ALGORITHMIC SEMI-ALGEBRAIC GEOMETRY AND TOPOLOGY : LECTURE 2

SAUGATA BASU

Abstract. In this lecture we discuss the main algorithmic problems in semi-algebraic geometry and topology. We also discuss some of the basic tools used in the currently most efficient algorithms for solving these problems.

Contents

1. Main Algorithmic Problems

Algorithmic problems in semi-algebraic geometry typically consist of the following. We are given as input a finite family, $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$, as well as a formula defining a $\mathcal{P}$-semi-algebraic set S. The task is to decide whether certain geometric and topological properties hold for S, and in some cases also computing certain topological invariants of S. Some of the most basic problems include the following.

Given a $\mathcal{P}$-semi-algebraic set $S \subset \mathrm{R}^k$:

(1) decide whether it is empty or not,
(2) given two points $x, y \in S$, decide if they are in the same connected component of S and if so output a semi-algebraic path in S joining them,
(3) compute semi-algebraic descriptions of the connected components of S,

2000 MATHEMATICS SUBJECT CLASSIFICATION PRIMARY 14P10, 14P25; SECONDARY 68W30

(4) compute semi-algebraic descriptions of the projection of S onto some linear subspace of R^k (this problem is also known as the quantifier elimination problem for the first order theory of the reals and many other problems can be posed as special cases of this very general problem).

At a deeper level we have problems of a more topological flavor, such as:

(5) compute the cohomology groups of S, its Betti numbers, its Euler-Poincaré characteristic etc.,
(6) compute a semi-algebraic triangulation of S as well as
(7) compute a decomposition of S into semi-algebraic smooth pieces of various dimensions which fit together nicely (a Whitney-regular stratification).

The complexity of an algorithm for solving any of the above problems is measured in terms of the following three parameters:

- the number of polynomials, $s = \#\mathcal{P}$,
- the maximum degree, $d = \max_{P\in\mathcal{P}} \deg(P)$, and
- the number of variables, k.

Definition 1.1 (Complexity)**.** A typical input to the algorithms considered in this survey will be a set of polynomials with coefficients in an ordered ring D (which can be taken to be the ring generated by the coeffcients of the input polynomials). By complexity of an algorithm we will mean the number of arithmetic operations (including comparisons) performed by the algorithm in the ring D. In case the input polynomials have integer coefficients with bounded bit-size, then we will often give the bit-complexity, which is the number of bit operations performed by the algorithm. We refer the reader to [11, Chapter 8] for a full discussion about the various measures of complexity.

Even though the goal is always to design algorithms with the best possible complexity in terms of all the parameters s, d, k, the relative importance of the parameters is very much application dependent. For instance, in applications in *computational geometry* it is the *combinatorial* complexity (that is the dependence on s) that is of paramount importance, the *algebraic* part depending on d, as well as the dimension k, are assumed to be bounded by constants. On the other hand in algorithmic real algebraic geometry, and in applications in complexity theory, the algebraic part depending on d is considered to be equally important.

1.1. **Brief History.** Even though there exist algorithms for solving all the above problems, the main research problem is to design *efficient* algorithms for solving them. The complexity of the first decision procedure given by Tarski [27] to solve Problems 1 and 4 listed in Section 1 is not elementary recursive, which implies that the running time cannot be bounded by a function of the size of the input which is a fixed tower of exponents. The first algorithm with a significantly better worst-case time bound was given by

Collins [16] in 1976. His algorithm had a worst case running time doubly exponential in the number of variables. Collins' method is to obtain a cylindrical algebraic decomposition of the given semi-algebraic set (see Section 3.1 below for definition). Once this decomposition is computed most topological questions about semi-algebraic sets such as those listed in Section 1 can be answered. However, this method involves cascading projections which involve squaring of the degrees at each step resulting in a complexity which is doubly exponential in the number of variables.

Most of the recent work in algorithmic semi-algebraic geometry has focused on obtaining *single exponential time* algorithms – that is algorithms with complexity of the order of $(sd)^{k^{O(1)}}$ rather than $(sd)^{2^k}$. An important motivating reason behind the search for such algorithms, is the following theorem due to Gabrielov and Vorobjov [17] (see [24, 28, 23, 2], as well as the survey article [9], for work leading up to this result).

2. Recent Algorithmic Results

In this section we list some of the recent progress on the algorithmic problem of determining the Betti numbers of semi-algebraic sets.

- In [10], an algorithm with single exponential complexity is given for computing the first Betti number of semi-algebraic sets.
- The above result is generalized in [4], where a single exponential time algorithm is given for computing the first ℓ Betti numbers of semi-algebraic sets, where ℓ is allowed to be any constant. More precisely, an algorithm is described that takes as input a description of a $\mathcal{P}$-semi-algebraic set $S \subset \mathrm{R}^k$, and outputs the first $\ell+1$ Betti numbers of S, $b_0(S), \ldots, b_\ell(S)$. The complexity of the algorithm is $(sd)^{k^{O(\ell)}}$, where $s = \#(\mathcal{P})$ and $d = \max_{P\in\mathcal{P}} \deg(P)$, which is single exponential in k for ℓ any constant.
- In [5], a *polynomial* time algorithm is given for computing a constant number of the top Betti numbers of semi-algebraic sets defined by quadratic inequalities. If the number of inequalities is fixed then the algorithm computes all the Betti numbers in polynomial time. More precisely, an algorithm is described which takes as input a semi-algebraic set, S, defined by $P_1 \geq 0, \ldots, P_s \geq 0$, where each $P_i \in \mathrm{R}[X_1, \ldots, X_k]$ has degree ≤ 2, and computes the top ℓ Betti numbers of S, $b_{k-1}(S), \ldots, b_{k-\ell}(S)$, in polynomial time. The complexity of the algorithm is $\sum_{i=0}^{\ell+2} \binom{s}{i} k^{2^{O(\min(\ell,s))}}$. For fixed ℓ, the complexity of the algorithm can be expressed as $s^{\ell+2}k^{2^{O(\ell)}}$, which is polynomial in the input parameters s and k. For fixed s, we obtain by letting $\ell = k$, an algorithm for computing all the Betti numbers of S whose complexity is $k^{2^{O(s)}}$.
- In [12], a polynomial time algorithm is obtained for computing a constant number of the lowest Betti numbers of semi-algebraic sets defined as the projection of semi-algebraic sets defined by few by

