On the Combinatorial and Algebraic Complexity of Quantifier Elimination

SAUGATA BASU AND RICHARD POLLACK

New York University, New York, New York

AND

MARIE-FRANÇOISE ROY

Université de Rennes, Rennes, France

Abstract. In this paper, a new algorithm for performing quantifier elimination from first order formulas over real closed fields is given. This algorithm improves the complexity of the asymptotically fastest algorithm for this problem, known to this date. A new feature of this algorithm is that the role of the algebraic part (the dependence on the degrees of the input polynomials) and the combinatorial part (the dependence on the number of polynomials) are separated. Another new feature is that the degrees of the polynomials in the equivalent quantifier-free formula that is output, are independent of the number of input polynomials. As special cases of this algorithm, new and improved algorithms for deciding a sentence in the first order theory over real closed fields, and also for solving the existential problem in the first order theory over real closed fields, are obtained.

Categories and Subject Descriptors: F4.3 [**Mathematical Logic and Formal Languages**]: Formal Languages—*decision problems*.

General Terms: Algorithms, Theory

Additional Key Words and Phrases: Quantifier elimination, real closed fields, Tarski–Seidenberg principle

1. *Introduction*

1.1. STATEMENT OF THE PROBLEMS. We are given a set of s polynomials, $\mathcal{P} = \{P_1, P_2, \ldots, P_s\}$, in k variables, $X_1, \ldots, X_k$, each of degree at most d with

The work of S. Basu was supported in part by National Science Foundation (NSF) grants CCR 94-02640 and CCR 94-24398.

The work of R. Pollack was supported in part by NSF grants CCR 94-02640 and CCR 94-24398.

The work of M.-F. Roy was supported in part by the project ESPRIT-BRA 6846POSSO and by European Community contract CHRX-CT94-0506.

Authors' addresses: S. Basu and R. Pollack, Courant Institute of Mathematical Sciences, New York University, New York, NY 10012; M.-F. Roy, IRMAR (URA CNRS 305), Université de Rennes, Campus de Beaulieu, 35042 Rennes Cedex, France.

coefficients in a real closed field R. The *sign*, $\text{sign}(a)$, of an element $a \in R$ is 0 if $a = 0$, 1 if $a > 0$ and -1 if $a < 0$.

The *decision problem for the existential theory of the reals* is to decide the truth or falsity of a sentence

$$(X_1, \ldots, X_k) F(P_1, \ldots, P_s),$$

where $F(P_1, \ldots, P_s)$ is a quantifier-free Boolean formula with atoms of the form $\text{sign}(P_i(X_1, \ldots, X_k)) = \sigma$, with $\sigma \in \{0, 1, -1\}$. This problem is equivalent to deciding whether or not a given semi-algebraic set is empty.

If, instead of having a single block of variables quantified by the same quantifier the given sentence has several blocks of variables with alternating quantifiers, the problem is called the *general decision problem* for the first order theory of the reals. In this problem, we are to decide the truth or falsity of a first order sentence of the form

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

where $Q_i \in \{\quad, \quad\}$, $Q_i \neq Q_{i+1}$, $X^{[i]}$ is a block of k_i variables,

$$\sum_{1 \leq i \leq \omega} k_i = k,$$

and $F(P_1, \ldots, P_s)$ is a quantifier-free Boolean formula with atoms of the form $\text{sign}(P_i(X^{[\omega]}, \ldots, X^{[1]})) = \sigma$, where $\sigma \in \{0, 1, -1\}$. Note that the decision problem for the existential theory corresponds to $\omega = 1$.

The third and principal problem we consider is the *quantifier elimination problem*. We are given a set, $\mathcal{P} = \{P_1, \ldots, P_s\}$, of s polynomials in $k + \ell$ variables, $X_1, \ldots, X_k, Y_1, \ldots, Y_\ell$. The degrees of the polynomials are again bounded by d and their coefficients lie in a real closed field as in the previous problems. We are given a first-order formula of the form

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

(henceforth denoted $\Phi(Y)$) where $Q_i \in \{\quad, \quad\}$, $Q_i \neq Q_{i+1}$, $Y = (Y_1, \ldots, Y_\ell)$ is a block of ℓ free variables, $X^{[i]}$ is a block of k_i variables with $\sum_{1 \leq i \leq \omega} k_i = k$, and $F(P_1, \ldots, P_s)$ is a quantifier-free Boolean formula with atomic predicates of the form $\text{sign}(P_i(Y, X^{[\omega]}, \ldots, X^{[1]})) = \sigma$ where $\sigma \in \{0, 1, -1\}$.

The quantifier elimination problem is to construct a quantifier-free Boolean formula, $\Psi(Y)$, such that for any $y \in R^\ell$, $\Phi(y)$ is true if and only if $\Psi(y)$ is true. Note that the general decision problem corresponds to the case where $\ell = 0$.

1.2. History. The fact that there exist algorithms solving these three problems was first proved by Tarski [1951] (see also Seidenberg [1954]). However, the complexity of his algorithm is not elementary recursive. The first algorithm with a reasonable worst-case time bound was given by Collins [1975]. His algorithm had a worst case running time doubly exponential in the number of variables.

Grigor'ev and Vorobjov [1992] gave an algorithm to solve the decision problem for the existential theory of the reals whose time complexity is singly exponential in the number of variables. Canny [1993a], Heintz et al. [1990], and Renegar

[1992] improved this result in several directions, the best bound of $(sd)^{O(k)}$ being due to Renegar [1992].

