COMPUTATIONAL REAL ALGEBRAIC GEOMETRY

Bhubaneswar Mishra

INTRODUCTION

Computational real algebraic geometry studies various algorithmic 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 1). The associated geometric structures are then examined via an exploration of the *semi-algebraic sets* (Section 2). Algorithmic problems for semi-algebraic sets are considered next. In particular, there is a discussion of real algebraic numbers and their representation which relies on such classical theorems as Sturm's theorem and Thom's Lemma (Section 3). This discussion is followed by a description of semi-algebraic sets using the concept of *cylindrical algebraic decomposition* (CAD) both in one and higher dimensions (Sections 4 & 5). This leads to brief descriptions of two algorithmic approaches for the decision and quantifier elimination problems (Section 6): namely, Collin's algorithm based on CAD and some more recent approaches based on critical points techniques and a reduction scheme transforming the multivariate problem to easier univariate problems. These new approaches rely on the work of several groups of researchers: Grigor'ev and Vorobjov, Canny, Heintz et. al., Renegar and Basu et. al. A few representative applications of computational algebra concludes this chapter (Section 7).

31.1 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 any arbitrary Tarski formula in the first-order theory of reals. As a result of Tarski's work [Tar51], we have the following theorem.

Theorem 1

- *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) 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, …, x_n.

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's 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's and z's, 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 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), then

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

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

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

prenex Tarski formula: A Tarski formula of the form

$$\Big(Q\ x_1\Big)\ \Big(Q\ x_2\Big)\ \cdots \Big(Q\ x_n\Big)\ \Big[\phi(y_1, y_2, \ldots, y_r, x_1, \ldots, x_n)\Big],$$

where ϕ is quantifier-free. The string of quantifiers $(Q\ x_1)\ (Q\ x_2) \cdots (Q\ x_n)$ 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 such that the same variable does not occur as free and bound, 3) Move negations inward and finally, 4) Push quantifiers to the left.

extension of a Tarski formula $\Phi(y_1, \ldots, y_r)$ with free variables $\{y_1, \ldots, y_r\}$: The set of all $\langle \zeta_1, \ldots, \zeta_r \rangle \in \mathbb{R}^r$ such that

$$\Phi(\zeta_1, \ldots, \zeta_r) = \mathsf{True}.$$

THE DECISION PROBLEM

The general *decision problem* for the first-order theory of reals is to determine if a *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 is due to Collins [Col75] and 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 [Can88b, Can93], Heintz et. al. [HRS89, HRS90], Renegar [Ren92a,b,c]) and most recently by Basu et. al. [BPR95].

In the following, we assume that our Tarski sentence is presented as shown below, 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 being distinct), $\mathbf{x}^{[i]}$ is a partition of all the variables

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

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

$$g_i\left(\mathbf{x}^{[1]},\ldots,\mathbf{x}^{[\omega]}\right) \mathrel{\substack{>\\=\\<}} 0, \quad i = 1,\ldots,m.$$

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 total of m 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 n, n_i, ω, m and d and the bit complexity will involve L as well.

Table 31.1 highlights a representative set of known bit-complexity results for the decision problem.

QUANTIFIER ELIMINATION PROBLEM

Formally, given a Tarski formula of the form,

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

TABLE 31.1 Some selected set of Time Complexity results

General or Existential	Time Complexity	Source
General	$L^3(md)^{2^{O(\Sigma n_i)}}$	[Col75]
Existential	$L^{O(1)}(md)^{O(n^2)}$	[GV92]
General	$L^{O(1)}(md)^{(O(\sum n_i))^{4\omega-2}}$	[Gri88]
Existential	$L^{1+o(1)}\ (m)^{(n+1)}\ (d)^{O(n^2)}$	[Can88b, Can93]
General	$(L \log L \log\log L)(md)^{(2^{O(\omega)})\Pi n_i}$	[Ren92a,b,c]
Existential	$(L \log L \log\log L) m\ (m/n)^n\ (d)^{O(n)}$	[BPR94b]
General	$(L \log L \log\log L)(m)^{\Pi(n_i+1)}(d)^{\Pi O(n_i)}$	[BPR94b]

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.