quadratic inequalities. More precisely, let $S \subset \mathbb{R}^{k+m}$ be a closed and bounded semi-algebraic set defined by $P_1 \geq 0, \ldots, P_\ell \geq 0$, where $P_i \in \mathbb{R}[X_1, \ldots, X_k, Y_1, \ldots, Y_m]$, and $\deg(P_i) \leq 2, 1 \leq i \leq \ell$. Let π denote the standard projection from $\mathbb{R}^{k+m}$ onto $\mathbb{R}^m$. An algorithm is described for computing the the first q Betti numbers of $\pi(S)$, whose complexity is $(k+m)^{2^{O((q+1)\ell)}}$. For fixed q and ℓ, the bound is polynomial in $k+m$.

- The complexity estimates for all the algorithms mentioned above included both the combinatorial and algebraic parameters. As mentioned before, in applications in computational geometry the algebraic part of the complexity is treated as a constant. In this context, an interesting question is how efficiently can one compute the Betti numbers of an arrangement of n closed and bounded semi-algebraic sets, $S_1, \ldots, S_n \subset \mathrm{R}^k$, where each S_i is described using a constant number of polynomials with degrees bounded by a constant. Such arrangements are ubiquitous in computational geometry (see [1]). A naive approach using triangulations would entail a complexity of $O(n^{2^k})$. This problem is considered in [3] where an algorithm is described for computing ℓ-th Betti number, $b_\ell(\bigcup_{i=1}^{n} S_i)$, $0 \leq \ell \leq k-1$, using $O(n^{\ell+2})$ algebraic operations. Additionally, one has to perform linear algebra on integer matrices of size bounded by $O(n^{\ell+2})$. All previous algorithms for computing the Betti numbers of arrangements triangulated the whole arrangement giving rise to a complex of size $O(n^{2^k})$ in the worst case. Thus, the complexity of computing the Betti numbers (other than the zero-th one) for these algorithms was $O(n^{2^k})$. This is the first algorithm for computing $b_\ell(\bigcup_{i=1}^{n} S_i)$ that does not rely on such a global triangulation, and has a graded complexity which depends on ℓ.

3. Algorithmic Preliminaries

In this section we give a brief overview of the basic algorithmic constructions from semi-algebraic geometry that play a role in the design of more sophisticated algorithms. These include cylindrical algebraic decomposition (Section 3.1), the critical point method (Section 3.2), and the construction of roadmaps of semi-algebraic sets (Section 3.3).

3.1. **Cylindrical Algebraic Decomposition.**

As mentioned earlier one fundamental technique for computing topological invariants of semi-algebraic sets is through *Cylindrical Algebraic Decomposition*. Even though the mathematical ideas behind cylindrical algebraic decomposition were known before (see for example [22]), Collins [16] was the first to apply cylindrical

algebraic decomposition in the setting of algorithmic semi-algebraic geometry. Schwartz and Sharir [26] realized its importance in trying to solve the motion planning problem in robotics, as well as computing topological properties of semi-algebraic sets. Variants of the basic cylindrical algebraic decomposition have also been used in several papers in computational geometry. For instance in the paper by Chazelle et al. [14], a truncated version of cylindrical decomposition is described whose combinatorial (though not the algebraic) complexity is single exponential. This result has found several applications in discrete and computational geometry (see for instance [15]).

Definition 3.1 (Cylindrical Algebraic Decomposition)**.** A cylindrical algebraic decomposition of R^k is a sequence $\mathcal{S}_1, \ldots, \mathcal{S}_k$ where, for each $1 \leq i \leq k$, $\mathcal{S}_i$ is a finite partition of R^i into semi-algebraic subsets, called the cells of level i, which satisfy the following properties:

- Each cell $S \in \mathcal{S}_1$ is either a point or an open interval.
- For every $1 \leq i < k$ and every $S \in \mathcal{S}_i$, there are finitely many continuous semi-algebraic functions

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

such that the cylinder $S \times \mathrm{R} \subset \mathrm{R}^{i+1}$ is the disjoint union of cells of $\mathcal{S}_{i+1}$ which are:
  - either the graph of one of the functions $\xi_{S,j}$, for $j = 1, \ldots, \ell_S$:

$$\{(x', x_{j+1}) \in S \times \mathrm{R} \mid x_{j+1} = \xi_{S,j}(x')\} ,$$

  - or a band of the cylinder bounded from below and from above by the graphs of the functions $\xi_{S,j}$ and $\xi_{S,j+1}$, for $j = 0, \ldots, \ell_S$, where we take $\xi_{S,0} = -\infty$ and $\xi_{i,\ell_S+1} = +\infty$:

$$\{(x', x_{j+1}) \in S \times \mathrm{R} \mid \xi_{S,j}(x') < x_{j+1} < \xi_{S,j+1}(x')\} .$$

We note that every cell of a cylindrical algebraic decomposition is semi-algebraically homeomorphic to an open i-cube $(0,1)^i$ (by convention, $(0,1)^0$ is a point).

A cylindrical algebraic decomposition adapted to a finite family of semi-algebraic sets $T_1, \ldots, T_\ell$ is a cylindrical algebraic decomposition of R^k such that every T_i is a union of cells. (see Figure 1).

Definition 3.2. Given a finite set $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$, a subset S of R^k is is $\mathcal{P}$-invariant if every polynomial $P \in \mathcal{P}$ has a constant sign (> 0, < 0, or $= 0$) on S. A cylindrical algebraic decomposition of R^k adapted to $\mathcal{P}$ is a cylindrical algebraic decomposition for which each cell $C \in \mathcal{S}_k$ is $\mathcal{P}$-invariant. It is clear that if S is $\mathcal{P}$-semi-algebraic, a cylindrical algebraic decomposition adapted to $\mathcal{P}$ is a cylindrical algebraic decomposition adapted to S.

One important result which underlies most algorithmic applications of cylindrical algebraic decomposition is the following (see [11, Chapter 11] for an easily accessible exposition).

