37 COMPUTATIONAL AND QUANTITATIVE REAL ALGEBRAIC GEOMETRY

Saugata Basu and Bhubaneswar Mishra

INTRODUCTION

Computational and quantitative real algebraic geometry studies various algorithmic and quantitative questions dealing with the *real solutions* of a system of equalities, inequalities, and inequations of polynomials over the real numbers. This emerging field is largely motivated by the power and elegance with which it solves a broad and general class of problems arising in robotics, vision, computer-aided design, geometric theorem proving, etc.

The algorithmic problems that arise in this context are formulated as decision problems for the *first-order theory of reals* and the related problems of *quantifier elimination* (Section 37.1), as well as problems of computing topological invariants of semi-algebraic sets. The associated geometric structures are then examined via an exploration of the *semialgebraic sets* (Section 37.2). Algorithmic problems for semialgebraic sets are considered next. In particular, Section 37.2 discusses real algebraic numbers and their representation, relying on such classical theorems as Sturm's theorem and Thom's Lemma (Section 37.3). This discussion is followed by a description of semialgebraic sets using the concept of *cylindrical algebraic decomposition* (CAD) in both one and higher dimensions (Sections 37.4 and 37.5). This concept leads to brief descriptions of two algorithmic approaches for the decision and quantifier elimination problems (Section 37.6): namely, Collins's algorithm based on CAD, and some more recent approaches based on critical points techniques and on reducing the multivariate problem to easier univariate problems. These new approaches rely on the work of several groups of researchers: Grigor'ev and Vorobjov [Gri88, GV88], Canny [Can87, Can90], Heintz et al. [HRS90], Renegar [Ren91, Ren92a, Ren92b, Ren92c], and Basu et al. [BPR96]. In Section 37.7 we describe certain mathematical results on bounding the topological complexity of semi-algebraic sets, and in Section 37.8 we discuss some algorithms for computing topological invariants of semi-algebraic sets. In Section 37.9 we describe some quantitative results from metric semi-algebraic geometry. These have proved useful in applications in computer science. In Section 37.10 we discuss the connection between quantitative bounds on the topology of semi-algebraic sets, and the polynomial partitioning method that have gained prominence recently in discrete and computational geometry. Finally, we give a few representative applications of computational semi-algebraic geometry in Section 37.11.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

37.1 FIRST-ORDER THEORY OF REALS

The *decision problem* for the first-order theory of reals is to determine if a *Tarski sentence* in the first-order theory of reals is true or false. The *quantifier elimination problem* is to determine if there is a logically equivalent quantifier-free formula for an arbitrary Tarski formula in the first-order theory of reals. As a result of Tarski's work, we have the following theorem.

THEOREM 37.1.1 [Tar51]

- Let Ψ be a Tarski sentence. There is an effective decision procedure for Ψ.
- Let Ψ be a Tarski formula. There is a quantifier-free formula ϕ logically equivalent to Ψ. If Ψ involves only polynomials with rational coefficients, then so does the sentence ϕ.

Tarski formulas are formulas in a first-order language (defined by Tarski in 1930 [Tar51]) constructed from equalities, inequalities, and inequations of polynomials over the reals. Such formulas may be constructed by introducing logical connectives and universal and existential quantifiers to the atomic formulas. *Tarski sentences* are Tarski formulas in which all variables are bound by quantification.

GLOSSARY

Term: A constant, variable, or term combining two terms by an arithmetic operator: $\{+, -, \cdot\}$. A constant is a real number. A variable assumes a real number as its value. A term contains finitely many such algebraic variables: $x_1, x_2, \ldots, x_k$.

Atomic formula: A formula comparing two terms by a binary relational operator: $\{=, \neq, >, <, \geq, \leq\}$.

Quantifier-free formula: An atomic formula, a negation of a quantifier-free formula given by the unary Boolean connective $\{\neg\}$, or a formula combining two quantifier-free formulas by a binary Boolean connective: $\{\Rightarrow, \wedge, \vee\}$. *Example*: The formula $(x^2 - 2 = 0) \wedge (x > 0)$ defines the (real algebraic) number $+\sqrt{2}$.

Tarski formula: If $\phi(y_1, \ldots, y_r)$ is a quantifier-free formula, then it is also a Tarski formula. All the variables y_i are ***free*** in ϕ. Let $\Phi(y_1, \ldots, y_r)$ and $\Psi(z_1, \ldots, z_s)$ be two Tarski formulas (with free variables y_i and z_i, respectively); then a formula combining Φ and Ψ by a Boolean connective is a Tarski formula with free variables $\{y_i\} \cup \{z_i\}$. Lastly, if $\mathcal{Q}$ stands for a quantifier (either universal $\forall$ or existential $\exists$) and if $\Phi(y_1, \ldots, y_r, x)$ is a Tarski formula (with free variables x and $y_1, \ldots, y_r$), then

$$\Big(\mathcal{Q}\, x\Big)\ \Big[\Phi(y_1, \ldots, y_r, x)\Big]$$

is a Tarski formula with only the y's as free variables. The variable x is ***bound*** in $(\mathcal{Q}\, x)[\Phi]$.

Tarski sentence: A Tarski formula with no free variable.
Example: $(\exists\, x)\ (\forall\, y)\ [y^2 - x < 0]$. This Tarski sentence is false.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

Prenex Tarski formula: A Tarski formula of the form

$$\Big(\mathcal{Q}\, x_1\Big)\, \Big(\mathcal{Q}\, x_2\Big)\, \cdots \Big(\mathcal{Q}\, x_k\Big)\, \Big[\phi(y_1, y_2, \ldots, y_r, x_1, \ldots, x_k)\Big],$$

where ϕ is quantifier-free. The string of quantifiers $(\mathcal{Q}\, x_1)\, (\mathcal{Q}\, x_2) \cdots\, (\mathcal{Q}\, x_k)$ is called the ***prefix*** and ϕ is called the ***matrix***.

Prenex form of a Tarski formula, Ψ: A prenex Tarski formula logically equivalent to Ψ. For every Tarski formula, one can find its prenex form using a simple procedure that works in four steps: (1) eliminate redundant quantifiers; (2) rename variables so that the same variable does not occur as free and bound; (3) move negations inward; and finally, (4) push quantifiers to the left.

THE DECISION PROBLEM

The general ***decision problem*** for the first-order theory of reals is to determine if a given Tarski sentence is true or false. A particularly interesting special case of the problem is when all the quantifiers are existential. We refer to the decision problem in this case as the ***existential problem*** for the first-order theory of reals.

The general decision problem was shown to be decidable by Tarski [Tar51]. However, the complexity of Tarski's original algorithm could only be given by a very rapidly-growing function of the input size (e.g., a function that could not be expressed as a bounded tower of exponents of the input size). The first algorithm with substantial improvement over Tarski's algorithm was due to Collins [Col75]; it has a doubly-exponential time complexity in the number of variables appearing in the sentence. Further improvements have been made by a number of researchers (Grigor'ev-Vorobjov [Gri88, GV88], Canny [Can88, Can93], Heintz et al. [HRS89, HRS90], Renegar [Ren92a, Ren92b, Ren92c]) and most recently by Basu et al. [BPR96, Bas99a].

In the following, we assume that our Tarski sentence is presented in its prenex form:

$$(\mathcal{Q}_1 \mathbf{x}^{[1]})\, (\mathcal{Q}_2 \mathbf{x}^{[2]})\, \cdots\, (\mathcal{Q}_\omega \mathbf{x}^{[\omega]})\, [\psi(\mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[\omega]})],$$

where the $\mathcal{Q}_i$'s form a sequence of alternating quantifiers (i.e., $\forall$ or $\exists$, with every pair of consecutive quantifiers distinct), with $\mathbf{x}^{[i]}$ a partition of the variables

$$\bigcup_{i=0}^{\omega} \mathbf{x}^{[i]} = \{x_1, x_2, \ldots, x_k\} \triangleq \mathbf{x}, \quad \text{and} \quad |\mathbf{x}^{[i]}| = k_i,$$

and where ψ is a quantifier-free formula with atomic predicates consisting of polynomial equalities and inequalities of the form

$$g_i\left(\mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[\omega]}\right) \gtreqless 0, \quad i = 1, \ldots, s.$$

Here, g_i is a multivariate polynomial (over $\mathbb{R}$ or $\mathbb{Q}$, as the case may be) of total degree bounded by d. There are a total of s such polynomials. The special case $\omega = 1$ reduces the problem to that of the existential problem for the first-order theory of reals.

If the polynomials of the basic equalities, inequalities, inequations, etc., are over the rationals, then we assume that their coefficients can be stored with at most L bits. Thus the arithmetic complexity can be described in terms of k, k_i, ω, s, and d, and the bit complexity will involve L as well.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

TABLE 37.1.1 Selected time complexity results.

GENERAL OR EXISTENTIAL	TIME COMPLEXITY	SOURCE
General	$L^3(sd)^{2^{O(\Sigma k_i)}}$	[Col75]
Existential	$L^{O(1)}(sd)^{O(k^2)}$	[GV92]
General	$L^{O(1)}(sd)^{(O(\sum k_i))^{4\omega-2}}$	[Gri88]
Existential	$L^{1+o(1)}\ (s)^{(k+1)}\ (d)^{O(k^2)}$	[Can88, Can93]
General	$(L\log L\log\log L)(sd)^{(2^{O(\omega)})\Pi k_i}$	[Ren92a, Ren92b, Ren92c]
Existential	$(L\log L\log\log L)s\ (s/k)^k\ (d)^{O(k)}$	[BPR96]
General	$(L\log L\log\log L)(s)^{\Pi(k_i+1)}(d)^{\Pi O(k_i)}$	[BPR96]

Table 37.1.1 highlights a representative set of known bit-complexity results for the decision problem.

QUANTIFIER ELIMINATION PROBLEM

Formally, given a Tarski formula of the form,

$$\Psi(\mathbf{x}^{[0]}) = (\mathcal{Q}_1\mathbf{x}^{[1]})\ (\mathcal{Q}_2\mathbf{x}^{[2]})\ \cdots\ (\mathcal{Q}_\omega\mathbf{x}^{[\omega]})\ [\psi(\mathbf{x}^{[0]},\mathbf{x}^{[1]},\ldots,\mathbf{x}^{[\omega]})]\,,$$

where ψ is a quantifier-free formula, the ***quantifier elimination problem*** is to construct another quantifier-free formula, $\phi(\mathbf{x}^{[0]})$, such that $\phi(\mathbf{x}^{[0]})$ holds if and only if $\Psi(\mathbf{x}^{[0]})$ holds. Such a quantifier-free formula takes the form

$$\phi(\mathbf{x}^{[0]}) \equiv \bigvee_{i=1}^{I}\bigwedge_{j=1}^{J_i}\left(f_{i,j}(\mathbf{x}^{[0]}) \gtreqless 0\right),$$

where $f_{i,j} \in \mathbb{R}[\mathbf{x}^{[0]}]$ is a multivariate polynomial with real coefficients.

The current best bounds were given by Basu et. al. [BPR96] and are summarized as follows:

$$\begin{aligned} I &\leq (s)^{\Pi(k_i+1)}(d)^{\Pi\, O(k_i)} \\ J_i &\leq (s)^{\Pi_{i>0}(k_i+1)}(d)^{\Pi_{i>0}\, O(k_i)}. \end{aligned}$$

The total degrees of the polynomials $f_{i,j}(\mathbf{x}^{[0]})$ are bounded by

$$(d)^{\Pi_{i>0}\, O(k_i)}.$$

Nonetheless, comparing the above bounds to the bounds obtained in *semilinear geometry*, it appears that the "combinatorial part" of the complexity of both the formula and the computation could be improved to $(s)^{\Pi_{i>0}(k_i+1)}$. Basu [Bas99a] proved the following bound (with improved combinatorial part) for the size of the equivalent quantifier-free formula

$$I, J_i \leq (s)^{\Pi_{i>0}(k_i+1)}(d)^{k_0'\,\Pi_{i>0}\, O(k_i)},$$

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

where $k_0' = \min(k_0 + 1, \tau \prod_{i>0}(k_i + 1))$ and τ is a bound on the number of free-variables occurring in any polynomial in the original Tarski formula. The total degrees of the polynomials $f_{i,j}(\mathbf{x}^{[0]})$ are still bounded by

$$(d)^{\prod_{i>0} O(k_i)}.$$

Furthermore, the algorithmic complexity of Basu's procedure involves only $(s)^{\prod_{i>0}(k_i+1)}(d)^{k_0' \prod_{i>0} O(k_i)}$ arithmetic operations.

