ALGORITHMS IN REAL ALGEBRAIC GEOMETRY: A SURVEY

SAUGATA BASU

Abstract. We survey both old and new developments in the theory of algorithms in real algebraic geometry – starting from effective quantifier elimination in the first order theory of reals due to Tarski and Seidenberg, to more recent algorithms for computing topological invariants of semi-algebraic sets. We emphasize throughout the complexity aspects of these algorithms and also discuss the computational hardness of the underlying problems. We also describe some recent results linking the computational hardness of decision problems in the first order theory of the reals, with that of computing certain topological invariants of semi-algebraic sets. Even though we mostly concentrate on exact algorithms, we also discuss some numerical approaches involving semi-definite programming that have gained popularity in recent times.

1. Introduction

We survey developments in the theory of algorithms in real algebraic geometry – starting from the first effective quantifier elimination procedure due to Tarski and Seidenberg, to more recent work on efficient algorithms for quantifier elimination, as well as algorithms for computing topological invariants of semi-algebraic sets – such as the number semi-algebraically connected components, Euler-Poincaré characteristic, Betti numbers etc. Throughout the survey, the emphasis is on the worst-case complexity bounds of these algorithms, and the continuing effort to design algorithms with better complexity. Our goal in this survey is to describe these algorithmic results (including stating precise complexity bounds in most cases), and also give some indications of the techniques involved in designing them. We also describe some hardness results which show the intrinsic difficulty of some of these problems.

1.1. **Notation.** We first fix some notation. Throughout, R will denote a ***real closed field*** (for example, the field $\mathbb{R}$ of real numbers or $\mathbb{R}_{\rm alg}$ of real algebraic numbers), and we will denote by C the algebraic closure of R.

A ***semi-algebraic subset*** of R^k is a set defined by a finite system of polynomial equalities and inequalities, or more generally by a Boolean formula whose atoms are polynomial equalities and inequalities. Given a finite set $\mathcal{P}$ of polynomials in $\mathrm{R}[X_1,\ldots,X_k]$, a subset S of R^k is ***$\mathcal{P}$-semi-algebraic*** if S is the realization of a Boolean formula with atoms $P=0$, $P>0$ or $P<0$ with $P\in\mathcal{P}$ (we will call such a formula a quantifier-free $\mathcal{P}$-formula).

Key words and phrases. Algorithms, Complexity, Semi-algebraic Sets, Betti Numbers .

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

It is clear that for every semi-algebraic subset S of R^k there exists a finite set $\mathcal{P}$ of polynomials in $\mathrm{R}[X_1,\ldots,X_k]$ such that S is $\mathcal{P}$-semi-algebraic. We call a semi-algebraic set a ***$\mathcal{P}$-closed*** semi-algebraic set if it is defined by a Boolean formula with no negations with atoms $P=0$, $P\geq 0$, or $P\leq 0$ with $P\in\mathcal{P}$.

For an element $a\in\mathrm{R}$ we let

$$\mathrm{sign}(a)=\begin{cases}0 & \text{if } a=0,\\ 1 & \text{if } a>0,\\ -1 & \text{if } a<0.\end{cases}$$

A ***sign condition*** on $\mathcal{P}$ is an element of $\{0,1,-1\}^{\mathcal{P}}$. For any semi-algebraic set $Z\subset\mathrm{R}^k$ the ***realization of the sign condition σ over Z***, $\mathcal{R}(\sigma,Z)$, is the semi-algebraic set

$$\{x\in Z \mid \bigwedge_{P\in\mathcal{P}}\mathrm{sign}(P(x))=\sigma(P)\},$$

and in case $Z=\mathrm{R}^k$ we will denote $\mathcal{R}(\sigma,Z)$ by just $\mathcal{R}(\sigma)$.

If $\mathcal{P}$ is a finite subset of $\mathrm{R}[X_1,\ldots,X_k]$, we write the set of zeros of $\mathcal{P}$ in R^k as

$$\mathrm{Z}(\mathcal{P},\mathrm{R}^k)=\{x\in\mathrm{R}^k \mid \bigwedge_{P\in\mathcal{P}}P(x)=0\}.$$

Given a semi-algebraic set $S\subset\mathrm{R}^k$, we will denote by $b_i(S)$ the i-th ***Betti number*** of S, that is the rank of the i-th homology group of S (see [18] for precise definitions of homology groups for semi-algebraic sets defined over arbitrary real closed fields). Note that $b_0(S)$ is the number of semi-algebraically connected components of S. We will denote by $b(S)$ the sum $\sum_{i\geq 0}b_i(S)$.

For $x\in\mathrm{R}^k$ and $r>0$, we will denote by $\mathrm{B}_k(x,r)$ (resp. $\mathbf{S}^{k-1}(x,r)$) the open ball (resp. the sphere) with center x and radius r in R^k. When $x=0$, we will write $B_k(r)$ (resp. $\mathbf{S}^{k-1}(r)$) instead of $B_k(0,r)$ (resp. $\mathbf{S}^{k-1}(0,r)$). We will also denote the unit ball (resp. sphere) in R^k centered at 0 by B_k (resp. $\mathbf{S}^{k-1}$).

1.2. **Main algorithmic problems.** Algorithmic problems in semi-algebraic geometry typically consist of the following. We are given as input a finite family, $\mathcal{P}\subset\mathrm{R}[X_1,\ldots,X_k]$. The main algorithmic problems can be roughly divided into two classes (though we will see later in Section 3.4 how they are related from the point of computational complexity).

The first class of problems has a logical flavor. It includes the following.

Given a quantified $\mathcal{P}$-formula Φ (with or without free variables), the task is to:

(1) (***The Quantifier Elimination Problem***) Compute a quantifier-free formula equivalent to Φ.
(2) (***The General Decision Problem***) This is a special case of the previous problem when Φ has no free variables, and the problem is to decide the truth or falsity of Φ.
(3) (***The Existential Problem***) This is a special case of the last problem when there is exactly one block of existential quantifiers; equivalently, the problem can be stated as deciding whether a given $\mathcal{P}$-semi-algebraic set is empty or not.

The second class of problems has a more geometric and/or topological flavor. Given a description of a $\mathcal{P}$-semi-algebraic set $S\subset\mathrm{R}^k$ 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.

(1) (***Deciding Emptiness***) Decide whether S is empty or not (this is the same as the Existential Problem described above).
(2) (***Deciding Connectivity***) Given two points $x, y \in S$, decide if they are in the same semi-algebraically connected component of S and if so output a semi-algebraic path in S connecting them.
(3) ***(Describing Connected Components)*** Compute semi-algebraic descriptions of the semi-algebraically connected components of S.

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

(4) ***(Computing Betti Numbers)*** Compute the cohomology groups of S, its Betti numbers, its Euler-Poincaré characteristic etc..
(5) ***(Computing Triangulations)*** Compute a semi-algebraic triangulation of S as well as,
(6) ***(Computing Regular Stratifications)*** compute a decomposition of S into semi-algebraic smooth pieces of various dimensions satisfying certain extra regularity conditions (for example, Whitney conditions (a) and(b)).

The complexity of an algorithm (see Definition 1.1 below) for solving any of the above problems is measured in terms of the following three parameters:

- the number of polynomials, $s = \text{card } \mathcal{P}$,
- the maximum degree, $d = \max_{P \in \mathcal{P}} \deg(P)$, and
- the number of variables, k (and in case of quantifier elimination problems, the block decomposition of the k variables).

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 coefficients 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 [18, Chapter 8] for a full discussion about the various measures of complexity.

The rest of the paper is organized as follows. In Section 2, we describe known algorithms for quantifier elimination in the theory of the reals, starting from Tarski's algorithm, algorithms via cylindrical algebraic decomposition, and finally more modern algorithms using the critical points method. We also discuss some variants of quantifier elimination problem that arise in applications, as well as certain approaches using complex geometry of polar varieties that give efficient probabilistic algorithms. We also discuss the known lower bounds for real quantifier elimination.

In Section 3, we concentrate on algorithms for computing topological properties of semi-algebraic sets – including connectivity property via construction of roadmaps, computing the generalized Euler-Poincaré characteristic of semi-algebraic sets, as well as computing the Betti numbers of semi-algebraic sets. Throughout this section the emphasis is on algorithms with singly exponential complexity bounds. We also discuss certain results that are special to semi-algebraic sets defined by quadratic inequalities, or more generally where the defining polynomials have at most quadratic dependence on most of the variables. We also point out the significance

of some of the results from the point of view of computational complexity theory. Finally, we discuss a recent reduction result linking the complexity of the problem of computing the Betti numbers of semi-algebraic sets, with that of the decision problem in the first order theory of the real with a fixed number of quantifier block.

In Section 4, we discuss numerical algorithms for polynomial optimization using the "sums-of-square" approach. The main algorithmic tool here is "interior-point algorithms for semi-definite programming" and we discuss the known results on the computational complexity of the semi-definite programming problem.

We end with a list of open problems (Section 5).

Warning. There are several interesting topics which come under the purview of algorithms in real algebraic geometry that have been left out of this survey (because of lack of space as well as the author's lack of expertise in some of these topics). For example, we do not make any attempt to survey the extremely broad area of research concerning efficient implementation of theoretically efficient algorithms, specific low dimensional applications such as computing the topology of curves and surfaces, computing certificates of positivity of polynomials (for archimedean as well as non-archimedean real closed fields), homotopy continuation algorithms for solving real systems etc. There are multiple excellent sources available for most of these topics. Finally, algorithmic real algebraic geometry has a great variety of applications, due to the ubiquity of semi-algebraic sets arising in different areas of science and engineering – including robotics, molecular chemistry, theoretical computer science, database theory etc. We do not make any attempt to survey these applications.

2. Quantifier elimination and related problems

We begin appropriately with the first algorithm (in the modern sense) in real algebraic geometry which is a starting point of the subject.

2.1. The Tarski-Seidenberg Theorem and effective quantifier elimination.

Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathrm{R}[X_1, \ldots, X_k, Y_1, \ldots, Y_\ell]$, and $\Phi(Y)$ a first-order formula given by

$$(Q_\omega X^{[\omega]}) \ldots (Q_1 X^{[1]}) F(P_1, \ldots, P_s),$$

where $Q_i \in \{\forall, \exists\}$, $Q_i \neq Q_{i+1}$, $Y = (Y_1, \ldots, Y_\ell)$ is a block of ℓ free variables, $X^{[i]}$ is a block of k_i variables with $\sum_{1 \leq i \leq \omega} k_i = k$, and $F(P_1, \ldots, P_s)$ is a quantifier-free Boolean formula with atomic predicates of the form $\mathrm{sign}(P_i(Y, X^{[\omega]}, \ldots, X^{[1]})) = \sigma$ where $\sigma \in \{0, 1, -1\}$. (Letting Π denote the partition of the blocks of variables $X_1, \ldots, X_k$ into the ω blocks of sizes $k_1, \ldots, k_\omega$, we call a formula such as Φ, having the block structure specified by Π to be a $(\mathcal{P}, \Pi)$-formula.)

The Tarski-Seidenberg theorem states that

Theorem 2.1. [72] *There exists a quantifier-free formula, $\Psi(Y)$, such that for any $y \in R^\ell$, $\Phi(y)$ is true if and only if $\Psi(y)$ is true.*

The quantifier elimination problem is to algorithmically construct such a formula.

2.1.1. *Algorithm arising from Tarski's proof.* Tarski's proof [72] of the existence of quantifier elimination in the theory of the reals was effective and was based on Sturm's theorem for counting real roots of polynomials in one variable with real coefficients used in a parametric way. A modern treatment of this proof can

be found in [18, Chapter 2]. The complexity of this procedure was not formally analysed in Tarski's paper. However, the algorithm eliminates one variable at a time using a parametrized version of Euclidean remainder sequence, and as a result the number and degrees of the polynomials in the remaining variables grow rather fast, and it is not possible to bound the complexity of the algorithm by any function which is a tower of exponents (in the input parameters) of a fixed height, which implies that the complexity of Tarski's algorithm is not *elementary recursive*. An elementary recursive algorithm for the General Decision Problem was found later by Monck [54].

2.1.2. *Cylindrical Algebraic Decomposition.* 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 [52]), Collins [33, 34] was the first to apply cylindrical algebraic decomposition in the setting of algorithmic semi-algebraic geometry. Schwartz and Sharir [70] realized its importance in trying to solve the motion planning problem in robotics, as well as computing topological properties of semi-algebraic sets. Similar ideas leading to doubly exponential algorithms was also developed by Wüthrich [74].

Definition 2.2 (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 $\xi_{i,\ell_S+1} = +\infty$:

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

Definition 2.3. 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 [18, Chapter 11] for an easily accessible exposition).

Theorem 2.4. [34, 74] *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 $s = \operatorname{card} \mathcal{P}$ and $d = \max_{P \in \mathcal{P}} \deg(P)$.*

Cylindrical algebraic decomposition provides an alternative (and more efficient compared to Tarski's) algorithm for quantifier elimination, since (using the same notation as in the previous section) the semi-algebraic subset of R^ℓ defined by $\Phi(Y)$, is a union of cells (of various dimensions) in a cylindrical algebraic decomposition of $\mathrm{R}^{k+\ell}$ adapted to $\mathcal{P}$ (cf. Definition 2.3), where $Y_1, \ldots, Y_\ell$ are the last ℓ variables. This last fact is a consequence of the "cylindrical" structure of the decomposition. The complexity of such an algorithm is bounded by the complexity of computing the cylindrical decomposition and is doubly exponential. More precisely, the complexity is bounded by $(sd)^{2^{O(k+\ell)}}$.