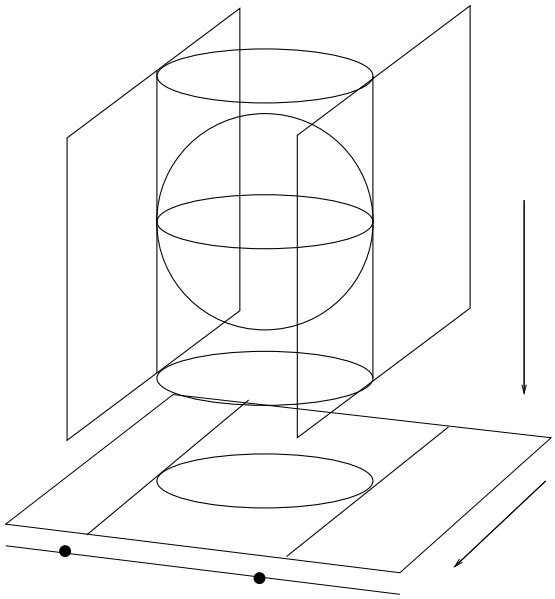

FIGURE 1. Example of cylindrical algebraic decomposition of R^3 adapted to a sphere.

Theorem 3.3. *For every finite set $\mathcal{P}$ of polynomials in $\mathrm{R}[X_1, \ldots, X_k]$, there is a cylindrical decomposition of R^k adapted to $\mathcal{P}$. Moreover, such a decomposition can be computed in time $(sd)^{2^{O(k)}}$, where $s = \#\mathcal{P}$ and $d = \max_{P \in \mathcal{P}} \deg(P)$.*

The cylindrical algebraic decomposition obtained in Theorem 3.3 can in fact be refined to give a semi-algebraic triangulation of any given semi-algebraic set within the same complexity bound.

Recall that

Definition 3.4 (Semi-algebraic Triangulation)**.** A semi-algebraic triangulation of a semi-algebraic set S is a simplicial complex K together with a semi-algebraic homeomorphism from $|K|$ to S.

The following theorem states that such triangulations can be computed for any closed and bounded semi-algebraic set with double exponential complexity.

Theorem 3.5. *Let $S \subset \mathrm{R}^k$ be a closed and bounded semi-algebraic set, and let $S_1, \ldots, S_q$ be semi-algebraic subsets of S. There exists a simplicial complex K in R^k and a semi-algebraic homeomorphism $h : |K| \to S$ such that each S_j is the union of images by h of open simplices of K. Moreover, the vertices of K can be chosen with rational coordinates.*

Moreover, if S and each S_i are $\mathcal{P}$-semi-algebraic sets, then the semi-algebraic triangulation (K, h) can be computed in time $(sd)^{2^{O(k)}}$, where $s = \#\mathcal{P}$ and $d = \max_{P\in\mathcal{P}} \deg(P)$.

3.2. **The Critical Point Method.** As mentioned earlier, all algorithms using cylindrical algebraic decomposition have double exponential complexity. Algorithms with single exponential complexity for solving problems in semi-algebraic geometry are mostly based on the *critical point method*. This method was pioneered by several researchers including Grigoriev and Vorobjov [20, 19], Renegar [25], Canny [13], Heintz, Roy and Solernò [21], Basu, Pollack and Roy [6] amongst others. In simple terms, the critical point method is nothing but a method for finding at least one point in every semi-algebraically connected component of an algebraic set. It can be shown that for a bounded nonsingular algebraic hyper-surface, it is possible to change coordinates so that its projection to the X_1-axis has a finite number of non-degenerate critical points. These points provide at least one point in every semi-algebraically connected component of the bounded nonsingular algebraic hyper-surface. Unfortunately this is not very useful in algorithms since it provides no method for performing this linear change of variables. Moreover when we deal with the case of a general algebraic set, which may be unbounded or singular, this method no longer works.

In order to reduce the general case to the case of bounded nonsingular algebraic sets, we use an important technique in algorithmic semi-algebraic geometry – namely, perturbation of a given real algebraic set in R^k using one or more infinitesimals. The perturbed variety is then defined over a non-archimedean real closed extension of the ground field – namely the field of algebraic Puiseux series in the infinitesimal elements with coefficients in R.

Since the theory behind such extensions might be unfamiliar to some readers, we introduce here the necessary algebraic background referring the reader to [11, Section 2.6] for full detail and proofs.

3.2.1. *Infinitesimals and the Field of Algebraic Puiseux Series.*

Definition 3.6 (Puiseux series)**.** A *Puiseux series* in ε with coefficients in R is a series of the form

$$\overline{a} = \sum_{i\geq k} a_i \varepsilon^{i/q}, \tag{3.1}$$

with $k \in \mathbb{Z}$, $i \in \mathbb{Z}$, $a_i \in \mathrm{R}$, q a positive integer.

It is a straightforward exercise to verify that the field of all Puiseux series in ε with coefficients in R is an ordered field. The order extends the order of R, and ε is an infinitesimally small and positive, i.e. is positive and smaller than any positive $r \in \mathrm{R}$.

NOTATION 1. The field of Pusisex series in ε with coefficients in R contains as a subfield, the field of Puiseux series which are algebraic over $\mathrm{R}[\varepsilon]$. We

denote by $\mathrm{R}\langle\varepsilon\rangle$ the field of algebraic Puiseux series in ζ with coefficients in R.

The following theorem is classical (see for example [11, Section 2.6] for a proof).

Theorem 3.7. *The field $\mathrm{R}\langle\varepsilon\rangle$ is real closed.*

Definition 3.8 (The $\lim_\varepsilon$ map)**.** When $a \in \mathrm{R}\langle\varepsilon\rangle$ is bounded by an element of R, $\lim_\varepsilon(a)$ is the constant term of a, obtained by substituting 0 for ε in a.

