Calculs topologiques sur les ensembles semi-algébriques Résultats récents et problèmes ouverts

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

February 6, 2005

Main reference

Algorithms in Real Algebraic Geometry
Saugata Basu
Richard Pollack
Marie-Françoise Roy
Springer-Verlag 2003

1 Introduction

- (1) count the number of real roots of a univariate polynomial, Sturm 1836
- (2)(ETR) decide whether a semi-algebraic set has a real solution Tarski 1939 (undecidable on integers Matiyasevich 1973)
- (3) decide whether a semi-algebraic set is connected cylindrical decomposition techniques : Lojasiewicz, Collins (1960-70)
- (4) stratification: decompose a semi-algebraic set in smooth manifolds of various dimensions by Collins cylindrical algebraic decomposition
- (5) compute the topological invariants (Betti numbers) of semi algebraic sets by CAD

complexity results

- two main methods for topology: cylindrical decomposition and critical point method.

- (2) (ETR) and (3) polynomial in s, d and τ, doubly exponential in k by CAD, singly exponential in k by critical points method (see Basu/Pollack/Roy)
- (4) and (5) polynomial is, d, and τ, doubly exponential k by CAD, singly exponential ? partial results for Betti one (this talk Basu/Pollack/Roy 2004) for the first Betti numbers (Basu 2004)

complexity results (continued, special case of quadratic polynomials)

- based on previous work of Barvinok: number of connected components polynomial in k
- (2') (ETR) in the quadratic case: polynomial in k (Grigor'ev Pasechnik)
- (3') polynomial in k ? open
- (5') top Betti numbers: polynomial in k (Basu 2004)

efficiency

- Fabrice Rouillier (using Jean-Charles Faugère Grobner basis computations)
- Mohab Safey, Philippe Trebuchet
- applications....

2 Cylindrical decomposition

2.1 Subresultants

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

$$\mathrm{SH}_j(P,Q) = \underbrace{\begin{pmatrix} a_p & \cdots & \cdots & \cdots & \cdots & a_0 & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & a_p & \cdots & \cdots & \cdots & \cdots & a_0 \\ & & & b_q & \cdots & \cdots & \cdots & b_0 \\ & & b_q & \cdots & \cdots & \cdots & b_0 & \\ & \iddots & \iddots & \iddots & \iddots & \iddots & & \\ b_q & \cdots & \cdots & \cdots & b_0 & & & \end{pmatrix}}_{p+q-j} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} q-j \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} p-j \end{matrix}$$

- *j-th (signed) subresultant coefficient* $\mathrm{sr}_j(P,Q)$: determinant of the square matrix obtained by taking the $p+q-2j$ first columns of $\mathrm{SR}_j(P,Q)$

important for cylindrical decomposition

Proposition 2.1 $\deg(\gcd(P,Q)) = \ell$ *if and only if*

$$\mathrm{sr}_0(P,Q) = \ldots = \mathrm{sr}_{\ell-1}(P,Q) = 0, \mathrm{sr}_\ell(P,Q) \neq 0$$

2.2 Cylindrical decomposition: doubly exponential complexity

- *decomposition* of a semi-algebraic set: partition in a finite number of semi-algebraic sets
- *cylindrical algebraic decomposition* of $\mathbb{R}^k$: sequence $\mathcal{S}_1, \ldots, \mathcal{S}_k$, where $\mathcal{S}_i$ decomposes $\mathbb{R}^i$ 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 $\xi_{S,j}$

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

  such that the cylinder $S \times \mathbb{R} \subset \mathbb{R}^{i+1}$ 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 $\xi_{S,j+1}$
- subset S of $\mathbb{R}^k$ $\mathcal{P}$ *-invariant*: every polynimial $P \in \mathcal{P}$ has a constant sign (> 0, < 0, or $= 0$) on S.
- *cylindrical algebraic decomposition of* $\mathbb{R}^k$ *adapted to* $\mathcal{P}$:cylindrical algebraic decomposition such that each $S \in \mathcal{S}_k$ is $\mathcal{P}$-invariant