Lower bound results for the quantifier elimination problem can be found in Davenport and Heintz [DH88]. They showed that for every k, there exists a Tarski formula Ψ_k with k quantifiers, of length $O(k)$, and of constant degree, such that any quantifier-free formula ψ_k logically equivalent to Ψ_k must involve polynomials of

$$\text{degree} = 2^{2^{\Omega(k)}} \quad \text{and} \quad \text{length} = 2^{2^{\Omega(k)}}.$$

Note that in the simplest possible case (i.e., $d = 2$ and $k_i = 2$), upper and lower bounds are doubly-exponential and match well. This result, however, does not imply a similar lower bound for the decision problems.

From the point of view of hardness, it is easily seen that the problem of deciding a sentence in the existential theory of the reals (with integer coefficients) is **NP**-hard in the Turing model of computation, and it was proved by Blum, Shub and Smale [BSS89], that deciding whether a real polynomial of degree 4 has a real zero in $\mathbb{R}^n$ is $\mathbf{NP}_{\mathbb{R}}$-complete in the Blum-Shub-Smale model of computations [BCSS98].

37.2 SEMIALGEBRAIC SETS

Every quantifier-free formula composed of polynomial inequalities and Boolean connectives defines a semialgebraic set. Thus, these semialgebraic sets play an important role in real algebraic geometry.

GLOSSARY

Semialgebraic set: A subset $S \subseteq \mathbb{R}^k$ defined by a set-theoretic expression involving a system of polynomial inequalities

$$S = \bigcup_{i=1}^{I} \bigcap_{j=1}^{J_i} \Big\{ (\xi_1, \ldots, \xi_k) \in \mathbb{R}^k \;\mid\; \operatorname{sgn}(f_{i,j}(\xi_1, \ldots, \xi_k)) = s_{i,j} \Big\},$$

where the $f_{i,j}$'s are multivariate polynomials over $\mathbb{R}$ and the $s_{i,j}$'s are corresponding sets of signs in $\{-1, 0, +1\}$.

Real algebraic set, real algebraic variety: A subset $Z \subseteq \mathbb{R}^k$ defined by a system of algebraic equations.

$$Z = \Big\{ (\xi_1, \ldots, \xi_k) \in \mathbb{R}^n \;\mid\; f_1(\xi_1, \ldots, \xi_k) = \cdots = f_m(\xi_1, \ldots, \xi_k) = 0 \Big\},$$

where the f_i's are multivariate polynomials over $\mathbb{R}$. For any finite set of polynomials $\mathcal{P} \subset \mathbb{R}[x_1, \ldots, x_k]$ we denote by $\operatorname{Zer}(\mathcal{P}, \mathbb{R}^k)$ the associated real algebraic set in $\mathbb{R}^k$. Real algebraic sets are also referred to as real algebraic varieties, or just as varieties if the ambient space is clear from context.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

Semialgebraic map: A map $\theta : S \to T$, from a semialgebraic set $S \subseteq \mathbb{R}^k$ to a semialgebraic set $T \subseteq \mathbb{R}^\ell$, such that its graph $\{(x, \theta(x)) \in \mathbb{R}^{k+\ell} : s \in S\}$ is a semialgebraic set in $\mathbb{R}^{k+\ell}$. Note that projection, being linear, is a semialgebraic map.

Dimension of a semi-algebraic set: For any semi-algebraic set S, the dimension of S is the maximum number i, such that there exists a semi-algebraic injective map from $(0,1)^i$ to S.

Real dimension of a real algebraic variety: The real dimension of a real algebraic variety $V \subset \mathbb{R}^k$ is the dimension of V as a semi-algebraic set and is at most k. Note also that the real dimension of V is at most the *complex dimension* of the Zariski closure of V in $\mathbb{C}^k$, i.e., the smallest complex sub-variety of $\mathbb{C}^k$ which contains V. We refer the reader to [BCR98] for intricacies of dimension theory of real and complex varieties.

TARSKI-SEIDENBERG THEOREM

Equivalently, semialgebraic sets can be defined as

$$S = \Big\{(\xi_1, \ldots, \xi_k) \in \mathbb{R}^k \quad | \quad \psi(\xi_1, \ldots, \xi_k) = \mathsf{True}\Big\},$$

where $\psi(x_1, \ldots, x_k)$ is a quantifier-free formula involving n algebraic variables. As a direct corollary of Tarski's theorem on quantifier elimination, we see that extensions of Tarski formulas are also semialgebraic sets.

While real algebraic sets are quite interesting and would be natural objects of study in this context, *they are not closed under projection onto a subspace*. Hence they tend to be unwieldy. However, *semialgebraic sets are closed under projection*. This follows from a more general result: the famous ***Tarski-Seidenberg theorem*** which is an immediate consequence of quantifier elimination, since images are described by formulas involving only existential quantifiers.

THEOREM 37.2.1 *(Tarski-Seidenberg Theorem)* [Tar51]
Let S be a semialgebraic set in $\mathbb{R}^k$, and let $\theta : \mathbb{R}^k \to \mathbb{R}^\ell$ be a semialgebraic map. Then $\theta(S)$ is semialgebraic in $\mathbb{R}^\ell$.

In fact, semialgebraic sets can be defined simply as the smallest class of subsets of $\mathbb{R}^k, k \geq 0$, containing real algebraic sets and closed under projection.

GLOSSARY

Connected component of a semialgebraic set: A maximal connected subset of a semialgebraic set. Semialgebraic sets have a finite number of connected components and these are also semialgebraic.

Semialgebraic decomposition of a semialgebraic set S: A finite collection $\mathcal{K}$ of disjoint connected semialgebraic subsets of S whose union is S. The collection of connected components of a semialgebraic set forms a semialgebraic decomposition. Thus, every semialgebraic set admits a semialgebraic decomposition.

Set of sample points for S: A finite number of points meeting every nonempty connected component of S.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

Sign assignment: A vector of sign values of a set of polynomials at a point p. More formally, let $\mathcal{P} \subset \mathbb{R}[X_1, \ldots, X_k]$.

Any point $p = (\xi_1, \ldots, \xi_k) \in \mathbb{R}^k$ has a ***sign assignment*** with respect to $\mathcal{P}$ as follows:

$$\mathrm{sgn}_{\mathcal{P}}(p) = \Big(\mathrm{sgn}(f(\xi_1, \ldots, \xi_k)) \mid f \in \mathcal{P}\Big).$$

A sign assignment induces an equivalence relation: Given two points p, $q \in \mathbb{R}^k$, we say

$$p \sim_{\mathcal{P}} q, \quad \text{if and only if} \quad \mathrm{sgn}_{\mathcal{P}}(p) = \mathrm{sgn}_{\mathcal{P}}(q).$$

Sign class of $\mathcal{P}$: An equivalence class in the partition of $\mathbb{R}^k$ defined by the equivalence relation $\sim_{\mathcal{P}}$.

Semialgebraic decomposition for $\mathcal{P}$: A finite collection of disjoint connected semialgebraic subsets $\{C_i\}$ such that each C_i is contained in some semialgebraic sign class of $\mathcal{P}$. That is, the sign of each $f \in \mathcal{P}$ is ***invariant*** in each C_i. The collection of connected components of the sign-invariant sets for $\mathcal{P}$ forms a semialgebraic decomposition for $\mathcal{P}$.

Cell decomposition for $\mathcal{P}$: A semialgebraic decomposition for $\mathcal{P}$ into finitely many disjoint semialgebraic subsets $\{C_i\}$ called ***cells***, such that each cell C_i is homeomorphic to $\mathbb{R}^{\delta(i)}$, $0 \leq \delta(i) \leq k$. $\delta(i)$ is called the ***dimension of the cell*** C_i, and C_i is called a ***$\delta(i)$-cell***.

Cellular decomposition for $\mathcal{P}$: A cell decomposition for $\mathcal{P}$ such that the closure $\overline{C_i}$ of each cell C_i is a union of cells C_j: $\overline{C_i} = \cup_j C_j$.

Realization of a first-order formula: For any finite family of polynomials $\mathcal{P} \subset \mathbb{R}[x_1, \ldots, x_k]$, we call an element $\sigma \in \{0, 1, -1\}^{\mathcal{P}}$, a *sign condition* on $\mathcal{P}$. For any semi-algebraic set $Z \subset \mathbb{R}^k$, and a sign condition $\sigma \in \{0, 1, -1\}^{\mathcal{P}}$, we denote by $\mathrm{Reali}(\sigma, Z)$ the semi-algebraic set defined by

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

and call it the *realization* of σ on Z.

$\mathcal{P}$- and $\mathcal{P}$-closed semi-algebraic sets: More generally, we call any Boolean formula Φ with atoms, $P\{=, >, <\}0, P \in \mathcal{P}$, a *$\mathcal{P}$-formula*. We call the realization of Φ, namely the semi-algebraic set

$$\mathrm{Reali}\left(\Phi, \mathbb{R}^k\right) \quad = \quad \left\{\mathbf{x} \in \mathbb{R}^k \mid \Phi(\mathbf{x})\right\}$$

a *$\mathcal{P}$-semi-algebraic set*. Finally, we call a Boolean formula without negations, and with atoms $P\{\geq, \leq\}0$, $P \in \mathcal{P}$, a *$\mathcal{P}$-closed formula*, and we call the realization, $\mathrm{Reali}\left(\Phi, \mathbb{R}^k\right)$, a *$\mathcal{P}$-closed semi-algebraic set*.

Betti numbers of semi-algebraic sets: For any semi-algebraic set S we denote by $b_i(S)$, the rank of the i-th homology group, $\mathrm{H}_i(S, \mathbb{Z})$, of S, and by $b(S) = \sum_i b_i(S)$. In particular, $b_0(S)$ equals the number of connected components of S.

Generalized Euler-Poincaré characteristic of semi-algebraic sets: The *Euler-Poincaré characteristic*, $\chi(S)$, of a closed and bounded semi-algebraic set $S \subset \mathbb{R}^k$ is defined as $\chi(S) = \sum_i (-1)^i b_i(S)$. The Euler-Poincaré characteristic defined above for closed and bounded semi-algebraic set can be extended additively to all semi-algebraic sets, and this additive invariant is then known as the generalized Euler-Poincaré characteristic.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

37.3 REAL ALGEBRAIC NUMBERS

Real algebraic numbers are real roots of rational univariate polynomials and provide finitary representation for some of the basic objects (e.g., sample points). Furthermore, we note that (1) real algebraic numbers have effective finitary representation, (2) field operations and polynomial evaluation on real algebraic numbers are efficiently (polynomially) computable, and (3) conversions among various representations of real algebraic numbers are efficiently (polynomially) computable. The key machinery used in describing and manipulating real algebraic numbers relies upon techniques based on the Sturm-Sylvester theorem, Thom's lemma, resultant construction, and various bounds for real root separation.

GLOSSARY

Real algebraic number: A real root α of a univariate polynomial $p(t) \in \mathbb{Z}[t]$ with integer coefficients.

Polynomial for α: A univariate polynomial p such that α is a real root of p.

Minimal polynomial of α: A univariate polynomial p of minimal degree defining α as above.

Degree of a nonzero real algebraic number: The degree of its minimal polynomial. By convention, the degree of the 0 polynomial is $-\infty$.

Real closed field: An ordered field in which every positive element is a square, and every odd degree polynomial has a root.

OPERATIONS ON REAL ALGEBRAIC NUMBERS

Note that if α and β are real algebraic numbers, then so are $-\alpha$, α^{-1} (assuming $\alpha \neq 0$), $\alpha+\beta$, and $\alpha\cdot\beta$. These facts can be constructively proved using the algebraic properties of a resultant construction.

THEOREM 37.3.1

The real algebraic numbers form a field.

A real algebraic number α can be represented by a polynomial for α and a component that identifies the root. There are essentially three types of information that may be used for this identification: *order* (where we assume the real roots are indexed from left to right), *sign* (by a vector of signs), or *interval* (an interval that contains exactly one root).

A classical technique due to Sturm and Sylvester shows how to compute the number of real roots of a univariate polynomial $p(t)$ in an interval $[a, b]$. One important use of this classical theorem is to compute a sequence of relatively small (nonoverlapping) intervals that isolate the real roots of p.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

GLOSSARY

Sturm sequence of a pair of polynomials $p(t)$ and $q(t) \in \mathbb{R}[t]$:

$$\overline{\text{STURM}}(p, q) = \left\langle \hat{r}_0(t), \hat{r}_1(t), \ldots, \hat{r}_s(t) \right\rangle,$$

where

$$\begin{aligned}
\hat{r}_0(t) &= p(t) \\
\hat{r}_1(t) &= q(t) \\
&\vdots \\
\hat{r}_{i-1}(t) &= \hat{q}_i(t)\, \hat{r}_i(t) - \hat{r}_{i+1}(t), \qquad \deg(\hat{r}_{i+1}) < \deg(\hat{r}_i) \\
&\vdots \\
\hat{r}_{s-1}(t) &= \hat{q}_s(t)\, \hat{r}_s(t).
\end{aligned}$$

Number of variations in sign of a finite sequence $\overline{c}$ of real numbers: Number of times the entries change sign when scanned sequentially from left to right; denoted $\text{Var}(\overline{c})$.