Currently the best bounds are due to Basu et. al. [BPR94b] and are summarized as follows:

$$\begin{aligned} I &\leq (m)^{\prod (n_i+1)} (d)^{\prod O(n_i)} \\ J_i &\leq (m)^{\prod_{i>0} (n_i+1)} (d)^{\prod_{i>0} O(n_i)}. \end{aligned}$$

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

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

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

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

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

31.2 SEMI-ALGEBRAIC SETS

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

GLOSSARY

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

$$S = \bigcup_{i=1}^{I} \bigcap_{j=1}^{J_i} \left\{ \langle \xi_1, \ldots, \xi_n \rangle \in \mathbb{R}^n \ : \ \mathrm{sgn}(f_{i,j}(\xi_1, \ldots, \xi_n)) = s_{i,j} \right\},$$

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

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

$$Z = \left\{ \langle \xi_1, \ldots, \xi_n \rangle \in \mathbb{R}^n \ : \ f_1(\xi_1, \ldots, \xi_n) = \cdots = f_m(\xi_1, \ldots, \xi_n) = 0 \right\},$$

where f_i's are multivariate polynomials over $\mathbb{R}$.

semi-algebraic map: A map $\theta : S \to T$, from a semi-algebraic set $S \subseteq \mathbb{R}^m$ to a semi-algebraic set $T \subseteq \mathbb{R}^n$ such that its graph

$$\left\{ \langle s, \theta(s) \rangle \in \mathbb{R}^{m+n} : s \in S \right\}$$

is a semi-algebraic set in $\mathbb{R}^{m+n}$. Note that projection is semi-algebraic (since, linear) map.

TARSKI-SEIDENBERG THEOREM

Equivalently, semi-algebraic sets can be defined as

$$S = \left\{ \langle \xi_1, \ldots, \xi_n \rangle \in \mathbb{R}^n \ : \ \psi(\xi_1, \ldots, \xi_n) = \mathsf{True} \right\}.$$

where $\psi(x_1, \ldots, x_n)$ 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 semi-algebraic sets.

While real algebraic sets are quite interesting as they 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, *semi-algebraic 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.

Tarski-Seidenberg Theorem
Let S be a semi-algebraic set in $\mathbb{R}^m$ and

$$\theta : \mathbb{R}^m \to \mathbb{R}^n$$

be a semi-algebraic map. Then $\theta(S)$ is semi-algebraic in $\mathbb{R}^n$.

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

GLOSSARY

connected component of a semi-algebraic set: A maximal connected subset of a semi-algebraic set. Semi-algebraic sets have a finite number of connected components and these are also semi-algebraic.

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

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

sign assignment: A vector of sign values of a set of polynomials at a point p. More formally, let $\mathcal{F}$ be a set of real multivariate polynomials in n variables. Any point $p = \langle \xi_1, \ldots, \xi_n \rangle \in \mathbb{R}^n$ has a *sign assignment* with respect to $\mathcal{F}$ as follows:

$$\mathrm{sgn}_{\mathcal{F}}(p) = \Big\langle \mathrm{sgn}(f(\xi_1, \ldots, \xi_n)) : f \in \mathcal{F} \Big\rangle.$$

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

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

sign class of $\mathcal{F}$: An equivalence class in the partition of $\mathbb{R}^n$ defined by the equivalence relation $\sim_{\mathcal{F}}$.

