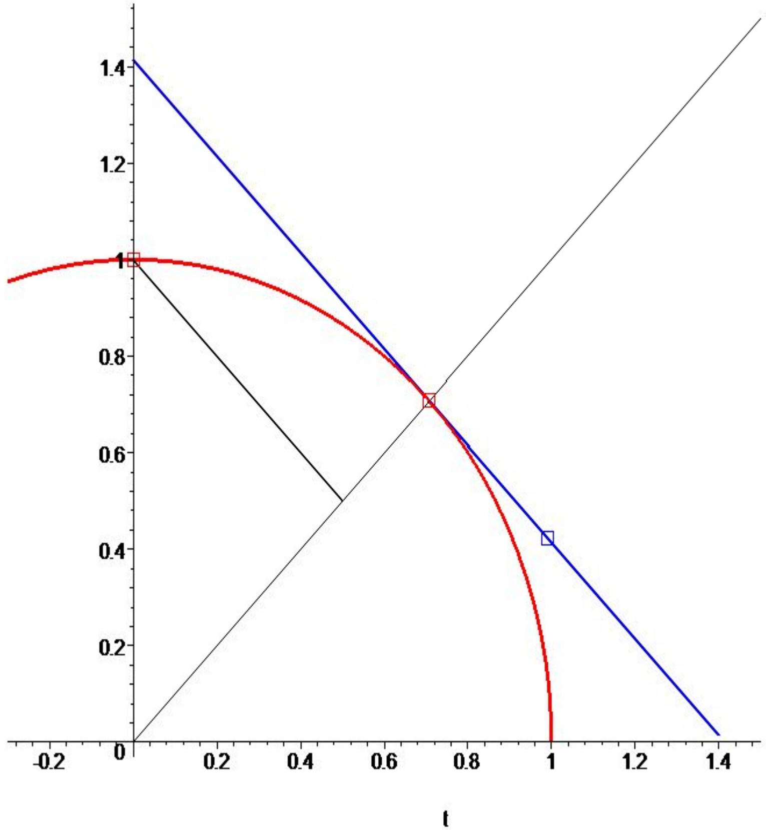
$T_z\mathbb{P}_n(\mathbb{C})$

N. Op. Picture IV



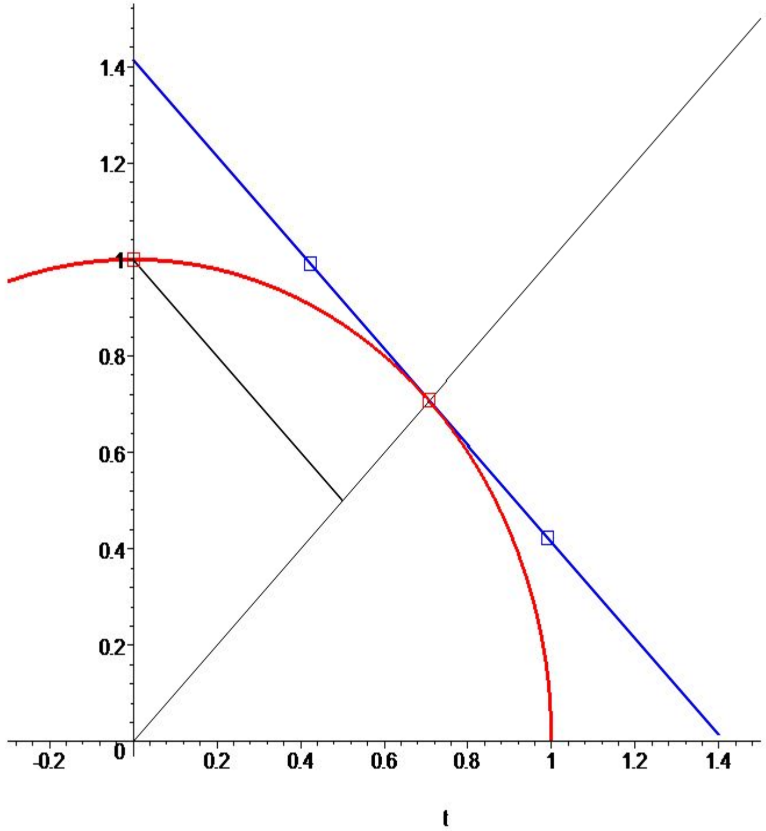
$f(z) \in T_0\mathbb{C}^n = \mathbb{C}^n \qquad T_z\mathbb{P}_n(\mathbb{C})$

$\boxed{\text{N. Op. Picture V}}$



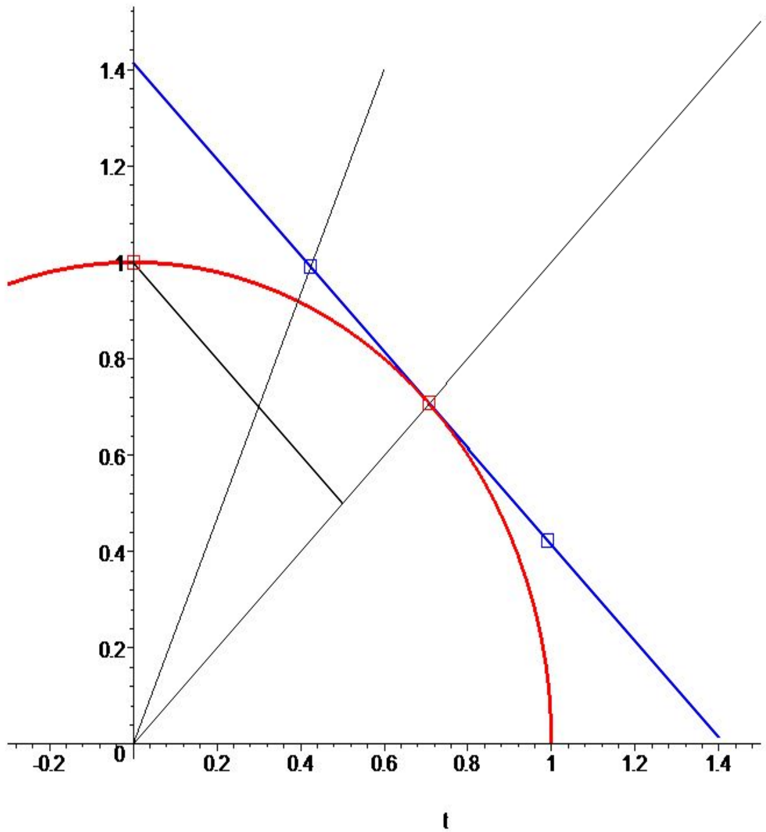
$$T_z f^{-1} f(z) \in T_z \mathbb{P}_n(\mathbb{C})$$