Remark 2.5. The technique of cylindrical algebraic decomposition is also used in algorithms for computing topological properties of semi-algebraic sets. After making a generic linear change of co-ordinates, the cylindrical algebraic decomposition algorithm yields a finite cell complex from which topological invariants of the underlying semi-algebraic sets can be extracted. It should be noted that a change of co-ordinates is needed to obtain a cell complex. However, in certain applications a change of co-ordinates is not allowed (see [21] for one such application). It is an interesting open question if there always exists a semi-algebraic cell decomposition adapted to a given finite family of polynomials, having a cylindrical structure with respect to the given co-ordinates.

2.1.3. *Lower bound.* Given the doubly exponential upper bound on the complexity of quantifier elimination algorithm that follows from cylindrical algebraic decomposition, it is interesting to ask whether it is at all possible to do better. This question was investigated by Davenport and Heintz [38] who proved a doubly exponential *lower bound* on the complexity of real quantifier elimination, by constructing a sequence of quantified formula having the property that any equivalent sequence of quantifier-free formulas would necessarily have doubly exponential growth in size. However, the quantified formulas in the sequence they constructed had a large number of quantifier alternations (linear in the number of variables). Thus, while it is impossible to hope for better than doubly exponential dependence in the number, ω, of quantifier alternations, it might still be possible to obtain algorithms with much better complexity (i.e. singly exponential in the number of variables) if we fix the number of quantifier alternations. This is what we describe next.

2.2. **The critical points method and singly exponential algorithms.** As mentioned earlier, all algorithms using cylindrical algebraic decomposition have doubly exponential complexity. Algorithms with singly exponential complexity for solving problems in semi-algebraic geometry are mostly based on the *critical points method*. This method was pioneered by several researchers including Grigoriev and Vorobjov [44, 43], Renegar [65], Canny [31], Heintz, Roy and Solernò [46], Basu, Pollack and Roy [13] amongst others. In simple terms, the ***critical points 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 [18, Section 2.6] for full detail and proofs.

2.2.1. *Infinitesimals and the field of algebraic Puiseux series.*

Definition 2.6 (Puiseux series)**.** A ***Puiseux series*** in ε with coefficients in R is a series of the form

$$\overline{a} = \sum_{i \geq k} a_i \varepsilon^{i/q}, \tag{2.1}$$

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 Puiseux 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 ε with coefficients in R.

The following theorem is classical (see for example [18, Section 2.6] for a proof).

Theorem 2.7. *The field* $\mathrm{R}\langle\varepsilon\rangle$ *is real closed.*

Definition 2.8 (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 2.9. A typical example of the application of the lim map can be seen in Figures 1 and 2 below. The first picture depicts the algebraic set $\mathrm{Z}(Q, \mathrm{R}^3)$, while the second depicts the algebraic set $\mathrm{Z}(\mathrm{Def}(Q, \zeta, 4), \mathrm{R}\langle\zeta\rangle^3)$ (where we substituted a very small positive number for ζ in order to able display this set), where Q and $\mathrm{Def}(Q, \zeta, 4)$ are defined by Eqn. (2.4) and Eqn. (2.3) respectively The algebraic sets $\mathrm{Z}(Q, \mathrm{R}^3)$ and $\mathrm{Z}(\mathrm{Def}(Q, \zeta, 4), \mathrm{R}\langle\zeta\rangle^3)$ are related by

$$\mathrm{Z}(Q, \mathrm{R}^3) = \lim_{\zeta} \mathrm{Z}(\mathrm{Def}(Q, \zeta, 4), \mathrm{R}\langle\zeta\rangle^3).$$

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

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

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

The variety Z_{b} is the intersection of the sphere $S^k(0, 1/\varepsilon)$ of center 0 and radius $\frac{1}{\varepsilon}$ with a cylinder based $\mathrm{Ext}(Z, \mathrm{R}\langle\varepsilon\rangle)$ (and is hence bounded over $\mathrm{R}\langle\varepsilon\rangle$). The intersection of Z_{b} with the hyper-plane $X_{k+1} = 0$ is the intersection of Z with the sphere $S^{k-1}(0, 1/\varepsilon)$ of center 0 and radius $\frac{1}{\varepsilon}$. 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 [18] then relates the semi-algebraically connected component of Z with those of Z_{b} and this allows us to reduce the problem of finding points on every semi-algebraically connected component of a possibly unbounded algebraic set to the same problem on bounded algebraic sets.

Proposition 2.10. *Let N be a finite number of points meeting every semi-algebraically connected component of Z_{b}. Then $\pi(N)$ meets every semi-algebraically connected component of the extension* $\mathrm{Ext}(Z, \mathrm{R}\langle\varepsilon\rangle)$.

We obtain immediately using Proposition 2.10 a method for finding a point in every semi-algebraically 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.

2.2.2. *Representation of points.* One important aspect in any algorithm in real algebraic geometry is how to represent points whose co-ordinates belong to some real algebraic extension of the ordered ring D generated by the coefficients of the input polynomials. There are as usual several options, such as representing an arbitrary real algebraic number using isolating intervals, or by Thom encodings etc. In the singly-exponential algorithms described in the book [18], points in R^k are represented by *univariate representations* and an associated *Thom encoding*. Even though we will not need any further detail about these representations in this survey, given their importance in most of the algorithms that we refer to, we include their precise definitions below.

Definition 2.11 (Thom encoding)**.** Let $P \in \mathrm{R}[X]$ and $\sigma \in \{0, 1, -1\}^{\mathrm{Der}(P)}$, a sign condition on the set $\mathrm{Der}(P)$ of derivatives of P. The sign condition σ is a ***Thom encoding*** of $x \in \mathrm{R}$ if $\sigma(P) = 0$ and σ is the sign condition taken by the set $\mathrm{Der}(P)$ at x. Given a Thom encoding σ, we denote by $x(\sigma)$ the root of P in R specified by σ.

(Note that the use of Thom encoding to represent algebraic numbers was introduced in algorithmic real algebraic geometry by Coste and Roy in [35].)

Definition 2.12 (Univariate representations and real univariate representations)**.** A ***k-univariate representation*** is a $k+2$-tuple of polynomials of $\mathrm{R}[T]$,

$$(f(T), g_0(T), g_1(T), \ldots, g_k(T)),$$

such that f and g_0 are coprime.

The ***points associated*** to a univariate representation are the points

$$\left(\frac{g_1(t)}{g_0(t)}, \ldots, \frac{g_k(t)}{g_0(t)}\right) \in \mathrm{C}^k$$

where $t \in \mathrm{C}$ is a root of $f(T)$.

A ***real k-univariate representation*** is a pair u, σ where u is a k-univariate representation and σ is the Thom encoding of a root of f, $t_\sigma \in \mathrm{R}$. The ***point associated*** to the real univariate representation is the point

$$\left(\frac{g_1(t_\sigma)}{g_0(t_\sigma)}, \ldots, \frac{g_k(t_\sigma)}{g_0(t_\sigma)}\right) \in \mathrm{R}^k.$$

Remark 2.13. By parametrizing the definition of a real k-univariate representation (lets say by a co-ordinate function such as X_1) one obtains descriptions of semi-algebraic curves. These ***curve segment representations*** play an important role in algorithms for computing roadmaps of semi-algebraic sets (see Section 3.1 below).

2.2.3. *Deformation techniques to deal with singular varieties.* 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, $\mathrm{Def}(Q, \zeta, d)$, of the polynomial Q (where $d = \deg(Q)$). 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 [18, Section 12.1]), which makes possible efficient computation of these pseudo-critical values and points. We refer the reader to [18, Chapter 12] for a full exposition including the definition and basic properties of Gröbner basis.

The deformation $\mathrm{Def}(Q, \zeta, d)$ 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

$$G_k(\bar{d}, c) = c^{\bar{d}}(X_1^{\bar{d}} + \cdots + X_k^{\bar{d}} + X_2^2 + \cdots + X_k^2) - (2k-1), \tag{2.2}$$

$$\mathrm{Def}(Q, \zeta, d) = \zeta G_k(\bar{d}, c) + (1-\zeta)Q. \tag{2.3}$$

The algebraic set $\mathrm{Z}(\mathrm{Def}(Q, \zeta, d), \mathrm{R}\langle\zeta\rangle^k)$ is a bounded and non-singular hypersurface 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 $\mathrm{Z}(\mathrm{Def}(Q, \zeta, d), \mathrm{R}\langle\zeta\rangle^k)$ form a finite set of points. We take the images of these points under $\lim_\zeta$ (cf. Definition 2.8) 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 2.14. 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

$$Q = X_2^2 - X_1^2 + X_1^4 + X_2^4 + X_3^4. \tag{2.4}$$

Then, $\mathrm{Z}(Q, \mathrm{R}^3)$ is a bounded algebraic subset of R^3 shown below in Figure 1. Notice that $\mathrm{Z}(Q, \mathrm{R}^3)$ has a singularity at the origin. The surface $\mathrm{Z}(\mathrm{Def}(Q, \zeta, 4), \mathrm{R}^3)$ with a small positive real number substituted for ζ is shown in Figure 2. Notice that this surface is non-singular, but has a different homotopy type than $\mathrm{Z}(Q, \mathrm{R}^3)$ (it has three semi-algebraically connected components compared to only one of $\mathrm{Z}(Q, \mathrm{R}^3)$). However, the semi-algebraic set bounded by $\mathrm{Z}(\mathrm{Def}(Q, \zeta, 4), \mathrm{R}^3)$ (i.e. the part inside the larger component but outside the smaller ones) is homotopy equivalent to $\mathrm{Z}(Q, \mathrm{R}^3)$.

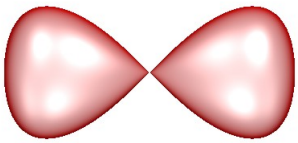

FIGURE 1. The algebraic set $\mathrm{Z}(Q, \mathrm{R}^3)$.

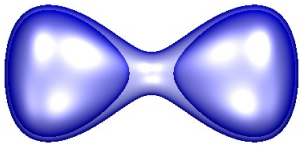

FIGURE 2. The algebraic set $\mathrm{Z}(\mathrm{Def}(Q, \zeta, 4), \mathrm{R}^3)$.

By computing algebraic representations (see [18, 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 semi-algebraically 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 semi-algebraically 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 [18, Proposition 13.2].

The following theorem which is the best result of this kind appears in [14].

Theorem 2.15. [14] *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 (i.e. the part that depends on s) of the algorithm in Theorem 2.15 depends on the dimension of the variety rather than that of the ambient space.

2.3. **Singly exponential quantifier elimination algorithms.** The algorithm with singly exponential algorithm for computing sample points in every semi-algebraically connected component of every realizable sign condition of a family of polynomials used in a parametrized way is a very important ingredient in designing algorithms with singly exponential complexity for real quantifier elimination. More precisely, it allows us the eliminate one whole block of variables (quantified by the same quantifier) at one time, unlike in algorithms based on cylindrical algebraic decomposition, where the elimination has to proceed one variable at a time *regardless of the block structure of the quantifiers*. The singly exponential algorithm for eliminating one block of variables at a time is formalized as the ***Block Elimination Algorithm*** [18, Chapter 14] and does the following. Given a finite family of polynomials $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k, Y_1, \ldots, Y_\ell]$, the Block Elimination Algorithm produces as output a family of polynomials $\mathrm{BElim}_X(\mathcal{P}) \subset \mathrm{R}[Y_1, \ldots, Y_\ell]$. The family $\mathrm{BElim}_X(\mathcal{P})$ has the following important property that justifies its name. For each semi-algebraically connected component, $C \subset \mathrm{R}^\ell$, of each realizable sign condition of $\mathrm{BElim}_X(\mathcal{P})$, the set of realizable sign conditions of $\mathcal{P}(y) \subset \mathrm{R}[X_1, \ldots, X_k]$ stay invariant as y is allowed to vary over C. The Block Elimination Algorithm also produces a set of parametrized (by y) sample points which are guaranteed to meet each semi-algebraically connected component of the set of realizable sign conditions of $\mathcal{P}(y) \subset \mathrm{R}[X_1, \ldots, X_k]$. The complexity of this algorithm is bounded by $s^{k+1} d^{O(\ell+k)}$, where as usual $s = \mathrm{card}\ \mathcal{P}$ and d is a bound on the degrees of the polynomials in $\mathcal{P}$.

2.3.1. *Sign Determination Algorithm.* The *Block Elimination Algorithm* is one important ingredient of the critical point based quantifier elimination algorithm. The other important ingredient is a ***Sign Determination Algorithm*** that allows one to compute the vector of signs of a family, $\mathcal{P}$, of s polynomials in $\mathrm{D}[X]$ at the real roots of a fixed polynomial $Q \in \mathrm{D}[X]$, with complexity $sd^{O(1)}$, where d is a bound on the degrees of the polynomials in $\mathcal{P}$ and Q. This algorithm was first discovered

by Ben-Or, Kozen and Reif [25] and extended by Roy and Szpirglas [67] (see also [58] for recent improvements). This algorithm has also been generalized to the multi-variate case (where the zeros of Q could be positive dimensional), and this is described below in Section 3.3.