Example 3.9. A typical example of the application of the lim map can be seen in Figures 2 and 3 below. The first picture depicts the algebraic set $\mathrm{Z}(Q, \mathrm{R}^3)$, while the second depicts the algebraic set $\mathrm{Z}(\bar{Q}, \mathrm{R}\langle\zeta\rangle^3)$ (where we substituted a very small positive number for ζ in order to able display this set), where Q and $\bar{Q}$ are defined by Eqn. (3.4) and Eqn. (3.3) resp. The algebraic sets $\mathrm{Z}(Q, \mathrm{R}^3)$ and $\mathrm{Z}(\bar{Q}, \mathrm{R}\langle\zeta\rangle^3)$ are related by

$$\mathrm{Z}(Q, \mathrm{R}^3) = \lim_{\zeta} \mathrm{Z}(\bar{Q}, \mathrm{R}\langle\zeta\rangle^3).$$

Since we will often consider the semi-algebraic sets defined by the same formula, but over different real closed extensions of the ground field, the following notation is useful.

NOTATION 2. Let R' be a real closed field containing R. Given a semi-algebraic set S in R^k, the *extension* of S to R', denoted $\mathrm{Ext}(S, \mathrm{R}')$, is the semi-algebraic subset of R'^k defined by the same quantifier free formula that defines S.

The set $\mathrm{Ext}(S, \mathrm{R}')$ is well defined (i.e. it only depends on the set S and not on the quantifier free formula chosen to describe it). This is an easy consequence of the transfer principle.

We now return to the discussion of the critical point method. In order for the critical point method to work for all algebraic sets, we associate to a possibly unbounded algebraic set $Z \subset \mathrm{R}^k$ a bounded algebraic set $Z' \subset \mathrm{R}\langle\varepsilon\rangle^{k+1}$, whose semi-algebraically connected components are closely related to those of Z.

Let $Z = \mathrm{Z}(Q, \mathrm{R}^k)$ and consider

$$Z' = \mathrm{Z}(Q^2 + (\varepsilon^2(X_1^2 + \ldots + X_{k+1}^2) - 1)^2, \mathrm{R}\langle\varepsilon\rangle^{k+1}).$$

The set Z' is the intersection of the sphere S_ε^k of center 0 and radius $\dfrac{1}{\varepsilon}$ with a cylinder based on the extension of Z to $\mathrm{R}\langle\varepsilon\rangle$. The intersection of Z' with the hyperplane $X_{k+1} = 0$ is the intersection of Z with the sphere S_ε^{k-1} of center 0 and radius $\dfrac{1}{\varepsilon}$. Denote by π the projection from $\mathrm{R}\langle\varepsilon\rangle^{k+1}$ to $\mathrm{R}\langle\varepsilon\rangle^k$.

The following proposition which appears in [11] then relates the connected component of Z with those of Z' and this allows us to reduce the problem

of finding points on every connected component of a possibly unbounded algebraic set to the same problem on bounded algebraic sets.

Proposition 3.10. *Let N be a finite number of points meeting every semi-algebraically connected component of Z'. Then $\pi(N)$ meets every semi-algebraically connected component of the extension* $\mathrm{Ext}(Z', \mathrm{R}\langle\varepsilon\rangle)$ *of Z' to* $\mathrm{R}\langle\varepsilon\rangle$.

We obtain immediately using Proposition 3.10 a method for finding a point in every connected component of an algebraic set. Note that these points have coordinates in the extension $\mathrm{R}\langle\varepsilon\rangle$ rather than in the real closed field R we started with. However, the extension from R to $\mathrm{R}\langle\varepsilon\rangle$ preserves semi-algebraically connected components.

For dealing with possibly singular algebraic sets we define X_1-pseudo-critical points of $\mathrm{Z}(Q, \mathrm{R}^k)$ when $\mathrm{Z}(Q, \mathrm{R}^k)$ is a bounded algebraic set. These pseudo-critical points are a finite set of points meeting every semi-algebraically connected component of $\mathrm{Z}(Q, \mathrm{R}^k)$. They are the limits of the critical points of the projection to the X_1 coordinate of a bounded nonsingular algebraic hyper-surface defined by a particular infinitesimal perturbation, $\bar{Q}$, of the polynomial Q. Moreover, the equations defining the critical points of the projection on the X_1 coordinate on the perturbed algebraic set have a very special algebraic structure (they form a Gröbner basis [11, Section 12.1]), which makes possible efficient computation of these pseudo-critical values and points. We refer the reader to [11, Chapter 12] for a full exposition including the definition and basic properties of Gröbner basis.

The deformation $\bar{Q}$ of Q is defined as follows. Suppose that $\mathrm{Z}(Q, \mathrm{R}^k)$ is contained in the ball of center 0 and radius $1/c$. Let $\bar{d}$ be an even integer bigger than the degree d of Q and let

$$G_k(\bar{d}, c) = c^{\bar{d}}(X_1^{\bar{d}} + \cdots + X_k^{\bar{d}} + X_2^2 + \cdots + X_k^2) - (2k-1), \tag{3.2}$$

$$\bar{Q} = \zeta G_k(\bar{d}, c) + (1-\zeta)Q. \tag{3.3}$$

The algebraic set $\mathrm{Z}(\bar{Q}, \mathrm{R}\langle\zeta\rangle^k)$ is a bounded and non-singular hyper-surface lying infinitesimally close to $\mathrm{Z}(Q, \mathrm{R}^k)$ and the critical points of the projection map onto the X_1 co-ordinate restricted to $\mathrm{Z}(\bar{Q}, \mathrm{R}\langle\zeta\rangle^k)$ form a finite set of points. We take the images of these points under $\lim_\zeta$ (cf. Definition 3.8) and we call the points obtained in this manner the X_1-pseudo-critical points of $\mathrm{Z}(Q, \mathrm{R}^k)$. Their projections on the X_1-axis are called pseudo-critical values.

Example 3.11. We illustrate the perturbation mentioned above by a concrete example. Let $k = 3$ and $Q \in \mathrm{R}[X_1, X_2, X_3]$ be defined by

$$Q = X_2^2 - X_1^2 + X_1^4 + X_2^4 + X_3^4. \tag{3.4}$$

Then, $\mathrm{Z}(Q, \mathrm{R}^3)$ is a bounded algebraic subset of R^3 shown below in Figure 2. Notice that $\mathrm{Z}(Q, \mathrm{R}^3)$ has a singularity at the origin. The surface $\mathrm{Z}(\bar{Q}, \mathrm{R}^3)$ with a small positive real number substituted for ζ is shown in Figure 3.