Grigor'ev [1988] achieved doubly exponential complexity in the number of blocks for the general decision problem. It should be noted that for a fixed value of ω, this is only singly exponential in the number of variables. Heintz et al. [1990], and Renegar [1992] extended this result to quantifier elimination. Renegar's [1992] algorithms that solve the general decision problem in time $(sd)^{\prod O(k_i)}$, and the quantifier elimination problem in time $(sd)^{(\ell+1)\prod O(k_i)}$ were the best to date.

1.3. Statement of Our Results. In this paper, we present a new algorithm for performing quantifier elimination from first order formulas over real closed fields.

We denote by D the smallest subring of R containing the coefficients of the input polynomials. All the computations of our algorithms take place in D. We define the complexity of our algorithms to be the number of arithmetic operations (additions, multiplications, and sign determinations in the ring D).

Our algorithms are *well-behaved* in the sense that they have the following properties.

—The complexity is the product of a combinatorial part depending on the number s of input polynomials and an algebraic part depending on the degree d of the input polynomials;

—If $D = \mathbf{Z}$, the bit-sizes of the integers in the output and in the intermediate computations are bounded by the bit-size of the input integers times the algebraic part of the complexity;

—If we evaluate the complexity in terms of arithmetic operations and Boolean operations, the length L of the input formula enters as a parameter describing the input. The number of arithmetic and Boolean operations performed by our algorithms is bounded by the number of arithmetic operations performed by the algorithm multiplied by a linear factor in L;

—The algorithm is well parallelizable, that is, it can be described by an arithmetic network whose depth is a polynomial in the log of the sequential complexity (see Heintz et al. [1990]).

The fact that our algorithms are well parallelizable is a consequence of the fact that all our subroutines are based on linear algebra subroutines that are well parallelizable (see Berkowitz [1984]).

We prove the following theorems:

Theorem 1.3.1 (The Quantifier Elimination Problem). *Given a set*,

$$\mathcal{P} = \{P_1, \ldots, P_s\},$$

of s polynomials each of degree at most d, in $k + \ell$ variables, with coefficients in a real closed field R and a first-order formula

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

where $Q_i \in \{\ ,\ \}$, $Q_i \neq Q_{i+1}$, $Y = (Y_1, \ldots, Y_\ell)$ *is a block of* ℓ *free variables*, $X^{[i]}$ *is a block of* k_i *variables*, $\sum_{1 \leq i \leq \omega} k_i = k$, *and* $F(P_1, \ldots, P_s)$ *is a quantifier-free Boolean formula with atomic predicates of the form*

$$sign(P_i(Y, X^{[\omega]}, \ldots, X^{[1]})) = \sigma$$

with $\sigma \in \{0, 1, -1\}$, *there exists an equivalent quantifier-free formula*,

$$\Psi(Y) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} (sign(P_{ij}(Y)) = \sigma_{ij})$$

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

$$I \leq s^{(\ell+1)\Pi_i(k_i+1)} d^{(\ell+1)\Pi_i O(k_i)},$$

$$J_i \leq s^{\Pi_i(k_i+1)} d^{\Pi_i O(k_i)},$$

and the degrees of the polynomials $P_{ij}(y)$ *are bounded by* $d^{\Pi_i O(k_i)}$. *Moreover, we present a well-behaved algorithm to compute* $\Psi(Y)$ *using* $s^{(\ell+1)\Pi(k_i+1)} d^{(\ell+1)\Pi O(k_i)}$ *arithmetic operations in* D.

When $\ell = 0$, we have:

THEOREM 1.3.2 (THE GENERAL DECISION PROBLEM). *Given a set*,

$$\mathcal{P} = \{P_1, \ldots, P_s\},$$

of s polynomials each of degree at most d in k variables with coefficients in a real closed field R and a first order sentence,

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

where $Q_i \in \{\ ,\ \}$, $Q_i \neq Q_{i+1}$, $X^{[i]}$ *is a block of* k_i *variables*, $\sum_{1 \leq i \leq \omega} k_i = k$, *and* $F(P_1, \ldots, P_s)$ *is a quantifier-free Boolean formula with atomic predicates of the form* $sign(P_i(X^{[\omega]}, \ldots, X^{[1]})) = \sigma$ *there exists a well-behaved algorithm to decide the truth of the formula that uses* $s^{\Pi(k_i+1)} d^{\Pi O(k_i)}$ *arithmetic operations in* D.

When $\omega = 1$, the following theorem, which is the decision problem of the existential theory, is an immediate consequence of Theorem 1.3.2.

THEOREM 1.3.3 (THE DECISION PROBLEM FOR THE EXISTENTIAL THEORY). *Given a set*,

$$\mathcal{P} = \{P_1, \ldots, P_s\},$$

of s polynomials each of degree at most d in k variables with coefficients in a real closed field R and a first-order sentence,

$$(X_1, \ldots, X_k) F(P_1, \ldots, P_s)$$

where $F(P_1, \ldots, P_s)$ *is a quantifier-free Boolean formula with atomic predicates of the form*, $sign(P_i(X_1, \ldots, X_k)) = \sigma$ *with* $\sigma \in \{0, 1, -1\}$, *there exists a well-behaved algorithm to decide the truth of the formula that uses* $s^{k+1} d^{O(k)}$ *arithmetic operations in* D.

It might appear that Theorems 1.3.2 and 1.3.3 should simply be corollaries of Theorem 1.3.1. However, the proof of Theorem 1.3.3 is built on the ingredients of the proof of Theorem 1.3.2, which in turn is built on the ingredients of the proof of Theorem 1.3.1.