For a vector of polynomials $\overline{P} = \langle p_1(t), \ldots, p_m(t) \rangle$ and a real number a:

$$\text{Var}_a(\overline{P}) \;=\; \text{Var}(\overline{P}(a)) \;=\; \text{Var}(\langle p_1(a), \ldots, p_m(a) \rangle).$$

Formal derivative: $p'(t) = D(p(t))$, where $D \colon \mathbb{R}[t] \to \mathbb{R}[t]$ is the (formal) derivative map, taking t^n to nt^{n-1} and $a \in \mathbb{R}$ (a constant) to 0.

STURM-SYLVESTER THEOREM

THEOREM 37.3.2 *Sturm-Sylvester Theorem* [Stu35, Syl53]

Let $p(t)$ and $q(t) \in \mathbb{R}[t]$ be two real univariate polynomials. Then, for any interval $[a, b] \subseteq \mathbb{R} \cup \{\pm\infty\}$ (where $a < b$):

$$\text{Var}\Big[\overline{P}\Big]_a^b = c_p\Big[q > 0\Big]_a^b - c_p\Big[q < 0\Big]_a^b,$$

where

$$\begin{aligned}
\overline{P} &\triangleq \overline{\text{STURM}}(p, p'q), \\
\text{Var}\Big[\overline{P}\Big]_a^b &\triangleq \text{Var}_a(\overline{P}) - \text{Var}_b(\overline{P}),
\end{aligned}$$

and $c_p[\mathcal{P}]_a^b$ counts the number of distinct real roots (without counting multiplicity) of p in the interval (a, b) at which the predicate $\mathcal{P}$ holds.

Note that if we take $S_p \triangleq \overline{\text{STURM}}(p, p')$ (i.e., $q = 1$) then

$$\begin{aligned}
\text{Var}\Big[S_p\Big]_a^b &= c_p\Big[\mathsf{True}\Big]_a^b - c_p\Big[\mathsf{False}\Big]_a^b \\
&= \#\text{ of distinct real roots of } p \text{ in } (a, b).
\end{aligned}$$

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

COROLLARY 37.3.3

Let $p(t)$ and $q(t)$ be two polynomials with coefficients in a real closed field K. For any interval $[a, b]$ as before, we have

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c_p\Big[q = 0\Big]_a^b \\ c_p\Big[q > 0\Big]_a^b \\ c_p\Big[q < 0\Big]_a^b \end{bmatrix} = \begin{bmatrix} \mathrm{Var}\Big[\overline{\mathrm{STURM}}(p, p')\Big]_a^b \\ \mathrm{Var}\Big[\overline{\mathrm{STURM}}(p, p'q)\Big]_a^b \\ \mathrm{Var}\Big[\overline{\mathrm{STURM}}(p, p'q^2)\Big]_a^b \end{bmatrix}.$$

These identities as well as some related algorithmic results (the so-called BKR-algorithm) are based on results of Ben-Or et al. [BOKR86] and their extensions by others. Using this identity, it is a fairly simple matter to decide the sign conditions of a single univariate polynomial q at the roots of a univariate polynomial p. It is possible to generalize this idea to decide the sign conditions of a sequence of univariate polynomials $q_0(t)$, $q_1(t)$, ..., $q_n(t)$ at the roots of a single polynomial $p(t)$ and hence give an efficient (both sequential and parallel) algorithm for the decision problem for Tarski sentences involving univariate polynomials. Further applications in the context of general decision problems are described below.

GLOSSARY

Fourier sequence of a real univariate polynomial $p(t)$ of degree n:

$$\overline{\mathrm{FOURIER}}(p) = \Big\langle p^{(0)}(t) = p(t),\ p^{(1)}(t) = p'(t),\ \ldots, p^{(n)}(t)\ \Big\rangle,$$

where $p^{(i)}$ is the ith derivative of p with respect to t.

Sign-invariant region of $\mathbb{R}$ determined by a sign sequence $\overline{s}$ with respect to $\overline{\mathrm{FOURIER}}(p)$: The region $R(\overline{s})$ with the property that $\xi \in R(\overline{s})$ if and only if $\mathrm{sgn}(p^{(i)}(\xi)) = s_i$.

THOM'S LEMMA

LEMMA 37.3.4 *Thom's Lemma* [Tho65]

Every nonempty sign-invariant region $R(\overline{s})$ (determined by a sign sequence $\overline{s}$ with respect to $\overline{\mathrm{FOURIER}}(p)$) must be connected, i.e., consists of a single interval.

Let $\mathrm{sgn}_\xi(\overline{\mathrm{FOURIER}}(p))$ be the sign sequence obtained by evaluating the polynomials of $\overline{\mathrm{FOURIER}}(p)$ at ξ. Then as an immediate corollary of Thom's lemma, we have:

COROLLARY 37.3.5

Let ξ and ζ be two real roots of a real univariate polynomial $p(t)$ of positive degree $n > 0$. Then $\xi = \zeta$, if

$$\mathrm{sgn}_\xi(\overline{\mathrm{FOURIER}}(p')) = \mathrm{sgn}_\zeta(\overline{\mathrm{FOURIER}}(p')).$$

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

REPRESENTATION OF REAL ALGEBRAIC NUMBERS

Let $p(t)$ be a univariate polynomial of degree d with integer coefficients. Assume that the distinct real roots of $p(t)$ have been enumerated as follows:

$$\alpha_1 < \alpha_2 < \cdots < \alpha_{j-1} < \alpha_j = \alpha < \alpha_{j+1} < \cdots < \alpha_l,$$

where $l \leq d = \deg(p)$. Then we can represent any of its roots uniquely and in a finitary manner.

GLOSSARY

Order representation of an algebraic number: A pair consisting of its polynomial p and its index j in the monotone sequence enumerating the real roots of p: $\langle\alpha\rangle_o = \langle p, j\rangle$. *Example*: $\langle\sqrt{2}+\sqrt{3}\rangle_o = \langle x^4 - 10x^2 + 1, 4\rangle$.

Sign representation of an algebraic number: A pair consisting of its polynomial p and a sign sequence $\overline{s}$ representing the signs of its Fourier sequence evaluated at the root: $\langle\alpha\rangle_s = \langle p, \overline{s} = \mathrm{sgn}_\alpha(\overline{\mathrm{FOURIER}}(p'))\rangle$. *Example*: $\langle\sqrt{2}+\sqrt{3}\rangle_s = \langle x^4 - 10x^2 + 1, (+1, +1, +1)\rangle$. The validity of this representation follows easily from Thom's Lemma.

Interval representation of an algebraic number: A triple consisting of its polynomial p and the two endpoints of an isolating interval, (l, r) $(l, r \in \mathbb{Q}, l < r)$, containing only α: $\langle\alpha\rangle_i = \langle p, l, r\rangle$. *Example*: $\langle\sqrt{2}+\sqrt{3}\rangle_i = \langle x^4 - 10x^2 + 1, 3, 7/2\rangle$.

37.4 UNIVARIATE DECOMPOSITION

In the one-dimensional case, a semialgebraic set is the union of finitely many intervals whose endpoints are real algebraic numbers. For instance, given a set of univariate defining polynomials:

$$\mathcal{F} = \Big\{ f_i(x) \in \mathbb{Q}[x] \quad | \quad i = 1, \ldots, m \Big\},$$

we may enumerate all the real roots of the f_i's (i.e., the real roots of the single polynomial $F = \prod f_i$) as

$$-\infty < \xi_1 < \xi_2 < \cdots < \xi_{i-1} < \xi_i < \xi_{i+1} < \cdots < \xi_s < +\infty,$$

and consider the following finite set $\mathcal{K}$ of elementary intervals defined by these roots:

$$[-\infty, \xi_1), \ [\xi_1, \xi_1], \ (\xi_1, \xi_2), \ \ldots,$$
$$(\xi_{i-1}, \xi_i), \ [\xi_i, \xi_i], \ (\xi_i, \xi_{i+1}), \ \ldots, \ [\xi_s, \xi_s], \ (\xi_s, +\infty].$$

Note that $\mathcal{K}$ is, in fact, a cellular decomposition for $\mathcal{F}$. Any semialgebraic set S defined by $\mathcal{F}$ is simply the union of a subset of elementary intervals in $\mathcal{K}$. Furthermore, for each interval $C \in \mathcal{K}$, we can compute a sample point α_C as follows:

$$\alpha_C = \begin{cases} \xi_1 - 1, & \text{if } C = [-\infty, \xi_1); \\ \xi_i, & \text{if } C = [\xi_i, \xi_i]; \\ (\xi_i + \xi_{i+1})/2, & \text{if } C = (\xi_i, \xi_{i+1}); \\ \xi_s + 1, & \text{if } C = (\xi_s, +\infty]. \end{cases}$$

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

Now, given a first-order formula involving a single variable, its validity can be checked by evaluating the associated univariate polynomials at the sample points. Using the algorithms for representing and manipulating real algebraic numbers, we see that the bit complexity of the decision algorithm is bounded by $(Lmd)^{O(1)}$. The resulting cellular decomposition has no more than $2md + 1$ cells.

Using variants of the theorem due to Ben-Or et al. [BOKR86], Thom's lemma, and some results on parallel computations in linear algebra, one can show that this univariate decision problem is "well-parallelizable," i.e., the problem is solvable by uniform circuits of bounded depth and polynomially many "gates" (simple processors).

37.5 MULTIVARIATE DECOMPOSITION

A straightforward generalization of the standard univariate decomposition to higher dimensions is provided by Collins's cylindrical algebraic decomposition [Col75]. In order to represent a semialgebraic set $S \subseteq \mathbb{R}^k$, we may assume recursively that we can construct a cell decomposition of its projection $\pi(S) \subseteq \mathbb{R}^{k-1}$ (also a semialgebraic set), and then decompose S as a union of the ***sectors*** and ***sections*** in the cylinders above each cell of the projection, $\pi(S)$.

This procedure also leads to a cell decomposition of S. One can further assign an algebraic sample point in each cell of S recursively in a straightforward manner.

If $\mathcal{F}$ is a set of polynomials defining the semialgebraic set $S \subseteq \mathbb{R}^k$, then at no additional cost, we may in fact compute a cell decomposition for $\mathcal{P}$ using the procedure described above. Such a decomposition leads to a *cylindrical algebraic decomposition* for $\mathcal{P}$.

GLOSSARY

Cylindrical algebraic decomposition (CAD): A recursively defined cell decomposition of $\mathbb{R}^k$ for $\mathcal{P}$. The decomposition is a cellular decomposition if the set of defining polynomials $\mathcal{P}$ satisfies certain nondegeneracy conditions.

In the recursive definition, the cells of k-dimensional CAD are constructed from a $(k-1)$-dimensional CAD: Every $(k-1)$-dimensional CAD cell C' has the property that the distinct real roots of $\mathcal{F}$ over C' vary continuously as a function of the points of C'.

Moreover, the following quantities remain invariant over a $(k-1)$-dimensional cell: (1) the total number of complex roots of each polynomial of $\mathcal{F}$; (2) the number of distinct complex roots of each polynomial of $\mathcal{F}$; and (3) the total number of common complex roots of every distinct pair of polynomials of $\mathcal{F}$.

These conditions can be expressed by a set $\Phi(\mathcal{F})$ of at most $O(sd)^2$ polynomials in $k-1$ variables, obtained by considering *principal subresultant coefficients* (PSC's). Thus, they correspond roughly to *resultants* and *discriminants*, and ensure that the polynomials of $\mathcal{P}$ do not intersect or "fold" in a cylinder over a $(k-1)$-dimensional cell. The polynomials in $\Phi(\mathcal{P})$ are each of degree no more than d^2.