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

cell decomposition for $\mathcal{F}$: A semi-algebraic decomposition for $\mathcal{F}$ into finitely many disjoint semi-algebraic subsets, $\{C_i\}$, called *cells* such that we have the following: each cell C_i is homeomorphic to $\mathbb{R}^{\delta(i)}$, $0 \le \delta(i) \le n$. $\delta(i)$ is called the *dimension of the cell* C_i, and C_i is called a $\delta(i)$-*cell*.

cellular decomposition for $\mathcal{F}$: A cell decomposition for $\mathcal{F}$ such that the closure of each cell C_i, $\overline{C_i}$, is a union of cells C_j:

$$\overline{C_i} = \bigcup_j C_j.$$

CONNECTED COMPONENTS OF SEMI-ALGEBRAIC SETS

A consequence of the Milnor-Thom result [Mil64, Tho65] gives a bound for the number (zeroth Betti number, $B_0(S)$) of connected components of a basic semi-algebraic set S which is polynomial in the number m and degree d of the polynomials defining S and singly exponential in the number of variables, n. The current best bound for $B_0(S)$ is due to Pollack and Roy [PR93]: namely, $B_0(S) = (O(md/n))^n$.

A key problem in computational real algebraic geometry is to compute at least one point in each connected component of each non-empty sign assignment. An elegant solution to this problem is obtained by Collin's *cylindrical algebraic decomposition* or CAD, which is, in fact, a cell decomposition. A related question is to provide a finitary representation for these sample points, e.g., each coordinate of the sample point may be a *real algebraic number*.

Currently, the best algorithm computing a finite set of points of bounded size which intersects *every connected component* of each non-empty sign conditions is due to Basu et. al. [BPR95] and has an arithmetic time-complexity of $m(m/n)^n d^{O(n)}$.

31.3 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 rely upon techniques based on 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 0 is $-\infty$.

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 2 *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 choices: *order* (where we assume the real roots are indexed from left to right), *sign* (by a vector of signs) and *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 (non-overlapping) intervals that isolate the real roots of p.

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

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

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

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 $D: \mathbb{R}[t] \to \mathbb{R}[t]$ is the (formal) derivative map, taking t^n to nt^{n-1} and $a \in \mathbb{R}$ (a constant) to 0.

STURM-SYLVESTER THEOREM

Sturm-Sylvester Theorem *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

$$\begin{array}{rcl} \overline{P} & \triangleq & \overline{\text{STURM}}(p, p'q), \quad \textit{and} \\ \text{Var}\Big[\overline{P}\Big]_a^b & \triangleq & \text{Var}_a(\overline{P}) - \text{Var}_b(\overline{P}). \end{array}$$

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

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

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

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

These identities as well as some related algorithmic results (the so-called BKR-algorithm) are based on the results due to Ben-Or et. al. [BKR86] 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 later.

GLOSSARY

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

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

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

sign-invariant region: of $\mathbb{R}$ determined by a sign sequence $\overline{s}$ with respect to $\overline{\text{FOURIER}}(p)$:

The region $R(\overline{s})$, such that $\xi \in R(\overline{s})$ if and only if $\text{sgn}(p^{(i)}(\xi)) = s_i$.

THOM'S LEMMA

Thom's Lemma *Every nonempty sign-invariant region $R(\overline{s})$ (determined by a sign sequence $\overline{s}$ with respect to $\overline{\text{FOURIER}}(p)$) 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 *Let ξ and ζ be two real roots of a real univariate polynomial $p(t)$ of positive degree $n > 0$. Then $\xi = \zeta$, if*

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

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 the Thom's Lemma.

interval representation of an algebraic number: A triple consisting of its polynomial, p, and the two end points 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*: $\langle\sqrt{2}+\sqrt{3}\rangle_i = \langle x^4 - 10x^2 + 1, 3, 7/2\rangle$.

31.4 UNIVARIATE DECOMPOSITION

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

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

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 semi-algebraic 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:

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

Now, given a first-order formula involving a single variable, the validity of it can be inferred 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. [BKR86], 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" (i.e., simple processors).

31.5 MULTIVARIATE DECOMPOSITION

A straightforward generalization of the standard univariate decomposition to higher dimensions is provided by Collin's *cylindrical algebraic decomposition* (CAD). In order to represent a semi-algebraic set $S \subseteq \mathbb{R}^n$, we may assume recursively that we can construct a cell decomposition of its projection $\pi(S) \subseteq \mathbb{R}^{n-1}$ (also a semi-algebraic 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 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 semi-algebraic set $S \subseteq \mathbb{R}^n$, then at no additional cost, we may in fact compute a cell decomposition for $\mathcal{F}$ using the procedure described above. Such a decomposition leads to a *cylindrical algebraic decomposition* (or CAD) for $\mathcal{F}$.