2.3.2. *Quantifier Elimination Algorithm.* The above ingredients (namely, the *Block Elimination Algorithm* and the *Sign Determination Algorithm*), along with numerous technical detail which we omit in this survey, allows one to prove the following result.

Theorem 2.16. [18] *Let $\mathcal{P}$ be a set of at most s polynomials each of degree at most d in $k+\ell$ variables with coefficients in a real closed field* R*, and let* Π *denote a partition of the list of variables $(X_1,\ldots,X_k)$ into blocks, $X_{[1]},\ldots,X_{[\omega]}$, where the block $X_{[i]}$ has size $k_i, 1 \leq i \leq \omega$. Given $\Phi(Y)$, a $(\mathcal{P},\Pi)$-formula, there exists an equivalent quantifier free formula,*

$$\Psi(Y) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} (\bigvee_{n=1}^{Ni,j} \operatorname{sign}(P_{ijn}(Y)) = \sigma_{ijn}),$$

where $P_{ijn}(Y)$ are polynomials in the variables Y, $\sigma_{ijn} \in \{0,1,-1\}$,

$$I \leq s^{(k_\omega+1)\cdots(k_1+1)(\ell+1)} d^{O(k_\omega)\cdots O(k_1)O(\ell)},$$

$$J_i \leq s^{(k_\omega+1)\cdots(k_1+1)} d^{O(k_\omega)\cdots O(k_1)},$$

$$N_{ij} \leq d^{O(k_\omega)\cdots O(k_1)},$$

and the degrees of the polynomials $P_{ijk}(y)$ are bounded by $d^{O(k_\omega)\cdots O(k_1)}$. Moreover, there is an algorithm to compute $\Psi(Y)$ with complexity

$$s^{(k_\omega+1)\cdots(k_1+1)(\ell+1)} d^{O(k_\omega)\cdots O(k_1)O(\ell)}$$

in D*, denoting by* D *the ring generated by the coefficients 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 $\tau d^{O(k_\omega)\cdots O(k_1)O(\ell)}$.*

Remark 2.17. The algorithmic results described in Section 2.2 are based on one common technique – namely, by taking a well chosen infinitesimal perturbation, one can replace any bounded, real (possibly singular) variety $V \subset \mathrm{R}^k$, by a non-singular variety defined over an (non-archimedean) extension of R, and the projection map on some co-ordinate (say X_1) restricted to this variety has non-degenerate critical points, which moreover are defined by a zero-dimensional system of equations which is nicely behaved (is automatically a Gröbner basis). The limits of these critical points belong to the given variety V and moreover they meet every semi-algebraically connected component of V. This technique (which is rather special to real algebraic geometry as opposed to complex geometry) has several advantages from the point of view of algorithmic complexity. The first advantage is that it is not necessary to choose any generic co-ordinate system or direction to project on. Secondly, the method does not care about how singular the given variety V is or even its dimension. Moreover, it is possible to relate the topology (up to semi-algebraic homotopy equivalence) of V with the infinitesimal "tube" around it which is bounded by the perturbed hyper-surface (say V'). This reduces most algorithmic problems of computing topological invariants of V, to that of the well-behaved

hyper-surface V'. Since the degree of the polynomial defining V' is at most twice that of the one defining V, and the computations take place in the original ring adjoined with at most a constant many (i.e. their number is independent of the input parameters s, d and k) infinitesimals, the complexity is well controlled. The main disadvantage of the approach (which could a drawback from the point of view of practical implementation point) is that computations with even a constant many infinitesimals are quite expensive (even though they do not affect the asymptotic complexity bounds). Also, the process of taking algebraic limits at the end can be quite cumbersome. Nevertheless, this perturbation approach remains the only one which gives deterministic algorithms with the best known worst case complexity estimates.

2.4. **Intrinsic complexity and complex algebraic techniques.** The model for studying complexity of algorithms in this survey is that the size of the input is measured in terms of the number of coefficients needed to specify the input polynomials in the dense representation. Since this number is determined by the following parameters:

(1) the number of variables, k;
(2) the number of polynomials, s;
(3) the degrees of the polynomials, d;

it makes sense to state the complexity estimates in terms of s, d and k.

There is another body of work (see for example [1, 2, 68, 69, 47]) in which the goal is to obtain algorithms for computing sample points on each semi-algebraically connected component of a given real algebraic variety $V \subset \mathrm{R}^k$, whose complexity is bounded by a *polynomial* function of some *intrinsic* invariant of the variety V or in some cases the length of *straight line programs* encoding the input polynomials. In this approach, the real variety V is considered as the real part of the complex variety $V_{\mathrm{C}} \subset \mathrm{C}^k$ (where C is the algebraic closure of R), and the intrinsic invariant, $\delta(V) = \delta(V_{\mathrm{C}})$ depends only on the geometry of the complex variety V_{C}, and not on the particular presentation of it by the given input polynomials. If d is a bound on the degrees of the polynomials defining V, then $\delta(V)$ is bounded by $O(d)^k$ and could be as large as d^k in the worst case. However, $\delta(V)$ could be smaller in special cases.

Since these algorithms aim at complexity in terms of some geometric invariant of the variety itself, the infinitesimal perturbation techniques described in the previous sections is not available, since such a perturbation will not in general preserve this invariant. Hence, one needs to work directly with the given variety. For example, one needs to prove that under certain assumptions on the variety, the critical points of a generic projection (also called the polar variety) is non-singular (see [3]). The theory of *geometric resolutions* (see [2]) play an important role in these algorithms.

One feature of the algorithms that follow from these techniques is that it is necessary to choose generic co-ordinates which cannot be done deterministically within the claimed complexity bounds. As such one obtains *probabilistic* (as opposed to deterministic) algorithms, meaning that these algorithms always run within the stated complexity time bounds, but is guaranteed to give correct results only with high probability.

2.5. **Variants of quantifier elimination and applications.** In certain applications (most notably in the theory of constraint databases) one needs to perform

quantifier elimination in a more generalized setting than that discussed above. For instance, it is sometimes necessary to eliminate quantifiers not just from one formula, but a whole sequence of formulas described in some finite terms, where the number of free variables is allowed to grow in the sequence. Clearly, the quantifier elimination algorithms described previously is not sufficient for this purpose since their complexity depends on the number of free variables.

We describe below a variant of the quantifier elimination problem which was introduced in [6] motivated by a problem in constraint databases.

2.5.1. *The Uniform Quantifier Elimination Problem.*

Definition 2.18. We call a sequence,

$$\{\phi_n(T_1,\ldots,T_\ell,Y_1,\ldots,Y_n) \mid n>0\}$$

of first-order formulas ϕ_n in the language of ordered fields, to be a ***uniform sequence*** if each ϕ_n has the form,

$$\phi_n(T_1,\ldots,T_\ell,Y_1,\ldots,Y_n) =$$

$$Q^1_{1\leq k_1\leq n}\ldots Q^\omega_{1\leq k_\omega\leq n}\phi(T_1,\ldots,T_\ell,Y_{k_1},\ldots,Y_{k_\omega}),$$

where $Q^i\in\{\vee,\wedge\}, 1\leq i\leq\omega$ and ϕ is some fixed $(\ell+\omega)$-ary quantifier-free first-order formula.

Thus for every n, ϕ_n is a first order formula with $\ell+n$ free variables. We will refer to the variables $T_1,\ldots,T_\ell$ as *parameters*.

Given a uniform sequence of formulas $\Phi=\{\phi_n \mid n>0\}$, where

$$\phi_n(T_1,\ldots,T_\ell,Y_1,\ldots,Y_n) =$$

$$Q^1_{1\leq k_1\leq n}\ldots Q^\omega_{1\leq k_\omega\leq n}\phi(T_1,\ldots,T_\ell,Y_{k_1},\ldots,Y_{k_\omega}),$$

we define the *size* of Φ to be the length of the formula ϕ.

Example 2.19. Consider the uniform sequence of formulas

$$\phi_n(T_1,Y_1,\ldots,Y_n) = \bigwedge_{1\leq k_1\leq n}(Y_{k_1}-T_1=0),\ \ n>0.$$

Consider the sequence of quantified formulas, $(\exists T_1)\phi_n(T_1,Y_1,\ldots,Y_n)$. In this example, it is easily seen that letting

$$\Psi_n = \bigwedge_{1\leq k_1\leq n}\bigwedge_{1\leq k_2\leq n}(Y_{k_1}-Y_{k_2}=0),$$

we get a uniform sequence of quantifier-free formulas satisfying,

$$\Psi_n(Y_1,\ldots,Y_n)\Leftrightarrow(\exists T_1)\phi_n(T_1,Y_1,\ldots,Y_n)$$

for every $n>0$.

The ***uniform quantifier elimination problem*** is to eliminate quantifiers from a uniform sequence of formulas and obtain another *uniform* sequence of quantifier free formulas.

The following is proved in [6].

Theorem 2.20. *(Uniform Quantifier Elimination) Let,*

$$\Phi = \{\phi_n(T_1, \ldots, T_\ell, Y_1, \ldots, Y_n) \mid n > 0\}$$

be a uniform sequence of formulas with parameters $T_1, \ldots, T_\ell$, where

$$\phi_n(T_1, \ldots, T_\ell, Y_1, \ldots, Y_n) =$$

$$Q^1_{1 \leq k_1 \leq n} \ldots Q^\omega_{1 \leq k_\omega \leq n} \phi(T_1, \ldots, T_\ell, Y_{k_1}, \ldots, Y_{k_\omega}).$$

Let the number of different $(\ell + \omega)$-variate polynomials appearing in ϕ be s and let their degrees be bounded by d.

Let $R_1, \ldots, R_m \in \{\exists, \forall\}$, $R_i \neq R_{i+1}$, and let $T^{[1]}, \ldots, T^{[m]}$ be a partition of the variables, $T_1, \ldots, T_\ell$ into m blocks of size $\ell_1, \ldots, \ell_m$, where $\sum_{1 \leq i \leq m} \ell_i = \ell$.

Then, there exists an algorithm that outputs a quantifier-free first order formula, $\psi(Y_{k_1}, \ldots, Y_{k_{\omega'}})$, along with $Q^i \in \{\bigvee, \bigwedge\}, 1 \leq i \leq \omega'$, such that for every $n > 0$

$$\psi_n(Y_1, \ldots, Y_n) = Q^1_{1 \leq k_1 \leq n} \ldots Q^{\omega'}_{1 \leq k_{\omega'} \leq n} \psi(Y_{k_1}, \ldots, Y_{k_{\omega'}})$$

$$\Leftrightarrow (R_1 T^{[1]}) \ldots (R_m T^{[m]}) \phi_n(Y_1, \ldots, Y_n, T_1, \ldots, T_\ell).$$

The complexity of the algorithm is bounded by

$$s^{\prod_i (\ell_i + 1)} d^{\omega \prod_i O(\ell_i^2)},$$

and the size of the formula ψ is bounded by

$$s^{\prod_i (\ell_i + 1)} d^{\omega \prod_i O(\ell_i^2)} \text{size}(\phi).$$

Remark 2.21. In [6] Theorem 2.20 is used to prove the equivalence of two different semantics and in the theory of constraint databases. However, it also has applications in logic. For example, in the same paper it is used to prove that semi-algebraic connectivity is not expressible by a first-order formula (see [6] for a precise definition of first-order expressibility). This inexpressibility result has as a consequence that we cannot hope to use quantifier-elimination directly to check whether a given semi-algebraic set is semi-algebraically connected (unlike other first-order expressible topological properties such as being open or closed etc. where it is possible to do so). Note that the inexpressibility result was also proved by more abstract model theoretic methods in [26].

The technique used in the proof of Theorem 2.20 is also used in [6] to give an algorithm for ordinary quantifier elimination whose complexity depends on the size of the input formula, and which has better complexity than the algorithm in Theorem 2.16 in case the input formula has a small size. This algorithm is called ***Local Quantifier Elimination Algorithm*** in [18].

3. Computing topological invariants of semi-algebraic sets

As remarked above (see Remark 2.21), an effective algorithm for deciding connectivity of semi-algebraic sets does not automatically follow from the Tarski-Seidenberg principle. However, one can decide questions about connectivity (as well as compute other topological invariants such as the Betti numbers) using effective triangulation of semi-algebraic sets via Cylindrical Algebraic Decomposition. However, such an algorithm will necessarily have doubly exponential complexity.

Most of the recent work in algorithmic semi-algebraic geometry has focused on obtaining *singly 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 [41] (see also [40]) (see [59, 73, 53, 7], as well as the survey article [16], for work leading up to this result) which gives singly exponential upper bound on the topological complexity of semi-algebraic sets measured by the sum of their Betti numbers.

