Using infinitesimals for algorithms in real algebraic geometry

by Marie-Françoise Roy
IRMAR (UMR CNRS 6625), Université de Rennes

IPAM,April 12, 2014

talk based on several papers written with S. Basu and/or R. Pollack
see Algorithms in Real Algebraic Geometry **S. Basu, R. Pollack, M.-F. R**.

1 Motivation

critical point method : basis for many quantitative results in real algebraic geometry (starting with Oleinik-Petrovskii-Thom-Milnor)

wish : use critical point method in algorithms in real algebraic geometry with singly exponential complexity in problems such as existential theory of the reals, deciding connectivity (and more)

also in the quadratic and symmetric case (see talk by Cordian Riener)

requires general position, reached through various deformation tricks

in these algorithms, "small enough" is through the use of infinitesimals

Cylindrical Decomposition is doubly exponential (unavoidable if use repeated projections, see preceeding lectures)

Critical point method

based on Morse theory

nonsingular bounded compact hypersurface

$$V = \{M \in R^k\,,\ H(M) = 0\},$$

i.e. such that

$$\mathrm{Grad}_M(H) = \left[\frac{\partial H}{\partial X_1}(M), \ldots, \frac{\partial H}{\partial X_k}(M)\right]$$

does not vanish on the zeros of H in C^k

critical points of the projection on the $X_1 -$ axis meet all the connected components of V

when the X_1 direction is a Morse function, there are $d(d-1)^{k-1}$ such critical points (Bezout),

$$H(M) = \frac{\partial H}{\partial X_2}(M) = \ldots, \frac{\partial H}{\partial X_k}(M) = 0, \tag{1}$$

(project directly on one line rather than repeated projections)

so : want to find a point in every connected components in time polynomial in $(1/2)d(d-1)^{k-1}$ i.e. $d^{O(k)}$

BUT

an hypersurface is not always smooth and bounded

choosing a Morse function is difficult

basic problem : take a point outside an hypersurface (the set of directions which are NOT Morse functions) of degree d^k: costs $d^{O(k^2)}$ ... too much ...

Idea : perform a deformation so that (1) has automatically a finite number of solutions, which are going to be easy to compute...

2 Definitions

R is a **real closed field** : ordered field $+$ every positive number is a square$+$ satisfying the intermediate value theorem for polynomials

Elementary analysis for polynomials : Rolle's theorem, real root counting

Logical properties : quantifier elimination, transfer

Geometrical properties : finiteness properties of various kinds

$C = R[i]$ is algebraically closed

Examples

Real closed fields can be archimedean (every positive number is smaller than a natural number) : subfields of $\mathbb{R}$, such as $\mathbb{R}_{\mathrm{alg}}$, the real algebraic numbers, which is the real closure of $\mathbb{Q}$.

They can also have infinitesimals elements.

Puiseux series

$R\langle\langle\varepsilon\rangle\rangle$field of **real Puiseux series** in ε with coefficients in R

ε is positive and smaller than any positive element of R

rational exponents are needed such as : $\sqrt{\varepsilon}$

series of the form

$$\sum_{i\geqslant i_0} a_i\,\varepsilon^{i/q}$$

where $i_0\in\mathbb{Z}$, $q\in\mathbb{N}$, $a_i\in R$

positive is a_{i_0} is positive

contains the field $R(\varepsilon)$

Exercise: Prove that any positive element has a square root

$R\langle\varepsilon\rangle$real closure of $R(\varepsilon)$ smallest real closed field containing $R(\epsilon)$
two possible descriptions
1 **algebraic real Puiseux series** in ε with coefficients in R
2 **germs of semi-algebraic continuous functions**
$f \backsim g$ iff $\exists t_0, t_0 > 0, \forall t, 0 < t < t_0, f(t) = g(t)$
$f < g$ iff $\exists t_0, t_0 > 0, \forall t, 0 < t < t_0, f(t) < g(t)$
An algebraic real Puiseux series defines a germ of semi-algebraic function

Example : $\varepsilon^{1/3}$ is a solution of the equation $y^3 = \varepsilon$ and defines the germ of semi-algebraic function associated to $y = x^{1/3}$

Exercise : Prove that the germ of x is infinitesimal gives a rigorous interpretation of “for a positive and small enough number” in the context of real algebraic geometry (functions are only polynomials, semi-algebraic functions, this is NOT non standard analysis ...)

$$\sum_{i \geqslant i_0} a_i \, \varepsilon^{i/q}$$

where $i_0 \in \mathbb{Z}$, $q \in \mathbb{N}$, $a_i \in R$

limit ? no analysis: constant term of a bounded Puiseux series !