GLOSSARY

cylindrical algebraic decomposition (CAD): A recursively defined cell decomposition of $\mathbb{R}^n$ for $\mathcal{F}$. The decomposition is a cellular decomposition if the set of defining polynomials $\mathcal{F}$ satisfies certain non-degeneracy conditions.

In the recursive definition, the cells of n-dimensional CAD are constructed from an $(n-1)$-dimensional CAD: Every $(n-1)$-dimensional CAD cell 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 $(n-1)$-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 of at most $O(md)^2$ many $(n-1)$-variate polynomials, $\Phi(\mathcal{F})$, obtained by considering *principal subresultant coefficients* (PSC's). These PSC's generalize the concepts of *resultants* and *discriminants*, and ensure that the polynomials of $\mathcal{F}$ do not "intersect" or "fold" in a cylinder over an $(n-1)$-dimensional cell. The polynomials in $\Phi(\mathcal{F})$ are each of degree no more than d^2.

More formally, an $\mathcal{F}$-sign-invariant cylindrical algebraic decomposition of $\mathbb{R}^n$ is:

- Base Case: $n = 1$. A univariate cellular decomposition of $\mathbb{R}^1$ as in the previous section.
- Inductive Case: $n > 1$. Let $\mathcal{K}'$ be a $\Phi(\mathcal{F})$-sign-invariant CAD of $\mathbb{R}^{n-1}$. For each cell $C' \in \mathcal{K}'$, define an *auxiliary polynomial* $g_{C'}(x_1, \ldots, x_{n-1}, x_n)$ as the product of those polynomials of $\mathcal{F}$ that do not vanish over the $(n-1)$-dimensional cell, C'. The real roots of the auxiliary polynomial g'_C over C' give rise to a finite (perhaps, zero) number of semi-algebraic continuous functions, which partition the cylinder $C' \times (\mathbb{R} \cup \{\pm\infty\})$ into finitely many $\mathcal{F}$-sign-invariant "slices." The auxiliary polynomials are of degree no larger than md.

  Assume that the polynomial $g_{C'}(p', x_n)$ 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 31.1):

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

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

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

CYLINDRICAL ALGEBRAIC DECOMPOSITION

If we assume that the dimension n is a fixed constant, then the preceding cylindrical algebraic decomposition algorithm is polynomial in $m = |\mathcal{F}|$ and $d = \deg(\mathcal{F})$.

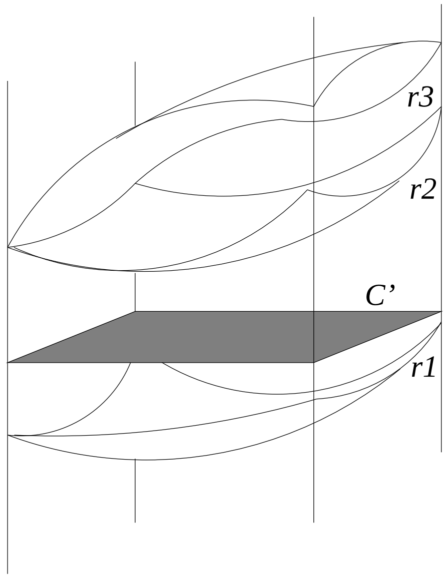

Figure 31.1
Sections and sectors "slicing" the cylinder over a lower dimensional cell.

However, the algorithm can be easily seen to be doubly exponential in n as the number of polynomials produced at the lowest dimension is

$$\left(md\right)^{2^{O(n)}},$$

each of degree no larger than $d^{2^{O(n)}}$. 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 Heinz [DH88], and related to their lower bound for the quantifier elimination problem, discussed earlier (§ 31.1).