Theorem 3.1. [41] *For a $\mathcal{P}$-semi-algebraic set $S \subset \mathrm{R}^k$, the sum of the Betti numbers of S is bounded by $(O(skd))^k$, where $s = \operatorname{card} \mathcal{P}$, and $d = \max_{P\in\mathcal{P}} \deg(P)$.*

For the special case of $\mathcal{P}$-closed semi-algebraic sets the following slightly better bound was known before [7] (and this bound is used in an essential way in the proof of Theorem 3.1). Using the same notation as in Theorem 3.1 above we have

Theorem 3.2. [7] *For a $\mathcal{P}$-closed semi-algebraic set $S \subset \mathrm{R}^k$, the sum of the Betti numbers of S is bounded by $(O(sd))^k$.*

Remark 3.3. These bounds are asymptotically tight, as can be already seen from the example where each $P \in \mathcal{P}$ is a product of d generic polynomials of degree one. The number of semi-algebraically connected components of the $\mathcal{P}$-semi-algebraic set defined as the subset of R^k where all polynomials in $\mathcal{P}$ are non-zero is clearly bounded from below by $(Csd)^k$ for some constant C.

3.1. **Roadmaps.** Theorem 2.15 gives a singly 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 semi-algebraically connected component of the given semi-algebraic set, even though the set of sample points is guaranteed to meet each such semi-algebraically connected component. In order to obtain connectivity information in singly 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 semi-algebraically connected inside each semi-algebraically connected component of the given set. Roadmaps were first introduced by Canny [31], but similar constructions were considered as well by Grigoriev and Vorobjov [43] and Gournay and Risler [42]. Our exposition below follows that in [15, 18] 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 $S_y = S \cap \pi^{-1}_{1\ldots j}(y)$.

Definition 3.4 (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:

- 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

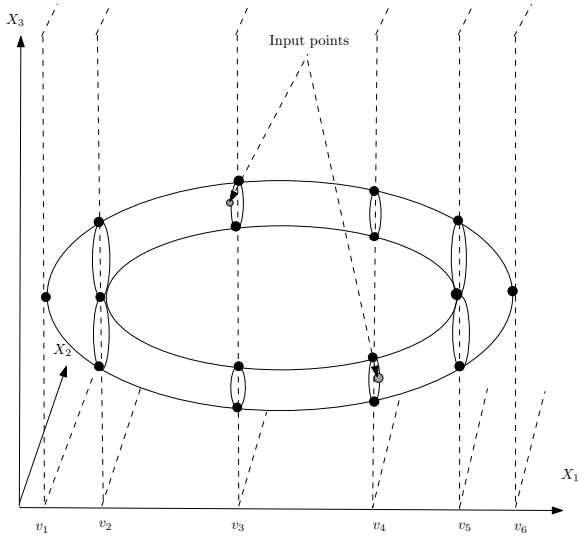

FIGURE 3. Roadmap of the torus in R^3.

precise description of how the construction can be performed algorithmically can be found in [18]. 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 3.4 (cf. Proposition 3.5).

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 3 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 semi-algebraically 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 hyper-planes 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 hyper-plane* is an hyper-plane 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 hyper-planes 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 hyper-plane 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 [15] (see also [18]).

Proposition 3.5. *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.

3.1.1. *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 [15, 18].

Theorem 3.6. [15, 18] *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 3.6 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.

3.1.2. *Recent developments.* Very recently Schost and Safey el Din [39] have given a *probabilistic* algorithm for computing the roadmap of a smooth, bounded real algebraic hyper-surface in R^k defined by a polynomial of degree d, whose complexity is bounded by $d^{O(k^{3/2})}$. Complex algebraic techniques related to the geometry of polar varieties play an important role in this algorithm. More recently, a *deterministic* algorithm for computing roadmaps of *arbitrary* real algebraic sets with the same complexity bound, has also been obtained [20]. This algorithm is based on techniques coming from semi-algebraic geometry and can be seen as a direct generalization of Proposition 3.5 above. The main new idea is to consider the critical points of projection maps onto a co-ordinate subspace of dimension bigger than 1 (in fact, of dimension $\sqrt{k}$). As a result the dimensions in the recursive calls to the algorithm decreases by $\sqrt{k}$ at each step of the recursion (compared to the case of the ordinary roadmap algorithms where it decreases by 1 in each step). This results in the improved complexity. One also needs to prove suitable generalizations of the results guaranteeing the connectivity of the roadmap (see [18, Chapter 15]) in this more general situation.

3.1.3. *Parametrized paths.* One important idea in the algorithm for computing the first Betti number of semi-algebraic sets, is the construction of certain semi-algebraic sets called *parametrized paths*. Under a certain hypothesis, these sets are semi-algebraically contractible. Moreover, there exists an algorithm for computing a covering of a given basic semi-algebraic set, $S \subset \mathrm{R}^k$, by a singly exponential number of parametrized paths.

Parametrized Paths. We are given a polynomial $Q \in \mathrm{R}[X_1, \ldots, X_k]$ such that $\mathrm{Z}(Q, \mathrm{R}^k)$ is bounded and a finite set of polynomials $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$.

The main technical construction underlying the algorithm for computing the first Betti number in [19], is to obtain a covering of a given $\mathcal{P}$-closed semi-algebraic set contained in $\mathrm{Z}(Q, \mathrm{R}^k)$ by a family of semi-algebraically contractible subsets. This construction is based on a parametrized version of the connecting algorithm: we compute a family of polynomials such that for each realizable sign condition σ on this family, the description of the connecting paths of different points in the realization, $\mathcal{R}(\sigma, \mathrm{Z}(Q, \mathrm{R}^k))$, are uniform. We first define parametrized paths. A parametrized path is a semi-algebraic set which is a union of semi-algebraic paths having a special property called the *divergence property* in [19].

More precisely,

Definition 3.7 (Parametrized paths)**.** A ***parametrized path*** γ is a continuous semi-algebraic mapping from $V \subset \mathrm{R}^{k+1} \to \mathrm{R}^k$, such that, denoting by $U = \pi_{1\ldots k}(V) \subset \mathrm{R}^k$, there exists a semi-algebraic continuous function $\ell : U \to [0, +\infty)$, and there exists a point a in R^k, such that

(1) $V = \{(x, t) \mid x \in U, 0 \leq t \leq \ell(x)\}$,
(2) $\forall\, x \in U,\ \gamma(x, 0) = a$,
(3) $\forall\, x \in U,\ \gamma(x, \ell(x)) = x$,
(4)
$$\forall\, x \in U, \forall\, y \in U, \forall\, s \in [0, \ell(x)], \forall\, t \in [0, \ell(y)]$$
$$(\gamma(x, s) = \gamma(y, t) \Rightarrow s = t)\,,$$
(5)
$$\forall\, x \in U, \forall\, y \in U, \forall\, s \in [0, \min(\ell(x), \ell(y))]$$

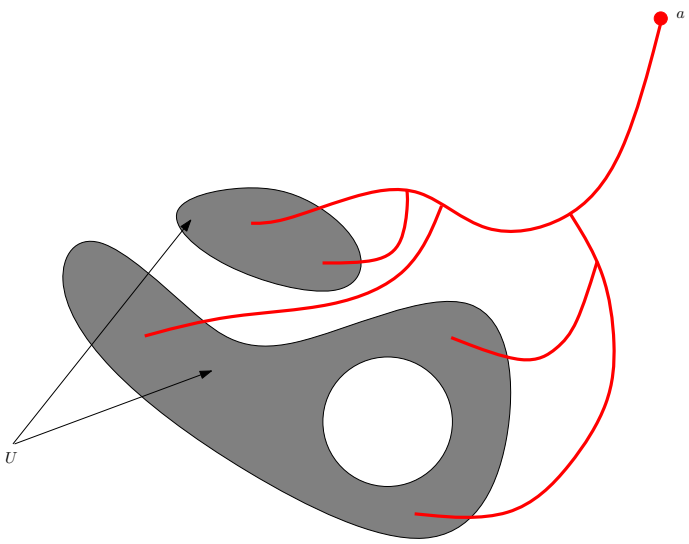

FIGURE 4. A parametrized path

$$(\gamma(x,s) = \gamma(y,s) \Rightarrow \forall\, t \leq s\ \gamma(x,t) = \gamma(y,t))\,.$$

Given a parametrized path, $\gamma : V \to \mathrm{R}^k$, we will refer to $U = \pi_{1\ldots k}(V)$ as its *base*. Also, any semi-algebraic subset $U' \subset U$ of the base of such a parametrized path, defines in a natural way the restriction of γ to the base U', which is another parametrized path, obtained by restricting γ to the set $V' \subset V$, defined by $V' = \{(x,t) \mid x \in U', 0 \leq t \leq \ell(x)\}$.

The following proposition which appears in [19] describes a crucial property of parametrized paths, which makes them useful in algorithms for computing Betti numbers of semi-algebraic sets.

Proposition 3.8. [19] *Let $\gamma : V \to R^k$ be a parametrized path such that $U = \pi_{1\ldots k}(V)$ is closed and bounded. Then, the image of γ is semi-algebraically contractible.*

For every point x of $\mathrm{Z}(Q, \mathrm{R}^k)$, denote by $\sigma(x)$ the sign condition on $\mathcal{P}$ at x. Let $\mathcal{R}(\overline{\sigma}(x), \mathrm{Z}(Q, \mathrm{R}^k)) = \{x \in \mathrm{Z}(Q, \mathrm{R}^k) \mid \bigwedge_{P \in \mathcal{P}} \ \mathrm{sign}(P(x)) \in \overline{\sigma}(x)(P)\}$, where $\overline{\sigma}$ is the relaxation of σ defined by

$$\begin{cases} \overline{\sigma} = \{0\} & \text{if} \quad \sigma = 0, \\ \overline{\sigma} = \{0, 1\} & \text{if} \quad \sigma = 1, \\ \overline{\sigma} = \{0, -1\} & \text{if} \quad \sigma = -1. \end{cases}$$

We say that $\overline{\sigma}(x)$ is the ***weak sign condition*** defined by x on $\mathcal{P}$. We denote by $\mathcal{P}(x)$ the union of $\{Q\}$ and the set of polynomials in $\mathcal{P}$ vanishing at x.

The following theorem appears in [19].

Theorem 3.9. *Moreover, there exists an algorithm that takes as input a finite set of polynomials $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$, and produces as output,*

- *a finite set of polynomials $\mathcal{A} \subset \mathrm{R}[X_1, \ldots, X_k]$,*

- *a finite set Θ of quantifier free formulas, with atoms of the form $P = 0, P > 0, P < 0,\ P \in \mathcal{A}$, such that for every semi-algebraically connected component S of the realization of every weak sign condition on $\mathcal{P}$ on $\mathrm{Z}(Q, \mathrm{R}^k)$, there exists a subset $\Theta(S) \subset \Theta$ such that $S = \bigcup_{\theta \in \Theta(S)} \mathcal{R}(\theta, \mathrm{Z}(Q, \mathrm{R}^k))$,*
- *for every $\theta \in \Theta$, a parametrized path*

$$\gamma_\theta : V_\theta \to \mathrm{R}^k,$$

with base $U_\theta = \mathcal{R}(\theta, \mathrm{Z}(Q, \mathrm{R}^k))$, such that for each $y \in \mathcal{R}(\theta, \mathrm{Z}(Q, \mathrm{R}^k))$, $\mathrm{Im}\ \gamma_\theta(y, \cdot)$ is a semi-algebraic path which connects the point y to a distinguished point a_θ of some roadmap $\mathrm{RM}(\mathrm{Z}(\mathcal{P}' \cup \{Q\}, \mathrm{R}^k))$ where $\mathcal{P}' \subset \mathcal{P}$, staying inside $\mathcal{R}(\overline{\sigma}(y), \mathrm{Z}(Q, \mathrm{R}^k))$.

Moreover, the complexity of the algorithm is $s^{k'+1} d^{O(k^4)}$, where s is a bound on the number of elements of $\mathcal{P}$ and d is a bound on the degrees of Q and the elements of $\mathcal{P}$.

3.2. **Computing higher Betti numbers.** It clear that the Betti numbers of a semi-algebraic set which is closed and bounded can be computed using elementary linear algebra once we have a triangulation of the set. However, triangulations of semi-algebraic sets are expensive to compute, requiring doubly exponential time.

One basic idea that underlies some of the recent progress in designing algorithms for computing the Betti numbers of semi-algebraic sets is that the cohomology groups of a semi-algebraic set can often be computed from a sufficiently well-behaved covering of the set *without having to triangulate the set*.

The idea of computing cohomology from "good" covers is an old one in algebraic topology and the first result in this direction is often called the "Nerve Lemma". In this section we give a brief introduction to the Nerve Lemma and its generalizations.

We first define formally the notion of a cover of a closed, bounded semi-algebraic set.

Definition 3.10 (Cover)**.** Let $S \subset \mathrm{R}^k$ be a closed and bounded semi-algebraic set. A cover, $\mathcal{C}(S)$, of S consists of an ordered index set, which by a slight abuse of language we also denote by $\mathcal{C}(S)$, and a map that associates to each $\alpha \in \mathcal{C}(S)$ a closed and bounded semi-algebraic subset $S_\alpha \subset S$ such that

$$S = \bigcup_{\alpha \in \mathcal{C}(S)} S_\alpha.$$

For $\alpha_0, \ldots, \alpha_p, \in \mathcal{C}(S)$, we associate to the formal product, $\alpha_0 \cdots \alpha_p$, the closed and bounded semi-algebraic set

$$S_{\alpha_0 \cdots \alpha_p} = S_{\alpha_0} \cap \cdots \cap S_{\alpha_p}. \tag{3.1}$$

Recall that the 0-th simplicial cohomology group of a closed and bounded semi-algebraic set X, $\mathrm{H}^0(X)$, can be identified with the $\mathbb{Q}$-vector space of $\mathbb{Q}$-valued locally constant functions on X. Clearly the dimension of $\mathrm{H}^0(X)$ is equal to the number of connected components of X.