N. Op. Picture VI



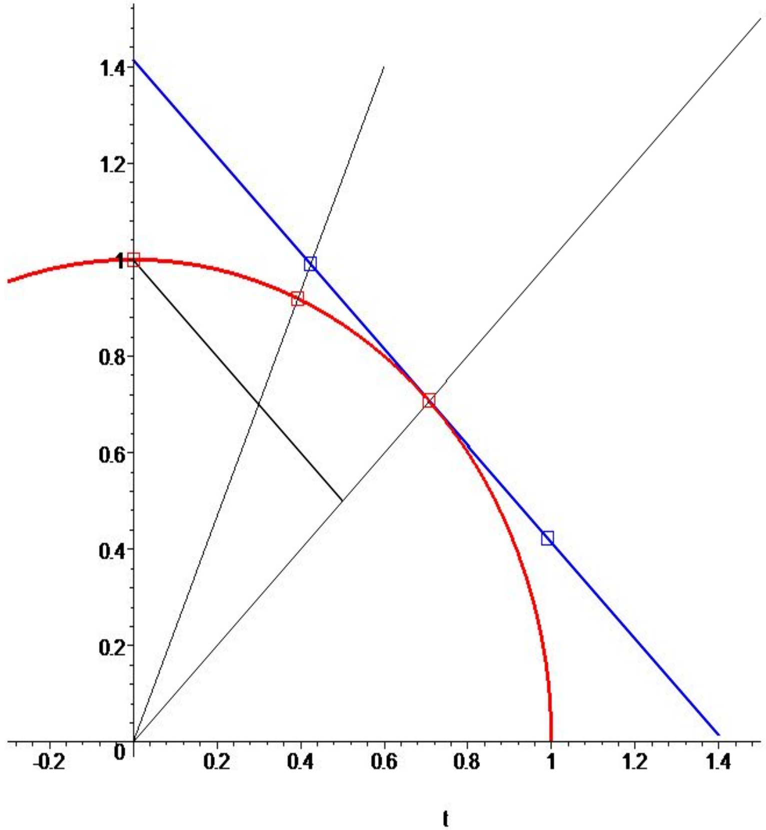
$$-T_z f^{-1} f(z) \in T_z \mathbb{P}_n(\mathbb{C})$$

N. Op. Picture VII



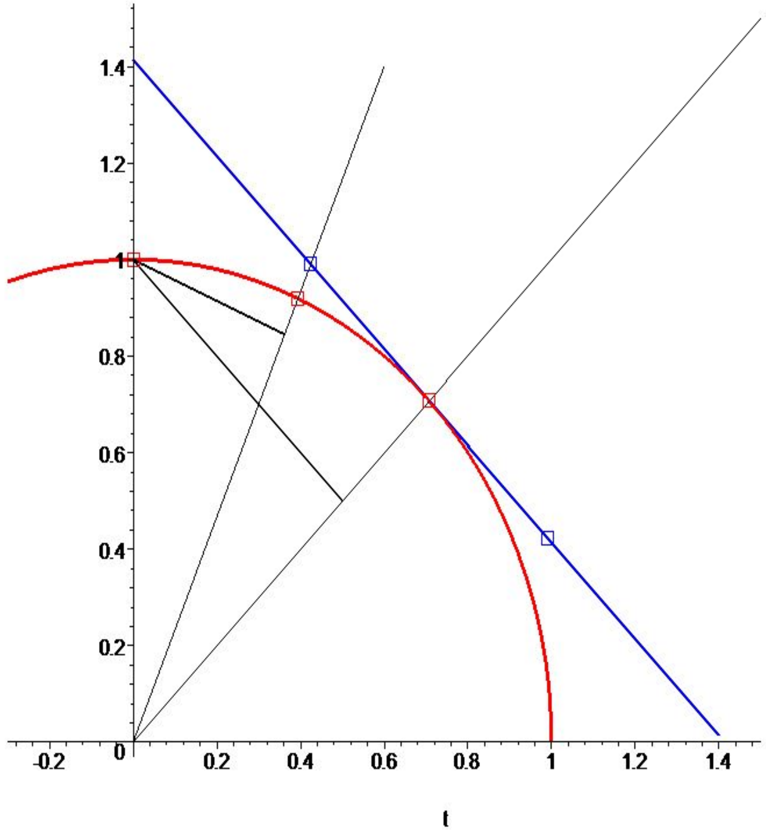
$$z - T_z f^{-1} f(z) \in T_z \mathbb{P}_n(\mathbb{C})$$

N.Op. Picture VIII



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

N.Op. Picture IX



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

* INPUT: *A System of Homogeneous Polynomials*

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

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

A zero $\zeta \in V(F)$

An Approximate Zero(Smale'81) a point $z\mathbb{P}_n(\mathbb{C})$ such that Newton's operator N_F applied to z converges very fast to the zero.