CONSTRUCTING SAMPLE POINTS

Cylindrical algebraic decomposition provides a sample point in every sign-invariant connected component for $\mathcal{F}$. But, 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 projections. 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 semi-algebraic set. From these critical points, it will be possible to create at least one sample point per connected component. Using Bezout's bound, it is seen that only a singly exponential number of sample points are 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 semi-algebraic 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.

31.6 ALGORITHMIC APPROACHES

COLLIN'S 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 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

$$q \;=\; \alpha^{[0]} = \langle \alpha_1, \ldots, \alpha_n \rangle \;\in\; \mathbb{R}^n,$$

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 semi-algebraic 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. The reason we can do this is 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

$$(Q_1\mathbf{x}^{[1]})\ (Q_2\mathbf{x}^{[2]})\ \cdots\ (Q_\omega\mathbf{x}^{[\omega]})\ [\psi(\mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[\omega]})],$$

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

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

such that the 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

$$(Q_2 x_2)\ \cdots\ (Q_n x_n)\ [\psi(\alpha_{C_1}, x_2, \ldots, x_n)] = \mathsf{True}.$$

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

$$(Q_3 x_3)\ \cdots\ (Q_n x_n)\ [\psi(\alpha_{C_1}, \alpha_{C_{12}}, x_3, \ldots, x_n)] = \mathsf{True},$$

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 $(i-1)^{\text{th}}$ 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 $\mathcal{K} = \mathcal{K}_n$. Because we only have finitely many sample points to deal with, the universal quantifiers can be replaced by finitely many conjunctions and the existential quantifiers by disjunctions. Thus, we label every node at the $(i-1)^{\text{th}}$ 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 method and a slight modification of the CAD algorithm described earlier.

NEW APPROACHES USING CRITICAL POINTS

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

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

Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ 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

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

and encodes a sample point $\langle \frac{q_1(\alpha)}{q_0(\alpha)}, \ldots, \frac{q_n(\alpha)}{q_0(\alpha)} \rangle$. 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 following sequence of univariate polynomials

$$f_1(q_1/q_0, \ldots, q_n/q_0),\ \ldots,\ f_m(q_1/q_0, \ldots, q_n/q_0),$$

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 and compute the polynomials p and q's (for example by the u-resultant method in Renegar's algorithm).

Thus 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 differs from Renegar's algorithm primarily in the manner 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. Now if we carry out the same computation as before, over the ambient field $\mathbb{R}(\mathbf{y})$, then we get a set of *parameterized* univariate polynomial sequences, each of the form

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

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

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

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

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

Also, one may observe that the *parameter space* $\mathbf{y}$ can be partitioned into semi-algebraic 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, that were introduced earlier.

31.7 APPLICATIONS

Computational real algebraic geometry finds applications in robotics, vision, computer aided design, geometric theorem proving, etc. Important problems in robotics include the kinematic modeling, the inverse kinematic solution, the computation of the workspace and workspace singularities, the planning of an obstacle-avoiding motion of a robot in a cluttered environment, etc.—all arising from the algebraic-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 surfaces, smoothing surfaces, etc., the classification of various algebraic surfaces, the algebraic or geometric invariants associated with a surface, the effect of various affine or projective transformation of a surface, the description of surface boundaries, etc.

To give an example of the nature of the solution 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 (made 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.

The algorithm proceeds in several steps. The first main step translates the problem to the *configuration space*, a parameter space which is 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 semi-algebraic 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). As in [SS83], this path planning process can be carried out using Collin's CAD and yields an algorithm with doubly exponential time complexity. A singly exponential time complexity algorithm (the *road-map algorithm* [Can88a]) has been devised by Canny. The basic road-map algorithm has been improved and extended by several researchers over the last decade (Heintz et. al., Gournay and Risler, Grigor'ev and Vorobjov and Canny). The main idea of Canny's algorithm is to determine a one-dimensional connected subset (called "road-map") of the connected components of the free space. Once these road-maps are available, one can use them to link up two points in the same connected component. The main geometric idea is to construct road-maps starting from the critical sets of some projection function.