More formally, a $\mathcal{P}$-sign-invariant cylindrical algebraic decomposition of $\mathbb{R}^k$ is:

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

- BASE CASE: $k = 1$. A univariate cellular decomposition of $\mathbb{R}^1$ as in the previous section.
- INDUCTIVE CASE: $k > 1$. Let $\mathcal{K}'$ be a $\Phi(\mathcal{P})$-sign-invariant CAD of $\mathbb{R}^{k-1}$. For each cell $C' \in \mathcal{K}'$, define an ***auxiliary polynomial*** $g_{C'}(x_1, \ldots, x_{k-1}, x_k)$ as the product of those polynomials of $\mathcal{P}$ that do not vanish over the $(k-1)$-dimensional cell, C'. The real roots of the auxiliary polynomial g'_C over C' give rise to a finite number (perhaps zero) of semialgebraic continuous functions, which partition the cylinder $C' \times (\mathbb{R} \cup \{\pm\infty\})$ into finitely many $\mathcal{P}$-sign-invariant "slices." The auxiliary polynomials are of degree no larger than sd.
  Assume that the polynomial $g_{C'}(p', x_k)$ has l distinct real roots for each $p' \in C'$: $r_1(p'), r_2(p'), \ldots, r_l(p')$, each r_i being a continuous function of p'. The following sectors and sections are cylindrical over C' (see Figure 37.5.1.):

$$\begin{aligned}
C_0^* &= \Big\{\langle p', x_k\rangle \mid p' \in C' \wedge x_k \in [-\infty, r_1(p'))\Big\},\\
C_1 &= \Big\{\langle p', x_k\rangle \mid p' \in C' \wedge x_k \in [r_1(p'), r_1(p')]\Big\},\\
C_1^* &= \Big\{\langle p', x_k\rangle \mid p' \in C' \wedge x_k \in (r_1(p'), r_2(p'))\Big\},\\
&\vdots\\
C_l^* &= \Big\{\langle p', x_k\rangle \mid p' \in C' \wedge x_k \in (r_l(p'), +\infty]\Big\}.
\end{aligned}$$

  The k-dimensional CAD is thus the union of all the sections and sectors computed over the cells of the $(k-1)$-dimensional CAD.

A straightforward recursive algorithm to compute a CAD follows from the above description.

CYLINDRICAL ALGEBRAIC DECOMPOSITION

If we assume that the dimension k is a fixed constant, then the preceding cylindrical algebraic decomposition algorithm is polynomial in $s = |\mathcal{P}|$ and $d = \deg(\mathcal{P})$. However, the algorithm can be easily seen to be doubly-exponential in k as the number of polynomials produced at the lowest dimension is $(sd)^{2^{O(k)}}$, each of degree no larger than $d^{2^{O(k)}}$. The number of cells produced by the algorithm is also *doubly-exponential*. This bound can be seen to be tight by a result due to Davenport and Heintz [DH88], and is related to their lower bound for the quantifier elimination problem (Section 37.1).

CONSTRUCTING SAMPLE POINTS

Cylindrical algebraic decomposition provides a sample point in every sign-invariant connected component for $\mathcal{P}$. However, the total number of sample points generated is doubly-exponential, while the number of connected components of all sign conditions is only singly-exponential. In order to avoid this high complexity (both algebraic and combinatorial) of a CAD, many recent techniques for constructing sample points use a single projection to a line instead of a sequence of cascading pro-

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

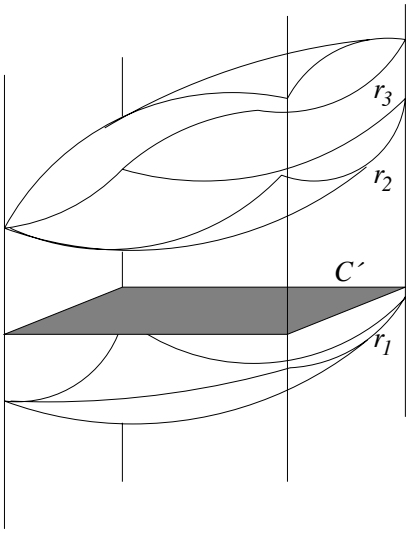

FIGURE 37.5.1
Sections and sectors "slicing" the cylinder over a lower dimensional cell.

jections. For instance, if one chooses a height function carefully then one can easily enumerate its critical points and then associate at least two such critical points to every connected component of the semialgebraic set. From these critical points, it will be possible to create at least one sample point per connected component. Using Bézout's bound, it is seen that only a singly-exponential number of sample points is created, thus improving the complexity of the underlying algorithms.

However, in order to arrive at the preceding conclusion using critical points, one requires certain genericity conditions that can be achieved by symbolically deforming the underlying semialgebraic sets. These infinitesimal deformations can be handled by extending the underlying field to a field of *Puiseux series*. Many of the significant complexity improvements based on these techniques have been due to a careful choice of the symbolic perturbation schemes which results in keeping the number of perturbation variables small.

Currently, the best algorithm for computing a finite set of points of bounded size that intersects *every connected component* of each nonempty sign condition is due to Basu et al. [BPR98] and has an arithmetic time-complexity of $s(s/k)^k d^{O(k)}$, where s is the number of polynomials, d the maximum degree, and k the number of variables.

37.6 ALGORITHMIC APPROACHES

COLLINS' APPROACH

The decision problem for the first-order theory of reals can be solved easily using a cylindrical algebraic decomposition. First consider the existential problem for a

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

sentence with only existential quantifiers,

$$(\exists\, \mathbf{x}^{[0]})\ [\psi(\mathbf{x}^{[0]})].$$

This sentence is true if and only if there is a $q \in C$, a sample point in the cell C,

$$q \ = \ \alpha^{[0]} = (\alpha_1, \ldots, \alpha_k) \ \in \ \mathbb{R}^k,$$

such that $\psi(\alpha^{[0]})$ is true. Thus we see that the decision problem for the purely existential sentence can be solved by simply evaluating the matrix ψ over the finitely many sample points in the associated CAD. This also implies that the existential quantifiers could be replaced by finitely many disjunctions ranging over all the sample points. Note that the same arguments hold for any semialgebraic decomposition with at least one sample point per sign-invariant connected component.

In the general case, one can describe the decision procedure by means of a search process that proceeds *only on* the coordinates of the sample points in the cylindrical algebraic decomposition. This follows because a sample point in a cell acts as a representative for any point in the cell as far as the sign conditions are concerned.

Consider a Tarski sentence

$$(\mathcal{Q}_1\mathbf{x}^{[1]})\ (\mathcal{Q}_2\mathbf{x}^{[2]})\ \cdots\ (\mathcal{Q}_\omega\mathbf{x}^{[\omega]})\ [\psi(\mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[\omega]})],$$

with $\mathcal{F}$ the set of polynomials appearing in the matrix ψ. Let $\mathcal{K}$ be a cylindrical algebraic decomposition of $\mathbb{R}^k$ for $\mathcal{F}$. Since the cylindrical algebraic decomposition produces a sequence of decompositions:

$$\mathcal{K}_1 \text{ of } \mathbb{R}^1, \ \ \mathcal{K}_2 \text{ of } \mathbb{R}^2, \ \ \ldots, \ \ \mathcal{K}_k \text{ of } \mathbb{R}^k,$$

such that each cell $C_{i-1,j}$ of $\mathcal{K}_i$ is cylindrical over some cell C_{i-1} of $\mathcal{K}_{i-1}$, the search progresses by first finding cells C_1 of $\mathcal{K}_1$ such that

$$(\mathcal{Q}_2 x_2)\ \cdots\ (\mathcal{Q}_k x_k)\ [\psi(\alpha_{C_1}, x_2, \ldots, x_k)] = \mathsf{True}.$$

For each C_1, the search continues over cells C_{12} of $\mathcal{K}_2$ cylindrical over C_1 such that

$$(\mathcal{Q}_3 x_3)\ \cdots\ (\mathcal{Q}_k x_k)\ [\psi(\alpha_{C_1}, \alpha_{C_{12}}, x_3, \ldots, x_k)] = \mathsf{True},$$

etc. Finally, at the bottom level the truth properties of the matrix ψ are determined by evaluating at all the coordinates of the sample points.

This produces a tree structure, where each node at the $(i-1)$th level corresponds to a cell $C_{i-1} \in \mathcal{K}_{i-1}$ and its children correspond to the cells $C_{i-1,j} \in \mathcal{K}_i$ that are cylindrical over C_{i-1}. The leaves of the tree correspond to the cells of the final decomposition $\mathcal{K} = \mathcal{K}_k$. Because we only have finitely many sample points, the universal quantifiers can be replaced by finitely many conjunctions and the existential quantifiers by disjunctions. Thus, we label every node at the $(i-1)$th level "AND" (respectively, "OR") if $\mathcal{Q}_i$ is a universal quantifier $\forall$ (respectively, $\exists$) to produce a so-called AND-OR tree. The truth of the Tarski sentence is thus determined by simply evaluating this AND-OR tree.

A quantifier elimination algorithm can be devised by a similar reasoning and a slight modification of the CAD algorithm described above.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

NEW APPROACHES USING CRITICAL POINTS

In order to avoid the cascading projections inherent in Collins's algorithm, the new approaches employ a single projection to a one-dimensional set by using critical points in the manner described above. As before, we start with a sentence with only existential quantifiers,

$$(\exists\, \mathbf{x}^{[0]})\ [\psi(\mathbf{x}^{[0]})].$$

Let $\mathcal{P} = \{f_1, \ldots, f_s\}$ be the set of polynomials appearing in the matrix ψ.

Under certain genericity conditions, it is possible to produce a set of sample points such that every sign-invariant connected component of the decomposition induced by $\mathcal{F}$ contains at least one such point. Furthermore, these sample points are described by a set of univariate polynomial sequences, where each sequence is of the form

$$p(t), q_0(t), q_1(t), \ldots, q_k(t),$$

and encodes a sample point $\langle \frac{q_1(\alpha)}{q_0(\alpha)}, \ldots, \frac{q_k(\alpha)}{q_0(\alpha)} \rangle$. Here α is a root of p. Now the decision problem for the existential theory can be solved by deciding the sign conditions of the sequence of univariate polynomials

$$f_1(q_1/q_0, \ldots, q_k/q_0),\ \ldots,\ f_s(q_1/q_0, \ldots, q_k/q_0),$$

at the roots of the univariate polynomial $p(t)$. Note that we have now reduced a multivariate problem to a univariate problem and can solve this by the BKR approach.

In order to keep the complexity reasonably small, one needs to ensure that the number of such sequences is small and that these polynomials are of low degree. Assuming that the polynomials in $\mathcal{F}$ are in general position, one can achieve this complexity and compute the polynomials p and q_i (for example, by the u-resultant method in Renegar's algorithm [Ren92a, Ren92b, Ren92c]).

If the genericity conditions are violated, one needs to symbolically deform the polynomials and carry out the computations on these polynomials with additional perturbation parameters. The Basu-Pollack-Roy (BPR) algorithm [BPR98, BPR96] differs from Renegar's algorithm primarily in the manner in which these perturbations are made so that their effect on the algorithmic complexity is controlled.

Next consider an existential Tarski formula of the form

$$(\exists\, \mathbf{x}^{[0]})\ [\psi(\mathbf{y}, \mathbf{x}^{[0]})],$$

where $\mathbf{y}$ represents the free variables. If we carry out the same computation as before over the ambient field $\mathbb{R}(\mathbf{y})$, we get a set of *parameterized* univariate polynomial sequences, each of the form

$$p(\mathbf{y}, t), q_0(\mathbf{y}, t), q_1(\mathbf{y}, t), \ldots, q_k(\mathbf{y}, t).$$

For a fixed value of $\mathbf{y}$, say $\bar{y}$, the polynomials

$$p(\bar{y}, t), q_0(\bar{y}, t), q_1(\bar{y}, t), \ldots, q_k(\bar{y}, t)$$

can then be used as before to decide the truth or falsity of the sentence

$$(\exists\, \mathbf{x}^{[0]})\ [\psi(\bar{y}, \mathbf{x}^{[0]})].$$

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

Also, one may observe that the *parameter space* $\mathbf{y}$ can be partitioned into semialgebraic sets so that all the necessary information can be obtained by computing at sample values $\bar{y}$.

This process can be extended to ω blocks of quantifiers, by replacing each block of variables by a finite number of cases, each involving only one new variable; the last step uses a CAD method for these ω-many variables.

37.7 TOPOLOGICAL COMPLEXITY OF SEMI-ALGEBRAIC SETS

One useful feature of semi-algebraic sets is that they admit uniform bounds on their topological complexity (measured by their Betti numbers) in terms of the number and degrees of polynomials appearing in the first-order formulas defining them. The uniformity refers to the fact that these bounds are independent of the coefficients of the defining polynomials (unlike for example the bounds in Theorems 37.9.1, 37.9.2, 37.9.3, and 37.9.4).