Previously, the fastest algorithm for the quantifier elimination problem due to Renegar [1992], had complexity $(sd)^{(\ell+1)^{\Pi O(k_i)}}$ and the degrees of the polynomials in the output formula were bounded by $(sd)^{(\ell+1)^{\Pi O(k_i)}}$. In our algorithm, the bound on the degrees of the polynomials in the output formula are independent of s. Another noteworthy point about our algorithms for these problems is that the combinatorial and algebraic parts of the complexity are separated. The algebraic complexity of our algorithm is the same as that of Renegar's algorithm and we use many of his techniques as well. The combinatorial complexity of our algorithm is better than that of Renegar's algorithm.

In order to decide the truth or falsity of a quantified formula, we construct a certain nested set of sign conditions, with a "cylindrical by block structure", which we define below. Once this set is constructed, it is easy to decide the truth or falsity of the given formula by evaluating the Boolean formula $F(P_1, \ldots, P_s)$ for every sign condition of $\mathcal{P}$ occurring in this set.

Let $\mathcal{P} = \{P_1, \ldots, P_s\}$ be a set of s polynomials in k variables $(X_1, \ldots, X_k)$, and let Π denote the partition of the set of variables $(X_1, \ldots, X_k)$ into blocks, $X^{[1]}, \ldots, X^{[\omega]}$, where the block $X^{[i]}$ is of size k_i, $1 \leq i \leq \omega$. For $x^{[\omega]} \in R^{k_\omega}, \ldots, x^{[1]} \in R^{k_1}$, let

$$\mathrm{SIGN}_{\Pi,0}(\mathcal{P})(x^{[\omega]}, \ldots, x^{[1]}) =$$

$$(\mathrm{sign}(P_1(x^{[\omega]}, \ldots, x^{[1]})), \ldots, \mathrm{sign}(P_s(x^{[\omega]}, \ldots, x^{[1]}))).$$

For $x^{[i+1]} \in R^{k_{i+1}}, \ldots, x^{[\omega]} \in R^{k_\omega}$, and for all i, $0 < i \leq \omega$, we recursively define,

$$\mathrm{SIGN}_{\Pi,i}(\mathcal{P})(x^{[\omega]}, \ldots, x^{[i+1]}) = \{\mathrm{SIGN}_{\Pi,i-1}(\mathcal{P})(x^{[\omega]}, \ldots, x^{[i+1]}, x^{[i]}) | x^{[i]} \in R^{k_i}\}.$$

Finally, we define

$$\mathrm{SIGN}_{\Pi}(\mathcal{P}) = \mathrm{SIGN}_{\Pi,\omega}(\mathcal{P}).$$

It is easy to decide the truth or falsity of the formula,

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

from the set $\mathrm{SIGN}_{\Pi}(\mathcal{P})$ which we call the *total list of signs of* $\mathcal{P} = (P_1, \ldots, P_s)$ with respect to the partition Π of the variables, into the blocks, $(X^{[\omega]}, \ldots, X^{[1]})$.

Note that the set $\mathrm{SIGN}_{\Pi}(\mathcal{P})$ is a set of nested sets, where the nesting is of depth ω. When there is only one block of variables, we denote it by $\mathrm{SIGN}(\mathcal{P})$.

We prove a bound on the size of the set $\mathrm{SIGN}_{\Pi}(\mathcal{P})$, in the following theorem, which is the key to proving Theorems 1.3.1 and 1.3.2.

THEOREM 1.3.4. *Let* Π *denote a partition of the set of variables* $(X_1, \ldots, X_k)$ *into blocks,* $X^{[1]}, \ldots, X^{[\omega]}$, *where the block* $X^{[i]}$ *is of size* k_i, $1 \leq i \leq \omega$. *Then the size of the set* $SIGN_{\Pi}(\mathcal{P})$ *is bounded by* $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$. *Moreover, there exists a well-behaved algorithm that computes this set using* $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$ *arithmetic operations in* D.

The remainder of this paper is organized as follows: In Section 2, we present some results that are used in the rest of the paper. Some of these results are classical and others are quite recent. We strive to be as self-contained as possible.

Section 3 is devoted to the existential theory of the reals. We need the following definitions:

The sign condition $\sigma \in \{0, 1, -1\}^s$ is called *non-empty* (with respect to $\mathcal{P}$) if there is a point $x \in R^k$ such that

$$(\text{sign}(P_1(x)), \ldots, \text{sign}(P_s(x))) = \sigma.$$

The *realization* of the sign condition σ in R is the set

$$\{x \in R^k | (\text{sign}(P_1(x)), \ldots, \text{sign}(P_s(x))) = \sigma\}.$$

Our method to solve the existential theory of the reals is to compute a set of points that meets every connected component of the realization of every non-empty sign condition of a set of polynomials (henceforth referred to as *cells*). The main new idea of our method is to prove (using Proposition 2.3.1) that we need only produce points in cells of algebraic sets that are defined by polynomial equations of degree d. In a real closed field, an algebraic set defined by m equations of degree d can be described by a single equation of degree $2d$ (by taking the sum of squares). It is this simple observation that makes the degrees of the output polynomials independent of the number of input polynomials. Only the number of algebraic sets we consider will depend on s. If the original set of polynomials satisfy a certain general position requirement (see Section 2) that no $k + 1$ of them have a common zero, then the number of algebraic sets we need to consider is small ($O(s^k)$ rather than exponential in s). With this in mind, we replace the set of input polynomials by a related perturbed set of polynomials and prove (using Proposition 2.3.5) that these polynomials are in general position. We then make further perturbations on the polynomials defining the algebraic sets on which we want to compute points so that the perturbed algebraic sets have convenient geometric properties. Namely, that they are smooth, bounded and have a finite number of critical points in the X_1 direction. This is proved in Lemma 2.3.6 and Proposition 2.3.7. After we compute points in every connected component of these perturbed algebraic sets (by computing the critical points of these sets in the X_1 direction), these points intersect every cell of the perturbed polynomials, and we recover points corresponding to the original set of polynomials using Proposition 2.2.1.