OFFSET SURFACE CONSTRUCTION IN SOLID MODELING

Given a polynomial $f(x, y, z)$, implicitly describing an algebraic surface in the 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 given below

$$(x-u)^2 + (y-v)^2 + (z-w)^2 - r^2 = 0, \tag{31.1}$$
$$f(u,v,w) = 0, \tag{31.2}$$
$$(x-u)t_{1,1} + (y-v)t_{1,2} + (z-w)t_{1,3} = 0, \tag{31.3}$$
$$(x-u)t_{2,1} + (y-v)t_{2,2} + (z-w)t_{2,3} = 0, \tag{31.4}$$

describes a hyper-surface in the six-dimensional space with coordinates (x, y, z, u, v, w), which, when projected onto 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, consult [Hof89].

GEOMETRIC THEOREM PROVING

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

$$\begin{array}{rcl} \text{Hypotheses} & : & f_1(x_1, \ldots, x_n) = 0, \ldots, f_r(x_1, \ldots, x_n) = 0. \\ \text{Conclusion} & : & g(x_1, \ldots, x_n) = 0. \end{array}$$

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

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

$$\Big(\forall\, x_1, \ldots, x_n\Big) \Big[\Big(f_1 = 0 \wedge \cdots \wedge f_r = 0\Big) \;\Rightarrow\; g = 0 \Big]. \qquad (31.5)$$

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

$$\Big(\exists\, x_1, \ldots, x_n, z\Big) \Big[f_1 = 0 \wedge \cdots \wedge f_r = 0 \wedge gz - 1 = 0 \Big]. \qquad (31.6)$$

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, ..., x_n, 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 is 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].)

31.8 SOURCES AND RELATED MATERIAL

SURVEYS

All results not given an explicit reference may be traced in these surveys.

- [Mis93]: A text book 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.

- [CJ95]: An anthology of key papers in computational real algebra and real algebraic geometry. Contains reprints of the following papers cited in this chapter: [BPR95, Col75, Ren91, Tar51].

- [AB88]: A special issue of the *Journal of Symbolic Computation* 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 text book on real algebra and real algebraic geometry.
- [BCR87]: A self-contained text book in French on real algebra and real algebraic geometry. An English edition is under preparation.
- [HRR91]: A survey of many classical and recent results in computational real algebra.
- [Cha94]: A survey of the connection 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]: Collin'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,b,c].
- [Lat91]: A comprehensive text book 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 robot motion planning problem and the connectivity of semi-algebraic sets using CAD. Contains several improved algorithmic results in computational real algebra.
- [Can88a]: Gives a singly exponential time algorithm for 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 X: Latombe's Chapter on Robotics.
Chapter X: Sharir's Chapter on Motion Planning.

References

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

[BPR95] 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*, (edited by B. Caviness and J. Johnson) [CJ95], Springer-Verlag, 1995.

[BPR94b] S. Basu, R. Pollack and M.-F. Roy. On the Combinatorial and Algebraic Complexity of Quantifier Elimination (Extended Abstract). In *Proceedings of the Foundations of Computer Science*, pp. 632–641, 1994.

[BR90] R. Benedetti and J.-J. Risler. *Real Algebraic and Semi-Algebraic Sets*. Hermann, Édireurs des Sciences et des Arts, Paris, 1990.

[BKR86] M. Ben-Or, D. Kozen and J. Reif. The Complexity of Elementary Algebra and Geometry. *Journal of Computer and Systems Sciences*, **32**:251–264, 1986.

[BCR87] J. Bochnak, M. Coste and M.-F. Roy. *Géométrie Algébrique Réelle*. Springer-Verlag, New York, 1987.

[Can88a] J.F. Canny. *The Complexity of Robot Motion Planning*. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1988.

[Can88b] J.F. Canny. Some Algebraic and Geometric Computations in PSPACE. In *Proc. Twentieth ACM Symp. on Theory of Computing*, pp. 460–467, 1988.

[Can93] J.F. Canny. Improved Algorithms for Sign Determination and Existential Quantifier Elimination. *The Computer Journal*, **36**:409–418, 1993.