The first results on bounding the Betti numbers of real varieties were proved by Oleĭnik and Petrovskiĭ [PO49], Thom [Tho65] and Milnor [Mil64]. Using a Morse-theoretic argument and Bézout's theorem they proved (using $b(S)$ to denote the sum of the Betti numbers of a semi-algebraic set S):

THEOREM 37.7.1 [PO49, Tho65, Mil64]
Let $\mathcal{Q} \subset \mathbb{R}[x_1, \ldots, x_k]$ with $\deg(Q) \leq d, Q \in \mathcal{Q}$. Then,

$$b(\mathrm{Zer}(\mathcal{Q}, \mathbb{R}^k)) \leq d(2d-1)^{k-1}. \tag{37.7.1}$$

More generally, if $S \subset \mathbb{R}^k$ is defined by $P_1 \geq 0, \ldots, P_s \geq 0$, with

$$P_i \in \mathbb{R}[x_1, \ldots, x_k], \deg(P_i) \leq d, 1 \leq i \leq d,$$

then

$$b(S) \leq sd(2sd-1)^{k-1}. \tag{37.7.2}$$

Theorem 37.7.1 was later generalized to arbitrary semi-algebraic sets defined by quantifier-free formulas in two steps. In the first step, Theorem 37.7.1 was extended to a particular class of semi-algebraic sets, namely $\mathcal{P}$-closed semi-algebraic sets, where $\mathcal{P} \subset \mathbb{R}[x_1, \ldots, x_k]$ is a finite family of polynomials. The following theorem appears in [BPR05a] and sharpens an earlier result of [Bas99b].

THEOREM 37.7.2 [BPR05a]
If $S \subset \mathbb{R}^k$ is a $\mathcal{P}$-closed semi-algebraic set, then

$$b(S) \leq \sum_{i=0}^{k} \sum_{j=0}^{k-i} \binom{s+1}{j} 6^j d(2d-1)^{k-1}, \tag{37.7.3}$$

where $s = \mathrm{card}(\mathcal{P}) > 0$ and $d = \max_{P \in \mathcal{P}} \deg(P)$.

Using an additional ingredient (namely, a technique to replace an arbitrary semi-algebraic set by a locally closed one with a very controlled increase in the

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

number of polynomials used to describe the given set), Gabrielov and Vorobjov [GV05] extended Theorem 37.7.2 to arbitrary $\mathcal{P}$-semi-algebraic sets with only a small increase in the bound. Their result in conjunction with Theorem 37.7.2 gives the following theorem.

THEOREM 37.7.3 [GV09]
If $S \subset \mathbb{R}^k$ is a $\mathcal{P}$-semi-algebraic set, then

$$b(S) \leq \sum_{i=0}^{k} \sum_{j=0}^{k-i} \binom{2ks+1}{j} 6^j d(2d-1)^{k-1}, \tag{37.7.4}$$

where $s = \mathrm{card}(\mathcal{P})$ and $d = \max_{P \in \mathcal{P}} \deg(P)$.

The bounds mentioned above have many applications, for example, providing upper bounds on the number of distinct configurations of n points in $\mathbb{R}^k$ as well as on the number of combinatorial types of polytopes [GP86a, GP86b], in geometric transversal theory [GPW95], and for proving lower bounds for membership testing in certain algebraic models of computations [Yao97, MMP96, GV15].

37.8 COMPUTING TOPOLOGICAL INVARIANTS OF SEMI-ALGEBRAIC SETS

The problem of computing topological invariants of semi-algebraic sets is an important problem that has attracted much attention. Unlike the problem of quantifier-elimination or deciding Tarski sentences, 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. For instance, in one of their seminal papers, Schwartz and Sharir [SS83] gave an algorithm for computing the homology groups of S using cylindrical algebraic decomposition. Their algorithm necessarily has 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 $(sd)^{2^k}$, where s is the number of polynomials in the input, d the maximum degree of the polynomials in the input and k the number of variables.

ROADMAPS OF SEMI-ALGEBRAIC SETS

Singly-exponential time algorithms for counting the number of connected components of semi-algebraic sets, or for computing a semi-algebraic path connecting two points in the same connected component, all use the notion of a "roadmap," first introduced by Canny [Can87], who also gave a singly exponential time algorithm to compute it. A roadmap of a semi-algebraic set S is a one-dimensional connected subset which is connected inside each connected component of the S. Once these roadmaps are available, they can be used to link up two points in the same connected component. The main geometric idea is to construct roadmaps starting from

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

the critical sets of some projection function. The basic roadmap algorithm has been improved and extended by several researchers (Heintz et al. [HRS90], Gournay and Risler [GR93], Grigor'ev and Vorobjov [Gri88, GV88], and Canny [Can87, Can90]). 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 [BPR00, BPR16].

THEOREM 37.8.1 [BPR00, BPR16]

Let $Q \in \mathbb{R}[x_1, \ldots, x_k]$ with $\mathrm{Zer}(Q, \mathbb{R}^k)$ of dimension k' and let $\mathcal{P} \subset \mathbb{R}[x_1, \ldots, x_k]$ 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 $\mathrm{Zer}(Q, \mathbb{R}^k)$. There is an algorithm which computes a roadmap $\mathrm{RM}(S)$ for S with complexity $s^{k'+1}d^{O(k^2)}$.

Theorem 37.8.1 immediately implies that there is an algorithm whose output is exactly one point in every semi-algebraically connected component of S and whose complexity is bounded by $s^{k'+1}d^{O(k^2)}$. In particular, this algorithm counts the number of semi-algebraically connected components of S within the same time bound.

Schost and Safey el Din [SS10] have given a *probabilistic* algorithm for computing the roadmap of a smooth, bounded real algebraic hyper-surface in $\mathbb{R}^k$ 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 [BRS$^+$14].

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 dimension 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 strategy results in the improved complexity. One also needs to prove suitable generalizations of the results guaranteeing the connectivity of the roadmap (see [BPR16, Chapter 15]) in this more general situation.

The recursive schemes used in the algorithms in [SS10] and [BRS$^+$14] have a common defect in that they are unbalanced in the following sense. The dimension of the fibers in which recursive calls are made is equal to $k - \sqrt{k}$ (in the classical case this dimension is $k-1$), which is much larger than the dimension of the "polar variety" which is $\sqrt{k}$ (this dimension is equal to 1 in the classical case). While being less unbalanced than in the classical case (which accounts for the improvement in the complexity), there is scope for further improvement if these two dimensions can be made roughly equal. There are certain formidable technical obstructions to be overcome to achieve this.

This challenge was tackled in [BR14] where an algorithm based on a balanced (divide-and-conquer) scheme is given for computing a roadmap of an algebraic set. The following theorem is proved.

THEOREM 37.8.2 [BR14]

There exists an algorithm that takes as input:

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

1. *a polynomial* $P \in \mathbb{R}[x_1, \ldots, x_k]$, *with* $\deg(P) \leq d$;
2. *a finite set,* A, *of real univariate representations whose associated set of points,* $\mathcal{A} = \{p_1, \ldots, p_m\}$, *is contained in* $V = \mathrm{Zer}(P, \mathbb{R}^k)$, *and such that the degree of the real univariate representation representing* p_i *is bounded by* D_i *for* $1 \leq i \leq m$;

and computes a roadmap of V *containing* $\mathcal{A}$. *The complexity of the algorithm is bounded by*

$$\left(1 + \sum_{i=1}^{m} D_i^{O(\log^2(k))}\right)(k^{\log(k)}d)^{O(k\log^2(k))}.$$

The size of the output is bounded by $(\mathrm{card}(\mathcal{A}) + 1)(k^{\log(k)}d)^{O(k\log(k))}$, *while the degrees of the polynomials appearing in the descriptions of the curve segments and points in the output are bounded by*

$$(\max_{1\leq i\leq m} D_i)^{O(\log(k))}(k^{\log(k)}d)^{O(k\log(k))}.$$

A probabilistic algorithm based on a similar divide-and-conquer strategy which works for smooth, bounded algebraic sets, and with a slightly better complexity is given in [SS13]. As in [SS10], complex algebraic (as opposed to semi-algebraic) techniques play an important role in this algorithm.

COMPUTING BETTI NUMBERS OF SEMI-ALGEBRAIC SETS

Algorithms for computing roadmaps of semi-algebraic sets immediately yield a (singly exponential complexity) algorithm for computing the number of connected components (or in other words, the zero-th Betti number) of a semi-algebraic set S. Computing higher Betti numbers of semi-algebraic sets with singly exponential complexity is more difficult. The best known result in this direction is the following, which generalizes an earlier result [BPR08] giving a singly exponential algorithm for computing the first Betti number of a semi-algebraic set.

THEOREM 37.8.3 [Bas06]

For any given ℓ, *there is an algorithm that takes as input a* $\mathcal{P}$*-formula describing a semi-algebraic set* $S \subset \mathbb{R}^k$, *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.

COMPUTING GENERALIZED EULER-POINCARÉ CHARACTERISTIC OF SEMI-ALGEBRAIC SETS

Another topological invariant of semi-algebraic sets for which a singly exponential algorithm is known is the generalized Euler-Poincaré characteristic. It was shown in [Bas99b] that the Euler-Poincaré characteristic of a given $\mathcal{P}$-closed semi-algebraic set can be computed in $(ksd)^{O(k)}$ time.

The following result (which should be viewed as a generalization of the univariate sign determination algorithm) appears in [BPR05b].

THEOREM 37.8.4 [BPR05b]

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

There exists an algorithm which given an algebraic set $Z = \mathrm{Zer}(Q, \mathbb{R}^k) \subset \mathbb{R}^k$ and a finite set of polynomials $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathbb{R}[x_1, \ldots, x_k]$, computes the list of the generalized Euler-Poincaré characteristics of the realizations of all realizable sign conditions of $\mathcal{P}$ on Z.

If the degrees of the polynomials in $\mathcal{P} \cup \{Q\}$ are bounded by d, and the real dimension of $Z = \mathrm{Zer}(Q, \mathbb{R}^k)$ is k', then the complexity of the algorithm is

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

37.9 QUANTITATIVE RESULTS IN METRIC SEMI-ALGEBRAIC GEOMETRY

There are certain metric results that follow from the algorithmic results mentioned above which are very useful in practice. These results have several applications. For example, they are needed for efficient stopping criteria in algorithms that use sub-division methods to compute certificates of positivity of a given polynomial over some compact semi-algebraic subset of $\mathbb{R}^k$ (for example, over the standard simplex) [BCR08].

The following theorem is an example of the metric upper bounds referred to above. It provides an explicit upper bound on the radius of a ball centered at the origin which is guaranteed to meet every semi-algebraically connected component of any given semi-algebraic set in terms of the number s, the maximum degree d, and a bound τ on the bit sizes of the coefficients of the defining polynomials.

To state the result precisely we first introduce the following notation. Given an integer n, we denote by $\mathrm{bit}(n)$ the number of bits of its absolute value in the binary representation. Note that

$$\mathrm{bit}(nm) \leq \mathrm{bit}(n) + \mathrm{bit}(m), \tag{37.9.1}$$

$$\mathrm{bit}\left(\sum_{i=1}^{n} m_i\right) \leq \mathrm{bit}(n) + \sup_{i=1}^{n}(\mathrm{bit}(m_i)). \tag{37.9.2}$$

THEOREM 37.9.1 [BR10]

Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathbb{Z}[x_1, \ldots, x_k]$ and suppose that $P \in \mathcal{P}$ have degrees at most d, and the coefficients of $P \in \mathcal{P}$ have bit sizes at most τ. Then there exists a ball centered at the origin of radius

$$\left((2DN(2N-1)+1)2^{(2N-1)(\tau''+\mathrm{bit}(2N-1)+\mathrm{bit}(2DN+1))}\right)^{1/2}$$

where

$$\begin{aligned}
d' &= \sup(2(d+1), 6),\\
D &= k(d'-2)+2,\\
N &= d'(d'-1)^{k-1},\\
\tau'' &= N(\tau_2' + \mathrm{bit}(N) + 2\mathrm{bit}(2D+1) + 1),\\
\tau_2' &= \tau_1' + 2(k-1)\mathrm{bit}(N) + (2k-1)\mathrm{bit}(k),\\
\tau_1' &= D(\tau_0' + 4\mathrm{bit}(2D+1) + \mathrm{bit}(N)) - 2\mathrm{bit}(2D+1) - \mathrm{bit}(N),\\
\tau_0' &= 2\tau + k\mathrm{bit}(d+1) + \mathrm{bit}(2d') + \mathrm{bit}(s)
\end{aligned}$$

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

intersecting every semi-algebraically connected component of the realization of every realizable sign condition on $\mathcal{P}$.