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

$d_T :=$ tangent "distance" .

Condition Number ([Shub–Smale, 86–96])

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

Condition Number Theorem : *Discriminant Variety in* $\mathbb{P}(\mathcal{H}_{(d)})$.

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

$$\Sigma := \bigcup_{\zeta \in \mathbb{P}_n(\mathbb{C})} \Sigma_\zeta. \quad \text{(Systems with a critical zero).}$$

Fiber Distance : $\rho(F,\zeta) := d_P(F, \Sigma_\zeta)$.

Theorem 5 (Shub-Smale, 91)

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

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

Theorem 6 (Smale,81) *Si :*

$$d_T(z,\zeta) \leq \frac{3-\sqrt{7}}{d^{\frac{3}{2}}\mu_{norm}(F,\zeta)},$$

then, z is an approximate zero associated to some zero ζ of F.

NON–UNIVERSAL ALGORITHMICS

* INPUT:

A System $F \in \mathbb{P}(\mathcal{H}_{(d)})$,

* OUTPUT:

UNIVERSAL SOLVING: **An** *Approximate Zero* z **for each zero** $\zeta \in V(F)$.

Lower Complexity Bound: Bézout's Number ($\mathcal{D} := \prod_{i=1}^{n} d_i$) $\Rightarrow$ **Intractable**

Or:

NON-UNIVERSAL SOLVING : **An** *Approximate Zero* z **for some of the zeros** $\zeta \in V(F)$.

Complexity of Non–Universal Solving? (= Smale's 17th Problem)

Incidence Variety:

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

Two Canonical Projections:

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

Critical values of $\pi_1 = \Sigma$.

In fact, the following is a "covering map":

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

And the real codimension is: $codim_{\mathbb{P}(\mathcal{H}_{(d)})}(\Sigma) \geq 2.$

$\boxed{\text{NAMELY}}$

Except for a null measure subset, for each $F, G \in \mathbb{P}(\mathcal{H}_{(d)}) \setminus \Sigma$, :

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

where

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

and the following is also a "covering space":

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

Namely, for each $\zeta \in V(G)$ there is a curve:

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

An algorithmic Philosophy

Start at (G, ζ) ($t = 1$) and closely follow (by applying Newton's projective operator) a polygonal close to $\Gamma(F, G, \zeta)$ until you find an approximate zero of F.