We outline several important subroutines that are used by the algorithm. The most important subroutine is the *Sample Points Subroutine* that computes points in every cell of a set of polynomials. It in turn uses another subroutine, the *Cell Representatives Subroutine*, that computes points in every connected component of an algebraic set. Once we have computed points in every cell, we compute the signs of the given set of polynomials at these points. For this, we use a multidimensional variant [Pedersen et al. 1993] of the algorithm by Ben Or et al. [1986], which we call the *Sign Determination Subroutine.*

In Section 4, we present a few applications of the techniques developed to solve the existential problem of the reals. Particularly noteworthy, is the follow-

ing: Consider the problem of bounding the radius of a ball centered at the origin, which is guaranteed to intersect every cell of a finite set of polynomials, $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathbf{Z}[X_1, \ldots, X_k]$, whose degrees are bounded by d.

We prove the following results:

THEOREM 1.3.5. *Given a set $\mathcal{P}$ of s polynomials of degree d in k variables with coefficients in $\mathbf{Z}$ of bit length at most τ, then there exists a ball of radius $2^{O(\tau d^{O(k)})}$ intersecting every cell of $\mathcal{P}$.*

THEOREM 1.3.6. *Given a set $\mathcal{P}$ of s polynomials of degree d in k variables with coefficients in $\mathbf{Z}$ of bit length at most τ such that*

$$S = \{x \in R^k | P(x) > 0, P \in \mathcal{P}\}$$

is a nonempty set, then in every connected component of S, there exists a point whose coordinates are rational numbers a_i/b_i with a_i and b_i of bit length $\tau d^{O(k)}$.

This corollary improves the bound in Koiran [1993], where the dependence on k was doubly exponential as well as the bound in Grigor'ev and Vorobjov [1988], which depended on s.

In Section 5, we solve the general decision problem. We first describe a parametrized version of the *Sample Points Subroutine*, which uses a parametrized-version of the *Cell Representatives Subroutine.*

In Section 6, we present our algorithm for performing quantifier elimination. As a preliminary, we describe an *Inverse Sign Determination Subroutine* that we use to construct the quantifier-free formula. Our algorithms for the general decision problem and for the quantifier elimination problem have two phases. The first phase is the *elimination phase*, in which blocks of variables are successively replaced in a uniform way by single variables. The second phase is the *sign determination phase*, where the total list of signs is computed.

An announcement of these results appeared as an extended abstract in Basu et al. [1994].

2. *Preliminaries*

2.1. PUISEUX SERIES. In our algorithms, we construct points whose coordinates belong to the real closed field R. However, in some intermediate stages, we construct points whose coordinates lie in some real closed non-Archimedean extension of R. It is crucial that all the subroutines called by our algorithms work over an arbitrary real closed field. Though the coordinates of the points that we construct might lie in a nonarchimedean extension of R, all our computations will only involve arithmetic operations in the ring D generated by the coefficients of the input polynomials. The nonarchimedean extensions of R that we will be considering are the fields of Puiseux series in some infinitesimals with coefficients in R. We give the definition and some relevant properties of these fields and refer the reader to Bochnak et al. [1987] for more details.

We first give a definition: Given an ordered domain D contained in an ordered domain D' such that the order on D' extends the order on D, we say that $x \in D'$ is *infinitesimal positive* with respect to D if it is positive in D' and strictly smaller than any positive element of D.

We suggest that in order to understand the following definitions it is helpful to think of ϵ as positive and very small.

The field of Puiseux series in ϵ with coefficients in R (respectively, in $R[i]$, the algebraic closure of R), which we denote $R\langle\epsilon\rangle$ (respectively, $R[i]\langle\epsilon\rangle$) is defined as follows. Its elements are 0 and series of the form

$$\sum_{i\geq i_0, i\in\mathbf{Z}} a_i\epsilon^{i/q}$$

with $i_0 \in \mathbf{Z}$, $a_i \in R$ (respectively, $R[i]$), $a_{i_0} \neq 0$ and $q \in \mathbf{N}$. The initial term of a non-zero Puiseux series, $\sum_{i\geq i_0, i\in\mathbf{Z}} a_i\epsilon^{i/q}$, is $a_{i_0}\epsilon^{i_0/q}$ and its valuation is i_0/q.