Note that asymptotic bounds of the form $2^{\tau d^{O(k)}}$ for the same problem were known before [BPR16, GV88, Ren92a]. One point which needs some explanation is the fact that the number of polynomials, s, plays a role in the estimate in Theorem 37.9.1, while it does not appear in the formula $2^{\tau d^{O(k)}}$. The explanation for this situation is that the total number of polynomials of degree at most d in k variables with bit sizes bounded by τ is bounded by $(2^{\tau+1})^{\binom{d+k}{k}} = 2^{\tau d^{O(k)}}$.

A related result is the following bound on the minimum value attained by an integer polynomial restricted to a compact connected component of a basic closed semi-algebraic subset of $\mathbb{R}^k$ defined by polynomials with integer coefficients in terms of the degrees and the bit sizes of the coefficients of the polynomials involved.

THEOREM 37.9.2 [JPT13]

Let $\mathcal{P} = \{P_1, \ldots . P_s\} \subset \mathbb{Z}[x_1, \ldots, x_k]$ with $\deg(P) \leq d$ for all $P \in \mathcal{P}$, and let the coefficients of P have bit sizes bounded by τ. Let $Q \in \mathbb{Z}[x_1, \ldots, x_k]$, $\deg(Q) \leq d$, and let the bit sizes of the coefficients of Q be also bounded by τ. Let C be a compact connected component of the basic closed semi-algebraic set defined by $P_1 = \cdots = P_\ell = 0, P_{\ell+1} \geq 0, \ldots, P_s \geq 0$. Then the minimum value attained by Q over C is a real algebraic number of degree at most $2^{n-1}d^n$, and if it is not equal to 0, then its absolute value is bounded from below by

$$(2^{4-k/2} H d^k)^{-k 2^k d^k},$$

where $H = \max(2^\tau, 2k + 2s)$.

We discuss next a generalization of Theorem 37.9.1 which has proved to be useful in practice. Theorem 37.9.1 gives an upper bound on the radius of a ball meeting every connected component of the realizations of every realizable sign condition on a family of polynomials with integer coefficients. It is well known that the intersections of any semi-algebraic set $S \subset \mathbb{R}^k$ with open balls of large enough radius are semi-algebraically homeomorphic. This result is a consequence of the local conic structure of semi-algebraic sets [BCR98, Theorem 9.3.6].

Given a semi-algebraic set $S \subset \mathbb{R}^k$ defined by polynomials with coefficients in $\mathbb{Z}$, the following theorem gives a singly exponential upper bound on the radius of a ball having the following property. The *homotopy type* (not necessarily the homeomorphism type) of S is preserved upon intersection of S with all balls of larger radii.

THEOREM 37.9.3 [BV07]

Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathbb{Z}[x_1, \ldots, x_k]$ and suppose that $P \in \mathcal{P}$ have degrees at most d, and the coefficients of $P \in \mathcal{P}$ have bit sizes at most τ. Let $S \subset \mathbb{R}^k$ be a $\mathcal{P}$-semi-algebraic set.

There exists a constant $c > 0$, such that for any $R_1 > R_2 > 2^{\tau d^{ck}}$ we have,

1. *$S \cap \mathbf{B}_k(0, R_1) \simeq S \cap \mathbf{B}_k(0, R_2)$, and*
2. *$S \setminus \mathbf{B}_k(0, R_1) \simeq S \setminus \mathbf{B}_k(0, R_2)$*

(where $\simeq$ denotes homotopy equivalence, and for $R > 0$, $\mathbf{B}_k(0, R)$ denotes the closed ball of radius R centered at the origin).

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

THEOREM 37.9.4 [BV07]

Let $S \subset \mathbb{R}^m$ be a $\mathcal{P}$-semi-algebraic set, with $\mathcal{P} \subset \mathbb{Z}[x_1, \ldots, x_k]$ and $\mathbf{0} \in S$. Let $\deg(P) < d$ for each $P \in \mathcal{P}$, and the bit sizes of the coefficients of $P \in \mathcal{P}$ be less than τ. Then, there exists a constant $c > 0$ such that for every $0 < r < 2^{-\tau d^{ck}}$ the set $S \cap \mathbf{B}_k(0, r)$ is contractible.

37.10 CONNECTION TO INCIDENCE GEOMETRY

Recently there has been a major impetus to take a new look at the problem of bounding the topological complexity of semi-algebraic sets. It has come from the injection of algebraic techniques to attack certain long-standing open questions in incidence geometry (see for example [KMSS12, AMS13, SSS13, Zah13, SS14, Gut15b, Gut15a, SSZ15, MP15, Zah15]). The source of this impetus is the pioneering work of Guth and Katz [GK15], who following prior ideas of Elekes and Sharir [ES11], made a breakthrough in a long-standing problem of Erdős on the number of distinct distances between n points in a plane. Their main tool was a certain kind of decomposition (called "polynomial partitioning") using the polynomial ham-sandwich theorem due to Stone and Tukey [ST42], which played a somewhat analogous role that cuttings or trapezoidal decomposition [Mat02] played in the more classical Clarkson-Shor (see [CEG$^+$90]) type divide-and-conquer arguments for such problems. The polynomial partitioning result proved by Guth and Katz can be summarized as follows.

THEOREM 37.10.1 [GK15]

Let $\mathcal{S} \subset \mathbb{R}^k$ be a finite set of cardinality n, and $0 \leq r \leq n$. Then, there exists a polynomial $P \in \mathbb{R}[x_1, \ldots, x_k]$, with $\deg(P) \leq r^{1/k}$, having the property that for each connected component C of $\mathbb{R}^k \setminus \mathrm{Zer}(P, \mathbb{R}^k)$, $\mathrm{card}(C \cap \mathcal{S}) \leq O(n/r)$.

The "partitioning" refers to the partitioning of the complement of the hypersurface $\mathrm{Zer}(P, \mathbb{R}^k)$ (the zeros of P in $\mathbb{R}^k$) into its (open) connected components. The theorem ensures that each such connected component does not contain too many of the points. Moreover, using Theorem 37.7.1 one also has that the number of such connected components is bounded by $O(r)$. Notice that the theorem allows for the possibility that most (in fact all) the points in $\mathcal{S}$ are contained in the hypersurface $\mathrm{Zer}(P, \mathbb{R}^k)$.

The application of the partitioning theorem to concrete problems (say bounding incidences) leads to a dichotomy caused by the last observation. The open pieces of the decomposition are handled by induction, while a separate argument is needed for handling the co-dimension one piece, i.e., the hypersurface $\mathrm{Zer}(P, \mathbb{R}^k)$ itself. However, notice that P can have a degree not bounded by any constant when r is allowed to grow with n. The fact that this degree could depend on n (the number of points) and is not constant distinguishes the Guth-Katz technique from earlier decomposition based techniques (such as cuttings or trapezoidal decomposition [Mat02]). Because of this reason, when applying Guth-Katz technique to higher dimensional problems it is necessary to have more refined quantitative upper bounds in real algebraic geometry where the dependence on the degrees is more explicit. More precisely, one needs better bounds on the number of connected

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

components of the realizations of different sign conditions of a finite family of polynomials, $\mathcal{P}$, restricted to a given variety V. A bound on this number that took into account the real dimension of the variety V was known before (due to Basu, Pollack and Roy [BPR05a]), but this bound did not make a distinction between the dependence on the degrees of the polynomials in $\mathcal{P}$ and that of the polynomials defining V. In the Guth-Katz framework, such a distinction becomes crucial, since both these degrees could be large but the degree of the polynomials defining V is asymptotically much smaller than those of $\mathcal{P}$.

In [BB12] a stronger bound was proved on the number of connected components of the realizable sign conditions of a family of polynomials restricted to a variety, having a much more refined dependence on the degrees.

THEOREM 37.10.2 [BB12]

Let $\mathcal{Q}, \mathcal{P} \subset \mathbb{R}[x_1, \ldots, x_k]$ be finite subsets of polynomials such that $\deg(Q) \leq d_0$ for all $Q \in \mathcal{Q}$, $\deg P = d_P$ for all $P \in \mathcal{P}$, and the real dimension of $\mathrm{Zer}(\mathcal{Q}, \mathbb{R}^k)$ is $k' \leq k$. Suppose also that $\mathrm{card}\, \mathcal{P} = s$, and $\deg(P) \leq d, P \in \mathcal{P}$.

Then, the number of connected components of the realizations of all realizable sign conditions of $\mathcal{P}$ on $\mathrm{Zer}(\mathcal{Q}, \mathbb{R}^k)$ is bounded by $(sd)^{k'} d_0^{k-k'} O(1)^k$.

This result opened the doors to using the polynomial partitioning theorem in higher dimensions, and was used to that effect in several papers, for example [Zah12, Zah13, KMSS12, MP15] (see also the survey by Tao [Tao14]). It is also an ingredient in the analysis of the data structure for range searching with semi-algebraic sets due to Agarwal, Matoušek and Sharir [AMS13].

In more sophisticated applications of the polynomial partitioning method a further improvement was needed, in which the bound on the number of connected components depends on a sequence of degrees of arbitrary length. Since dimensions of real varieties (in contrast to complex varieties) can be rather badly behaved (for example, the real variety defined by one non-constant polynomial can be empty), a bound depending on the degree sequence must also take into account the dimensions of the intermediate varieties not just the final variety. This strategy leads to the following theorem.

THEOREM 37.10.3 [BB16]

Let $Q_1, \ldots, Q_\ell \in \mathbb{R}[x_1, \ldots, x_k]$ such that for each $i, 1 \leq i \leq \ell$, $\deg(Q_i) \leq d_i$. For $1 \leq i \leq \ell$, denote by $\mathcal{Q}_i = \{Q_1, \ldots, Q_i\}$, $V_i = \mathrm{Zer}(\mathcal{Q}_i, \mathbb{R}^k)$, and $\dim_{\mathbb{R}}(V_i) \leq k_i$. We set $V_0 = \mathbb{R}^k$, and adopt the convention that $k_i = k$ for $i \leq 0$. Suppose that $2 \leq d_1 \leq d_2 \leq \frac{1}{k+1} d_3 \leq \frac{1}{(k+1)^2} d_4 \leq \cdots \leq \frac{1}{(k+1)^{\ell-2}} d_\ell$. Then,

$$b_0(V_\ell) \leq O(1)^\ell O(k)^{2k} \left(\prod_{1 \leq j < \ell} d_j^{k_{j-1}-k_j} \right) d_\ell^{k_{\ell-1}},$$

and in particular if $\ell \leq k$,

$$b_0(V_\ell) \leq O(k)^{2k} \left(\prod_{1 \leq j < \ell} d_j^{k_{j-1}-k_j} \right) d_\ell^{k_{\ell-1}}.$$

We remark that the (complex) dimension of complex varieties behaves better than the real dimension of real varieties. To see the contrast, consider the following

example. Using the same notation as in Theorem 37.10.3, let for $1 \leq i \leq \ell$, $W_i \subset \mathbb{C}^k$ denote the complex variety defined by the set of polynomials $\mathcal{Q}_i$, and suppose that $W_i \neq \emptyset$. Then, for $1 \leq i < \ell$, $\dim(W_i) - 1 \leq \dim(W_{i+1}) \leq \dim(W_i)$, where $\dim(W_j)$ denotes the complex dimension of $W_j, 1 \leq j \leq \ell$. While the second inequality is also true for the sequence, $(\dim(V_i))_{1 \leq i \leq \ell}$, of real dimensions of the sequence of real varieties V_i, the first inequality is definitely not true in general.

Theorem 37.10.3 enabled progress on several incidence questions (see [Zah15, BS16]).

Aside from its applications in polynomial partitioning, Theorem 37.10.3 also remedies a well-known anomaly, which is that the naive statement of Bézout inequality, that the number of isolated solutions in $\mathbb{C}^n$ of a system of n polynomial equations in n variables is bounded by the product of their degrees, is no longer true for isolated solutions in $\mathbb{R}^n$. This is illustrated by the following well-known example [Ful98]. Let $k = 3$, and let

$$\begin{aligned} Q_1 &= x_3, \\ Q_2 &= x_3, \\ Q_3 &= \sum_{i=1}^{2} \left(\prod_{j=1}^{d} (x_i - j)^2 \right). \end{aligned}$$

The real variety defined by $\{Q_1, Q_2, Q_3\}$ is 0-dimensional, and has d^2 isolated (in $\mathbb{R}^3$) points, whereas the degree sequence is $(d_1, d_2, d_3) = (1, 1, 2d)$, and thus the bound predicted by the naive Bézout inequality is equal to $2d$.