For $\alpha_0, \alpha_1, \ldots, \alpha_p, \beta \in \mathcal{C}(S)$, and $\beta \notin \{\alpha_0, \ldots, \alpha_p\}$, let

$$r_{\alpha_0, \ldots, \alpha_p; \beta} : \mathrm{H}^0(S_{\alpha_0 \cdots \alpha_p}) \longrightarrow \mathrm{H}^0(S_{\alpha_0 \cdots \alpha_p \cdot \beta})$$

be the homomorphism defined as follows. Given a locally constant function, $\phi \in \mathrm{H}^0(S_{\alpha_0\cdots\alpha_p})$, $r_{\alpha_0\cdots\alpha_p;\beta}(\phi)$ is the locally constant function on $S_{\alpha_0\cdots\alpha_p\cdot\beta}$ obtained by restricting ϕ to $S_{\alpha_0\cdots\alpha_p\cdot\beta}$.

We define the generalized restriction homomorphisms

$$\delta^p : \bigoplus_{\alpha_0<\cdots<\alpha_p,\alpha_i\in\mathcal{C}(S)} \mathrm{H}^0(S_{\alpha_0\cdots\alpha_p}) \longrightarrow \bigoplus_{\alpha_0<\cdots<\alpha_{p+1},\alpha_i\in\mathcal{C}(S)} \mathrm{H}^0(S_{\alpha_0\cdots\alpha_{p+1}})$$

by

$$\delta^p(\phi)_{\alpha_0\cdots\alpha_{p+1}} = \sum_{0\leq i\leq p+1} (-1)^i r_{\alpha_0\cdots\hat{\alpha_i}\cdots\alpha_{p+1};\alpha_i}(\phi_{\alpha_0\cdots\hat{\alpha_i}\cdots\alpha_{p+1}}), \tag{3.2}$$

where $\phi \in \bigoplus_{\alpha_0<\cdots<\alpha_p\in\mathcal{C}(S)} \mathrm{H}^0(S_{\alpha_0\cdots\alpha_p})$ and $r_{\alpha_0\cdots\hat{\alpha_i}\cdots\alpha_{p+1};\alpha_i}$ is the restriction homomorphism defined previously. The sequence of homomorphisms δ^p gives rise to a complex, $\mathrm{L}^\bullet(\mathcal{C}(S))$, defined by

$$\mathrm{L}^p(\mathcal{C}(S)) = \bigoplus_{\alpha_0<\cdots<\alpha_p,\alpha_i\in\mathcal{C}(S)} \mathrm{H}^0(S_{\alpha_0\cdots\alpha_p}), \tag{3.3}$$

with the differentials $\delta^p : \mathrm{L}^p(\mathcal{C}(S)) \to \mathrm{L}^{p+1}(\mathcal{C}(S))$ defined as in Eqn. (3.2).

Definition 3.11 (Nerve complex)**.** The complex $\mathrm{L}^\bullet(\mathcal{C}(S))$ is called the *nerve complex* of the cover $\mathcal{C}(S)$.

For $\ell \geq 0$ we will denote by $\mathrm{L}^\bullet_\ell(\mathcal{C}(S))$ the truncated complex defined by

$$\begin{aligned}\mathrm{L}^p_\ell(\mathcal{C}(S)) &= \mathrm{L}^p(\mathcal{C}(S)),\ 0 \leq p \leq \ell,\\ &= 0,\ p > \ell.\end{aligned}$$

Notice that once we have a cover of S and we identify the semi-algebraically connected components of the various intersections, $S_{\alpha_0\cdots\alpha_p}$, we have natural bases for the vector spaces

$$\mathrm{L}^p(\mathcal{C}(S)) = \bigoplus_{\alpha_0<\cdots<\alpha_p,\alpha_i\in\mathcal{C}(S)} \mathrm{H}^0(S_{\alpha_0\cdots\alpha_p})$$

appearing as terms of the nerve complex. Moreover, the matrices corresponding to the homomorphisms δ^p in this basis depend only on the inclusion relationships between the semi-algebraically connected components of $S_{\alpha_0\cdots\alpha_{p+1}}$ and those of $S_{\alpha_0\cdots\alpha_p}$.

Definition 3.12 (Leray Property)**.** We say that the cover $\mathcal{C}(S)$ *satisfies the Leray property* if each non-empty intersection $S_{\alpha_0\cdots\alpha_p}$ is contractible.

Clearly, in this case

$$\begin{aligned}\mathrm{H}^0(S_{\alpha_0\cdots\alpha_p}) &\cong \mathbb{Q}, \quad \text{if } S_{\alpha_0\cdots\alpha_p} \neq \emptyset\\ &\cong 0, \quad \text{if } S_{\alpha_0\cdots\alpha_p} = \emptyset.\end{aligned}$$

It is a classical fact (usually referred to as the *Nerve Lemma*) that

Theorem 3.13 (Nerve Lemma)**.** *Suppose that the cover $\mathcal{C}(S)$ satisfies the Leray property. Then for each $i \geq 0$,*

$$\mathrm{H}^i(\mathrm{L}^\bullet(\mathcal{C}(S))) \cong \mathrm{H}^i(S).$$

(See for instance [66] for a proof.)

Remark 3.14. There are several interesting extensions of Theorem 3.13 (Nerve Lemma). For instance, if the Leray property is weakened to say that each t-ary intersection is $(k-t+1)$-connected, then one can conclude that the nerve complex is k-connected. We refer the reader to the article by Björner [27] for more details.

Notice that Theorem 3.13 gives a method for computing the Betti numbers of S using linear algebra from a cover of S by contractible sets for which all non-empty intersections are also contractible, once we are able to test emptiness of the various intersections $S_{\alpha_0 \cdots \alpha_p}$.

Now suppose that each individual member, S_{α_0}, of the cover is contractible, but the various intersections $S_{\alpha_0 \cdots \alpha_p}$ are not necessarily contractible for $p \geq 1$. Theorem 3.13 does not hold in this case. However, the following theorem is proved in [19] and underlies the singly exponential algorithm for computing the first Betti number of semi-algebraic sets described there.

Theorem 3.15. [19] *Suppose that each individual member, S_{α_0}, of the cover $\mathcal{C}(S)$ is contractible. Then,*

$$\mathrm{H}^i(\mathrm{L}_2^\bullet(\mathcal{C}(S))) \cong \mathrm{H}^i(S), \text{ for } i = 0, 1.$$

Remark 3.16. Notice that from a cover by contractible sets Theorem 3.15 allows us to compute using linear algebra, $b_0(S)$ and $b_1(S)$, once we have identified the non-empty semi-algebraically connected components of the pair-wise and triple-wise intersections of the sets in the cover and their inclusion relationships.

3.2.1. *Constructing coverings of closed semi-algebraic sets by closed contractible sets.* The parametrized paths obtained in Theorem 3.9 are not necessarily closed or even contractible, but become so after making appropriate modifications. At the same time it is possible to maintain the covering property, namely for any given $\mathcal{P}$-closed semi-algebraic S set, there exists a set of modified parametrized paths, whose union is S. Moreover, these modified sets are closed and contractible. We omit the details of this (technical) construction referring the reader to [19] for more detail. Putting together the constructions outlined above we have:

Theorem 3.17. *There exists an algorithm that given as input a $\mathcal{P}$-closed and bounded semi-algebraic set S, outputs a set of formulas $\{\phi_1, \ldots, \phi_M\}$ such that*

- *each $\mathcal{R}(\phi_i, \mathrm{R}'^k)$ is semi-algebraically contractible, and*
- $\bigcup_{1 \leq i \leq M} \mathcal{R}(\phi_i, \mathrm{R}'^k) = \mathrm{Ext}(S, \mathrm{R}')$,

where R' is some real closed extension of R. The complexity of the algorithm is bounded by $s^{(k+1)^2} d^{O(k^5)}$, where $s = \mathrm{card}\ \mathcal{P}$ and $d = \max_{P \in \mathcal{P}} deg(P)$.

3.2.2. *Computing the First Betti Number.* It is now an easy consequence of the existence of singly exponential time covering algorithm (Theorem 3.17), and Theorem 3.15 stated above, along with the fact that we can compute descriptions of the semi-algebraically connected components of semi-algebraic sets in singly exponential time, that we can compute the first Betti number of closed and bounded semi-algebraic sets in singly exponential time (see Remark 3.16 above), since the dimensions of the images and kernels of the homomorphisms of the complex, $\mathrm{L}_2^\bullet(\mathcal{C}(S))$ in Theorem 3.15, can then be computed using traditional algorithms from linear algebra. As mentioned earlier, for arbitrary semi-algebraic sets (not necessarily closed and bounded), there is a singly exponential time reduction to the closed and bounded case using the construction of Gabrielov and Vorobjov [40].

3.2.3. *Algorithm for Computing the First Few Betti Numbers.* Using the same ideas as above but with a more complicated recursive procedure to construct a suitable complex one has the following:

Theorem 3.18. [9] *For any given ℓ, there is an algorithm that takes as input a $\mathcal{P}$-formula describing a semi-algebraic set $S \subset \mathrm{R}^k$, and outputs $b_0(S), \ldots, b_\ell(S)$. The complexity of the algorithm is $(sd)^{k^{O(\ell)}}$, where $s = \mathrm{card}\ (\mathcal{P})$ and $d = \max_{P\in\mathcal{P}} \deg(P)$.*

Note that the complexity is singly exponential in k for every fixed ℓ.

3.3. **Computing generalized Euler-Poincaré characteristic.** As mentioned before in Section 2.3.1, efficient algorithms for sign determination of univariate polynomials described in [25, 67] are amongst the most basic algorithms in algorithmic real algebraic geometry. Given $\mathcal{P} \subset \mathrm{R}[X], Q \in \mathrm{R}[X]$ with card $\mathcal{P} = s$, and $\deg(P) \leq d$ for $P \in \mathcal{P} \cup \{Q\}$, these algorithms count for each realizable sign condition of the family $\mathcal{P}$, the cardinality of the set of real zeros of Q, lying in the realization of that sign condition. The complexity of the algorithm in [67] is $sd^{O(1)}$.

In the multidimensional case, it is no longer meaningful to talk about the cardinalities of the zero set of Q lying in the realizations of different sign conditions of $\mathcal{P}$. However, there exists another discrete valuation on semi-algebraic sets that properly generalizes the notion of cardinality. This valuation is the Euler-Poincaré characteristic.

The ***Euler-Poincaré characteristic***, $\chi(S)$, of a closed and bounded semi-algebraic set $S \subset \mathrm{R}^k$ is defined as

$$\chi(S) = \sum_i (-1)^i b_i(S),$$

where $b_i(S)$ is the rank of the i-th simplicial homology group of S. Note that with this definition, $\chi(\emptyset) = 0$, and $\chi(S) = \mathrm{card}\ S$, whenever card $S < \infty$. Moreover, χ is additive.

The Euler-Poincaré characteristic defined above for closed and bounded semi-algebraic set can be extended additively to all semi-algebraic sets. This ***generalized Euler-Poincaré characteristic*** is then a homeomorphism (but not a homotopy) invariant, and establishes an isomorphism between the ***Grothendieck ring,*** $K_0(\mathrm{sa})$, of homeomorphism classes of semi-algebraic sets and $\mathbb{Z}$.

The problem of determining the Euler-Poincaré characteristic of closed semi-algebraic sets was considered in [7] where an algorithm was presented for computing the Euler-Poincaré characteristic of a given closed semi-algebraic set defined by a quantifier-free Boolean formula without negation, with atoms of the form, $P_i \geq 0, P_i \leq 0$, for $1 \leq i \leq s$, $\deg(P_i) \leq d$. The complexity of the algorithm is $(ksd)^{O(k)}$. Moreover, in the special case when the coefficients of the polynomials in $\mathcal{P}$ are integers of bit lengths bounded by τ, the algorithm performs at most $(ksd)^{O(k)}\tau^{O(1)}$ bit operations.

The following result (which should be viewed as a generalization of the univariate sign determination algorithm) appears in [17].

Theorem 3.19. *There exists an algorithm which given an algebraic set $Z = \mathrm{Z}(Q, \mathrm{R}^k) \subset \mathrm{R}^k$ and a finite set of polynomials $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathrm{R}[X_1, \ldots, X_k]$, computes the list $\chi(\mathcal{P}, Z)$ indexed by elements, σ, of $\mathrm{Sign}(\mathcal{P}, Z)$. If the degrees of the polynomials in $\mathcal{P} \cup \{Q\}$ are bounded by d, and the real dimension of $Z = \mathrm{Z}(Q, \mathrm{R}^k)$*

is k', then the complexity of the algorithm is

$$s^{k'+1}O(d)^k + s^{k'}((k'\log_2(s) + k\log_2(d))d)^{O(k)}.$$

If the coefficients of the polynomials in $\mathcal{P} \cup \{Q\}$ are integers of bit-sizes bounded by τ, then the bit-sizes of the integers appearing in the intermediate computations and the output are bounded by $\tau((k'\log_2(s) + k\log_2(d))d)^{O(k)}$.