The unique order on $R\langle\epsilon\rangle$ is defined by $\sum_{i\geq i_0, i\in\mathbf{Z}} a_i\epsilon^{i/q} > 0$ if $a_{i_0} > 0$. The element ϵ of $R\langle\epsilon\rangle$ is infinitesimal positive with respect to R. The field $R\langle\epsilon\rangle$ is real closed [Bochnak et al. 1987] and the field $R[i]\langle\epsilon\rangle$ is algebraically closed [Walker 1950]. The elements of $R\langle\epsilon\rangle$ bounded over R form the *valuation ring* denoted $V(\epsilon)$; the elements of $V(\epsilon)$ are 0 or Puiseux series

$$\sum_{i\in\mathbf{N}} a_i\epsilon^{i/q}.$$

We denote by eval_ϵ the ring homomorphism from $V(\epsilon)$ to R which maps $\sum_{i\in\mathbf{N}} a_i\epsilon^{i/q}$ to a_0. A Puiseux series is infinitesimal if and only if it is mapped by eval_ϵ to 0. We can think of eval_ϵ as the evaluation of the Puiseux series at 0. If $S \subset R\langle\epsilon\rangle^k$, $\text{eval}_\epsilon(S)$ is the image under the map eval_ϵ of the points of S where eval_ϵ is defined (those points of S contained in $V(\epsilon)^k$).

The order on $R\langle\epsilon\rangle$ induces on $R(\epsilon)$ an order for which ϵ is infinitesimal positive. Similarly, if D is a ring contained in R, the unique order on $R\langle\epsilon\rangle$ induces on $D[\epsilon]$ an order for which ϵ is infinitesimal positive. It is easy to see that for $P \in D[\epsilon]$, $P(\epsilon) > 0$ if and only if for all $t \in R$ which are positive and small enough, $P(t) > 0$.

If D is a ring contained in R, then we call an element $\alpha \in R$ *algebraic over* D, if and only if α is a root of a polynomial $f(T) \in D[T]$. Moreover, the element $\alpha \in R$, is uniquely specified by the polynomial f, and the sign condition $(\text{sign}(f(\alpha)), \text{sign}(f'(\alpha)), \ldots, \text{sign}(f^{(deg(f))}(\alpha)))$, known as the Thom encoding [Coste and Roy 1988] of the root α.

If $\bar{\epsilon} = (\epsilon_1, \ldots, \epsilon_c)$ is some vector of variables we write $R\langle\bar{\epsilon}\rangle$ for $R\langle\epsilon_1\rangle\cdots\langle\epsilon_c\rangle$. Observe that for every $i \in \{1, \ldots, c-1\}$, ϵ_{i+1} is infinitesimal positive with respect to $R\langle\epsilon_1\rangle\cdots\langle\epsilon_i\rangle$. We write this as $\epsilon_1 \gg \cdots \gg \epsilon_c$ and say ϵ_2 is infinitesimal with respect to ϵ_1, etc. In some intermediate stages of our algorithms, the coordinates of the points that we compute lie in $R\langle\bar{\epsilon}\rangle$. However, these coordinates will always be algebraic over $D[\bar{\epsilon}]$, and hence are roots of some polynomials in $D[\bar{\epsilon}][t]$.

We often use the eval map on points with bounded coordinates. The following lemma allows us to perform this purely as an algebraic procedure.

LEMMA 2.1.1. *Suppose that $f \in D[\epsilon, 1/\epsilon][t]$ and $\alpha \in R\langle\epsilon\rangle$ is a real root of f that is bounded over R, where D is a ring contained in R, then $\beta = \text{eval}_\epsilon(\alpha)$ is a root of $f_0(t)$ where $f_0(t)$ is the coefficient of the lowest power of ϵ occurring in f when f is expressed in powers of ϵ.*

PROOF. Without loss of generality, assume that,

$$f(t, \epsilon) = f_0(t) + f_1(t)\epsilon + \cdots + f_d(t)\epsilon^d.$$

Since α is bounded over R, its valuation as a Puiseux series in ϵ is nonnegative. Let $\alpha = \sum_{i \geq i_0} \alpha_i \epsilon^{i/q}$, where $i_0 \geq 0$ and $q > 0$. We consider two cases, $i_0 = 0$ and $i_0 > 0$. If $i_0 = 0$, then $\beta = \text{eval}_\epsilon(\alpha) = \alpha_0$. If $f_0(\alpha_0)$ is not 0, substituting α for t in f, we see that $f_0(\alpha_0)$ is the initial term of the Puiseux series $f(\alpha, \epsilon)$. This is impossible since α is a root of f. Thus, $f_0(\alpha_0) = 0$. If $i_0 > 0$, then $\beta = \text{eval}_\epsilon(\alpha) = 0$. In this case, we prove that the constant term in the polynomial $f_0(t)$ is 0. Let

$$f_0(t) = a_0 + a_1 t + \cdots + a_n t^n.$$

If a_0 is not 0, substituting α for t in f, we see that $f(\alpha, \epsilon)$ has initial term a_0. This is impossible since α is a root of f.

Thus, in both cases, $\beta = \text{eval}_\epsilon(\alpha)$ is a root of $f_0(t)$. □

2.2. SOME REAL ALGEBRAIC GEOMETRY. We shall need some properties of semi-algebraically connected components and paths in semi-algebraic sets in R^k, where R is a real closed field. A full discussion of these can be found in Bochnak et al. [1987], but we offer a brief summary below.

The order relation on a real closed field R defines, as usual, the euclidean topology on R^k. Semi-algebraic sets are finite unions of sets defined by a finite number of polynomial equalities and inequalities, and semi-algebraic homeomorphisms are homeomorphisms whose graph is semi-algebraic.

In particular, we have the following elementary properties of semi-algebraic sets over a real closed field R (see also Bochnak et al. [1987]):

—The projection of a semi-algebraic set of $R^{k+\ell}$ on R^k is semi-algebraic. A subset of R^k defined by a first order formula of the language of ordered fields is semi-algebraic (this is the famous Tarski–Seidenberg principle).

