Two Algorithmic Methods in Real Algebraic Geometry

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

IPAM,March 27, 2014

- # 1 Some basic algorithmic problems

  - *effectivity*: existence of an algorithm,
    (1) **Real root counting**: count the number of real roots of a univariate polynomial, Sturm 1836

    (2) **Existential theory of the reals** decide whether a semi-algebraic set is empty Tarski 1939 (undecidable on integers Matiyasevich 1973)

    (3) **Algebraic certificates** find an algebraic certificate for the fact that a polynomial is non negative (Hilbert 17th problem) Kreisel 1953, emptyness of basic semi-algebraic sets (positivstellensatz) Lombardi 1993

(4) **Decide connectivity** decide whether a semi-algebraic set is connected : cylindrical decomposition: Lojasiewicz, Collins (1960-70), Schwartz-Sharir, describe connected components, also cylindrical decomposition

(5) **Stratification**: decompose a semi-algebraic set in smooth manifolds of various dimensions by cylindrical decomposition

(6) **Betti numbers** compute the topological invariants (Betti numbers) of semi algebraic sets using this stratification

also more general problems : deciding first order formulae, eliminating quantifiers and non-effectivity phenomena (see lecture by Michel Coste)

- *complexity*: function of size of the input (s number of polynomials, k number of variables, d degrees, τ bitsize)

(1) **Real root counting** complexity quasi linear in degree (Schonhage, Lickteig/R)

(2) **Existential theory of the reals** and (4) **Deciding connectivity** polynomial in s, d and τ, doubly exponential in k by cylindrical decomposition, singly exponential in k by critical points method (various contributions see Basu/Pollack/R book)

(3) **Algebraic certificates** : elementary complexity (tower of exponents of height 5, Lombardi/Perrucci/R) while single exponential complexity for Hilbert nullstellensatz (Kollar, Jelonek))

(5) **Stratification** and (6) **Computing Betti numbers** : polynomial in d, and τ, doubly exponential k by cylindrical decomposition. Singly exponential ? partial results for Betti one (Basu/Pollack/R 2004), for a few first Betti numbers (Basu 2004)

(2') **Existential theory of the reals** in the quadratic case: polynomial in k (Grigor'ev Pasechnik), also optimization

(6') **Betti numbers** in the quadratic case: for the top ones, polynomial in k (Basu 2004)

(2") **Existential theory of the reals** in the symmetric case: polynomial in k (Basu, Riener), also optimization

• 2 Real root counting : subresultants

$$
\begin{aligned}
P &= a_p X^p + a_{p-1} X^{p-1} + a_{p-2} X^{p-2} + \cdots + a_0, \\
Q &= b_q X^q + b_{q-1} X^{q-1} + \cdots + b_0
\end{aligned}
$$

$$
\mathrm{SH}_j(P,Q) = \begin{bmatrix}
a_p & \cdots & \cdots & \cdots & \cdots & a_0 & 0 & 0 \\
0 & \ddots & & & & & \ddots & 0 \\
\vdots & \ddots & a_p & \cdots & \cdots & \cdots & \cdots & a_0 \\
\vdots & & 0 & b_q & \cdots & \cdots & \cdots & b_0 \\
\vdots & \iddots & \iddots & & & & \iddots & 0 \\
0 & \iddots & & & & \iddots & \iddots & \vdots \\
b_q & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & 0
\end{bmatrix}.
$$

j-th subresultant $\mathrm{sr}_j(P,Q)$: determinant of $p+q-2j$ first columns

- ***important for complex root counting***

Proposition 1. $\deg(\gcd(P,Q)) > \ell$ *if and only if*

$$\mathrm{sr}_0(P,Q) = \cdots = \mathrm{sr}_\ell(P,Q) = 0.$$

proof easy: linear algebra

- *important for real root counting*

  Cauchy index of Q/P, $\mathrm{Ind}(Q/P)$: number of jumps from $-\infty$ to $+\infty$ minus number of jumps from $+\infty$ to $-\infty$

  Number of real roots $= \mathrm{Ind}(P'/P)$, also: number of roots with polynomial constraints

  $\mathrm{PmV}(s)$ = difference between the number of sign permanences and the number of sign variations in $s = s_p, \ldots, s_0$, if all elements of s are $\neq 0$ (more technical if there are zeroes)

Theorem 2. $$\mathrm{PmV}(\mathrm{sr}(P,Q)) = \mathrm{Ind}(Q/P).$$

proof: relate the subresultants of P, Q to those of Q, $-R$ where $R = \mathrm{Rem}(P,Q)$ and make an induction