If $i_0 < 0$, the Puiseux series is infinite (absolute value bigger than any element of R)

If $i_0 \geqslant 0$, the Puiseux series is bounded and the limit is a_{i_0} (“obtained by making $\varepsilon = 0$”)

very particular case of the method of ideal points (cf. Michel Coste’s talk) geometry on a general real closed field

semi-algebraic sets

compact ? $[0,1] \subset \mathbb{R}_{\mathrm{alg}}$ is not compact replace by closed and bounded

connected components ? $\mathbb{R}_{\mathrm{alg}}$ is not connected (think of π) need to be replaced by "semi-algebraically connected components" (only covers to consider are the semi-algebraic ones)

important to take into account the defining equations, $[0,\pi] \cap \mathbb{R}_{\mathrm{alg}}$ is NOT a semi-algebraic subset of $\mathbb{R}_{\mathrm{alg}}$ (not a finite union of points and intervals with end points algebraic numbers: **be aware of the syntax !**

$R \subset R'$, two real closed fields

extension of a semi-algebraic set $S \subset R^k$ (defined by polynomials with coefficients in R) to R'

description of S

$$S = \{x \in R^k |\, \Phi(x)\}$$

Φ can be a quantifier free formula, or a general first order formula (with parameters in the field R)

definition of the extension of S to R' $\mathrm{Ext}(S, R')$

$$\mathrm{Ext}(S, R') = \left\{x \in {R'}^k |\, \Phi(x)\right\}$$

This extension is well defined : if

$$S = \{x \in R^k | \, \Phi(x)\} = \{x \in R^k | \, \Psi(x)\}$$

$$\mathrm{Ext}(S, R') = \left\{x \in R'^k | \, \Phi(x)\right\} = \left\{x \in R'^k | \, \Psi(x)\right\}$$

uses quantifier elimination, completeness of the theory of real closed fields

Exercizes

S is non empty if and only if $\mathrm{Ext}(S, R')$ is non empty (hint: formula)

S is finite if and only if $\mathrm{Ext}(S, R')$ is finite (hint: formula)

$\dim(S) = \dim(\mathrm{Ext}(S, R'))$ (hint : CAD+formula)

also topology: same Betti numbers, same Euler-Poincaré characteristic

3 Sampling on an algebraic set

find (at least) a point in every semi-algebraically connected component of an algebraic set

several equations reduce to one equation by sum of squares (reals !)

bounded : intersect with big sphere (adds one infinitesimal)

deformation so : smooth and X_1 is a good Morse projection

(this is crucial for us since determining a good Morse projection would spoil the $d^{O(k)}$ complexity, and not determining a good Morse projection leads to a "probabilistic algorithm")

Deformation explained by an example

Let $Q \in R[X_1, X_2, X_3]$ be defined by

$$Q = X_2^2 - X_1^2 + X_1^4 + X_2^4 + X_3^4.$$

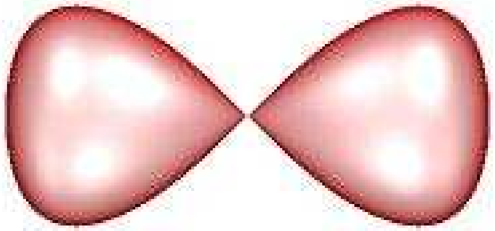

Figure 1.

$$\mathrm{Def}(Q,\varepsilon)=Q^2-\varepsilon\,(X_1^{10}+X_2^{10}+X_3^{10}+1).$$

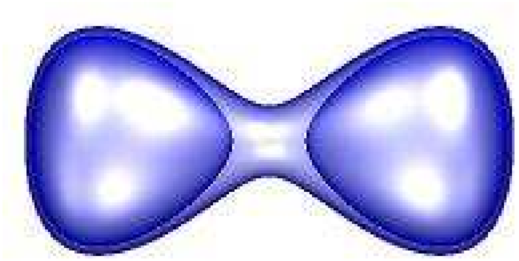

Figure 2.

special deformation such that X_1 is good : modify using an object which does what you want

geometric aspect

Def(Q,ε) defines a smoth hypersurface inside $R\langle\varepsilon\rangle^k$: By Sard's theorem the values of $t \in R$ such that Zer(Def$(Q,t)) \subset R^k$ is singular are in finite number, so for $0 < t < t_0$ small enough Zer(Def$(Q,t)) \subset R^k$ is smooth, so Zer(Def$(Q,\varepsilon)) \subset R\langle\varepsilon\rangle^k$ smooth

various **algebraic tools**

polynomials in $D[X_1, \ldots, X_k]$, D an ordered domain, computations take place there (example: subresultants used for real root counting are determinants of matrices with entries the coefficients ...)