—A semi-algebraic set S is *semi-algebraically connected* if it is not the disjoint union of two non-empty closed semi-algebraic sets in S. A *semi-algebraically connected component* of a semi-algebraic set S is a maximal semi-algebraically connected subset of S. A semi-algebraic set has a finite number of semi-algebraically connected components. In the case that the ground field R is the field of real numbers, semi-algebraically connected components of semi-algebraic sets are ordinary connected components.

—A *semi-algebraic path* between x and x' in R^k is a semi-algebraic subset γ, semi-algebraically homeomorphic to the unit interval of R through a semi-algebraic homeomorphism also denoted γ with $\gamma(0) = x$ and $\gamma(1) = x'$. A semi-algebraic set is semi-algebraically connected if and only if it is semi-algebraically path connected.

—Given a semi-algebraic set S in R^k, and a real closed field K containing R, the *extension* of S to K, S_K, is the subset of K^k defined by the same Boolean combination of equalities and inequalities that defines S. The semi-algebraically connected components of S_K are the extensions to K of the semi-algebraically connected components of S.

—Given a point x belonging to the closure of a semi-algebraic set $S \subset R^k$, there exists a semi-algebraic function γ from $[0, 1]$ to R^k with $\gamma(0) = x$, $\gamma((0, 1]) \subset S$ (this is the curve selection lemma). Moreover, this curve implies the existence of a point $z \in R\langle\epsilon\rangle^k \cap S_{R\langle\epsilon\rangle}$ such that $\text{eval}_\epsilon(z) = x$.

Let D be a subring of the real closed field R. A semi-algebraic set S is *defined over* D if it can be described as a finite union of sets defined by polynomial equalities and inequalities with coefficients in D.

Let $S(\epsilon)$ be a semi-algebraic set in $R\langle\epsilon\rangle^k$ defined over $D[\epsilon]$ and for $t \in R$ let $S(t)$ be the semi-algebraic set in R^k obtained by substituting t for ϵ in the definition of $S(\epsilon)$. Let $P(S(\epsilon))$ be a property of the semi-algebraic set $S(\epsilon)$, which is expressible by a first order formula $\Phi(\epsilon)(x_1, \cdots, x_k)$ with parameters in $D[\epsilon]$. Then, for t, positive and small enough $P(S(t))$ is a property of $S(t)$. This is an easy consequence of the Tarski–Seidenberg principle and of the way signs are computed in $D[\epsilon]$.

Given $Q \in R[x_1, \cdots x_k]$, we write $Z(Q)$ for the set of zeroes of Q in R^k, that is, $Z(Q) = \{x \in R^k | Q(x) = 0\}$.

The following proposition will be useful. The fact that S is semi-algebraic had previously appeared in Roy and Vorobjov [1994].

PROPOSITION 2.2.1. *If $S' \subset R\langle\epsilon\rangle^k$ is a semi-algebraic set defined over $D[\epsilon]$ and $S = eval_\epsilon(S')$, then S is a semi-algebraic set. Moreover, if S' is bounded over R and semi-algebraically connected, then S is semi-algebraically connected.*

PROOF. Suppose that $S' \subset R\langle\epsilon\rangle^k$ is described by a quantifier-free formula $\Phi(\epsilon)(X_1, \ldots, X_k)$. Introduce a new variable X_{k+1} and denote by

$$\Phi(X_1, \ldots, X_k, X_{k+1})$$

the result of substituting X_{k+1} for ϵ in $\Phi(\epsilon)(X_1, \ldots, X_k)$.

Embed R^k in R^{k+1} by sending $(X_1, \ldots, X_k)$ to $(X_1, \ldots, X_k, 0)$ so that S is a subset of $Z(X_{k+1})$. We prove that $S = \bar{T} \cap Z(X_{k+1})$ where

$$T = \{(x_1, \ldots, x_k, x_{k+1}) \in R^{k+1} | \Phi((x_1, \ldots, x_k, x_{k+1}) \text{ and } x_{k+1} > 0\}$$

and $\bar{T}$ is the closure of T in the Euclidean topology.

If $x \in S$, then there exists $z \in S'$ such that $\text{eval}_\epsilon(z) = x$. Let $B_x(r)$ denote the open ball of radius r centered at x. Since (z, ϵ) belongs to the extension of $B_x(r) \cap T$ to $R\langle\epsilon\rangle$ it follows that $B_x(r) \cap T$ is non-empty, and hence that $x \in \bar{T}$.

Conversely, let x be in $\bar{T} \cap Z(X_{k+1})$. The semi-algebraic curve selection lemma [Bochnak et al. 1987] asserts the existence of a semi-algebraic function γ from $[0, 1]$ to $\bar{T}$ with $\gamma(0) = x$ and $\gamma((0, 1]) \subset T$. This semi-algebraic function defines a point z whose coordinates lie in $R\langle\epsilon\rangle$ and belongs to S' and moreover $\text{eval}_\epsilon(z) = x$.

If S' is bounded over R by M and semi-algebraically connected, then there exists a positive t in R such that $T \cap (B_0(M) \times [0, t])$ is semi-algebraically connected. It follows easily that $S = \bar{T} \cap Z(X_{k+1}) = \bar{T} \cap (B_0(M) \times [0, t]) \cap Z(X_{k+1})$ is semi-algebraically connected. □

2.3. PERTURBATIONS. The following proposition reduces the problem of constructing points on semi-algebraically connected components of a basic closed semi-algebraic set to that of constructing points on semi-algebraically connected components of algebraic sets.