Théorème 2.2 *For every finite* $\mathcal{P} \subset \mathbb{R}[X_1, \ldots, X_k]$*, there exists a cylindrical algebraic decomposition of* $\mathbb{R}^k$ *adapted to* $\mathcal{P}$*.*

- idea: fix the degre of the gcd so that roots dont mix up
- use subresultant coefficient
- induction on number of variables
- elimination phase: iterated projection
- lifting phase : one point by cell
- algorithm very simple, Collins (1973)
- produces a lot of information
- solves (ETR) using sample points in cells
- semi-algebraic set: finite union of connected pieces, semi-algebraically homeomorphic to open cubes

- eliminates quantifiers (saturating first by derivatives)
- a cell is described by the sign condition realized at one of its points
- gives a stratification (saturating first by derivatives and making a linear change of coordinates)
- the closure of a cell is obtained by relaxing the sign conditions defining the cell
- gives connected components
- gives a triangulation
- reduces semi-algebraic algebraic topology to combinatorial algebraic topology
- gives all the Betti numbers
- inconveniences: complexity doubly exponential in the number of variables: eliminating one variable squares the degree.

3 Critical points method :single exponential complexity

- based on Morse, Oleinick, Petrowski, Thom, Milnor
- complexity: Grigori'ev/Vorobjov, Canny, Renegar, Heintz/Roy/Solerno, Basu/Pollack/Roy
- nonsingular bounded compact hypersurface $V = \{M \in \mathbb{R}^n \ , \ H(M) = 0\}$, i.e. such that

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

  does not vanish on the zeros of H in C^n.
- critical points of the projection on the X_1 axis meet all the connected components of V
- except special cases, $d(d-1)^{k-1}$ such critical points (Bezout),

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

3.1 At least a point in every connected component of an algebraic set

- reduction to smooth and bounded, with a finite number of critical points in the X_1 direction: infinitesimals and limits
- algebraic Puiseux series: computations with coefficients in $\mathbb{Z}[\varepsilon]$, be careful to bound degrees in ε during computations
- a point in every connected component of an algebraic set: finite number (single exponential) of critical points, which can be projected on a line
- RUR rational univariate representation (F. Rouillier)
- univariate techniques (Sturm, subresultants)
- complexity single exponential (polynomial in the number of critical points which is singly exponential)

Some details en the bounded algebraic case.
Suppose that

- $Q(x) \geq 0$ for every $x \in \mathbb{R}^k$,
- $\mathrm{Z}(Q, \mathbb{R}^k) \subset B(0, 1/c)$ for some $c \leq 1, c \in \mathrm{D}$,
- $d_1 \geq d_2 \cdots \geq d_k$,
- $\deg(Q) \leq d_1$, $\mathrm{tdeg}_{X_i}(Q) \leq d_i$ (maximal total degree of the monomials in Q containing the variable X_i), for $i = 2, \ldots, k$,
- $\bar{d}_i$ be an even number $> d_i, i = 1, \ldots, k$, and $\bar{d} = (\bar{d}_1, \ldots, \bar{d}_k)$.
- ζ be a variable and $\mathbb{R}\langle\zeta\rangle$ be the field of algebraic Puiseux series in ζ with coefficients in $\mathbb{R}$.

$$\begin{aligned} G_k(\bar{d}, c) &= c^{\bar{d}_1}(X_1^{\bar{d}_1} + \cdots + X_k^{\bar{d}_k} + X_2^2 + \cdots + X_k^2) - (2k-1), \\ \mathrm{Def}(Q, \bar{d}, c, \zeta) &= \zeta G_k(\bar{d}, c) + (1-\zeta)Q. \end{aligned}$$

Take $\lim_\zeta$ corresponds to take $\zeta = 0$ (with some precautions).

