Algorithms in Real Algebraic Geometry: A Survey

Saugata Basu

Panoramas et Synthèses

Numéro 51

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique

Panoramas & Synthèses
51, 2017, p. 107–153

ALGORITHMS IN REAL ALGEBRAIC GEOMETRY: A SURVEY

by

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.

Résumé **(Algorithmes en géométrie algébrique réelle : synthèse).** **–** On expose dans ce texte les résultats anciens et récents en théorie algorithmique de la géometrie algébrique réelle. On commence par décrire des méthodes effectives d'élimination des quantificateurs dans la théorie réelle du premier ordre initiée par Tarski et Seidenberg. On aborde également les problèmes liés à cette théorie. On décrit ensuite les algorithmes récents permettant de calculer des invariants topologiques des ensembles semi-algébriques. On s'intéresse plus particulièrement à la complexité de ces algorithmes. On analyse ensuite les liens entre la complexité des problèmes de décisions dans la théorie réelle du premier ordre et le calcul de certains invariants topologiques des ensembles semi-algébriques. On évoque finalement un volet plus numérique de cette théorie avec les méthodes d'optimisation en programmation semi-définie.

2010 Mathematics Subject Classification. **–** 14P10, 14P25; 68W30.
Key words and phrases. **–** Algorithms, Complexity, Semi-algebraic Sets, Betti Numbers, Roadmaps, Quantifier Elimination.

The author was partially supported by an NSF grants CCF-0915954, CCF-1319080 and DMS-1161629.

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 these algorithms. 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 $\mathbb{R}_{\mathrm{alg}}$ 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 $\mathscr{P}$ of polynomials in $\mathrm{R}[X_1,\ldots,X_k]$, a subset S of R^k is *$\mathscr{P}$-semi-algebraic* if S is the realization of a Boolean formula with atoms $P=0$, $P>0$ or $P<0$ with $P\in\mathscr{P}$ (we will call such a formula a quantifier-free $\mathscr{P}$-formula).

It is clear that for every semi-algebraic subset S of R^k there exists a finite set $\mathscr{P}$ of polynomials in $\mathrm{R}[X_1,\ldots,X_k]$ such that S is $\mathscr{P}$-semi-algebraic. We call a semi-algebraic set a *$\mathscr{P}$-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 $P\in\mathscr{P}$.

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

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

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

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

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

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 **[25]** 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. 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, $\mathscr{P} \subset \mathrm{D}[X_1, \ldots, X_k]$, where D is an ordered domain contained in the real closed field R. 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 $\mathscr{P}$-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 $\mathscr{P}$-semi-algebraic set is empty or not.

The second class of problems has a more geometric or topological flavor. Given a description of a $\mathscr{P}$-semi-algebraic set $S \subset \mathrm{R}^k$ the task is to decide whether certain geometric or 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 the existence of semi-algebraic connecting paths.*) Given two points $x, y \in S$, decide if they belong to the same semi-algebraically connected component of S.
3. (*Computing descriptions of semi-algebraic paths.*) Given two points $x, y \in S$, which belong to the same semi-algebraically connected component of S, output a description of a semi-algebraic path in S connecting x, y.
4. (*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 partition of S into smooth semi-algebraic subsets of various dimensions satisfying certain extra regularity conditions (for example, Whitney conditions (a) and(b)).

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 domain 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 function whose argument is the size of the input to the algorithm, measured by the number of number of polynomials, their degrees, and the number of variables, and whose value is the supremum over all inputs of size equal to the argument, of the number of arithmetic operations (including comparisons) performed by the algorithm in the domain D. In case the input polynomials have integer coefficients with bounded bit-size, then we will often give the bit-complexity, which gives an upper bound on the number of bit operations performed by the algorithm. We refer the reader to [**25**, Chapter 8] for a full discussion about the various measures of complexity.

The complexity of an algorithm (see Definition 1.1 above) 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).

The rest of the paper is organized as follows. In Section 2, we describe known algorithms for quantifier elimination in the first order 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 discuss some variants of the 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