- ***important for complexity***
  d degree, τ bitsize
  - computations in $\mathbb{Q}$, answers in $\mathbb{R}$
  - computed by a variant of remainder sequence $O(d)$ arithmetic operations $O(d^3\tau)$ bit operations
  - using that gcd and quotient suffice: $\tilde{O}(d)$ arithmetic operations and $\tilde{O}(d^2\tau)$ bit operations (Schonhage, Lickteig/R ....)
  - bitsize of intermediate computations controlled (determinants)
  - good specialization properties when there are parameters (determinants, so no denominators)

3 Cylindrical decomposition

- *cylindrical decomposition* of R^k

  sequence $\mathcal{S}_1, \ldots, \mathcal{S}_k$, where $\mathcal{S}_i$ decomposes R^i in *cells*, such that

  a) $S \in \mathcal{S}_1$ is either a point or an open interval

  b) for every $S \in \mathcal{S}_j$, $j < k$ there exist semi algebraic functions $\xi_{S,j}$

  $$\xi_{S,1} < \ldots < \xi_{S,\ell_S}: S \longrightarrow R\ ,$$

  such that the cylinder $S \times R \subset R^{i+1}$ is the disjoint union of cells of $\mathcal{S}_{i+1}$

  - either a *graph* $\Gamma_{S,j}$, of one of the $\xi_{S,j}$, pour $j = 1, \ldots, \ell_S$
  - or a *band* $B_{S,j}$ of the cylinder between the graphs of two functions $\xi_{S,j}$ and $\xi_{S,j+1}$

cylindrical algebraic decomposition adapted to a family of polynomials : on each cell the signs of the polynomials in $\mathcal{P}$ are fixed

- ***picture***: the sphere

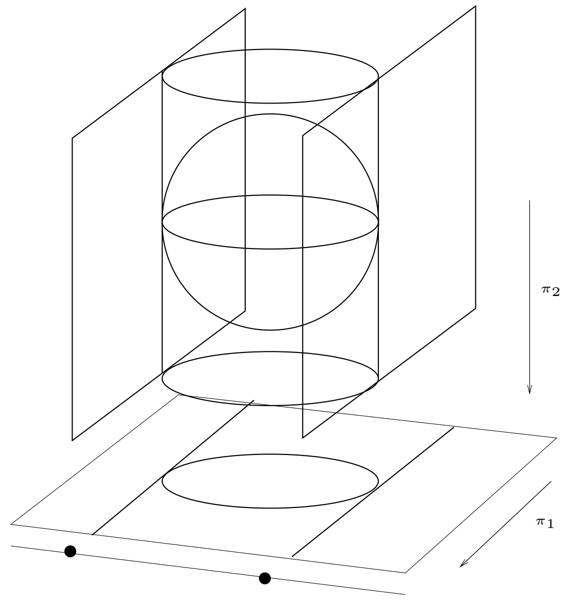

Figure 1. cylindrical decomposition adapted to the sphere

- **Theorem 3.** *For every finite $\mathcal{P} \subset R[X_1, ..., X_k]$, there exists a cylindrical algebraic decomposition of R^k adapted to $\mathcal{P}$.*

  idea: fix the degree of all gcd of two polynomials in the family so that roots dont mix up, using subresultant

  induction on number of variables

  as a consequence : semi-algebraic set: finite union of connected pieces, semi-algebraically homeomorphic to open cubes

- **cylindrical decomposition algorithm**

  projection phase : Elim($\mathcal{P}$) compute subresultants of pairs of (truncations of) polynomials in the family recursively

  above a connected component of the realization of a sign condition on Elim($\mathcal{P}$) the cylinder of sign conditions satisfied by $\mathcal{P}$ is fixed

  lifting phase : produce a sampling point in each cell starting from the line (needs to deal with real algebraic numbers)

advantages

very simple

produces a lot of information

solves the Existential theory of the reals (and much more, see Michel's talk)

Decides connectivity, describes connected components

gives a Stratification (after linear change of variables) thus all the Betti numbers

inconvenience: complexity doubly exponential in the number of variables:

eliminating one variable squares the degree and the number of polynomials

doubly exponential

$$O(s\,d)^{2^{k-1}}$$

(dependance in s doubly exponential even in o-minimal setting, see Saugata's talk)

Doubly exponential dependence of Cylindrical Decomposition is unavoidable. Lower bound due to Davenport and Heintz [1988].