Notice that this surface is non-singular, but has a different homotopy type than $\mathrm{Z}(Q, \mathrm{R}^3)$ (it has three connected components compared to only one of $\mathrm{Z}(Q, \mathrm{R}^3)$). However, the semi-algebraic set bounded by $\mathrm{Z}(\bar{Q}, \mathrm{R}^3)$ (i.e. the part inside the larger component but outside the smaller ones) is homotopy equivalent to $\mathrm{Z}(Q, \mathrm{R}^3)$.

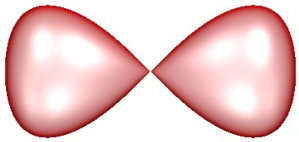

FIGURE 2. The algebraic set $\mathrm{Z}(Q, \mathrm{R}^3)$.

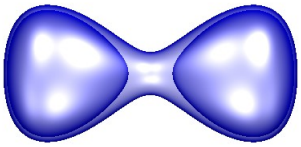

FIGURE 3. The algebraic set $\mathrm{Z}(\bar{Q}, \mathrm{R}^3)$.

By computing algebraic representations (see [11, Section 12.4] for the precise definition of such a representation) of the pseudo-critical points one obtains for any given algebraic set a finite set of points guaranteed to meet every connected component of this algebraic set. Using some more arguments from real algebraic geometry one can also reduce the problem of computing a finite set of points guaranteed to meet every connected component of the realization of every realizable sign condition on a given family of polynomials to finding points on certain algebraic sets defined by the input polynomials (or infinitesimal perturbations of these polynomials). The details of this argument can be found in [11, Proposition 13.2].

The following theorem which is the best result of this kind appears in [7].

Theorem 3.12. [7] *Let $\mathrm{Z}(Q, \mathrm{R}^k)$ be an algebraic set of real dimension k', where Q is a polynomial in $\mathrm{R}[X_1, \ldots, X_k]$ of degree at most d, and let $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$ be a set of s polynomials with each $P \in \mathcal{P}$ also of degree*

at most d. Let D *be the ring generated by the coefficients of Q and the polynomials in $\mathcal{P}$. There is an algorithm which computes a set of points meeting every semi-algebraically connected component of every realizable sign condition on $\mathcal{P}$ over $\mathrm{Z}(Q, \mathrm{R}\langle\varepsilon,\delta\rangle^k)$. The algorithm has complexity*

$$(k'(k-k')+1)\sum_{j\leq k'} 4^j \binom{s}{j} d^{O(k)} = s^{k'} d^{O(k)}$$

in D*. There is also an algorithm providing the list of signs of all the polynomials of $\mathcal{P}$ at each of these points with complexity*

$$(k'(k-k')+1)s\sum_{j\leq k'} 4^j \binom{s}{j} d^{O(k)} = s^{k'+1} d^{O(k)}$$

in D*.*

Notice that the combinatorial complexity of the algorithm in Theorem 3.12 depends on the dimension of the variety rather than that of the ambient space. Since we are mostly concentrating on single exponential algorithms in this part of the survey, we do not emphasize this aspect too much.

Notice that the combinatorial complexity of the algorithm in Theorem 3.12 depends on the dimension of the variety rather than that of the ambient space. Since we are mostly concentrating on single exponential algorithms in this part of the survey, we do not emphasize this aspect too much.

3.3. **Roadmaps.** Theorem 3.12 gives a single exponential time algorithm for testing if a given semi-algebraic set is empty or not. However, it gives no way of testing if any two sample points computed by it belong to the same connected component of the given semi-algebraic set, even though the set of sample points is guaranteed to meet each such connected component. In order to obtain connectivity information in single exponential time a more sophisticated construction is required – namely that of a *roadmap* of a semi-algebraic set, which is an one dimensional semi-algebraic subset of the given semi-algebraic set which is non-empty and connected inside each connected component of the given set. Roadmaps were first introduced by Canny [13], but similar constructions were considered as well by Grigoriev and Vorobjov [19] and Gournay and Risler [18]. Our exposition below follows that in [8, 11] where the most efficient algorithm for computing roadmaps is given. The notions of pseudo-critical points and values defined above play a critical role in the design of efficient algorithms for computing roadmaps of semi-algebraic sets.

We first define a roadmap of a semi-algebraic set. We use the following notation. We denote by $\pi_{1\ldots j}$ the projection, $x \mapsto (x_1, \ldots, x_j)$. Given a set $S \subset \mathrm{R}^k$ and $y \in \mathrm{R}^j$, we denote by $S_y = S \cap \pi_{1\ldots j}^{-1}(y)$.

Definition 3.13 (Roadmap of a semi-algebraic set)**.** Let $S \subset \mathrm{R}^k$ be a semi-algebraic set. A *roadmap* for S is a semi-algebraic set M of dimension at most one contained in S which satisfies the following roadmap conditions:

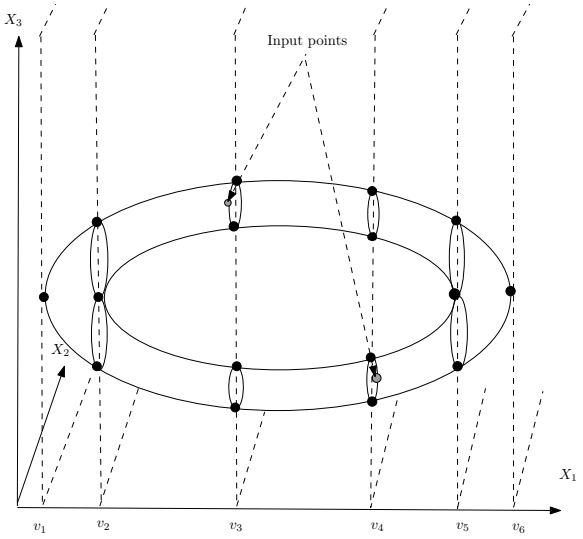

FIGURE 4. Roadmap of the torus in R^3.