37.11 APPLICATIONS

Computational real algebraic geometry finds applications in robotics, vision, computer-aided design, geometric theorem proving, and other fields. Important problems in robotics include kinematic modeling, the inverse kinematic solution, computation of the workspace and workspace singularities, and the planning of an obstacle-avoiding motion of a robot in a cluttered environment—all arising from the algebro-geometric nature of robot kinematics. In solid modeling, graphics, and vision, almost all applications involve the description of surfaces, the generation of various auxiliary surfaces such as blending and smoothing surfaces, the classification of various algebraic surfaces, the algebraic or geometric invariants associated with a surface, the effect of various affine or projective transformations of a surface, the description of surface boundaries, and so on.

To give examples of the nature of the solutions demanded by various applications, we discuss a few representative problems from robotics, engineering, and computer science.

ROBOT MOTION PLANNING

Given the initial and desired configurations of a robot (composed of rigid subparts) and a set of obstacles, find a collision-free continuous motion of the robot from the initial configuration to the final configuration.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

The algorithm proceeds in several steps. The first step translates the problem to ***configuration space***, a parameter space modeled as a low-dimensional algebraic manifold (assuming that the obstacles and the robot subparts are bounded by piecewise algebraic surfaces). The second step computes the set of configurations that avoid collisions and produces a semialgebraic description of this so-called "free space" (subspaces of the configuration space). Since the initial and final configurations correspond to two points in the configuration space, we simply have to test whether they lie in the same connected component of the free space. If so, they can be connected by a piecewise algebraic path. Such a path gives rise to an obstacle-avoiding motion of the robot(s) and can be computed using either Collins's CAD [SS83], yielding an algorithm with doubly-exponential time complexity, or by computing a roadmap (Theorem 37.8.1) which yields a singly exponential algorithm.

OFFSET SURFACE CONSTRUCTION IN SOLID MODELING

Given a polynomial $f(x, y, z)$, whose zeros define an algebraic surface in three-dimensional space, compute the envelope of a family of spheres of radius r whose centers lie on the surface f. Such a surface is called a (two-sided) ***offset surface*** of f.

Let $p = \langle x, y, z\rangle$ be a point on the offset surface and $q = \langle u, v, w\rangle$ be a ***footprint*** of p on f; that is, q is the point at which a normal from p to f meets f. Let $\vec{t_1} = \langle t_{1,1}, t_{1,2}, t_{1,3}\rangle$ and $\vec{t_2} = \langle t_{2,1}, t_{2,2}, t_{2,3}\rangle$ be two linearly independent tangent vectors to f at the point q. Then, we see that the system of polynomial equations

$$\begin{aligned}(x-u)^2 + (y-v)^2 + (z-w)^2 - r^2 &= 0,\\ f(u,v,w) &= 0,\\ (x-u)t_{1,1} + (y-v)t_{1,2} + (z-w)t_{1,3} &= 0,\\ (x-u)t_{2,1} + (y-v)t_{2,2} + (z-w)t_{2,3} &= 0,\end{aligned}$$

describes a surface in the (x, y, z, u, v, w) six-dimensional space, which, when projected into the three-dimensional space with coordinates (x, y, z), gives the offset surface in an implicit form. The offset surface is computed by simply eliminating the variables u, v, w from the preceding set of equations.

This approach (the ***envelope method***) of computing the offset surface has several problematic features: the method does not deal with self-intersection in a clean way and, sometimes, generates additional points not on the offset surface. For a discussion of these and several other related problems in solid modeling, see [Hof89] and Chapter 57 of this Handbook.

GEOMETRIC THEOREM PROVING

Given a geometric statement consisting of a finite set of hypotheses and a conclusion,

$$\begin{aligned}\text{Hypotheses} &: \quad f_1(x_1, \ldots, x_k) = 0, \ldots, f_r(x_1, \ldots, x_k) = 0\\ \text{Conclusion} &: \quad g(x_1, \ldots, x_k) = 0\end{aligned}$$

decide whether the conclusion $g = 0$ is a consequence of the hypotheses $((f_1 = 0) \wedge \cdots \wedge (f_r = 0))$.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

Thus we need to determine whether the following universally quantified first-order sentence holds:

$$\Big(\forall\, x_1, \ldots, x_k\Big)\ \Big[\ \Big((f_1 = 0) \wedge \cdots \wedge (f_r = 0)\Big)\ \Rightarrow\ g = 0\Big].$$

One way to solve the problem is by first translating it into the form: decide if the following existentially quantified first-order sentence is unsatisfiable:

$$\Big(\exists\, x_1, \ldots, x_k, z\Big)\ \Big[\ (f_1 = 0) \wedge \cdots \wedge (f_r = 0) \wedge (gz - 1) = 0\Big].$$

When the underlying domain is assumed to be the field of real numbers, then we may simply check whether the following multivariate polynomial (in $x_1, \ldots, x_k, z$) has no real root:

$$f_1^2 + \cdots + f_r^2 + (gz - 1)^2.$$

If, on the other hand, the underlying domain is assumed to be the field of complex numbers (an algebraically closed field), then other tools from computational algebra are used (e.g., techniques based on Hilbert's Nullstellensatz). In the general setting, some techniques based on Ritt-Wu characteristic sets have proven very powerful. See [Cho88].

For another approach to geometric theorem proving, see Section 57.4.

CONNECTION TO SEMIDEFINITE PROGRAMMING

Checking ***global nonnegativity*** of a function of several variables occupies a central role in many areas of applied mathematics, e.g., optimization problems with polynomial objectives and constraints, as in quadratic, linear and Boolean programming formulations. These problems have been shown to be NP-hard in the most general setting, but do admit good approximations involving polynomial-time computable relaxations (see Parillo [Par00]).

Provide checkable conditions or procedure for verifying the validity of the proposition

$$F(x_1, \ldots, x_k) \geq 0, \quad \forall x_1, \ldots, x_k,$$

where F is a multivariate polynomial in the ring of multivariate polynomials over the reals, $\mathbb{R}[x_1, \ldots, x_k]$.

An obvious necessary condition for F to be globally nonnegative is that it has even degree. On the other hand, a rather simple sufficient condition for a real-valued polynomial $F(x)$ to be globally nonnegative is the existence of a ***sum-of-squares decomposition***:

$$F(x_1, \ldots, x_k) = \sum_i f_i^2(x_1, \ldots, x_k), \quad f_i(x_1, \ldots, x_k) \in \mathbb{R}[x_1, \ldots, x_k].$$

Thus one way to solve the global nonnegativity problem is by finding a sum-of-squares decomposition. Note that since there exist globally nonnegative polynomials not admitting a sum-of-squares decomposition (e.g., the Motzkin form $x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2$), the procedure suggested below does not give a solution to the problem in all situations.

The procedure can be described as follows: express the given polynomial $F(x_1, \ldots, x_k)$ of degree $2d$ as a quadratic form in all the monomials of degree less than or equal to d:

$$F(x_1, \ldots, x_k) = z^T Q z, \quad z = [1, x_1, \ldots, x_k, x_1 x_2, \ldots x_k^d],$$

where Q is a constant matrix to be determined. If the above quadratic form can be solved for a positive semidefinite Q, then $F(x_1, \ldots, x_k)$ is globally nonnegative. Since the variables in z are not algebraically independent, the matrix Q is not unique, but lives in an affine subspace. Thus, we need to determine if the intersection of this affine subspace and the positive semidefinite matrix cone is nonempty. This problem can be solved by a ***semidefinite programming*** feasibility problem

$$\begin{aligned} \text{trace}(z z^T Q) &= F(x_1, \ldots, x_k), \\ Q &\succeq 0. \end{aligned}$$

The dimensions of the matrix inequality are $\binom{k+d}{d} \times \binom{k+d}{d}$ and are polynomial for a fixed number of variables (k) or fixed degree (d). Thus our question reduces to efficiently solvable semidefinite programming (SDP) problems.

37.12 SOURCES AND RELATED MATERIAL

SURVEYS

[Mis93]: A textbook for algorithmic algebra covering Gröbner bases, characteristic sets, resultants, and real algebra. Chapter 8 gives many details of the classical results in computational real algebra.

[BPR16] A textbook on algorithm in real algebraic geometry covering modern techniques and algorithms for solving the fundamental algorithmic problems in semi-algebraic geometry. Contains all relevant mathematical background including the theory of general real closed fields, real algebra, algebraic topology and Morse theory etc.

[Bas08] A survey of algorithms in semi-algebraic geometry and topology with particular emphasis on the connections to discrete and computational geometry.

[BHK+11] A collection of survey articles on modern developments in real algebraic geometry including modern developments in algorithmic real algebraic geometry.

[CJ98]: An anthology of key papers in computational real algebra and real algebraic geometry. Contains reprints of the following papers cited in this chapter: [BPR98, Col75, Ren91, Tar51].

[AB88]: A special issue of the *J. Symbolic Comput.* on computational real algebraic geometry. Contains several papers ([DH88, Gri88, GV88] cited here) addressing many key research problems in this area.

[BR90]: A very accessible and self-contained textbook on real algebra and real algebraic geometry.

[BCR98]: A self-contained textbook on real algebra and real algebraic geometry.

[HRR91]: A survey of many classical and recent results in computational real algebra.

[Cha94]: A survey of the connections among computational geometry, computational algebra, and computational real algebraic geometry.

[Tar51]: Primary reference for Tarski's classical result on the decidability of elementary algebra.

[Col75]: Collins's work improving the complexity of Tarski's solution for the decision problem [Tar51]. Also, introduces the concept of cylindrical algebraic decomposition (CAD).

[Ren91]: A survey of some recent results, improving the complexity of the decision problem and quantifier elimination problem for the first-order theory of reals. This is mostly a summary of the results first given in a sequence of papers by Renegar [Ren92a, Ren92b, Ren92c].

[Lat91]: A comprehensive textbook covering various aspects of robot motion planning problems and different solution techniques. Chapter 5 includes a description of the connection between the motion planning problem and computational real algebraic geometry.

[SS83]: A classic paper in robotics showing the connection between the robot motion planning problem and the connectivity of semialgebraic sets using CAD. Contains several improved algorithmic results in computational real algebra.

[Can87]: Gives a singly-exponential time algorithm for the robot motion planning problem and provides complexity improvement for many key problems in computational real algebra.

[Hof89]: A comprehensive textbook covering various computational algebraic techniques with applications to solid modeling. Contains a very readable description of Gröbner bases algorithms.

[Cho88]: A monograph on geometric theorem proving using Ritt-Wu characteristic sets. Includes computer-generated proofs of many classical geometric theorems.

RELATED CHAPTERS

Chapter 50: Algorithmic motion planning
Chapter 51: Robotics
Chapter 57: Solid modeling
Chapter 60: Geometric applications of the Grassmann-Cayley algebra

REFERENCES

[AB88] D. Arnon and B. Buchberger, editors, *Algorithms in Real Algebraic Geometry*. Special Issue: *J. Symbolic Comput.*, 5(1-2), 1988.

[AMS13] P.K. Agarwal, J. Matoušek, and M. Sharir. On range searching with semialgebraic sets. II. *SIAM J. Comput.*, 42:2039–2062, 2013.

[Bas99a] S. Basu. New results on quantifier elimination over real closed fields and applications to constraint databases. *J. ACM*, 46:537–555, 1999.

[Bas99b] S. Basu. On bounding the Betti numbers and computing the Euler characteristic of semi-algebraic sets. *Discrete Comput. Geom.*, 22:1–18, 1999.

[Bas06] S. Basu. Computing the first few Betti numbers of semi-algebraic sets in single exponential time. *J. Symbolic Comput.*, 41:1125–1154, 2006.

[Bas08] S. Basu. Algorithmic semi-algebraic geometry and topology—recent progress and open problems. In *Surveys on Discrete and Computational Geometry: Twenty Years Later*, vol. 453 of *Contemporary Math.*, pages 139–212, AMS, Providence, 2008.

[BB12] S. Barone and S. Basu. Refined bounds on the number of connected components of sign conditions on a variety. *Discrete Comput. Geom.*, 47:577–597, 2012.

[BB16] S. Barone and S. Basu. On a real analog of Bezout inequality and the number of connected components of sign conditions. *Proc. Lond. Math. Soc. (3)*, 112:115–145, 2016.

[BCR98] J. Bochnak, M. Coste, and M.-F. Roy. *Real Algebraic Geometry*. Springer-Verlag, Berlin, 1998. (Also in French, *Géométrie Algébrique Réelle*. Springer-Verlag, Berlin, 1987.)