after deformation $D[\varepsilon][X_1, \ldots, X_k]$

polynomial system solving: uses Groebner basis, the fact that the deformation involves high degree terms gives "automatic" Groebner basis

number of solutions $O(d)^k$, complexity in $D[\varepsilon]$: $d^{O(k)}$, degree in ε: $O(d)^k$,

so complexity in D $d^{O(k)}$

project to a line by a separating linear form: univariate polynomial depending on T, ε of degree $O(d)^k$

representation of points (which are necessarily algebraic Puiseux series, and not in the field of fractions of $D[\varepsilon]$) : rational functions of the root of a univariate polynomial

take the limit of these points: replace ε by 0 (details to take care of to avoid 0/0)

- ***complexity***

  Grigori'ev/Vorobjov, Canny, Renegar, Heintz/R./Solerno, Basu/Pollack/R.

  Sampling points of connected components of algebraic sets

  $$d^{O(k)}$$

  quasi-optimal since polynomial in the size of the output

4 Finding all realizable sign conditions

Existential theory of the reals

a point (at least) in every semi-algebraically connected component of all realizable sign conditions on a family of polynomials $\mathcal{P}$

not too many intersections: general position

more than k polynomials have no common zeroes (needs a new deformation)

$$H_k(d,i) = 1 + \sum_{1 \le j \le k} i^j \, X_j^d,$$

these particular polynomials are in general position, otherwise a non zero polynomial of degree k has more than k solutions

replace each $P_i \in \mathcal{P}$ by four polynomials depending on two infinitesimals

$$\begin{aligned} P_i^\star &= \{(1-\delta)\, P_i + \delta\, H_k(d',i), (1-\delta)\, P_i - \delta\, H_k(d',i), \\ &\quad (1-\delta)\, P_i + \delta\, \gamma\, H_k(d',i), (1-\delta)\, P_i - \delta\, \gamma\, H_k(d',i)\} \end{aligned}$$

with $d' > d$ (degree of polynomials in $\mathcal{P}$)
$\mathcal{P}^\star = \cup_{i=1}^s P_i^\star$ also in general position (in $R\langle \delta, \gamma \rangle^k$)

Proposition 1. *Let $C \subset R^k$ be a semi-algebraically connected component of the realization of the sign condition*

$$\begin{aligned} P_i &= 0, i \in I \subset \{1, \dots, s\}, \\ P_i &> 0, i \in \{1, \dots, s\} \setminus I. \end{aligned}$$

Then there exists a semi-algebraically connected component C' of the subset $\tilde{C} \subset R\langle \varepsilon, \delta, \gamma \rangle^k$ defined by the weak sign condition

$$-\gamma \, \delta \, H_k(d', i) \leq (1 - \delta) \, P_i \leq \gamma \, \delta \, H_k(d', i), \;\; i \in I,$$

$$(1 - \delta) \, P_i \geq \delta \, H_k(d', i), \;\; i \in \{1, \dots, s\} \setminus I$$

$$\varepsilon (X_1^2 + \cdots + X_k^2) \leq 1$$

such that $\lim_{\gamma} (C')$ is contained in the extension of C to $R\langle \varepsilon, \delta, \gamma \rangle$.

algebraic sampling in each of the algebraic sets defined by less that k polynomials in $\mathcal{P}^{\star}$: s-a connected components of all realizable sign conditions on $\mathcal{P}^{\star}$

s^k cases to consider, in each case algebraic sampling+sign determination

after deformation $D[\varepsilon, \delta, \gamma][X_1, \ldots, X_k]$

for each case sampling $d^{O(k)}$in $D[\varepsilon, \delta, \gamma]$

needed to find the sign of the polynomials at these points $s\, d^{O(k)}$

degree of the algebraic points $O(d)^{\,k}$ (no s)

degree in the infinitesimals $O(d)^{\,k}$

fixed number of infinitesimals ...