- RM_1 For every semi-algebraically connected component D of S, $D \cap M$ is semi-algebraically connected.
- RM_2 For every $x \in \mathrm{R}$ and for every semi-algebraically connected component D' of S_x, $D' \cap M \neq \emptyset$.

We describe the construction of a roadmap $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k), \mathcal{N})$ for a bounded algebraic set $\mathrm{Z}(Q, \mathrm{R}^k)$ which contains a finite set of points $\mathcal{N}$ of $\mathrm{Z}(Q, \mathrm{R}^k)$. A precise description of how the construction can be performed algorithmically can be found in [11]. We should emphasize here that $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k), \mathcal{N})$ denotes the semi-algebraic set output by the specific algorithm described below which satisfies the properties stated in Definition 3.13 (cf. Proposition 3.14).

Also, in order to understand the roadmap algorithm it is easier to first concentrate on the case of a bounded and non-singular real algebraic set in R^k (see Figure 4 below). In this case several definitions get simplified. For example, the pseudo-critical values defined below are in this case ordinary critical values of the projection map on the first co-ordinate. However, one should keep in mind that even if one starts with a bounded non-singular algebraic set, the input to the recursive calls corresponding to the critical sections (see below) are necessarily singular and thus it is not possible to treat the non-singular case independently.

A key ingredient of the roadmap is the construction of pseudo-critical points and values defined above. The construction of the roadmap of an algebraic set containing a finite number of input points $\mathcal{N}$ of this algebraic set is as

follows. We first construct X_2-pseudo-critical points on $\mathrm{Z}(Q, \mathrm{R}^k)$ in a parametric way along the X_1-axis by following continuously, as x varies on the X_1-axis, the X_2-pseudo-critical points on $\mathrm{Z}(Q, \mathrm{R}^k)_x$. This results in curve segments and their endpoints on $\mathrm{Z}(Q, \mathrm{R}^k)$. The curve segments are continuous semi-algebraic curves parametrized by open intervals on the X_1-axis and their endpoints are points of $\mathrm{Z}(Q, \mathrm{R}^k)$ above the corresponding endpoints of the open intervals. Since these curves and their endpoints include for every $x \in \mathrm{R}$ the X_2-pseudo-critical points of $\mathrm{Z}(Q, \mathrm{R}^k)_x$, they meet every connected component of $\mathrm{Z}(Q, \mathrm{R}^k)_x$. Thus, the set of curve segments and their endpoints already satisfy RM_2. However, it is clear that this set might not be semi-algebraically connected in a semi-algebraically connected component and so RM_1 might not be satisfied. We add additional curve segments to ensure connectedness by recursing in certain distinguished hyperplanes defined by $X_1 = z$ for distinguished values z.

The set of *distinguished values* is the union of the X_1-pseudo-critical values, the first coordinates of the input points $\mathcal{N}$, and the first coordinates of the endpoints of the curve segments. A *distinguished hyperplane* is an hyperplane defined by $X_1 = v$, where v is a distinguished value. The input points, the endpoints of the curve segments, and the intersections of the curve segments with the distinguished hyperplanes define the set of *distinguished points*.

Let the distinguished values be $v_1 < \ldots < v_\ell$. Note that amongst these are the X_1-pseudo-critical values. Above each interval (v_i, v_{i+1}) we have constructed a collection of curve segments $\mathcal{C}_i$ meeting every semi-algebraically connected component of $\mathrm{Z}(Q, \mathrm{R}^k)_v$ for every $v \in (v_i, v_{i+1})$. Above each distinguished value v_i we have a set of distinguished points $\mathcal{N}_i$. Each curve segment in $\mathcal{C}_i$ has an endpoint in $\mathcal{N}_i$ and another in $\mathcal{N}_{i+1}$. Moreover, the union of the $\mathcal{N}_i$ contains $\mathcal{N}$.

We then repeat this construction in each distinguished hyperplane H_i defined by $X_1 = v_i$ with input $Q(v_i, X_2, \ldots, X_k)$ and the distinguished points in $\mathcal{N}_i$. Thus, we construct distinguished values $v_{i,1}, \ldots, v_{i,\ell(i)}$ of $\mathrm{Z}(Q(v_i, X_2, \ldots, X_k), \mathrm{R}^{k-1})$ (with the role of X_1 being now played by X_2) and the process is iterated until for $I = (i_1, \ldots, i_{k-2}), 1 \leq i_1 \leq \ell, \ldots, 1 \leq i_{k-2} \leq \ell(i_1, \ldots, i_{k-3})$, we have distinguished values $v_{I,1} < \ldots < v_{I,\ell(I)}$ along the X_{k-1} axis with corresponding sets of curve segments and sets of distinguished points with the required incidences between them.

The following theorem is proved in [8] (see also [11]).

Proposition 3.14. *The semi-algebraic set* $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k), \mathcal{N})$ *obtained by this construction is a roadmap for* $\mathrm{Z}(Q, \mathrm{R}^k)$ *containing* $\mathcal{N}$.

Note that if $x \in \mathrm{Z}(Q, \mathrm{R}^k)$, $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k), \{x\})$ contains a path, $\gamma(x)$, connecting a distinguished point p of $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k))$ to x.

3.3.1. *The Divergence Property of Connecting Paths.* In applications to algorithms for computing Betti numbers of semi-algebraic sets it becomes

important to examine the properties of parametrized paths which are the unions of connecting paths starting at a given p and ending at x, where x varies over a certain semi-algebraic subset of $\mathrm{Z}(Q, \mathrm{R}^k)$.

We first note that for any $x = (x_1, \ldots, x_k) \in \mathrm{Z}(Q, \mathrm{R}^k)$ we have by construction that $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k))$ is contained in $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k), \{x\})$. In fact,

$$\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k), \{x\}) = \mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k)) \cup \mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k)_{x_1}, \mathcal{M}_{x_1}),$$

where $\mathcal{M}_{x_1}$ consists of $(x_2, \ldots, x_k)$ and the finite set of points obtained by intersecting the curves in $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k))$ parametrized by the X_1-coordinate with the hyperplane $\pi_1^{-1}(x_1)$.