PROPOSITION 2.3.1. *Let C be a non-empty semi-algebraically connected component of a basic closed semi-algebraic set defined by*

$$P_1 = \cdots = P_\ell = 0, P_{\ell+1} \geq 0, \ldots, P_s \geq 0.$$

We can find an algebraic set V defined by equations

$$P_1 = \cdots = P_\ell = P_{i_1} = \cdots = P_{i_m} = 0,$$

such that a semi-algebraically connected component C' of V is contained in C.

PROOF. Consider a maximal set of polynomials

$$\{P_1, \ldots, P_\ell, P_{i_1}, \ldots, P_{i_m}\},$$

where

$$m = 0 \qquad \text{or} \qquad \ell < i_1 < \cdots < i_m \leq s,$$

with the property that there exists a point $p \in C$ where

$$P_1 = \cdots = P_\ell = P_{i_1} = \cdots = P_{i_m} = 0.$$

Consider the connected component C' of the algebraic set defined by

$$P_1 = \cdots = P_\ell = P_{i_1} = \cdots = P_{i_m} = 0,$$

which contains p. We claim that $C' \subset C$. Suppose that there exists a point $q \in C'$ such that $q \notin C$. Then there exists a semi-algebraic path γ: $[0, 1] \to C'$ joining p to q in C'. Denote by q' the first point of the path γ on the boundary of C: More precisely, pick $t \in [0, 1]$ such that $\gamma([0, t]) \subset C$ and $t' > t$, $\gamma([0, t']) \not\subset C$, then we take $q' = \gamma(t)$. At least one of the polynomials, say P_j, $j \notin \{1, \ldots, \ell, i_1, \ldots, i_m\}$ must be 0 at q'. This violates the maximality of the set

$$\{P_1, \ldots, P_\ell, P_{i_1}, \ldots, P_{i_m}\}. \qquad \square$$

We next show how to reduce the problem of computing points in every cell defined by a set of s polynomials, $\mathcal{P}$, to computing points in every semi-algebraically connected component of the basic closed semi-algebraic sets defined by a perturbed set of $4s$ polynomials. Using Proposition 2.3.1, this will be done by computing a point in each algebraic set defined by this perturbed set.

Proposition 2.3.2 will guarantee that we recover points in every cell of the original polynomials, after we have computed points in every cell of a perturbed set of polynomials. Its statement and proof is very close to similar results appearing in Grigor'ev [1988] and Grigor'ev and Vorobjov [1988].

We will consider perturbations with an infinitely large element Ω and two additional positive infinitesimals δ, δ' with the ordering $1/\Omega \gg \delta \gg \delta'$.

PROPOSITION 2.3.2. *Let $\mathcal{P} \subset R[X_1, \ldots, X_k]$ be any set of s polynomials, $\{P_1, \ldots, P_s\}$ and suppose that, for all i, $H_i \in R[X_1, \ldots, X_k]$ is strictly positive. Let C be a semi-algebraically connected component of the set defined by*

$$P_1 = P_2 = \cdots = P_\ell = 0$$

$$P_{\ell+1} > 0, \ldots, P_s > 0.$$

Then there exists a semi-algebraically connected component C' of the semi-algebraic set in $R\langle 1/\Omega, \delta, \delta'\rangle^k$ defined by the following inequalities,

$$-\delta'\delta H_{4i} \leq (1-\delta')P_i \leq \delta'\delta H_{4i-1}, \qquad 1 \leq i \leq \ell,$$
$$(1-\delta')P_i \geq \delta H_{4i-3},\ \ell+1 \leq i \leq s$$
$$X_1^2 + \cdots + X_k^2 \leq \Omega^2$$

such that $eval_{\delta'}(C')$ is contained in the extension of C to $R\langle 1/\Omega, \delta\rangle$.

PROOF. If $x \in C$, then x satisfies the following equalities and inequalities

$$-\delta'\delta H_{4i} \leq (1-\delta')P_i \leq \delta'\delta H_{4i-1}, \qquad 1 \leq i \leq \ell,$$
$$(1-\delta')P_i \geq \delta H_{4i-3},\ \ell+1 \leq i \leq s,$$
$$X_1^2 + \cdots + X_k^2 \leq \Omega^2$$

in $R\langle 1/\Omega, \delta, \delta'\rangle^k$. Let C' be the semi-algebraically connected component of the semi-algebraic set in $R\langle 1/\Omega, \delta, \delta'\rangle^k$ defined by the above equalities and inequalities that contains x. It is clear that $\text{eval}_{\delta'}(C')$ is contained in the semi-algebraic set defined by the sign condition $P_1 = \cdots = P_\ell = 0, P_{\ell+1} > 0, \ldots, P_s > 0$, in $(R\langle 1/\Omega, \delta\rangle)^k$ and that it also contains $x \in C$. Since, by Proposition 2.2.1, $\text{eval}_{\delta'}(C')$ is also semi-algebraically connected, the statement of the proposition follows. □

In principle, after Proposition 2.3.1, there can be as many as $2^{O(s)}$ algebraic sets to consider. To limit the number of algebraic sets that our algorithms need to examine, we perturb the given polynomials to bring them into general position. We say that a set of polynomials, $\mathcal{P} = \{P_1, \ldots, P_s\}$, in k variables, is in *general position* if there are no $k+1$ polynomials in $\mathcal{P}$ that have a common zero in R^k. This is a weak notion of general position as we assume neither smoothness nor transversality.