Complexity $s^{k+1} d^{O(k)}$, quasi optimal also Euler-Poincaré characteristic of sign conditions

NB we replaced inequalities by weak inequalities, using two infinitesimals. If we are interested in one single sign condition, one infinitesimal is enough. But the complexity, for one single sign condition remains $s^{k+1}d^{O(k)}$

Two infinitesimals are enough to have a point in every connected component of every realizable sign condition, but to control more fully the topology more infinitesimals are needed: two infinitesimals for each homology group (cf talk by Nikolai Vorobjov)

quantitative "curve selection lemma" for free

$x \in \bar{S}$, $\exists t_0, \exists \varphi \colon [0, t_0) \to R, \varphi(0) = x, \varphi((0, t_0)) \subset S$

not true in analysis but true in real algebraic geometry: semi-algebraic sets are "tame"

result of Jelonek-Kurdyka Reaching generalized critical values of a polynomial (arxiv, august 2013): curve selection lemma "at infinity", based on affine curve selection lemma; obtain a path of degree $d^{O(k^2)}$

another approach (Basu/R., to be written)

using infinitesimals+sampling
$x \in \bar{S}$, $\forall t > 0, B(x,t) \cap S \neq \emptyset$ so $B(x,\varepsilon) \cap \mathrm{Ext}(S, R\langle\varepsilon\rangle) \neq \emptyset$
using sampling find a point γ in $B(x,\varepsilon) \cap \mathrm{Ext}(S, R\langle\varepsilon\rangle)$, $\lim(\gamma) = x$
γ is an algebraic Puiseux series, so defines a germ of semi-algebraic function i.e. a “little path”
quantitative analysis: degree in ε : $O(d)^k$

not totally immediate: needs to inspect the nature of computations made inside sampling: determinant of matrices of size $O(d)^k$ ...

5 Deciding connectivity

- ***Deciding connectivity***: roadmap
  - roadmap definition
    semi-algebraic set M of dimension at most one contained in S
    - RM$_1$ For every connected component D of S, $D \cap M$ is semi-algebraically connected.
    - RM$_2$ For every $x \in R$ and for every connected component D' of S_x, $D' \cap M \neq \emptyset$.

- the torus

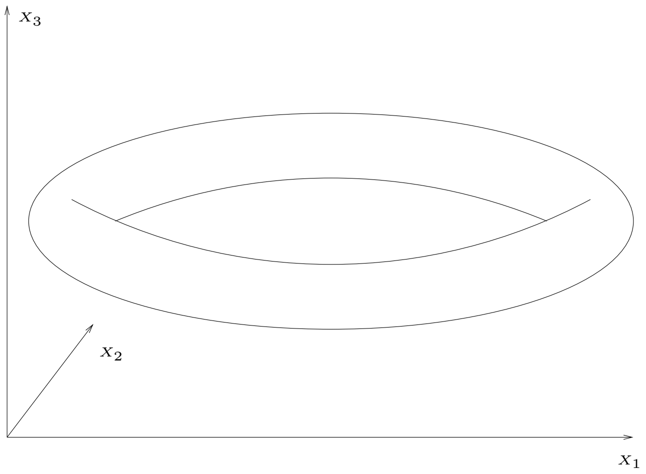

Figure 3. A torus in R^3

perform sampling points parametrically : for every value of X_1 find a point in every semi-algebraically connected component of the fiber

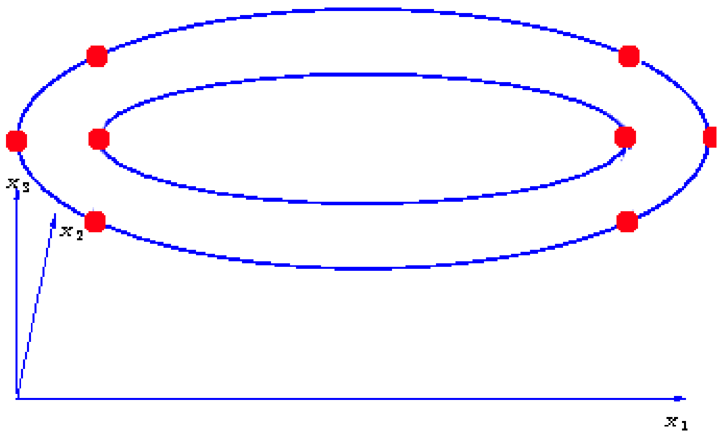

Figure 4. Parametrized sampling points on a torus in $\mathbb{R}^3$

then make a recursion, again hypersurface, in an hyperplane

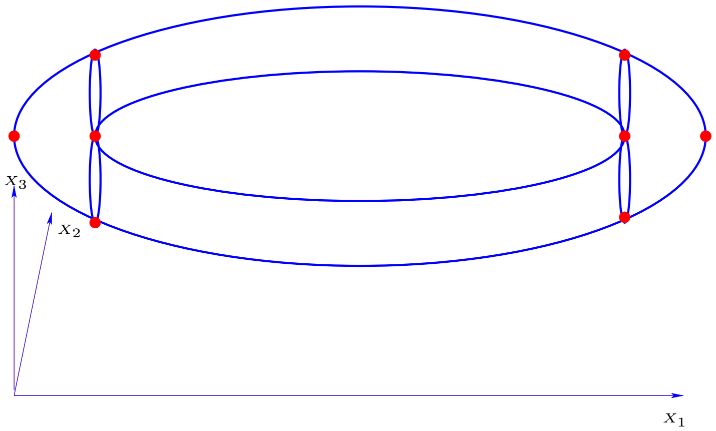

Figure 5. The roadmap of the torus

single exponential complexity : $d^{O(k^2)}$
(number of recursive calls)

So, complexity of classical roadmaps $d^{O(k^2)}$....