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

With Initial Pair

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

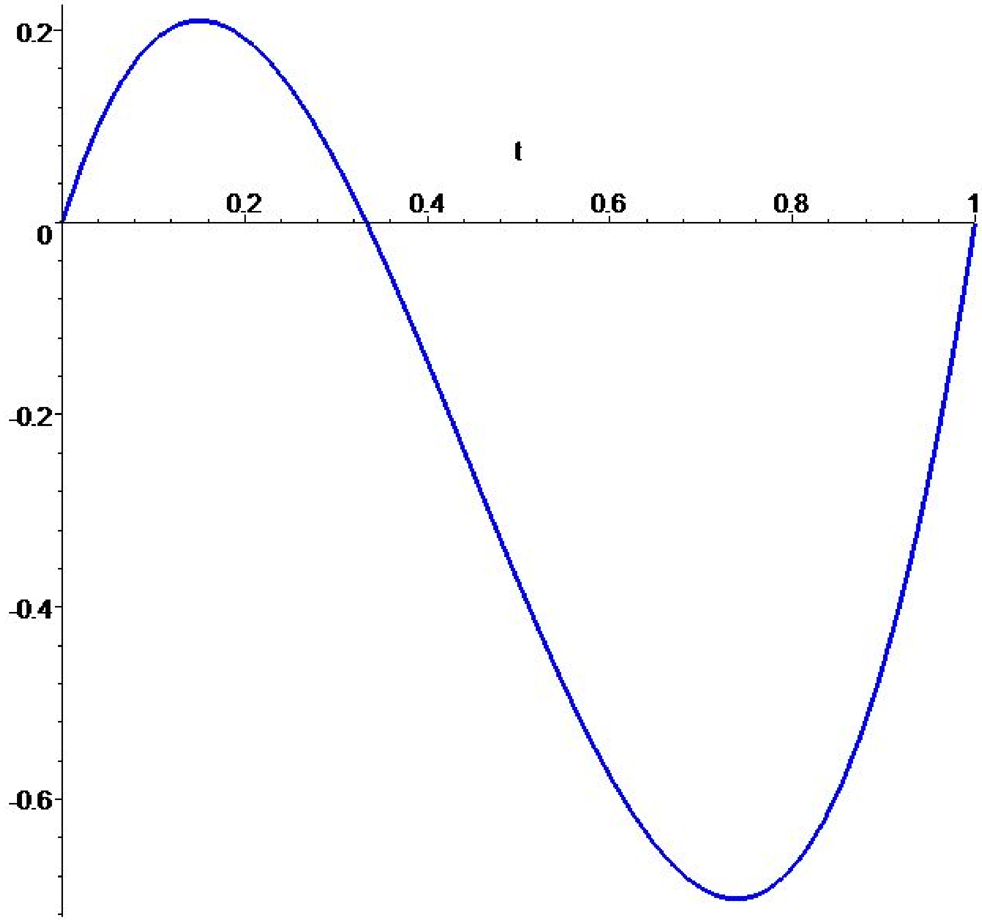
Following [F,G] and the cruve Γ

Output

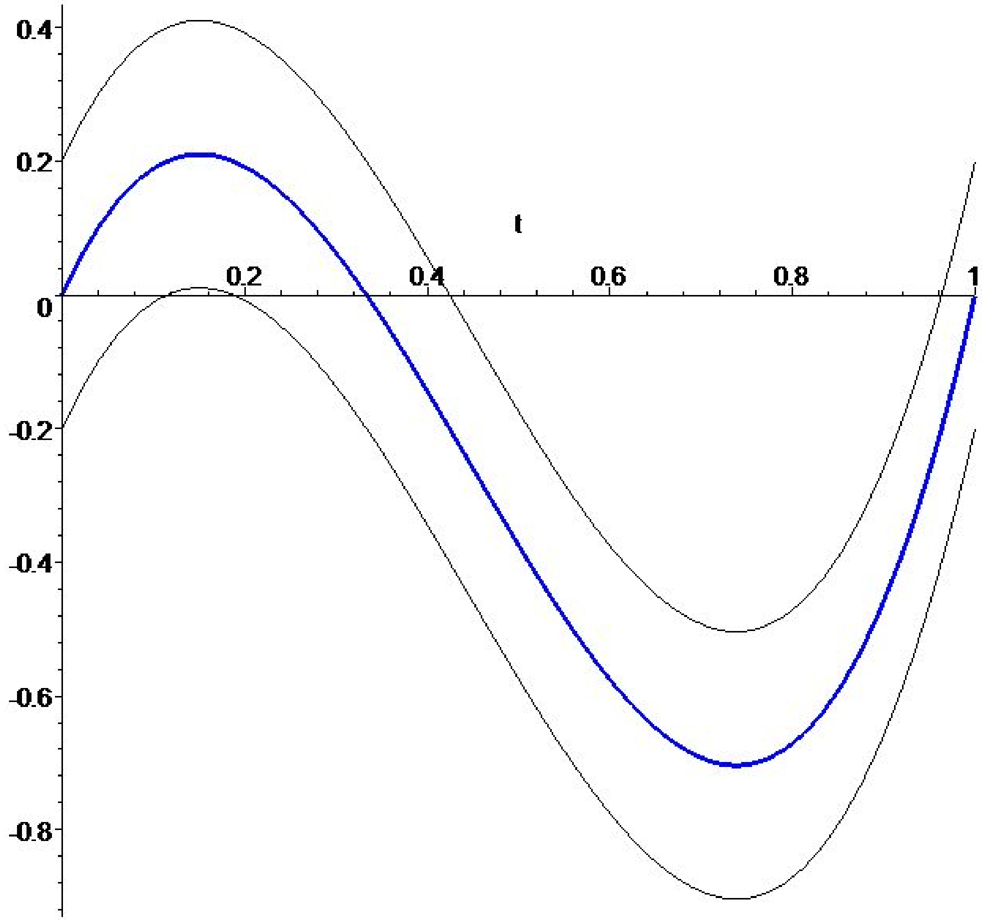
-- *Either ERROR*

-- *Or an approximate zero* $z \in \mathbb{P}_n(\mathbb{C})$ *associated to some zero* $\zeta \in \mathbb{P}_n(\mathbb{C})$ *of* $F \in \mathcal{H}_{(d)}$