Proposition 3.1 *The algebraic set* $\mathrm{Z}((Q, \bar{d}, c, \zeta), \mathbb{R}\langle\zeta\rangle^k)$ *is a nonsingular algebraic hypersurface bounded over* $\mathbb{R}$.

$$\lim_\zeta(\mathrm{Z}((Q, \bar{d}, c, \zeta), \mathbb{R}\langle\zeta\rangle^k)) = \mathrm{Z}(Q, \mathbb{R}^k).$$

Moreover $\mathrm{Z}((Q, \bar{d}, c, \zeta), \mathbb{R}\langle\zeta\rangle^k) \subset B(0, 1/c)$ *and* X_1 *has a finite number of critical points on* $\mathrm{Z}((Q, \bar{d}, c, \zeta), \mathbb{R}\langle\zeta\rangle^k)$.

X_1-pseudo-critical points are limits of X_1-critical points on $\mathrm{Z}((Q, \bar{d}, c, \zeta), \mathbb{R}\langle\zeta\rangle^k)$. They meet every connected componnent.

3.2 ETR: existential theory of the reals

- a point in every connected component of a semi-algebraic set: uses a new infinitesimal

Proposition 3.2 *C connected component of a set defined by $P_1 = \cdots = P_\ell = 0, P_{\ell+1} > 0, \cdots, P_s > 0$. There exist indices $i_1, \ldots, i_m$ and ε sufficiently small 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.*

- maybe too many non empty intersections
- trick to reach general position: again infinitesimals
- complexity single exponential $s^{k+1}d^{O(k)}$.

3.3 Compute connectivity

- perform (ETR) parametrically and then make a recursion: roadmap construction
- roadmap : dimension at most one, connected in each connected component, meets each connected component of each fiber along the X_1-axis
- construct connecting paths
- counts connected components: b_0 Betti number (dimension of homology)
- complexity $s^{k+1}d^{O(k^2)}$

3.4 Use parametrized paths

- parametrized connecting paths
- cover by contractible sets (parametrized paths)
- describe connected components: unions of points parametrically connected to points in the same connected components
- cover by closed contractible sets (construction of Gabrielov Vorobjov)
- use spectral sequences (slightly more advanced algebraic topology)
- computation of b_1 using Mayer-Vietoris sequences (Basu/Pollack/R 2004)
- computation of the first Betti numbers (Basu 2004): more spectral sequences

$A_1, \ldots, A_n$sub-complexes of a finite simplicial complex A such that $A = A_1 \cup \cdots \cup A_n$, $A_{i_0,\ldots,i_p}$ the sub-complex $A_{i_0} \cap \cdots \cap A_{i_p}$.

$C^i(A)$ the $\mathbb{Q}$-vector space of i co-chains of A, and $C^\bullet(A)$, the complex

$$\cdots \to C^{q-1}(A) \xrightarrow{d} C^q(A) \xrightarrow{d} C^{q+1}(A) \to \cdots$$

where $d : C^q(A) \to C^{q+1}(A)$ are the usual co-boundary homomorphisms.

The generalized Mayer-Vietoris sequence is the following exact sequence

$$0 \longrightarrow C^\bullet(A) \xrightarrow{r} \prod_{i_0} C^\bullet(A_{i_0}) \xrightarrow{\delta_1} \prod_{i_0<i_1} C^\bullet(A_{i_0,i_1})$$

$$\cdots \xrightarrow{\delta_{p-1}} \prod_{i_0<\cdots<i_p} C^\bullet(A_{i_0,\ldots,i_p}) \xrightarrow{\delta_p} \prod_{i_0<\cdots<i_{p+1}} C^\bullet(A_{i_0,\ldots,i_{p+1}}) \cdots$$

where r is induced by restriction and the connecting homomorphisms δ are defined by

$$(\delta\omega)_{i_0,\ldots,i_{p+1}}(s) = \sum_{0 \le i \le p+1} (-1)^i \omega_{i_0,\ldots,\hat{i_i},\ldots,i_{p+1}}(s),$$

($\hat{}$ denotes omission). Exactness is classical.