Divide and conquer roadmaps

S (very particular) basic closed semi-algebraic set of dimension p (a power of 2 for simplicity) inside R^k

divide consider a $p/2$-dimensional subset S^0 of S (think of a finite number of critical points, above each $y \in R^{p/2}$) and make recursive calls

- at S^0 itself

- at S^1, union of special fibers: $k - p/2$-dimensional linear spaces intersected with S (corresponding to places where the connectedness has to be controlled)

both of dimension $p/2$!

topological lemma : prove that (S, S^0, S^1) have good connectivity property

two points in $S^0 \cup S^1$ which are in the same s-a connected component of S are in the same s-a connected component of $S^0 \cup S^1$

then recurse : **conquer**

main difficulty to overcome: in recursive calls, no more an hypersurface in a smaller ambiant space but algebraic sets of various codimensions (even if the starting point is an hypersurface of dimension $k-1$)

genericity properties are difficult to maintain throughout the algorithm ...

Two approaches

-work of **Safey** and **Schost** in the case of a smooth hypersurface (probabilistic) using polar varieties

(probabilistic because not possible to find good Morse functions within the complexity aimed at)

-work of **Basu** and **R.** in the case of a general real algebraic set, using deformations and semi-algebraic techniques

paper under revision to appear in Discrete and Computational Geometry,

Our statement

Theorem 2.

Let V be the zero set of a polynomials of degree d in k variables and with coefficients in an ordered domain D. We describe

1. *algorithm for constructing a roadmap for V using $\left(k^{\log(k)}d\right)^{O(k\log^2(k))}$ arithmetic operations in D*
2. *algorithm for counting the number of connected components of V using $\left(k^{\log(k)}d\right)^{O(k\log^2(k))}$ arithmetic operations in D.*
3. *algorithm for deciding whether two given points belong to the same connected component of V using $\left(k^{\log(k)}d\right)^{O(k\log^2(k))}$ arithmetic operations in D.*

number of infinitesimals $4\log(k-1)$: four new infinitesimals per recursion level

first three infinitesimals $\zeta, \varepsilon, \delta$ used to modify S into $\tilde{S}$ so that a function G (chosen in advance) has a finite number of critical points when we consider a fiber where $p/2$ variables are fixed : this defines $\tilde{S}^{\,0}$ of dimension $p/2$ (in same ambiant space): critical point parametrized by $R\langle\zeta, \varepsilon, \delta\rangle^{p/2}$

then define special fibers in $R\langle\zeta, \varepsilon, \delta\rangle^{k-p/2}$: $\tilde{S}^1$ ensuring connectivity

for the deformation defining $\tilde{S}$: use the rows of a matrix with "good rank property" (all its square minors are non zero) for coefficients: technique coming from Jeronimo/Perrucci 's work on optimization (see Daniel Perrucci's talk)

$\lim\left(\tilde{S}\right) = S$

fourth infinitesimal : $\tilde{S}^0$ is covered by open charts and is the limit of closed (semi-algebraic) sets (shrinking a little these charts)

degree in the remaining variables and infinitesimals $O\big(k^{\log(k)}\, d\big)^{k\log(k)}$

There is so much we do not know

local conical structure (also at infinity) see Nikolai Vorobjov's problem in the session problem

$x \in S$, $\forall t, 0 < t < t_0$, $B(x,t) \cap S$ is homeomorphic to the cone centered at x and based on $S(x,t) \cap S$

Looks like (and is very similar to) the "curve selection lemma"

Property true for t small enough (i.e. $0 < t < t_0$), i.e. is true in $R\langle\varepsilon\rangle$

But we do not have a good bound (i.e. singly exponential in k) on the degree of the polynomials defining t_0. Related to the structure of singularities. For smooth situation, critical points are good, but the deformation "loses" information on singularities.

Emptyness, Euler-Poincaré characteristic, connectedness are well controlled using critical point method, topology in general is not.