3.4. **Relation between the complexity of quantifier elimination and the complexity of computing Betti numbers.** It is clear from the previous sections that there are two important strands of research in algorithms in real algebraic geometry, namely

(1) Algorithms for deciding sentences in the first-order theory of the reals (with several blocks of quantifiers);
(2) Computing topological invariants of semi-algebraic sets (such as their Betti numbers).

While these two classes of problems might seem quite different, the following reduction result gives a polynomial time reduction of the problem of deciding quantified sentences in the first order theory of the reals with a fixed number of quantifiers to the problem of computing Betti numbers of semi-algebraic sets. For technical reasons, the reduction is only proved for a certain sub-class of formulas which is defined more precisely below.

Definition 3.20. (Compact general decision problem with at most ω quantifier alternations ($\mathbf{GDP}^{\mathbf{c}}_{\omega}$))

Input. A sentence Φ in the first order theory of R

$$(Q_1\mathbf{X}^1 \in \mathbf{S}^{k_1}) \cdots (Q_\omega \mathbf{X}^\omega \in \mathbf{S}^{k_\omega})\phi(\mathbf{X}^1, \ldots, \mathbf{X}^\omega),$$

where for each $i, 1 \leq i \leq \omega$, $\mathbf{X}^i = (X^i_0, \ldots, X^i_{k_i})$ is a block of k_i+1 variables, $Q_i \in \{\exists, \forall\}$, with $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, and ϕ is a quantifier-free formula defining a *closed* semi-algebraic subset S of $\mathbf{S}^{k_1} \times \cdots \times \mathbf{S}^{k_\omega}$.

Output. True or False depending on whether Φ is true or false in the first order theory of R.

NOTATION 3. For any semi-algebraic set $S \subset \mathrm{R}^k$, we denote by $P_S(T)$, denote the ***Poincaré polynomial*** of S – namely,

$$P_S(T) := \sum_{i \geq 0} b_i(S)\, T^i.$$

Definition 3.21. (Computing the Poincaré polynomial of semi-algebraic sets (**Poincaré**))

Input. A quantifier-free formula defining a semi-algebraic set $S \subset \mathrm{R}^k$.
Output. The Poincaré polynomial $P_S(T)$.

The following reduction result appears in [24]. It says that with a mild hypothesis of compactness, the General Decision Problem with a fixed number of quantifier alternations can be reduced in polynomial time to the problem of computing Betti numbers of semi-algebraic sets.

Theorem 3.22. *For every $\omega > 0$, there is a deterministic polynomial time reduction of* $\mathbf{GDP}^{\mathbf{c}}_{\omega}$ *to* **Poincaré**.

The main ingredients in the proof of Theorem 3.22 is an efficient semi-algebraic realization of the iterated fibered join of a semi-algebraic set with itself over a semi-algebraic map, and Alexander duality that allows one to express the Poincaré polynomial of a semi-algebraic subset of the sphere in terms of its complement in the sphere.

3.5. **Effective semi-algebraic triangulation and stratification.** As mentioned above in Section 2.1.2 one obtains an algorithm for computing a semi-algebraic triangulation of semi-algebraic sets using cylindrical algebraic decomposition (after making a generic linear change of co-ordinates). The complexity of this is algorithm dominated by the cost of the performing the cylindrical algebraic decomposition, and is thus doubly exponential.

Algorithms for computing stratifications of semi-algebraic sets, such that the strata satisfy additional regularity conditions (such as Whitney conditions (a) and (b)) have been considered by several authors. Rannou [63] gave an algorithm for obtaining stratification with regularity conditions that imply the Whitney conditions. The complexity of this algorithm is doubly exponential in the depth of the stratification. Finding a singly exponential algorithm for computing stratifications of semi-algebraic sets remains a major open problem (see Section 5).

3.6. **Semi-algebraic sets defined by quadratic and partially quadratic systems.** A restricted class of semi-algebraic sets - namely, semi-algebraic sets defined by quadratic inequalities – has been considered by several researchers [4, 5, 45, 12]. As in the case of general semi-algebraic sets, the Betti numbers of such sets can be exponentially large in the number of variables, as can be seen in the following example.

Example 3.23. The set $S \subset \mathrm{R}^\ell$ defined by

$$Y_1(Y_1 - 1) \geq 0, \ldots, Y_\ell(Y_\ell - 1) \geq 0$$

satisfies $b_0(S) = 2^\ell$.

However, it turns out that for a semi-algebraic set $S \subset \mathrm{R}^\ell$ defined by m quadratic inequalities, it is possible to obtain upper bounds on the Betti numbers of S which are polynomial in ℓ and exponential only in m. The first such result is due to Barvinok [5], who proved the following theorem.

Theorem 3.24. [5] *Let $S \subset \mathrm{R}^\ell$ be defined by $Q_1 \geq 0, \ldots, Q_m \geq 0$, $\deg(Q_i) \leq 2, 1 \leq i \leq m$. Then $b(S) \leq \ell^{O(m)}$.*

Remark 3.25. Notice that the bound in Theorem 3.24 is polynomial in the dimension ℓ for fixed m, and this fact depends crucially on the assumption that the degrees of the polynomials $Q_1, \ldots, Q_m$ are at most two. For instance, the semi-algebraic set defined by a *single* polynomial of degree 4 can have Betti numbers exponentially large in ℓ, as exhibited by the semi-algebraic subset of R^ℓ defined by

$$\sum_{i=0}^{\ell} Y_i^2(Y_i - 1)^2 \leq 0.$$

The above example illustrates the delicate nature of the bound in Theorem 3.24, since a single inequality of degree 4 is enough to destroy the polynomial nature of the bound. In contrast to this, it is shown in Theorem 3.30 below that a polynomial

bound on the Betti numbers of S continues to hold, even if we allow a few (meaning any constant number) of the variables to occur with degrees larger than two in the polynomials used to describe the set S.

The bound on the sum of all the Betti numbers in Theorem 3.24 has exponential dependence on the number of inequalities. This dependence is unavoidable, since the semi-algebraic set $S \subset \mathrm{R}^k$ defined by

$$X_1(1 - X_1) \leq 0, \ldots, X_k(1 - X_k) \leq 0,$$

has $b_0(S) = 2^k$.

Hence, it is somewhat surprising that for any fixed constant ℓ, the Betti numbers $b_{k-1}(S), \ldots, b_{k-\ell}(S)$, of a basic closed semi-algebraic set $S \subset \mathrm{R}^k$ defined by quadratic inequalities, are polynomially bounded. The following theorem appears in [8].

Theorem 3.26. *Let* R *a real closed field and* $S \subset \mathrm{R}^k$ *be defined by*

$$P_1 \leq 0, \ldots, P_s \leq 0, \deg(P_i) \leq 2, 1 \leq i \leq s.$$

Then, for $\ell \geq 0$,

$$b_{k-\ell}(S) \leq \binom{s}{\ell} k^{O(\ell)}.$$

3.6.1. *Algorithm for testing emptiness.* The problem of deciding whether a given semi-algebraic set defined by a finite set of quadratic inequalities is empty or not was considered first by Barvinok [4] who proved the following theorem.

Theorem 3.27. [4] *There exists an algorithm which decides if a given system of inequalities* $Q_1 \geq 0, \ldots, Q_\ell \geq 0$, *with each* $Q_i \in \mathrm{R}[X_1, \ldots, X_k], \deg(Q_i) \leq 2$, *has a solution in* R^k, *whose complexity is bounded by* $k^{O(\ell)}$.

Barvinok's algorithm did not produce explicit sample points meeting every semi-algebraically connected component of the set of solutions (in the style of Theorem 2.15 in the general case). This was done by Grigoriev and Pasechnik [45]. In fact, they consider the following more general situation.

Let $S \subset \mathrm{R}^k$ be the pull-back of a $\mathcal{P}$-semi-algebraic subset $T \subset \mathrm{R}^\ell$ via a quadratic map $Q = (Q_1, \ldots, Q_\ell) : \mathrm{R}^k \to \mathrm{R}^\ell$, where $\mathcal{P} \subset \mathrm{R}[Y_1, \ldots, Y_\ell]$, $Q_1, \ldots, Q_\ell \in \mathrm{R}[X_1, \ldots, X_k]$ with $\deg(Q_i) \leq 2$ for $i = 1, \ldots, \ell$.

In [45] Grigoriev and Pasechnik give an algorithm that computes a set of sample points guaranteed to meet every semi-algebraically connected component of S whose complexity is bounded by $(ksd)^{O(\ell)}$ where $s = \text{card } \mathcal{P}$, and d is a bound on the degrees of the polynomials in $\mathcal{P}$.

Remark 3.28. Note that the problem of deciding the feasibility of even one quartic real polynomial equation is an **NP**-hard problem, and the same is true for systems of quadratic equations. Thus, there is little hope for obtaining a polynomial-time algorithm for either of these problems. The above results are somewhat surprising in that they imply in the quadratic case one obtains polynomial time algorithms for testing feasibility, provided the number of polynomials is kept fixed (see also Section 3.6.3 below). We refer the reader to [56] and [29] for precise definitions of the computational complexity classes that we refer to here and elsewhere in this survey.

3.6.2. *Computing the top few Betti numbers of basic semi-algebraic sets defined by quadratic inequalities.* Motivated by the polynomial bound on the top few Betti numbers of sets defined by quadratic inequalities (Theorem 3.26), the problem of obtaining a polynomial time algorithm to compute these numbers was investigated in [11] where the following result is proved.

Theorem 3.29. [11] *There exists an algorithm which given a set of s polynomials, $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathrm{R}[X_1, \ldots, X_k]$, with $\deg(P_i) \leq 2, 1 \leq i \leq s$, computes $b_{k-1}(S), \ldots, b_{k-\ell}(S)$, where S is the set defined by $P_1 \leq 0, \ldots, P_s \leq 0$. The complexity of the algorithm is*

$$\sum_{i=0}^{\ell+2} \binom{s}{i} k^{2^{O(\min(\ell,s))}}. \tag{3.4}$$

If the coefficients of the polynomials in $\mathcal{P}$ are integers of bit-sizes bounded by τ, then the bit-sizes of the integers appearing in the intermediate computations and the output are bounded by $\tau(sk)^{2^{O(\min(\ell,s))}}$.

3.6.3. *Significance from the computational complexity theory viewpoint.* Semi-algebraic sets defined by a system of quadratic inequalities have a special significance in the theory of computational complexity. Even though such sets might seem to be the next simplest class of semi-algebraic sets after sets defined by linear inequalities, from the point of view of computational complexity they represent a quantum leap. Whereas there exist (weakly) polynomial time algorithms for solving linear programming, solving quadratic feasibility problem is provably hard. For instance, it follows from an easy reduction from the problem of testing feasibility of a real quartic equation in many variables, that the problem of testing whether a system of quadratic inequalities is feasible is $\mathbf{NP}_{\mathrm{R}}$-complete in the Blum-Shub-Smale model of computation (see [29]). Assuming the input polynomials to have integer coefficients, the same problem is **NP**-hard in the classical Turing machine model, since it is also not difficult to see that the Boolean satisfiability problem can be posed as the problem of deciding whether a certain semi-algebraic set defined by quadratic inequalities is empty or not. Counting the number of semi-algebraically connected components of such sets is even harder. In fact, it is **PSPACE**-hard [64] (**PSPACE** is a complexity class which contains the entire polynomial hierarchy), and the proof of this results extend easily to the quadratic case. Moreover, it is proved in [11] for $\ell = O(\log k)$, computing the ℓ-th Betti number of a basic semi-algebraic set defined by quadratic inequalities in R^k is **PSPACE**-hard. In view of these hardness results, it is unlikely that there exist polynomial time algorithms for computing the Betti numbers (or even the first few Betti numbers) of such a set.

From this point of view, Theorem 3.29 is quite surprising, since it gives a polynomial time algorithm for computing certain Betti numbers of a class of semi-algebraic sets for which computing the zero-th Betti number is already **PSPACE**-hard.

3.6.4. *Semi-algebraic sets defined by partially quadratic systems.* We have discussed topological as well as algorithmic results concerning general semi-algebraic sets, as well as those defined by quadratic constraints In [23], the authors try to interpolate between results known for general semi-algebraic sets (defined by polynomials of arbitrary degrees) and those known for semi-algebraic sets defined by polynomials of degree at most 2. In order to do so they consider semi-algebraic sets defined by polynomial inequalities, in which the dependence of the polynomials on

a *subset of the variables* is at most quadratic. As a result we obtain common generalizations of the bounds stated in Theorems 3.2 and 3.24. Given any polynomial $P \in \mathrm{R}[X_1, \ldots, X_k, Y_1, \ldots, Y_\ell]$, we will denote by $\deg_X(P)$ (resp. $\deg_Y(P)$) the total degree of P with respect to the variables $X_1, \ldots, X_k$ (resp. $Y_1, \ldots, Y_\ell$).

Denote by

- $\mathcal{Q} \subset \mathrm{R}[Y_1, \ldots, Y_\ell, X_1, \ldots, X_k]$, a family of polynomials with
$$\deg_Y(Q) \leq 2, \deg_X(Q) \leq d, Q \in \mathcal{Q}, \mathrm{card}\ \mathcal{Q} = m,$$
- $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$, a family of polynomials with
$$\deg_X(P) \leq d, P \in \mathcal{P}, \mathrm{card}\ \mathcal{P} = s.$$

The following theorem that interpolates between Theorems 3.1 and 3.24 above is proved in [23].