Consider the following complex (which is no more exact)

$$0 \longrightarrow \prod_{i_0} C^\bullet(A_{i_0}) \xrightarrow{\delta_1} \prod_{i_0<i_1} C^\bullet(A_{i_0,i_1}) \xrightarrow{\delta_2} \prod_{i_0<\cdots<i_p} C^\bullet(A_{i_0,\ldots,i_2}) \cdots$$

$$\cdots \xrightarrow{\delta_{p-1}} \prod_{i_0<\cdots<i_p} C^\bullet(A_{i_0,\ldots,i_p}) \xrightarrow{\delta_p} \prod_{i_0<\cdots<i_{p+1}} C^\bullet(A_{i_0,\ldots,i_{p+1}}) \cdots$$

and the induced cohomology complex.

Proposition 3.3 *Let $A_1, \ldots, A_n$ be sub-complexes of a finite simplicial complex A such that $A = A_1 \cup \cdots \cup A_n$ and each A_i is contractible. Then,* $b_1(A) = \dim((\delta_2)) - \dim((\delta_1))$*, with*

$$\prod_i H^0(A_i) \xrightarrow{\delta_1} \prod_{i<j} H^0(A_{i,j}) \xrightarrow{\delta_2} \prod_{i<j<\ell} H^0(A_{i,j,\ell})$$

in other words three by three intersections suffice to compute b_1 when the cover is closed and contractible.

Proof: consider the following bi-graded double complex $\mathcal{M}^{p,q}$, with a total differential $D = \delta + (-1)^p d$, where

$$\mathcal{M}^{p,q} = \prod_{i_0,\ldots,i_p} C^q(A_{i_0,\ldots,i_p}).$$

$$
\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \uparrow d & & \uparrow d & & \uparrow d \\
0 & \longrightarrow & \prod_{i_0} C^3(A_{i_0}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1} C^3(A_{i_0,i_1}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1<i_2} C^3(A_{i_0,i_1,i_2}) & \longrightarrow \\
 & & \uparrow d & & \uparrow d & & \uparrow d \\
0 & \longrightarrow & \prod_{i_0} C^2(A_{i_0}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1} C^2(A_{i_0,i_1}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1<i_2} C^2(A_{i_0,i_1,i_2}) & \longrightarrow \\
 & & \uparrow d & & \uparrow d & & \uparrow d \\
0 & \longrightarrow & \prod_{i_0} C^1(A_{i_0}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1} C^1(A_{i_0,i_1}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1<i_2} C^1(A_{i_0,i_1,i_2}) & \longrightarrow \\
 & & \uparrow d & & \uparrow d & & \uparrow d \\
0 & \longrightarrow & \prod_{i_0} C^0(A_{i_0}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1} C^0(A_{i_0,i_1}) & \stackrel{\delta}{\longrightarrow} & \prod_{i_0<i_1<i_2} C^0(A_{i_0,i_1,i_2}) & \longrightarrow \\
 & & \uparrow d & & \uparrow d & & \uparrow d \\
 & & 0 & & 0 & & 0
\end{array}
$$

consider two spectral sequences (corresponding to taking horizontal or vertical filtrations respectively) ....

one of them degenerates ....

3.5 Practical computations of b_1

- Basu and Kettner (submitted to SOCG)
- use spectral sequences and consider intersections three by three
- now apply CAD (rather than critical point method)
- able to compute the topology of the union of 10 ellipsoids in three space
- classical CAD fails

3.6 Quadratic case: polynomial in k

- quadratic case, ℓ quadratic equations, dimension k
- derivatives of quadratic are linear
- go to $\ell + k$ variables
- a generic linear combination of ℓ matrices is of rank $k - \ell + 1$
- go to $2\ell - 1$ variables using linear algebra
- use there single exponential complexity

quadratic case (continued)

- few top Betti numbers (Saugata Basu)
- use Agrachev geometric results
- *Open problems*
- All Betti numbers (single exponential complexity)?
- Stratification (single exponential complexity)?
- Complexity in the quadratic case: besides ETR, global optimization and top Betti numbers, what is polynomial-time complexity ? Counting connected components ?