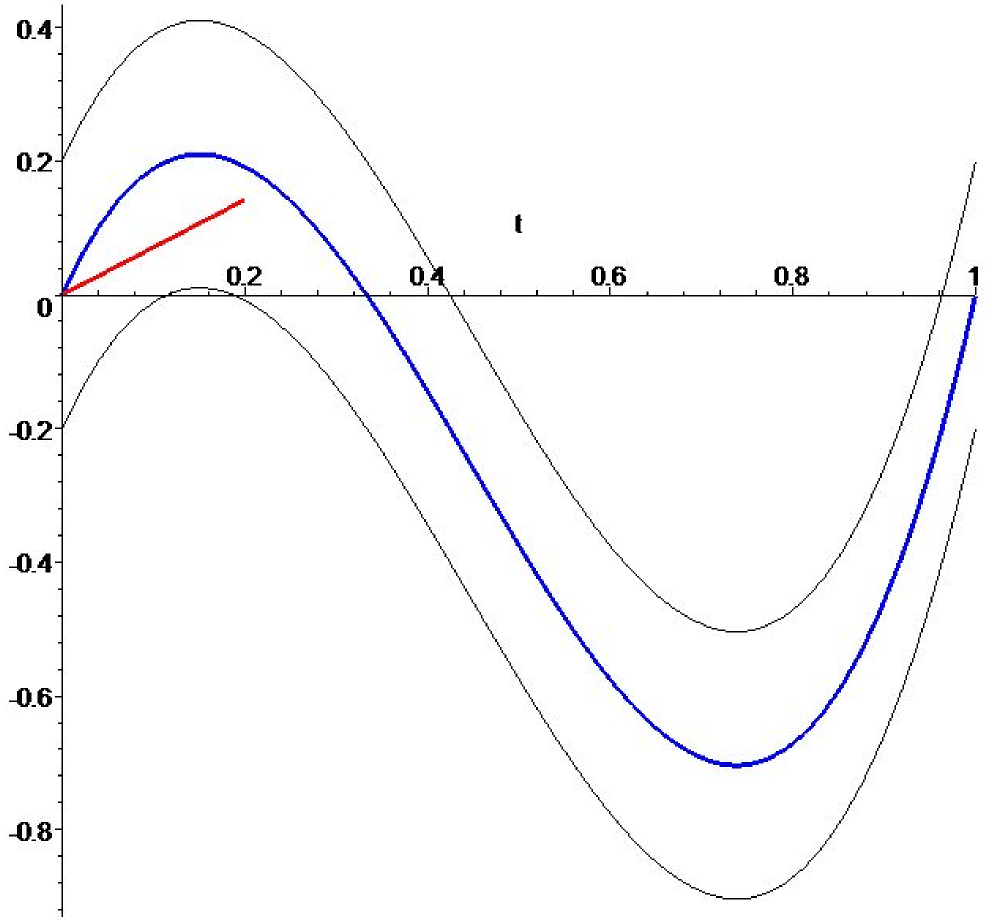
HD Picture I



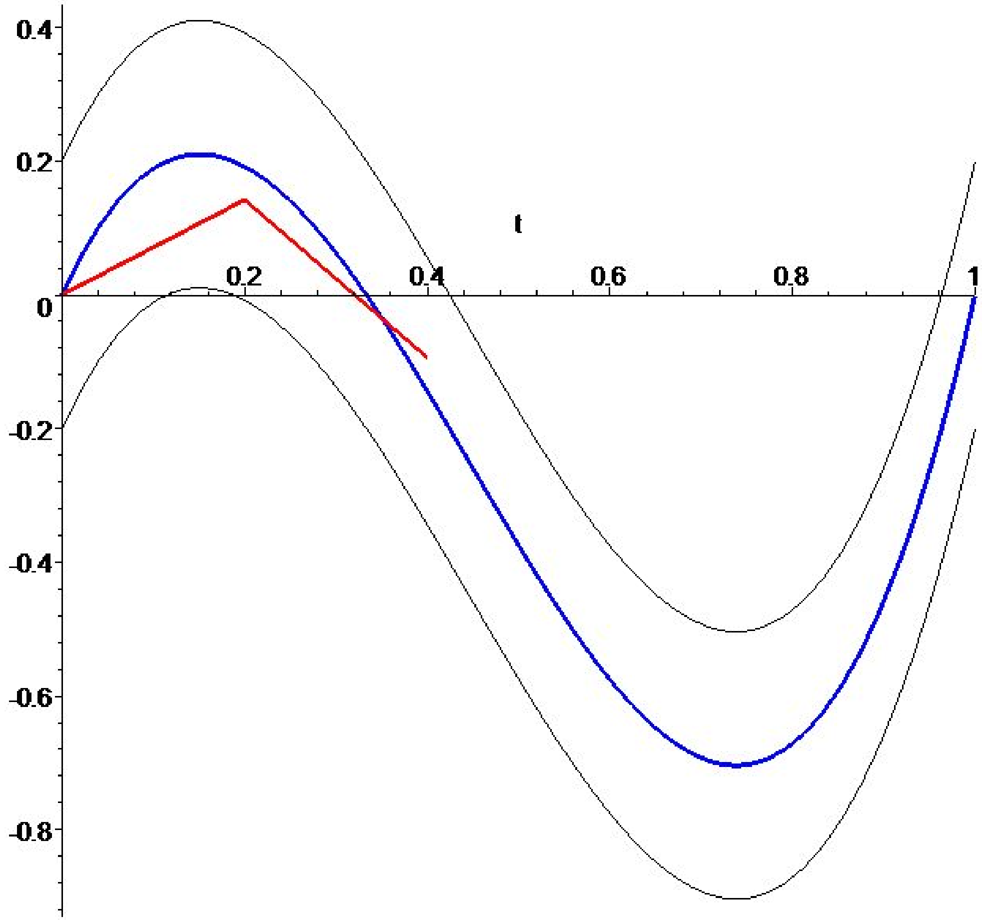
HD Picture II



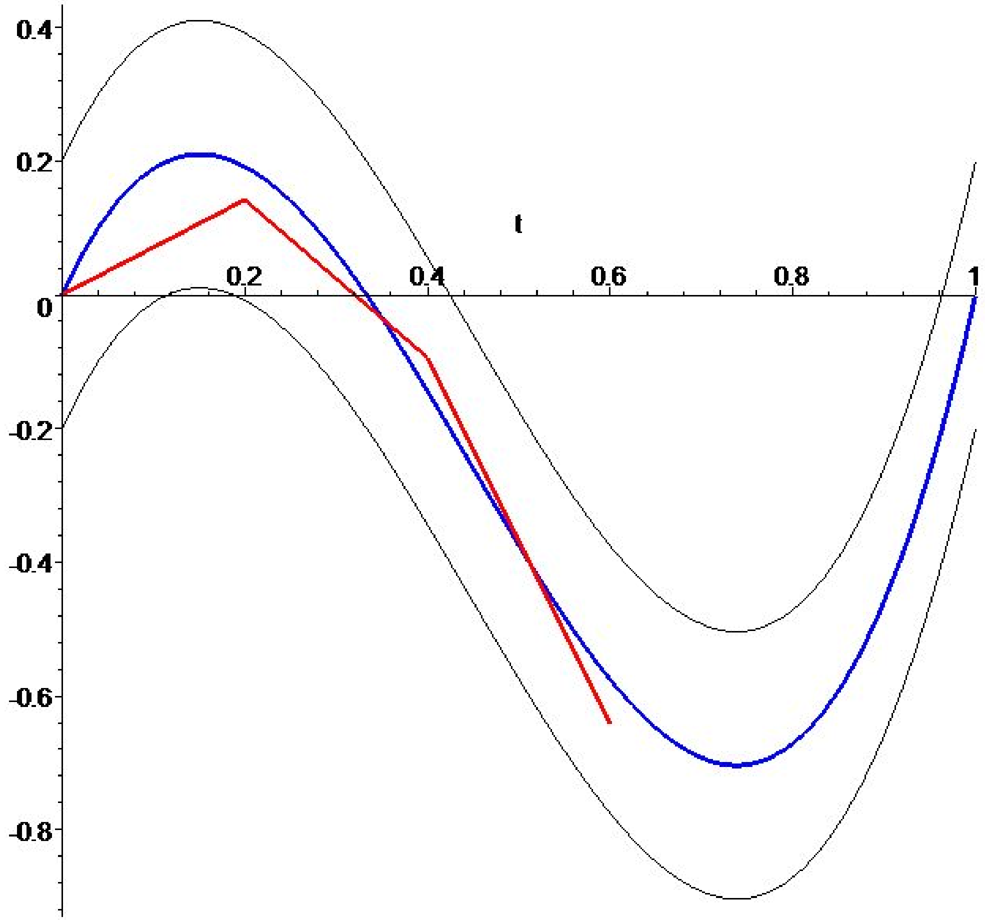
HD Picture III



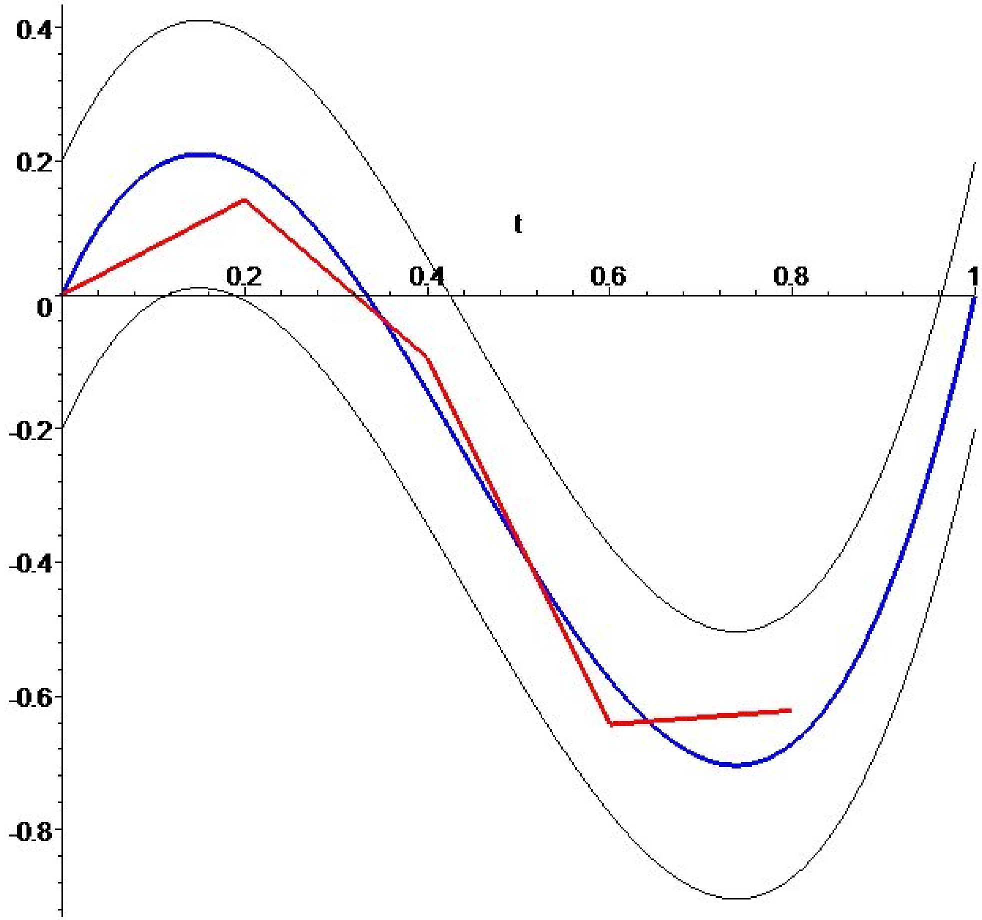
HD Picture IV



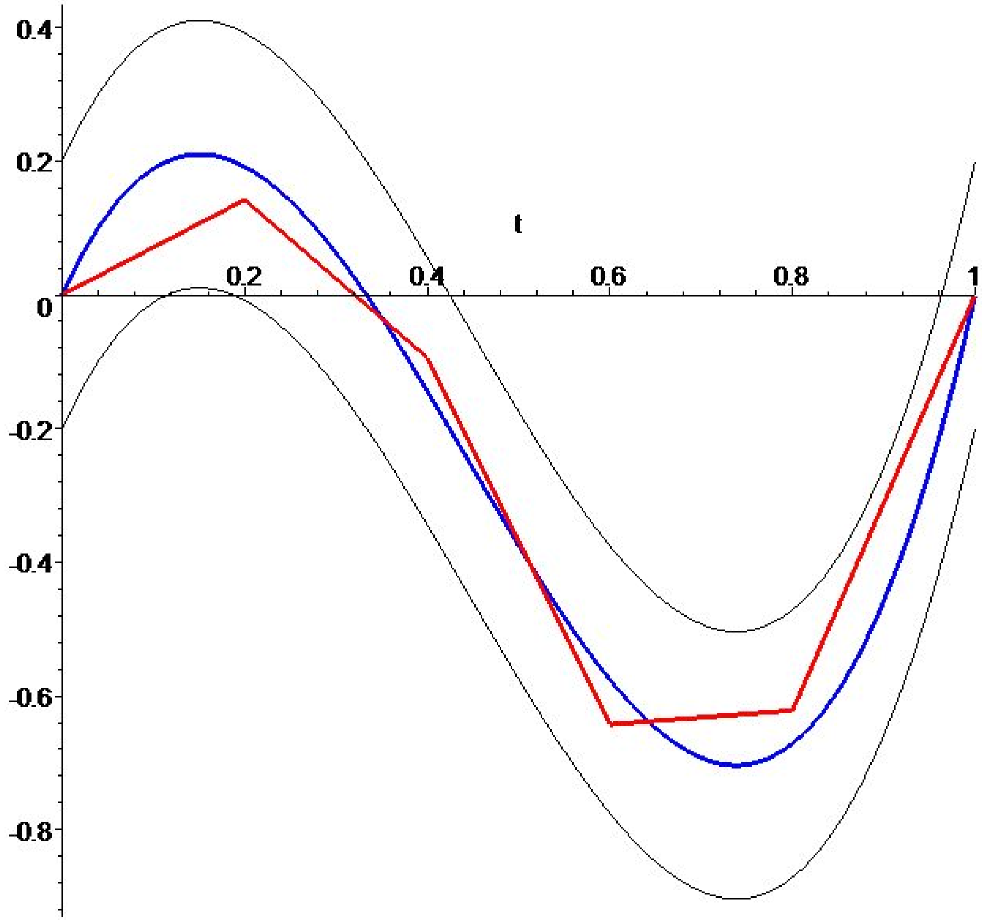
HD Picture V



HD Picture VI



HD Picture VII



THE PROBLEMS WITH THIS APPROACH (I)

Problem 1.- *What is the compexity of this method?*

Answer.–
– The complexity of each step is polynomial in the number of variables and the evaluation complexity of the input system. Thus, complexity mainly depends on the number of steps.

– The number of "homotopy steps" is bounded by $O(\mu_{norm}(\Gamma)^2)$ ([Shub-Smale, 91]), where

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

The Problems with this approach (II)

Problem 2.- *worst case complexity is doubly exponential in the number of variables (voir exemple dans [castro–Hagele–Morais–P., 01]), and then?*

Answer.–

– "Worst case complexity" does not suffice to explain the behavior. Look at average complexity!.

– The word "average" forces to have some probability distribution, . *which one?.*

Answer (Sub-problem 2b).–
– The set $\mathbb{P}(\mathcal{H}_{(d)})$ is a complex and compact Riemannian manifold. Thus, it has an associated measure (a volume form in $d\nu_{\mathbb{P}}$) such that the volume $\nu_{\mathbb{P}}[\mathbb{P}(\mathcal{H}_{(d)})]$ is finite. Then we also have a probability distribution.