Theorem 3.30. *Let $S \subset \mathrm{R}^{\ell+k}$ be a $(\mathcal{P} \cup \mathcal{Q})$-closed semi-algebraic set. Then*
$$b(S) \leq \ell^2(O(s+\ell+m)\ell d)^{k+2m}.$$
In particular, for $m \leq \ell$, we have $b(S) \leq \ell^2(O(s+\ell)\ell d)^{k+2m}$.

Notice that Theorem 3.30 can be seen as a common generalization of Theorems 3.2 and 3.24, in the sense that we recover similar bounds (that is bounds having the same shape) as in Theorem 3.2 (respectively Theorem 3.24) by setting ℓ and m (respectively s, d and k) to $O(1)$.

Note also that as a special case of Theorem 3.30 we obtain a bound on the sum of the Betti numbers of a semi-algebraic set defined over a quadratic map. As mentioned before, such sets have been considered from an algorithmic point of view in [45], where an efficient algorithm is described for computing sample points in every semi-algebraically connected component, as well as testing emptiness, of such sets.

More precisely we have:

Corollary 3.31. *Let $Q = (Q_1, \ldots, Q_k) : \mathrm{R}^\ell \to \mathrm{R}^k$ be a map where each $Q_i \in \mathrm{R}[Y_1, \ldots, Y_\ell]$ and $\deg(Q_i) \leq 2$. Let $V \subset \mathrm{R}^k$ be a $\mathcal{P}$-closed semi-algebraic set for some family $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$, with $\mathrm{card}\ \mathcal{P} = s$ and $\deg(P) \leq d, P \in \mathcal{P}$. Let $S = Q^{-1}(V)$. Then*
$$b(S) \leq \ell^2(O(s+\ell+k)\ell d)^{3k}.$$

The techniques developed in this paper for obtaining tight bounds on the Betti numbers of semi-algebraic sets defined by partly quadratic systems of polynomials also pave the way towards designing more efficient algorithms for computing the Euler-Poincaré characteristic as well as the Betti numbers of such sets.

The following theorem appears in [23].

Theorem 3.32. *There exists an algorithm that takes as input the description of a $(\mathcal{P} \cup \mathcal{Q})$-closed semi-algebraic set S (following the same notation as in Theorem 3.30) and outputs its the Euler-Poincaré characteristic $\chi(S)$. The complexity of this algorithm is bounded by $(\ell s m d)^{O(m(m+k))}$. In the case when S is a basic closed semi-algebraic set the complexity of the algorithm is $(\ell s m d)^{O(m+k)}$.*

The algorithm for computing all the Betti numbers has complexity $(\ell s m d)^{2^{O(m+k)}}$ and its description can be found in [22]. While the complexity of both the algorithms discussed above is *polynomial* for fixed m and k, the complexity of the algorithm

for computing the Euler-Poincaré characteristic is significantly better than that of the algorithm for computing all the Betti numbers.

Note that the first versions of both these algorithms for computing the Euler-Poincaré characteristic as well as the Betti numbers of semi-algebraic sets defined by purely quadratic constraints having complexity which is polynomial for fixed number of constraints, appeared first in [10] and [11] respectively. The extensions of these algorithms to semi-algebraic sets defined by partially quadratic systems were made in [23] and [22] respectively.

These latter results indicate that the problem of computing the Betti numbers of semi-algebraic sets defined by a constant number of polynomial inequalities is solvable in polynomial time, even if we allow a small (constant sized) subset of the variables to occur with degrees larger than two in the polynomials defining the given set.

4. Sums of squares and semi-definite programming

All the algorithms surveyed above have the feature that they are exact, and most of them work over arbitrary real closed fields (even non-archimedean ones). For example, the ring generated by the coefficients, D, could be the ordered ring, $\mathbb{Z}[\varepsilon]$ with ε positive and infinitesimal, contained in the real closed field $\mathrm{R} = \mathbb{R}_{\mathrm{alg}}\langle\varepsilon\rangle$ and all algorithms reported above would still work without any modification.

There are some other approaches to designing algorithms for solving systems of real polynomial equations or testing emptiness of semi-algebraic sets that deserve mention. These approaches strictly assume that the underlying real closed field is the field $\mathbb{R}$ of real numbers, and the computations are done with some finite precision. In other words, the algorithms are numerical rather than exact, and as such there is some possibility of error in the outputs. These algorithms are often used in practical applications, where exact or symbolic algorithms are deemed to be too expensive and small errors are considered not very significant.

We mention one such approach below.

4.1. **Deciding non-negativity of polynomials using sums-of-squares.** The problem is to decide whether a given polynomial $P \in \mathbb{R}[X_1, \ldots, X_k]$ is non-negative in $\mathbb{R}^k$. More generally, the problem is to decide whether a given polynomial $P \in \mathbb{R}[X_1, \ldots, X_k]$ is non-negative over a given basic, semi-algebraic subset $K \subset \mathbb{R}^k$.

There are also optimization versions of these problems namely.

Given $P \in \mathbb{R}[X_1, \ldots, X_k]$ compute

$$p^{\min} := \inf_{x \in \mathbb{R}^k} P(x).$$

More generally, Given $P \in \mathbb{R}[X_1, \ldots, X_k]$ and $K \subset \mathbb{R}^k$ a basic semi-algebraic set, compute

$$p^{\min} := \inf_{x \in K} P(x).$$

For purposes of exposition we concentrate on the first versions of these problems.

Let the degree of P be $2d$ and let $\mathrm{Pos}_{k,d}$ (resp. $\Sigma_{k,d}$) denote the cone of non-negative polynomials (resp. cone of sum of squares) in $\mathbb{R}[X_1, \ldots, X_k]$ of degree at most $2d$. Clearly $\Sigma_{k,d} \subset \mathrm{Pos}_{k,d}$ and as known since Hilbert, the inclusion is strict unless the pair (k, d) is of the form $(1, d), (k, 1)$ or $(k, d) = (2, 2)$ [30, Chapter 6]. Note that the cones $\mathrm{Pos}_{k,d}$ are in general not understood very well (for instance, their face structure, extreme rays etc.) and testing membership in them is clearly an

NP-hard problem. On the other hand, the cones $\Sigma_{k,d}$ are relatively well understood and membership in $\Sigma_{k,d}$ can be tested via semi-definite programming as a result of the following theorem.

For any symmetric, square matrix $X \in \mathbb{R}^{k\times k}$, we let $X \succeq 0$ denote that X is positive, semi-definite. For each $k, d \geq 0$, we denote by $\mathcal{M}_{k,d}$ the set of exponent vectors $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k$ with $|\alpha| = \sum_{i=1}^k \alpha_i \leq d$.

Theorem 4.1. [32, 61] *The following are equivalent.*

(1) $P = \sum_{\alpha\in\mathcal{M}_{k,d}} p_\alpha X^\alpha \in \Sigma_{k,d}$.

(2) *The following system in matrix variables* $X = (X_{\alpha,\beta})_{\alpha,\beta\in\mathcal{M}_{k,d}}$ *is feasible:*

$$\begin{aligned} X &\succeq 0 \\ \sum_{\beta,\gamma\in\mathcal{M}_{k,d},\beta+\gamma=\alpha} X_{\beta,\gamma} &= p_\alpha, \alpha \in \mathcal{M}_{k,2d}. \end{aligned}$$

The feasibility problem in the above theorem is an instance of the feasibility problem in the theory of ***semi-definite programming***. Semi-definite programming (or semi-definite optimization) is a generalization of linear programming, where the problem is to optimize a linear functional over some affine section of the cone of real symmetric positive semi-definite matrices in the space of $k \times k$ real symmetric matrices. Because of its wide ranging applicability, semi-definite programming has been the focus of intense effort on the part of researchers in optimization for developing efficient algorithms for solving semi-definite programming problems. As a result very efficient algorithms based on "interior point methods" (see [55]) have been developed for solving semi-definite optimization problems such as the one in Theorem 4.1. These algorithms are very efficient in practice, but there seems to be no definitive mathematical result which states that the running time is polynomial (in the bit-size of the input) (unlike in the case of linear programming).

Note that the polynomial optimization problems can also be "approximated" using the sum of squares cone just like above. For example, in order to compute

$$p^{\min} := \inf_{x\in\mathbb{R}^k} P(x) = \sup\{\rho \in \mathbb{R} \mid P - \rho \in \mathrm{Pos}_{k,d}\},$$

one computes

$$p^{\mathrm{sos}} := \sup\{\rho \in \mathbb{R} \mid P - \rho \in \Sigma_{k,d}\}.$$

Since, this latter problem is an example of semi-definite *optimization* problem and can be solved in practice using efficient interior points methods. Also note that since the latter problem involves optimization over a smaller cone we have that

$$p^{\mathrm{sos}} \leq p^{\min}.$$

The idea of "relaxing" polynomial optimization problems to semi-definite programming has been utilized by Lasserre [48, 50, 49], Parrilo [57] and others to obtain algorithms for performing polynomial optimization which perform well in practice (but see Remark 4.2 below).

Remark 4.2. While the idea of approximating the cone of non-negative polynomials by the smaller cone of sums of square seems to work well in practice for solving or approximating well solutions of polynomial optimization problems, one should be aware of certain negative results. Blekherman [28] proved that the ratio of the volumes of certain fixed sections of the cones $\Sigma_{k,d}$ and $\mathrm{Pos}_{k,d}$ goes to 0 with k

exponentially fast. This seems to indicate that the approximation of $\mathrm{Pos}_{k,d}$ by $\Sigma_{k,d}$ is very inaccurate as k grows (with d fixed).

We refer the reader to the excellent survey article by Laurent [51] for more detailed information about the sums-of-squares methods in algorithmic real algebraic geometry.

4.2. **Complexity of semi-definite programming.** Since semi-definite optimization problems play an important role in the sums-of-square approximation algorithms described above, it is important to be aware of the current complexity status of this problem. As noted above, while interior points algorithms for solving semi-definite programming problems are extremely efficient in practice, there is no definite result known placing the semi-definite programming problem in the class **P**. Khachiyan and Prokolab [60] proved that there exists a polynomial time algorithm for semi-definite programming in case the dimension is fixed. Using results proved by Ramana [62] on exact semi-definite duality theory, it can be deduced (see [71]) that semi-definite feasibility cannot be **NP**-complete unless **NP** = **co-NP** (a hypothesis not believed to be true). In the Blum-Shub-Smale model of computation over real machines [29], the semi-definite feasibility problem is clearly in the class $\mathbf{NP}_{\mathbb{R}}$, and it is unknown if it is any easier than ordinary real polynomial feasibility problem in this model.

5. Open problems

We list here some interesting open problems some of which could possibly be tackled in the near future.

Computing Betti numbers in singly exponential time ? Suppose $S \subset \mathrm{R}^k$ is a semi-algebraic set defined in terms of s polynomials, of degrees bounded by d. One of the most fundamental open questions in algorithmic semi-algebraic geometry, is whether there exists a singly exponential (in k) time algorithm for computing the Betti numbers of S. The best we can do so far is summarized in Theorem 3.18 which gives the existence of singly exponential time algorithms for computing the first ℓ Betti numbers of S for any constant ℓ. A big challenge is to extend these ideas to design an algorithm for computing all the Betti numbers of S.

Computing semi-algebraic triangulations in singly exponential time ? A related question is whether there exists an algorithm for computing semi-algebraic triangulations with singly exponential complexity. Clearly, such an algorithm would also make possible the computation of Betti numbers in singly exponential time.

More Efficient Algorithms for Computing the Number of Connected Components in the Quadratic Case ? As described in Section 3.6 for semi-algebraic sets in R^k defined by ℓ quadratic inequalities, there are algorithms for deciding emptiness, as well as computing sample points in every semi-algebraically connected component whose complexity is bounded by $k^{O(\ell)}$. We also have an algorithm for computing the Euler-Poincaré characteristic of such sets whose complexity is $k^{O(\ell)}$. However, the best known algorithm for computing the number of semi-algebraically connected components of such sets has complexity $k^{2^{O(\ell)}}$ (as a special case of the algorithm

for computing all the Betti numbers given in Theorem 3.26). This raises the question whether there exists a more efficient algorithm with complexity $k^{O(\ell)}$ or even $k^{O(\ell^2)}$ for counting the number of semi-algebraically connected components of such sets. Roadmap type constructions used for counting semi-algebraically connected components in the case of general semi-algebraic sets cannot be directly employed in this context, because such algorithms will have complexity exponential in k. Recent work by Coste and Moussa [36] on the geodesic diameter of semi-algebraic sets defined by few quadratic inequalities might contain some relevant hints towards this goal.

More Efficient Algorithms for Computing the Number of Connected Components for General Semi-algebraic Sets ? A very interesting open question is whether the exponent $O(k^2)$ in the complexity of roadmap algorithms (cf. Theorem 3.6) can be improved to $O(k)$, so that the complexity of testing connectivity becomes asymptotically the same as that of testing emptiness of a semi-algebraic set (cf. Theorem 2.15). Recent improvements in the complexity of roadmap algorithms described in Section 3.1.2 above, certainly gives some hope in this regard.