[BCR08] F. Boudaoud, F. Caruso, and M.-F. Roy. Certificates of positivity in the Bernstein basis. *Discrete Comput. Geom.*, 39:639–655, 2008.

[BCSS98] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, New York, 1998.

[BHK+11] S. Basu, J. Huisman, K. Krzysztof, V. Powers, and J.-P. Rolin. Real algebraic geometry. In *Real Algberaic Geometry*, Rennes, France, 2011.

[BOKR86] M. Ben-Or, D. Kozen, and J. Reif. The complexity of elementary algebra and geometry. *J. Comp. Systems Sci.*, 18:251–264, 1986.

[BPR96] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43:1002–1045, 1996.

[BPR98] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, *Texts Monogr. Symbol. Comput.*, pages 341–350, Springer-Verlag, Vienna, 1998.

[BPR00] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety. *J. Amer. Math. Soc.*, 13:55–82, 2000.

[BPR05a] S. Basu, R. Pollack, and M.-F. Roy. On the Betti numbers of sign conditions. *Proc. Amer. Math. Soc.*, 133:965–974, 2005.

[BPR05b] S. Basu, R. Pollack, and M.-F. Roy. Computing the Euler-Poincaré characteristics of sign conditions. *Comput. Complexity*, 14:53–71, 2005.

[BPR08] S. Basu, R. Pollack, and M.-F. Roy. Computing the first Betti number of a semi-algebraic set. *Found. Comput. Math.*, 8:97–136, 2008.

[BPR16] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*. Second edition, Springer, Berlin, 2006. Revised version of the second edition online at `http://perso.univ-rennes1.fr/marie-francoise.roy/`, 2016.

[BR10] S. Basu and M.-F. Roy. Bounding the radii of balls meeting every connected component of semi-algebraic sets. *J. Symbolic Comput.*, 45:1270–1279, 2010.

[BR90] R. Benedetti and J.-J. Risler. *Real Algebraic and Semi-algebraic Sets*. Actualités Mathématiques, Hermann, Paris, 1990.

[BR14] S. Basu and M.-F. Roy. Divide and conquer roadmap for algebraic sets. *Discrete Comput. Geom.*, 52:278–343, 2014.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

[BRS+14] S. Basu, M.-F. Roy, M. Safey El Din, and É. Schost. A baby step–giant step roadmap algorithm for general algebraic sets. *Found. Comput. Math.*, 14:1117–1172, 2014.

[BS16] S. Basu and M. Sombra. Polynomial partitioning on varieties of codimension two and point-hypersurface incidences in four dimensions. *Discrete Comput. Geom.*, 55:158-184, 2016.

[BSS89] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc. (N.S.)*, 21:1–46, 1989.

[BV07] S. Basu and N. Vorobjov. On the number of homotopy types of fibres of a definable map. *J. Lond. Math. Soc. (2)*, 76:757–776, 2007.

[Can87] J.F. Canny. *The Complexity of Robot Motion Planning.* MIT Press, Cambridge, 1988.

[Can88] J. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. 20th ACM Sympos. Theory Comput.*, pages 460–467, 1988.

[Can90] J. Canny. Generalised characteristic polynomials. *J. Symbolic Comput.*, 9:241–250, 1990.

[Can93] J. Canny. Improved algorithms for sign determination and existential quantifier elimination. *Comput. J.*, 36:409–418, 1993.

[CEG+90] K.L. Clarkson, H. Edelsbrunner, L.J. Guibas, M. Sharir, and E. Welzl. Combinatorial complexity bounds for arrangements of curves and spheres. *Discrete Comput. Geom.*, 5:99–160, 1990.

[Cha94] B. Chazelle. Computational geometry: A retrospective. In *Proc. 26th ACM Sympos. Theory Comput.*, pages 75–94, 1994.

[Cho88] S.-C. Chou. *Mechanical Geometry Theorem Proving.* Vol. 41 of *Mathematics and its Applications*, Reidel Publishing Co., Dordrecht, 1988.

[CJ98] B.F. Caviness and J.R. Johnson, editors. *Quantifier Elimination and Cylindrical Algebraic Decomposition. Texts Monogr. Symbol. Comput.*, Springer-Verlag, Vienna, 1998.

[Col75] G.E. Collins. Quantifier elimination for real closed fields by cylindric algebraic decomposition. In *Proc. 2nd GI Conf. on Automata Theory and Formal Languages*, vol. 33 of *Lecture Notes Comp. Sci.*, pages 134–183, Springer, Berlin, 1975.

[DH88] J.H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *J. Symbolic Comp.*, 5:29–35, 1988.

[ES11] G. Elekes and M. Sharir. Incidences in three dimensions and distinct distances in the plane. *Combin. Probab. Comput.*, 20:571–608, 2011.

[Ful98] W. Fulton. *Intersection theory.* Volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*, 2nd edition, Springer, Berlin, 1998.

[GK15] L. Guth and N.H. Katz. On the Erdős distinct distances problem in the plane. *Ann. of Math. (2)*, 181:155–190, 2015.

[GP86a] J.E. Goodman and R. Pollack. There are asymptotically far fewer polytopes than we thought. *Bull. Amer. Math. Soc. (N.S.)*, 14:127–129, 1986.

[GP86b] J.E. Goodman and R. Pollack. Upper bounds for configurations and polytopes in $\mathbb{R}^d$. *Discrete Comput. Geom.*, 1:219–227, 1986.

[GPW95] J.E. Goodman, R. Pollack, and R. Wenger. On the connected components of the space of line transversals to a family of convex sets. *Discrete Comput. Geom.*, 13:469–476, 1995.

[GR93] L. Gournay and J.-J. Risler. Construction of roadmaps of semi-algebraic sets. *Appl. Algebra Eng. Commun. Comput.*, 4:239–252, 1993.

[Gri88] D.Y. Grigoriev. Complexity of deciding Tarski algebra. *J. Symbolic Comput.*, 5:65–108, 1988.

[Gut15a] L. Guth. Distinct distance estimates and low degree polynomial partitioning. *Discrete Comput. Geom.*, 53:428–444, 2015.

[Gut15b] L. Guth. Polynomial partitioning for a set of varieties. *Math. Proc. Cambridge Philos. Soc.*, 159:459–469, 2015.

[GV88] D.Y. Grigoriev and N.N. Vorobjov, Jr. Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Comput.*, 5:37–64, 1988.

[GV92] D.Y. Grigoriev and N.N. Vorobjov, Jr. Counting connected components of a semi-algebraic set in subexponential time. *Comput. Complexity*, 2:133–186, 1992.

[GV05] A. Gabrielov and N. Vorobjov. Betti numbers of semialgebraic sets defined by quantifier-free formulae. *Discrete Comput. Geom.*, 33:395–401, 2005.

[GV09] A. Gabrielov and N. Vorobjov. Approximation of definable sets by compact families, and upper bounds on homotopy and homology. *J. Lond. Math. Soc. (2)*, 80:35–54, 2009.

[GV15] A. Gabrielov and N. Vorobjov. On topological lower bounds for algebraic computation trees. *Found. Comput. Math.*, to appear.

[Hof89] C.M. Hoffmann. *Geometric and Solid Modeling.* Morgan Kaufmann, San Mateo, 1989.

[HRR91] J. Heintz, T. Recio, and M.-F. Roy. Algorithms in real algebraic geometry and applications to computational geometry. In J.E. Goodman, R. Pollack, and W. Steiger, editors, *Discrete and Computational Geometry*, vol. 6 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 137–163, AMS, Providence, 1991.

[HRS89] J. Heintz, M.-F. Roy, and P. Solernó. On the complexity of semi-algebraic sets. In *Proc. IFIP 11th World Computer Congr.*, pages 293–298, North-Holland, Amsterdam, 1989.

[HRS90] J. Heintz, M.-F. Roy, and P. Solernó. Sur la complexité du principe de Tarski-Seidenberg. *Bull. Soc. Math. France*, 118:101–126, 1990.

[JPT13] G. Jeronimo, D. Perrucci, and E. Tsigaridas. On the minimum of a polynomial function on a basic closed semialgebraic set and applications. *SIAM J. Optim.*, 23:241–255, 2013.

[KMSS12] H. Kaplan, J. Matoušek, Z. Safernová, and M. Sharir. Unit distances in three dimensions. *Combin. Probab. Comput.*, 21:597–610, 2012.

[Lat91] J.-C. Latombe. *Robot Motion Planning.* Vol. 124 of *Internat. Ser. Engrg. Comp. Sci.*. Kluwer, Dordrecht, 1991.

[Mat02] J. Matoušek. *Lectures on Discrete Geometry.* Vol. 212 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2002.

[Mil64] J. Milnor. On the Betti numbers of real varieties. *Proc. Amer. Math. Soc.*, 15:275–280, 1964.

[Mis93] B. Mishra. *Algorithmic Algebra. Texts and Monographs in Computer Science*, Springer-Verlag, New York, 1993.

[MMP96] J.L. Montaña, J.E. Morais, and L.M. Pardo. Lower bounds for arithmetic networks. II. Sum of Betti numbers. *Appl. Algebra Engrg. Comm. Comput.*, 7:41–51, 1996.

[MP15] J. Matoušek and Z. Patáková. Multilevel polynomial partitions and simplified range searching. *Discrete Comput. Geom.*, 54:22–41, 2015.

[Par00] P.A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*, PhD Thesis, California Institute of Technology, Pasadena, 2000.

[PO49] I.G. Petrovskiĭ and O.A. Oleĭnik. On the topology of real algebraic surfaces. *Izvestiya Akad. Nauk SSSR. Ser. Mat.*, 13:389–402, 1949.

[Ren91] J. Renegar. Recent progress on the complexity of the decision problem for the reals. In J.E. Goodman, R. Pollack, and W. Steiger, editors, *Discrete and Computational Geometry*, vol. 6 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 287–308, AMS, Providence, 1991.

[Ren92a] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. I. Introduction. Preliminaries. The geometry of semi-algebraic sets. The decision problem for the existential theory of the reals. *J. Symbolic Comput.*, 13:255–299, 1992.

[Ren92b] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. II. The general decision problem. Preliminaries for quantifier elimination. *J. Symbolic Comput.*, 13:301–327, 1992.

[Ren92c] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. III. Quantifier elimination. *J. Symbolic Comput.*, 13:329–352, 1992.

[SS83] J.T. 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.

[SS10] M. Safey el Din and É. Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete Comput. Geom.*, 45:181–220, 2010.

[SS17] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63:48, 2017.

[SS14] M. Sharir and N. Solomon. Incidences between points and lines in $\mathbb{R}^4$. In *Proc. 30th Sympos. Comput. Geom.*, pages 189–197, ACM, New York, 2014.

[SSS13] M. Sharir, A. Sheffer, and J. Solymosi. Distinct distances on two lines. *J. Combin. Theory Ser. A*, 120:1732–1736, 2013.

[SSZ15] M. Sharir, A. Sheffer, and J. Zahl. Improved bounds for incidences between points and circles. *Combin. Probab. Comput.*, 24:490–520, 2015.

[ST42] A.H. Stone and J.W. Tukey. Generalized "sandwich" theorems. *Duke Math. J.*, 9:356–359, 1942.

[Stu35] C. Sturm. Mémoire sur la Résolution des Équations Numériques. *Mém. Savants Etrangers*, 6:271–318, 1835.

[Syl53] J.J. Sylvester. On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraic common measure. *Philos. Trans. Roy. Soc. London*, 143:407–548, 1853.

[Tao14] T. Tao. Algebraic combinatorial geometry: The polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. *EMS Surveys Math. Sci.*, 1:1–46, 2014.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.

[Tar51] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*, second edition. University of California Press, 1951.

[Tho65] 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 University Press, 1965.

[Yao97] A.C.-C. Yao. Decision tree complexity and Betti numbers. *J. Comput. Syst. Sci.*, 55:36–43, 1997.

[Zah12] J. Zahl. On the Wolff circular maximal function. *Illinois J. Math.*, 56:1281–1295, 2012.

[Zah13] J. Zahl. An improved bound on the number of point-surface incidences in three dimensions. *Contrib. Discrete Math.*, 8:100–121, 2013.

[Zah15] J. Zahl. A Szemerédi–Trotter type theorem in $\mathbb{R}^4$. *Discrete Comput. Geom.*, 54:513–572, 2015.

Preliminary version (July 19, 2017). To appear in the Handbook of Discrete and Computational Geometry, J.E. Goodman, J. O'Rourke, and C. D. Tóth (editors), 3rd edition, CRC Press, Boca Raton, FL, 2017.