• 4 Critical points: singly exponential complexity

- *geometrically*
  based on Morse, Oleinick, Petrowski, Thom, Milnor
  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 $X-$axis meet all the connected components of V
except special cases, $d(d-1)^{k-1}$ such critical points (Bezout),

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

general case

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

bounded by adding one variable and taking intersection between cylinder and big sphere

deformation so that it becomes smooth and X_1-is guaranteed to be a good Morse projection

(this is crucial for us since determining a good Morse projection would spoil the complexity, and not determining a good Morse projection leads to a "probabilistic algorithm" (see later for roadmaps))

Deformation explained by an example

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

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

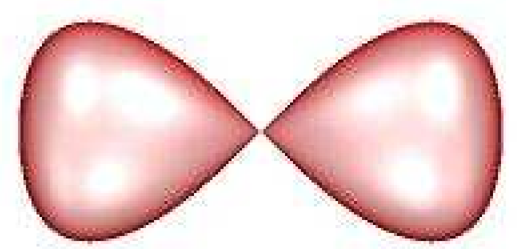

Figure 2.

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

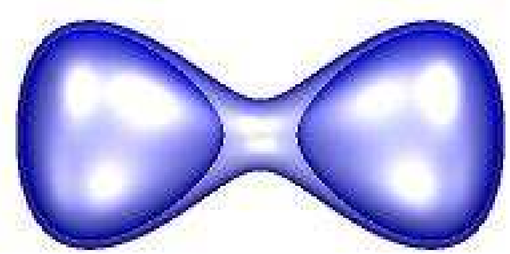

Figure 3.

special deformation such that X_1 is good (no linear change of variable)

- ***complexity***
  Grigori'ev/Vorobjov, Canny, Renegar, Heintz/Roy/Solerno, Basu/Pollack/Roy

  a point in every connected component of an algebraic set: finite number (single exponential) of critical points,
  polynomial system solving : complexity polynomial in the finite number of solutions
  projection on a well chosen line : solutions expressed in terms of roots of a univariate polynomial of degree the number of solutions

  Sampling points of connected components of algebraic sets

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

  quasi-optimal since polynomial in the sign of the output reduction to smooth and bounded: infinitesimals and limits

- infinitesimals ?

  $\mathbb{R}(\varepsilon)$ ordered by: $\varepsilon > 0$, $\varepsilon < r$ for every positive $r \in \mathbb{R}$

  field of algebraic Puiseux series $\mathbb{R}\langle\varepsilon\rangle$, real closure of $\mathbb{R}(\varepsilon)$

  computations in $\mathbb{Q}(\varepsilon)$, answers about $\mathbb{R}\langle\varepsilon\rangle$

  similar to computations over $\mathbb{Q}$, answer about $\mathbb{R}$

- limits ?

  no analysis: constant term of a bounded Puiseux series

- ***Existential theory of the reals***

  a point in every connected component of a semi-algebraic set

  - use infinitesimals

  Proposition 4. *C connected component of a set defined by*

  $$P_1 = \cdots = P_\ell = 0, P_{\ell+1} > 0, \cdots, P_s > 0$$

  exist indices $i_1, \ldots, i_m$ such that

  $$P_1 = \cdots = P_\ell = P_{i_1} - \varepsilon = \cdots P_{i_m} - \varepsilon = 0$$

  has a connected component D contained in C.

- ***complexity singly exponential***

  -not too many intersections: general position worst case (needs a new deformation)

  - for each algebraic set single exponential

  - $s^{k+1}d^{O(k)}$ for finding simultaneously sampling points in connected components of all non empty sign conditions

also Euler-Poincaré characteristic of sign conditions

More general results (see Michel's talk)