Such an improvement would go a long way in making this algorithm practically useful. It would also be of interest for studying metric properties of semi-algebraic sets because of the following. Applying Crofton's formula from integral geometry one immediately obtains as a corollary of Theorem 3.6 (using the same notation as in the theorem) an upper bound of $s^{k'+1}d^{O(k^2)}$ on the length of a semi-algebraic connecting path connecting two points in any semi-algebraically connected component of S (assuming that S is contained in the unit ball centered at the origin). An improvement in the complexity of algorithms for constructing connecting paths (such as the roadmap algorithm) would also improve the bound on the length of connecting paths. Recent results due to D'Acunto and Kurdyka [37] show that it is possible to construct semi-algebraic paths of length $d^{O(k)}$ between two points of S (assuming that S is a semi-algebraically connected component of a real algebraic set contained in the unit ball defined by polynomials of degree d). However, the semi-algebraic complexity of such paths cannot be bounded in terms of the parameters d and k. The improvement in the complexity suggested above, apart from its algorithmic significance, would also be an effective version of the results in [37].

Remove the compactness assumption in Theorem 3.22. More generally, investigate the role of compactness in the Blum-Shub-Smale model of computations over real closed fields (see [24] for more details).

6. Acknowledgment

The author was partially supported by an NSF grant CCF-0915954.

References

[1] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop. Polar varieties, real equation solving, and data structures: the hypersurface case. *J. Complexity*, 13(1):5–27, 1997.

[2] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop. Polar varieties and efficient real elimination. *Math. Z.*, 238(1):115–144, 2001.

[3] Bernd Bank, Marc Giusti, Joos Heintz, Mohab Safey El Din, and Eric Schost. On the geometry of polar varieties. *Appl. Algebra Engrg. Comm. Comput.*, 21(1):33–83, 2010.

[4] A. I. Barvinok. Feasibility testing for systems of real quadratic equations. *Discrete Comput. Geom.*, 10(1):1–13, 1993.
[5] A. I. Barvinok. On the Betti numbers of semialgebraic sets defined by few quadratic inequalities. *Math. Z.*, 225(2):231–244, 1997.
[6] S. Basu. New results on quantifier elimination over real closed fields and applications to constraint databases. *J. ACM*, 46(4):537–555, 1999.
[7] S. Basu. On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets. *Discrete Comput. Geom.*, 22(1):1–18, 1999.
[8] S. Basu. Different bounds on the different Betti numbers of semi-algebraic sets. *Discrete Comput. Geom.*, 30(1):65–85, 2003. ACM Symposium on Computational Geometry (Medford, MA, 2001).
[9] S. Basu. Computing the first few Betti numbers of semi-algebraic sets in single exponential time. *J. Symbolic Comput.*, 41(10):1125–1154, 2006.
[10] S. Basu. Efficient algorithm for computing the Euler-Poincaré characteristic of a semi-algebraic set defined by few quadratic inequalities. *Comput. Complexity*, 15(3):236–251, 2006.
[11] S. Basu. Computing the top few Betti numbers of semi-algebraic sets defined by quadratic inequalities in polynomial time. *Found. Comput. Math.*, 8(1):45–80, 2008.
[12] S. Basu and M. Kettner. A sharper estimate on the Betti numbers of sets defined by quadratic inequalities. *Discrete Comput. Geom.*, 39(4):734–746, 2008.
[13] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, 1996.
[14] S. Basu, R. Pollack, and M.-F. Roy. On computing a set of points meeting every cell defined by a family of polynomials on a variety. *J. Complexity*, 13(1):28–37, 1997.
[15] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety. *J. Amer. Math. Soc.*, 13(1):55–82, 2000.
[16] S. Basu, R. Pollack, and M.-F. Roy. Betti number bounds, applications and algorithms. In *Current Trends in Combinatorial and Computational Geometry: Papers from the Special Program at MSRI*, volume 52 of *MSRI Publications*, pages 87–97. Cambridge University Press, 2005.
[17] S. Basu, R. Pollack, and M.-F. Roy. Computing the Euler-Poincaré characteristics of sign conditions. *Comput. Complexity*, 14(1):53–71, 2005.
[18] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006 (second edition).
[19] S. Basu, R. Pollack, and M.-F. Roy. Computing the first Betti number of a semi-algebraic set. *Found. Comput. Math.*, 8(1):97–136, 2008.
[20] Saugata Basu, Marie-Françoise Roy, Mohab Safey El Din, and Eric Schost. Baby step-giant step roadmap algorithm for general algebraic sets. *manuscript*.
[21] Saugata Basu, Andrei Gabrielov, and Nicolai Vorobjov. Semi-monotone sets. *arXiv:1004.5047v1 [math.LO]*.
[22] Saugata Basu, Dmitrii V. Pasechnik, and Marie-Françoise Roy. Computing the Betti numbers of semi-algebraic sets defined by partly quadratic sytems of polynomials. *J. Algebra*, 321(8):2206–2229, 2009.
[23] Saugata Basu, Dmitrii V. Pasechnik, and Marie-Françoise Roy. Bounding the Betti numbers and computing the Euler-Poincaré characteristic of semi-algebraic sets defined by partly quadratic systems of polynomials. *J. Eur. Math. Soc. (JEMS)*, 12(2):529–553, 2010.
[24] Saugata Basu and Thierry Zell. Polynomial hierarchy, Betti numbers, and a real analogue of Toda's theorem. *Found. Comput. Math.*, 10(4):429–454, 2010.
[25] M. Ben-Or, D. Kozen, and J. Reif. The complexity of elementary algebra and geometry. *J. of Computer and Systems Sciences*, 18:251–264, 1986.
[26] Michael Benedikt, Guozhu Dong, Leonid Libkin, and Limsoon Wong. Relational expressive power of constraint query languages. *J. ACM*, 45(1):1–34, 1998.
[27] A. Björner. Topological methods. In R. Graham, M. Grotschel, and L. Lovasz, editors, *Handbook of Combinatorics*, volume II, pages 1819–1872. North-Holland/Elsevier, 1995.
[28] Grigoriy Blekherman. There are significantly more nonnegative polynomials than sums of squares. *Israel J. Math.*, 153:355–380, 2006.
[29] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.

[30] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie algébrique réelle (Second edition in english: Real Algebraic Geometry)*, volume 12 (36) of *Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]*. Springer-Verlag, Berlin, 1987 (1998).

[31] J. Canny. Computing road maps in general semi-algebraic sets. *The Computer Journal*, 36:504–514, 1993.

[32] M. D. Choi, T. Y. Lam, and B. Reznick. Sums of squares of real polynomials. In *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*, volume 58 of *Proc. Sympos. Pure Math.*, pages 103–126. Amer. Math. Soc., Providence, RI, 1995.

[33] G. E. Collins. Quantifier elimination for real closed fields by cylindric algebraic decomposition. In *Second GI Conference on Automata Theory and Formal Languages*, volume 33 of *Lecture Notes in Computer Science*, pages 134–183, Berlin, 1975. Springer- Verlag.

[34] G.E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *LNCS*, 33:134–183, 1975.

[35] M. Coste and M.-F. Roy. Thom's lemma, the coding of real algebraic numbers and the topology of semi-algebraic sets. *Journal of Symbolic Computation*, 5(1/2):121–129, 1988.

[36] Michel Coste and Seydou Moussa. Geodesic diameter of sets defined by few quadratic equations and inequalities. *arXiv:1004.5047v1 [math.LO]*.

[37] D. D'Acunto and K. Kurdyka. Bounds for gradient trajectories and geodesic diameter of real algebraic sets. *Bull. London Math. Soc.*, 38(6):951–965, 2006.

[38] James H. Davenport and Joos Heintz. Real quantifier elimination is doubly exponential. *J. Symbolic Comput.*, 5(1-2):29–35, 1988.

[39] Mohab Safey el Din and Eric Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete Comput. Geom.*, 45(1):181–220, 2010.

[40] A. Gabrielov and N. Vorobjov. Betti numbers of semialgebraic sets defined by quantifier-free formulae. *Discrete Comput. Geom.*, 33(3):395–401, 2005.

[41] Andrei Gabrielov and Nicolai Vorobjov. Approximation of definable sets by compact families, and upper bounds on homotopy and homology. *J. Lond. Math. Soc. (2)*, 80(1):35–54, 2009.

[42] L. Gournay and J. J. Risler. Construction of roadmaps of semi-algebraic sets. *Appl. Algebra Eng. Commun. Comput.*, 4(4):239–252, 1993.

[43] D. Grigoriev and N. Vorobjov. Counting connected components of a semi-algebraic set in subexponential time. *Comput. Complexity*, 2(2):133–186, 1992.

[44] D. Yu. Grigoriev and N. N. Vorobjov, Jr. Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Comput.*, 5(1-2):37–64, 1988.

[45] Dima Grigoriev and Dmitrii V. Pasechnik. Polynomial-time computing over quadratic maps. I. Sampling in real algebraic sets. *Comput. Complexity*, 14(1):20–52, 2005.

[46] 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*, 11:121–140, 1994.

[47] Gabriela Jeronimo, Daniel Perrucci, and Juan Sabia. On sign conditions over real multivariate polynomials. *Discrete Comput. Geom.*, 44(1):195–222, 2010.

[48] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817 (electronic), 2000/01.

[49] Jean B. Lasserre. Convergent SDP-relaxations in polynomial optimization with sparsity. *SIAM J. Optim.*, 17(3):822–843 (electronic), 2006.

[50] Jean B. Lasserre. A sum of squares approximation of nonnegative polynomials. *SIAM J. Optim.*, 16(3):751–765 (electronic), 2006.

[51] Monique Laurent. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*, volume 149 of *IMA Vol. Math. Appl.*, pages 157–270. Springer, New York, 2009.

[52] S. Lojasiewicz. Triangulation of semi-analytic sets. *Ann. Scuola Norm. Sup. Pisa, Sci. Fis. Mat.*, 18(3):449–474, 1964.

[53] J. Milnor. On the Betti numbers of real varieties. *Proc. Amer. Math. Soc.*, 15:275–280, 1964.

[54] L. Monck. An elemantary recursive decision procedure for $\mathrm{Th}(\mathbb{R}, +, \dot{})$. *Univ. of Calif., Berkeley, Dept. of Math., thesis*.

[55] Yurii Nesterov and Arkadii Nemirovskii. *Interior-point polynomial algorithms in convex programming*, volume 13 of *SIAM Studies in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1994.
[56] C. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.
[57] Pablo A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Math. Program.*, 96(2, Ser. B):293–320, 2003. Algebraic and geometric methods in discrete optimization.
[58] Daniel Perrucci. Linear solving for sign determination. *arXiv:0911.5707v1 [math.AG]*.
[59] I. G. Petrovskiĭ and O. A. Oleĭnik. On the topology of real algebraic surfaces. *Izvestiya Akad. Nauk SSSR. Ser. Mat.*, 13:389–402, 1949.
[60] Lorant Porkolab and Leonid Khachiyan. On the complexity of semidefinite programs. *J. Global Optim.*, 10(4):351–365, 1997.
[61] Victoria Powers and Thorsten Wörmann. An algorithm for sums of squares of real polynomials. *J. Pure Appl. Algebra*, 127(1):99–104, 1998.
[62] Motakuri V. Ramana. An exact duality theory for semidefinite programming and its complexity implications. *Math. Programming*, 77(2, Ser. B):129–162, 1997. Semidefinite programming.
[63] E. Rannou. The complexity of stratification computation. *Discrete Comput. Geom.*, 19(1):47–78, 1998.
[64] J. Reif. Complexity of the mover's problem and generalizations. In *IEEE Transactions on Robotics and Automation*, pages 421–427, 1979.
[65] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. I-III. *J. Symbolic Comput.*, 13(3):255–352, 1992.
[66] J. J. Rotman. *An Introduction to Algebraic Topology*. Springer-Verlag, 1988.
[67] M.-F. Roy and A. Szpirglas. Complexity of the computations with real algebraic numbers. *Journal of Symbolic computation*, 10:39–51, 1990.
[68] Mohab Safey El Din and Éric Schost. Polar varieties and computation of one point in each connected component of a smooth algebraic set. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 224–231 (electronic), New York, 2003. ACM.
[69] Mohab Safey El Din and Éric Schost. Properness defects of projections and computation of at least one point in each connected component of a real algebraic set. *Discrete Comput. Geom.*, 32(3):417–430, 2004.
[70] J. Schwartz and M. Sharir. On the piano movers' problem ii. general techniques for computing topological properties of real algebraic manifolds. *Adv. Appl. Math.*, 4:298–351, 1983.
[71] Sergey P. Tarasov and Mikhail N. Vyalyi. Semidefinite programming and arithmetic circuit evaluation. *Discrete Appl. Math.*, 156(11):2070–2078, 2008.
[72] A. Tarski. *A decision method for elementary algebra and geometry*. University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed.
[73] R. Thom. Sur l'homologie des variétés algébriques réelles. In *Differential and Combinatorial Topology (A Symposium in Honor of Marston Morse)*, pages 255–265. Princeton Univ. Press, Princeton, N.J., 1965.
[74] H. R. Wüthrich. Ein Entschiedungsverfahren für die Theorie der reell-abgeschlossenen Körper. *LNCS*, 43:138–162, 1976.

Department of Mathematics, Purdue University, West Lafayette, IN 47907, U.S.A.
E-mail address: sbasu@math.purdue.edu