[CJ95] B.F. Caviness and J.R. Johnson (Eds.). *Quantifier Elimination and Cylindrical Algebraic Decomposition*, Springer-Verlag, Wien, 1995.

[Cha94] B. Chazelle. Computational Geometry: A Retrospective. In *Proceedings of the 26th annual ACM Symposium on the Theory of Computing*, pp. 75–94, 1994.

[Cho88] S.C. Chou. *Mechanical Geometry Theorem Proving.* D. Reidel, Dordrecht, 1988.

[Col75] G. Collins. Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition. *Second GI Conference on Automata Theory and Formal Languages, Lecture Notes in Computer Science*, **33**:134–183. Springer-Verlag, Berlin, 1975. Also in [CJ95].

[DH88] J.H. Davenport and J. Heintz. Real Quantifier Elimination Is Doubly Exponential. *J. Symbolic Computation* [AB88], **5**(1-2):29–35, 1988.

[Gri88] D. Grigor'ev. The Complexity of Deciding Tarski Algebra. *Journal of Symbolic Computation* [AB88], **5**:65–108, 1988.

[GV88] D. Grigor'ev and N.N. Vorobjov. Solving Systems of Polynomial Inequalities in Subexponential Time. *Journal of Symbolic Computation* [AB88], **5**:37–64, 1988.

[GV92] D. Grigor'ev and N.N. Vorobjov. Counting Connected Components of a Semialgebraic Set in Subexponential Time. *Computational Complexity*, **2**:133–186, 1992.

[HRR91] J. Heintz, T. Recio and M.-F. Roy. Algorithms in Real Algebraic Geometry and Applications to Computational Geometry. *Discrete and Computational Geometry: Papers from the DIMACS Special Year*, (edited by J.E. Goodman, R. Pollack and W. Steiger), American Mathematical Society and Association of Computing Machinery, **6**:137–164, 1991.

[HRS89] J. Heintz, M.-F. Roy and P. Solernó. On the Complexity of Semi-Algebraic Sets. In *Proceedings IFIP 89*, pp. 293–298, San Francisco. North-Holland, 1989.

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

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

[Lat91] J.-C. Latombe. *Robot Motion Planning*. Kluwer Academic Press, Boston 1991.

[Mil64] M. Milnor. On the Betti Numbers of Real Algebraic Varieties. In *Proceedings of American Mathematical Society*, **15**:275–280, 1964.

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

[PR93] R. Pollack and M.-F. Roy. On the Number of Cells Defined by a Set of Polynomials. *C.R. Acad. Sci. Paris*, **316**:573–577, 1993.

[Ren91] J. Renegar. Recent Progress on the Complexity of the Decision Problem for the Reals. In *Discrete and Computational Geometry: Papers from the DIMACS Special Year*, (edited by J.E. Goodman, R. Pollack and W. Steiger), American Mathematical Society and Association of Computing Machinery, **6**:287–308, 1991. Also in [CJ95].

[Ren92a] J. Renegar. On the Computational Complexity and Geometry of the First-Order Theory of the Reals: Part I. Introduction. Preliminaries. The Geometry of Semi-algebraic Sets. The Decision Problem for the Existential Theory of Reals. *Journal of Symbolic Computation*, **13**(3):255–299, 1992.

[Ren92b] J. Renegar. On the Computational Complexity and Geometry of the First-Order Theory of the Reals: Part II. The General Decision Problem. Preliminaries for Quantifier Elimination. *Journal of Symbolic Computation*, **13**(3):301–327, 1992.

[Ren92c] J. Renegar. On the Computational Complexity and Geometry of the First-Order Theory of the Reals: Part III. Quantifier Elimination. *Journal of Symbolic Computation*, **13**(3):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. *Advances in Appl. Math.*, **4**:298–351, 1983.

[Tar51] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley, California, 1951. Also in [CJ95].

[Tho65] R. Thom. *Sur l'Homologie des Variétés Réelles*. Differential and Combinatorial Topology, Princeton University Press, Princeton, NJ, 255–265, 1965.