– The probability measure in $\mathbb{P}(\mathcal{H}_{(d)})$ equivalent to Gaussian distribution in the affine space $\mathcal{H}_{(d)}$.

Sub–problem 2c.–*Since computing is discrete, what is the distribution for discrete inputs (namely polynomials with coefficients in a discrete field)?.*

The Problems with this approach (IV)

Problem 3.– *Anyway, this approach is not defining an algorithm (since we have o initial pair). Is there a true algorithm of polynomial average complexity?.*

Answers.–

1.– Yes.

2.– Polynomial in the dimension of the space of inputs (dense encoding of polynomials).

Once again HD

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

Apply homotopic defomration (HD) *with initial pair*

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

following the curve $\Gamma(F, G, z)$ *of* $\Gamma = \pi_1^{-1}([F, G]))$ *that contains* (G, z).

Output:

– *Either ERROR*

– *or an approximate zero of* F.

HD with resources bounded by a function $\varphi(f, \varepsilon)$.

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

Perform $\varphi(f, \varepsilon)$ steps of homotopic deformation (HD) *with initial pair*

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

following the curve $\Gamma(F, G, z)$ *in* $\Gamma = \pi_1^{-1}([F, g]))$ *that contains* (G, z).

OUTPUT:

– *Either ERROR*

– *or an approximate zero of* F.

$\varepsilon-$EFFICIENT INITIAL PAIRS

Definition *A pair* $(G, \zeta) \in V$ *is* $\varepsilon-$*efficient if the resources function for the resources:*

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

For randomly chosen input system $F \in \mathbb{P}(\mathcal{H}_{(d)})$ *the algorithm HD with initial pair* (G, z) *and resources bound* φ *outputs un approximate zero of* F *with probability greater than:*

$$1 - \varepsilon.$$

HD WITH $\varepsilon-$EFFICIENT INITIAL PAIR

Let $(G_\varepsilon, \zeta_\varepsilon)$ be an $\varepsilon-$efficient initial pair.

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

Perform $\varphi(f, \varepsilon)$ steps of HD *with initial pair*

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

following $\Gamma(F, G_\varepsilon, \zeta_\varepsilon)$.

OUTPUT:

– *Either ERROR*

– *or an approximate zero of* F.

Theorem 7 *([Shub-Smale, BezV, Beltrán-P, Bez V 1/2] There exist $\varepsilon-$efficient initial pairs.*

Remark 8 *Even with $\zeta_\varepsilon = (1 : 0 : \cdots : 0)$.*

Smale 17th Problem.– How to construct $\varepsilon-$efficient initial pairs?.