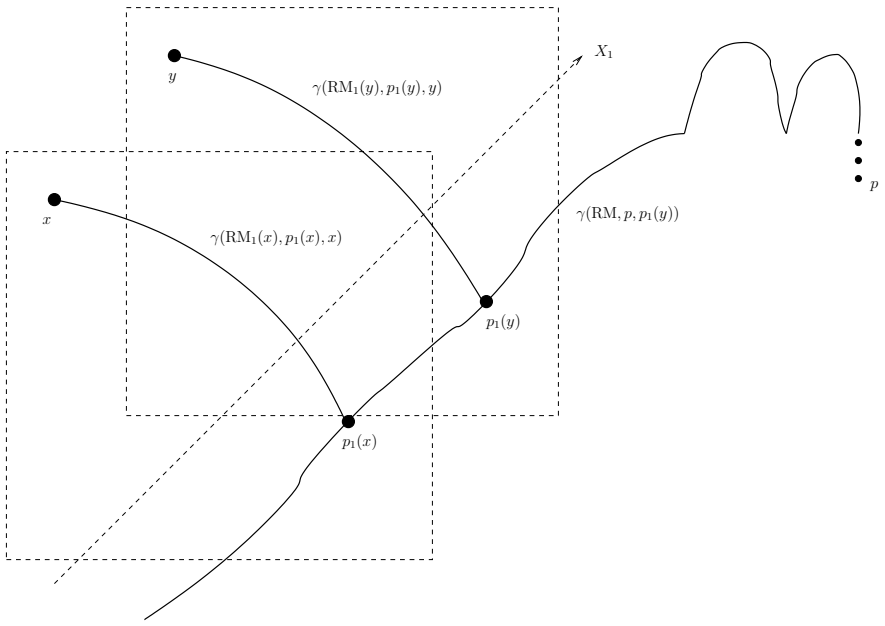

FIGURE 5. The connecting path $\Gamma(x)$.

A connecting path $\gamma(x)$ (with non-self intersecting image) joining a distinguished point p of $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k))$ to x can be extracted from $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k), \{x\})$. The connecting path $\gamma(x)$ consists of two consecutive parts, $\gamma_0(x)$ and $\Gamma_1(x)$. The path $\gamma_0(x)$ is contained in $\mathrm{RM}(\mathrm{Z}(Q, \mathrm{R}^k))$ and the path $\Gamma_1(x)$ is contained in $\mathrm{Z}(Q, \mathrm{R}^k)_{x_1}$. The part $\gamma_0(x)$ consists of a sequence of sub-paths $\gamma_{0,0}, \ldots, \gamma_{0,m}$. Each $\gamma_{0,i}$ is a semi-algebraic path parametrized by one of the co-ordinates $X_1, \ldots, X_k$, over some interval $[a_{0,i}, b_{0,i}]$ with $\gamma_{0,0}(a_{0,0}) = p$. The semi-algebraic maps

$$\gamma_{0,0}, \ldots, \gamma_{0,m}$$

and the end-points of their intervals of definition

$$a_{0,0}, b_{0,0}, \ldots, a_{0,m}, b_{0,m}$$

are all independent of x (up to the discrete choice of the path $\gamma(x)$ in $\mathrm{RM}(\mathrm{Z}(Q,\mathrm{R}^k),\{x\})$), except $b_{0,m}$ which depends on x_1.

Moreover, $\Gamma_1(x)$ can again be decomposed into two parts $\gamma_1(x)$ and $\Gamma_2(x)$ with $\Gamma_2(x)$ contained in $\mathrm{Z}(Q,\mathrm{R}^k)_{(x_1,x_2)}$ and so on.

If $y = (y_1,\ldots,y_k) \in \mathrm{Z}(Q,\mathrm{R}^k)$ is another point such that $x_1 \neq y_1$, then since $\mathrm{Z}(Q,\mathrm{R}^k)_{x_1}$ and $\mathrm{Z}(Q,\mathrm{R}^k)_{y_1}$ are disjoint, it is clear that

$$\mathrm{RM}(\mathrm{Z}(Q,\mathrm{R}^k),\{x\}) \cap \mathrm{RM}(\mathrm{Z}(Q,\mathrm{R}^k),\{y\}) = \mathrm{RM}(\mathrm{Z}(Q,\mathrm{R}^k)).$$

Now consider a connecting path $\gamma(y)$ extracted from $\mathrm{RM}(\mathrm{Z}(Q,\mathrm{R}^k),\{y\})$. The images of $\Gamma_1(x)$ and $\Gamma_1(y)$ are disjoint. If the image of $\gamma_0(y)$ (which is contained in $\mathrm{RM}(\mathrm{Z}(Q,\mathrm{R}^k))$ follows the same sequence of curve segments as $\gamma_0(x)$ starting at p (i.e. it consists of the same curves segments $\gamma_{0,0},\ldots,\gamma_{0,m}$ as in $\gamma_0(x)$), then it is clear that the images of the paths $\gamma(x)$ and $\gamma(y)$ has the property that they are identical up to a point and they are disjoint after it. This is called the *divergence property* in [10].

3.3.2. *Roadmaps of General Semi-algebraic Sets.* Using the same ideas as above and some additional techniques for controlling the combinatorial complexity of the algorithm it is possible to extend the roadmap algorithm to the case of semi-algebraic sets. The following theorem appears in [10, 11] and gives the most efficient algorithm for constructing roadmaps.

Theorem 3.15. [10, 11] *Let $Q \in \mathrm{R}[X_1,\ldots,X_k]$ with $\mathrm{Z}(Q,\mathrm{R}^k)$ of dimension k' and let $\mathcal{P} \subset \mathrm{R}[X_1,\ldots,X_k]$ be a set of at most s polynomials for which the degrees of the polynomials in $\mathcal{P}$ and Q are bounded by d. Let S be a $\mathcal{P}$-semi-algebraic subset of $\mathrm{Z}(Q,\mathrm{R}^k)$. There is an algorithm which computes a roadmap $\mathrm{RM}(S)$ for S with complexity $s^{k'+1}d^{O(k^2)}$ in the ring D generated by the coefficients of Q and the elements of $\mathcal{P}$. If $\mathrm{D} = \mathbb{Z}$, and the bit-sizes of the coefficients of the polynomials are bounded by τ, then the bit-sizes of the integers appearing in the intermediate computations and the output are bounded by $\tau d^{O(k^2)}$.*

Theorem 3.15 immediately implies that there is an algorithm whose output is exactly one point in every semi-algebraically connected component of S and whose complexity in the ring generated by the coefficients of Q and $\mathcal{P}$ is bounded by $s^{k'+1}d^{O(k^2)}$. In particular, this algorithm counts the number semi-algebraically connected component of S within the same time bound.