- ***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

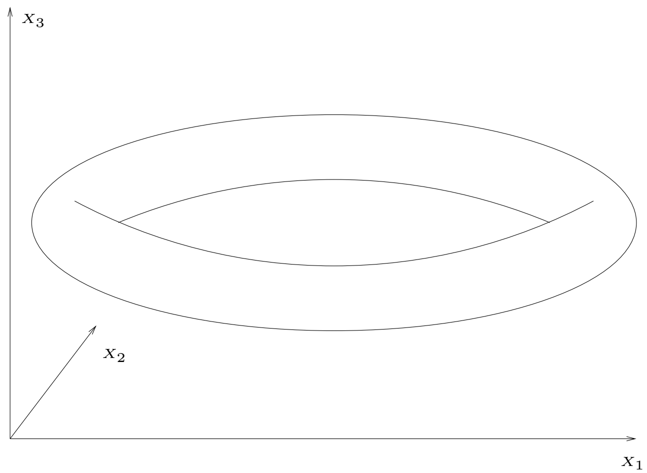

Figure 4. A torus in R^3

perform sampling points parametrically

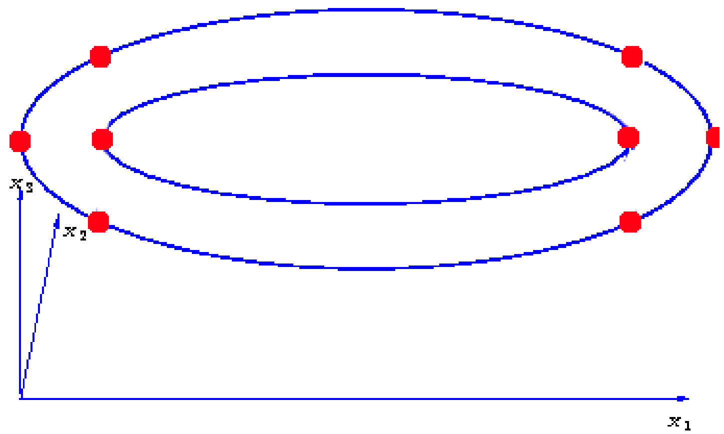

Figure 5. Parametrized sampling points on a torus in $\mathbb{R}^3$

then make a recursion

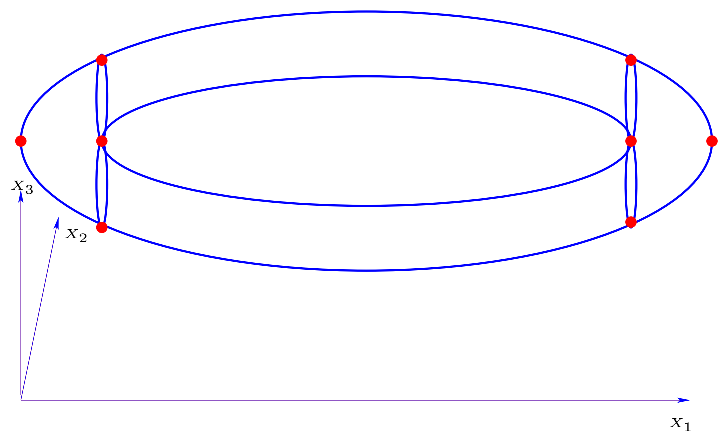

Figure 6. The roadmap of the torus

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

construct connecting path : roadmap through a point, counts connected components

- describe connected components

  parametrized connecting paths

  singly exponential complexity $d^{k^{O(1)}}$

- compute the first Betti number b_1 (Basu/Pollack/R 2004)

  cover by contractible sets using parametrized paths

  cover by closed contractible sets (using Gabrielov-Vorobjov reduction to $\mathcal{P}$-closed)

  use Mayer-Vietoris sequences

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

Some motivation behind trying to improve this result

- number of connected components of an algebraic set $\mathrm{Zer}(Q, R^k)$ is bounded by $O(d)^k$ where $d = \deg(Q)$
- algorithms for testing emptiness and for computing the Euler-Poincaré characteristic with complexity $d^{O(k)}$
- **D'Acunto, Kurdyka** : geodesic diameter of any connected component of a real variety (defined by polynomials of degree d) contained in an unit ball bounded by $d^{O(k)}$, no complexity bound on the description of the path
- many other algorithms in real algebraic geometry use roadmap construction as an intermediate step (i.e. describing connected components, computing higher Betti numbers)

Divide and conquer roadmaps

S basic closed semi-algebraic set

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

- at S^0 itself

- at S^1, union of certain $(k/2)$-dimensional linear spaces intersected with S

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

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)

even if the original situation is sufficiently generic, such 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

over 125 pages

(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, 50 pages

(but uses book Algorithms in Real Algebraic Geometry **Basu, Pollack, R.**, over 600 pages)

Statement

Theorem 5.

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

- # 5 Quadratic case: polynomial in k

  - **Sampling for algebraic sets** Grigor'ev Pasechnik
    s quadratic equations, dimension k
    derivatives of quadratic are linear
    go to $s+k$ variables
    a generic linear combination of s matrices of size $k+s$ is of rank $k-s+1$
    use there single exponential complexity

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

    similar results for optimization in the quadratic case

• 6 Symmetric case: polynomial in k

- **Existential theory of the reals**
  degree principle (Timofte, Riener)

  if $x \in R^k$ is an isolated point of a set defined by symmetric polynomials, its number of distinct coordinates if at most d

  Csq: existential theory of reals $(d\, s\, k)^{O(d)}$

  polynomial in k but exponential in d

  computation of the Euler-Poincaré characteristic (Basu/Riener, 2014) using symmetric Morse theory (see Cordian's talk in next workshop)

- ## 7 Open problems

Stratification (single exponential complexity)?
All Betti numbers (single exponential complexity)?
Extend results in quadratic case

Divide and conquer road map in the semi-algebraic case
Computation of connected components by divide and conquer

Symmetric Morse theory+divide and conquer for symmetric roadmap