Questor Sets

[Beltrán- P., 2006]

A subset $\mathcal{G} \subseteq V$ (incidence variety) is *a questor set for HD if:*

for every $\varepsilon > 0$ *the probability that a randomly chosen pair* $(G, \zeta) \in \mathcal{G}$ *is* $\varepsilon-$*efficient for HD is greater than*

$$1 - \varepsilon.$$

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

Guess at random $(G, \zeta) \in \mathcal{G}$

Apply $\varphi(f, \varepsilon)$ *deformation steps HD between* G *and* F*, starting at* (G, ζ)*.*

OUTPUT:

– *Either ERROR (with probability smaller than* ε*)*

– *or un approximate zero of* F *(with probability greater than* $1 - \varepsilon$*).*

COMMENTS

Minor: **It is a probabilistic algorithm**

Relevant: **The questor set $\mathcal{G}$ must be easy to construct and easy t handle .**

Theorem[*Beltrán, P. 2006*] *We succeeded to exhibit a constructible and easy to mhandle questor set.*

$e := (1 : 0 : \ldots : 0) \in \mathbb{P}_n(\mathbb{C})$ *a "pole" in the complex sphere.*

$V_e := \{F \in \mathcal{H}_{(d)} \ : \ F(e) = 0\}$. *Systems vanising at the "pole" e.*

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

The tangent mapping $T_eF := DF(e)$ *restricted to the tangent space* $T_e\mathbb{P}_n(\mathbb{C}) = e^{\perp} = \mathbb{C}^n \subseteq \mathbb{C}^{n+1}$.:

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

A First Approach

$L_e := \{F \in V_e \, : \, T_e F = F\}$. *"linear part" of the systems in* V_e.

$L_e^{\perp}$:= *Systems in* V_e *of order greater than 2 at* e.

Remark.- *$V_e, L_e, L_e^{\perp}$ are linear subspaces of $\mathcal{H}_{(d)}$ given by their coefficient list.*

Naïve Idea: *Consider*

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

Towards Questor Sets II (L_e)

$\mathcal{U}(n+1)$:= *unitary matrices defined in* $\mathbb{C}^{n+1}$.

$\mathcal{H}_{(1)} := \mathcal{M}_{n\times n+1}(\mathbb{C})$ **space of $n \times (n+1)$ complex matrices.**

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

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

$\boxed{\text{LINER PART } L_e}$

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

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

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

A useful constant

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

Towards a questor set III

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

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

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

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

Theorem 9 (Beltrán-P., 2005a) *For every degree list* $(d) := (d_1, \ldots, d_n)$, *the set*

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

is questor set of initial pairs for HD. Namely,

A system $(G, e) \in \mathcal{G}_{(d)}$ chosen at random is $\varepsilon-$efficient for HD with probability greater than

$$1 - \varepsilon.$$

THE ALGORITHM

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

Guess at random $(G, e) \in \mathcal{G}_{(d)}$ $(Guess\ (t, L, M)\ldots)$

Apply $\varphi(F, \varepsilon)$ **homotopic deformation steps**

OUTPUT: Either "ERROR" or an approximate zero z of F.

Meaning (I)

Theorem 10 [Beltrán-P,06] *There is a probabilistic algorithm (bounded error probability) for non–universal projective solving of systems of homogeneous polynomial equations such that for every positive real number* $\varepsilon > 0$*:*

- *The running time of the algorithm is at most:*

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

- *The probability that the algorithm outputs an approximate zero is greater than:*

$$1 - \varepsilon$$

Corollary 11 [Beltrán-P,06] *There is a probabilistic algorithm (bounded error probability) for non–universal projective solving of systems of homogeneous polynomial equations of degree 3 such that for every positive real number $\varepsilon > 0$:*

- *The running time of the algorithm is at most:*

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

- *The probability that the algorithm outputs an approximate zero is greater than:*

$$1 - \varepsilon$$

Remarque Taking $\varepsilon = 1/n^2$, the algorithm computes approximate zeros with probability greater than

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

in time

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

In [Beltrán-P., 07] we slighty modified our algorithm to get average complexity:

Definition 12 (Strong Questor Set) *A subset $\mathcal{G} \subseteq V$ is a strong questor set if*

$$E_{\mathcal{G}}[A_\varepsilon] \leq 10^4 n^5 N^3 d^{3/2} \varepsilon^2,$$

where

$$A_\varepsilon(G, z) := Prob_{\mathbb{P}(\mathcal{H}_{(d)})}[\mu_{norm}(F, G, z) > \varepsilon^{-1}].$$

Strong Questor Set

Theorem 13 (Beltrán-P.,07) *For every strong questor set $\mathcal{G}$, there is a measurable subset $\mathcal{C}$ such that the following holds:*

$$Prob_{\mathcal{G}}[\mathcal{C}] \geq 4/5.$$

For every $\varepsilon > 0$ and for every $(G, z) \in \mathcal{C}$, (G, z) is a $\varepsilon-$efficient initial pair.

Theorem 14 (Beltrán-P.,07) *The set $\mathcal{G}_{(d)}$ is a strong questor set.*

Corollary 15 *There is a bounded error probability algorithm of average polynomial time that for all but a zero measure subset of systems of homogeneous polynomial equations computes projective approximate zeros .*

By average complexity we mean:

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

$T_{\mathcal{P}}(f) :=$ *running time on input* f.

[Beltrán-P., 07] :

Corollary 16 *There is a bounded error probability algorithm of average polynomial time that for all but a zero measure subset of systems of homogeneous polynomial equations computes affine approximate zeros.*

By average complexity we mean:

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

$T_{\mathcal{A}}(f) :=$*running time on input* f.

[Beltrán-P., 07]

Theorem 17 *Let $\delta > 0$ be a positive real number. For every $F \in \mathbb{P}(\mathcal{H}_{(d)})$, let*

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

be the set of affine solutions Let

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

the maximal norm of its zeros.

Then, the probability that for a randomly chosen affine system $F \in \mathbb{P}(\mathcal{H}_{(d)})$ we have $||V_A(F)|| > \delta$ is at most:

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

.

In fact, we proved:

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

Immediate Open Questions

Real Solving ?: Zero–dimensional Case.

Singular Zeros: Homotopy Techniques?.

Adaptability to Other Input Data Structures: Does it work for straight–line programa input structure?.