References

1. P.. Agarwal and M. Sharir, *Arrangements and their applications*, Handbook of computational geometry (J. Urrutia J.R. Sack, ed.), North-Holland, Amsterdam, 2000, pp. 49–119. MR 1746675
2. S. Basu, *On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets*, Discrete Comput. Geom. **22** (1999), no. 1, 1–18.
3. ———, *Computing Betti numbers of arrangements via spectral sequences*, Journal of Computer and System Sciences **67** (2003), 244–262.

4. ———, *Computing the first few Betti numbers of semi-algebraic sets in single exponential time*, J. Symbolic Comput. **41** (2006), no. 10, 1125–1154. MR 2262087 (2007k:14120)
5. ———, *Computing the top few Betti numbers of semi-algebraic sets defined by quadratic inequalities in polynomial time*, Found. Comput. Math. **8** (2008), no. 1, 45–80.
6. S. Basu, R. Pollack, and M.-F. Roy, *On the combinatorial and algebraic complexity of quantifier elimination*, J. ACM **43** (1996), no. 6, 1002–1045. MR 98c:03077
7. ———, *On computing a set of points meeting every cell defined by a family of polynomials on a variety*, J. Complexity **13** (1997), no. 1, 28–37. MR 98d:14071
8. ———, *Computing roadmaps of semi-algebraic sets on a variety*, J. Amer. Math. Soc. **13** (2000), no. 1, 55–82. MR 1685780 (2000h:14048)
9. ———, *Betti number bounds, applications and algorithms*, Current Trends in Combinatorial and Computational Geometry: Papers from the Special Program at MSRI, MSRI Publications, vol. 52, Cambridge University Press, 2005, pp. 87–97.
10. ———, *Computing the first Betti number of a semi-algebraic set*, Found. Comput. Math. **8** (2008), no. 1, 97–136.
11. ———, *Algorithms in real algebraic geometry*, Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2009, online version. MR 1998147 (2004g:14064)
12. S. Basu and T. Zell, *On projections of semi-algebraic sets defined by few quadratic inequalities*, Discrete Comput. Geom. **39** (2008), no. 1-3, 100–122. MR 2383753
13. J. Canny, *Computing road maps in general semi-algebraic sets*, The Computer Journal **36** (1993), 504–514.
14. B. Chazelle, H. Edelsbrunner, L.J. Guibas, and M. Sharir, *A single-exponential stratification scheme for real semi-algebraic varieties and its applications*, Theoretical Computer Science **84** (1991), 77–105.
15. K. Clarkson, H. Edelsbrunner, L.J. Guibas, M. Sharir, and E. Welzl, *Combinatorial complexity bounds for arrangements of curves and spheres*, Discrete and Computational Geometry **5** (1990), 99–160.
16. G. E. Collins, *Quantifier elimination for real closed fields by cylindric algebraic decomposition*, Second GI Conference on Automata Theory and Formal Languages (Berlin), Lecture Notes in Computer Science, vol. 33, Springer- Verlag, 1975, pp. 134–183.
17. A. Gabrielov and N. Vorobjov, *Betti numbers of semialgebraic sets defined by quantifier-free formulae*, Discrete Comput. Geom. **33** (2005), no. 3, 395–401. MR 2121987 (2005i:14075)
18. L. Gournay and J. J. Risler, *Construction of roadmaps of semi-algebraic sets*, Appl. Algebra Eng. Commun. Comput. **4** (1993), no. 4, 239–252.
19. D. Grigoriev and N. Vorobjov, *Counting connected components of a semi-algebraic set in subexponential time*, Comput. Complexity **2** (1992), no. 2, 133–186.
20. D. Yu. Grigoriev and N. N. Vorobjov, Jr., *Solving systems of polynomial inequalities in subexponential time*, J. Symbolic Comput. **5** (1988), no. 1-2, 37–64. MR 949112 (89h:13001)
21. J. Heintz, M.-F. Roy, and P. Solernò, *Description of the connected components of a semialgebraic set in single exponential time*, Discrete and Computational Geometry **11** (1994), 121–140.
22. S. Lojasiewicz, *Triangulation of semi-analytic sets.*, Ann. Scuola Norm. Sup. Pisa, Sci. Fis. Mat. **18** (1964), no. 3, 449–474.
23. J. Milnor, *On the Betti numbers of real varieties*, Proc. Amer. Math. Soc. **15** (1964), 275–280. MR 0161339 (28 #4547)
24. I. G. Petrovskiĭ and O. A. Oleĭnik, *On the topology of real algebraic surfaces*, Izvestiya Akad. Nauk SSSR. Ser. Mat. **13** (1949), 389–402. MR 0034600 (11,613h)
25. J. Renegar, *On the computational complexity and geometry of the first-order theory of the reals. I-III.*, J. Symbolic Comput. **13** (1992), no. 3, 255–352.

26. J. Schwartz and M. Sharir, *On the piano movers' problem ii. general techniques for computing topological properties of real algebraic manifolds*, Adv. Appl. Math. **4** (1983), 298–351.
27. A. Tarski, *A decision method for elementary algebra and geometry*, University of California Press, Berkeley and Los Angeles, Calif., 1951, 2nd ed. MR 13,423a
28. R. Thom, *Sur l'homologie des variétés algébriques réelles*, Differential and Combinatorial Topology (A Symposium in Honor of Marston Morse), Princeton Univ. Press, Princeton, N.J., 1965, pp. 255–265. MR 0200942 (34 #828)

Department of Mathematics Purdue University, West Lafayette, IN 47907, U.S.A.

E-mail address: sbasu@math.purdue.edu