Henceforth, for any polynomial $P(X_1, \ldots, X_k)$, let $P^h(X_0, X_1, \ldots, X_k)$ denote the homogenization of P with respect to an additional variable X_0.

Define

$$H_i = 1 + \sum_{1 \leq j \leq k} i^j X_j^{d'}.$$

LEMMA 2.3.3. *For any positive integer d', the polynomials*

$$H_i^h = X_0^{d'} + \sum_{1 \leq j \leq k} i^j X_j^{d'}$$

are in general position in projective k-space over $R[i]$.

PROOF. Let $H = (X_0^{d'} + \sum_{1 \leq j \leq k} t^j X_j^{d'})$. If $k+1$ of the H_i^h had a common zero $\bar{x}$ in projective k-space over $R[i]$, substituting this root in H would give a nonzero univariate polynomial of degree at most k with $k+1$ distinct roots, which is impossible. □

Since a common zero of a set of H_i would certainly produce a common zero of the corresponding set of H_i^h we have:

COROLLARY 2.3.4. *The polynomials H_i are in general position.*

PROPOSITION 2.3.5 [RENEGAR 1992]. *With $d' \geq d$ and δ infinitesimal over R, the polynomials $(1 - \delta)P_i + \delta H_i$ are in general position.*

PROOF. Let $Q_{i,t} = (1 - t)P_i + tH_i$. Consider the set, T, of those t such that the $Q_{i,t}$ are in general position in projective k-space over $R[i]$. According to the preceding lemma the set T contains 1. Since being in general position in projective k-space over $R[i]$ is a stable condition, T contains an open interval containing 1. The set T is also Zariski constructible as it can be defined by a first order formula in the language of algebraically closed fields. By quantifier elimination over algebraically closed fields, a Zariski constructible set is either finite or the complement of a finite set. Thus the transcendental element δ belongs to the extension of T to $R(\delta)$. □

We next show how to perturb a polynomial so that the zero set of the perturbed polynomial is smooth and bounded, and the projection map of this set onto the first coordinate has a finite number of critical points.

LEMMA 2.3.6. *For $Q \in R[X_1, \ldots, X_k]$ of degree d, we let*

$$Q_1 = Q^2 + (X_1^2 + \cdots + X_{k+1}^2 - \Omega^2)^2 \in R(1/\Omega)[X_1, \ldots, X_{k+1}].$$

Then the algebraic set $Z(Q_1) \subset R\langle 1/\Omega\rangle^{k+1}$ is contained in the open ball with center 0 and radius $\Omega + 1$. Moreover, the extension of every semi-algebraically connected component of $Z(Q)$ to $R\langle 1/\Omega\rangle$, contains the projection onto $R\langle 1/\Omega\rangle^k$ of a semi-algebraically connected component of $Z(Q_1) \subset R\langle 1/\Omega\rangle^{k+1}$.

PROOF. The first part of the lemma is obvious from the definition of Q_1. Let C be a semi-algebraically connected component of $Z(Q)$ and choose $x \in C$. Then the projection of the component of $Z(Q_1)$ containing the point, $(x, (\Omega^2 - |x|^2)^{1/2})$ is contained in $C_{R\langle 1/\Omega\rangle}$. □

Given a polynomial $Q \in R[X_1, \ldots, X_k]$ we define the *total degree of Q in X_i* to be the maximal total degree of the monomials in Q containing the variable X_i.

PROPOSITION 2.3.7. *Given $Q \in R[X_1, \ldots, X_k]$ with degree at most d and nonnegative over R^k, suppose that for some $r \in R$ $Z(Q)$ is contained in the open ball with center 0 and radius r. Let $d_1, d_2 \ldots, d_k$ be the total degrees of Q in $X_1, X_2, \ldots, X_k$ respectively (and, without loss of generality, $d_1 \geq d_2 \geq \cdots \geq d_k$). Let*

$$Q_1 = (1 - \zeta)Q + \zeta(X_1^{2(d_1+1)} + \cdots + X_k^{2(d_k+1)} - k(r^{2(d_1+1)}))$$

where ζ is positive and infinitesimal over R. Then the following holds:

(1) *The algebraic set $Z(Q_1) \subset (R\langle\zeta\rangle)^k$ is bounded and smooth.*
(2) *The polynomials*,

$$\mathcal{Q} = \left(Q_1, \frac{\partial Q_1}{\partial X_2}, \ldots, \frac{\partial Q_1}{\partial X_k}\right)$$

form a Gröbner basis for the ideal they generate with respect to the degree lexicographical ordering with $X_1 > \cdots > X_k$.

(3) *The set of critical points of* $Z(Q_1)$ (*over* $R[i]\langle\zeta\rangle$) *of the projection map onto the* X_1 *coordinate* (*which is the set of common zeros of* $\mathfrak{Q}$ *over* $R[i]\langle\zeta\rangle$) *is finite.*

(4) *Let* K' *be the set of real critical points of this projection map* (*with coordinates in* $R\langle\zeta\rangle$). *For every semi-algebraically connected component,* C, *of* $Z(Q)$, *there is a point* $p \in K'$, *such that* $eval_\zeta(p)$ *belongs to* C.

PROOF

(1) Since Q is assumed to be nonnegative over R^k, any zero of Q_1 satisfies the inequality

$$X_1^{2(d_1+1)} + \cdots + X_k^{2(d_k+1)} \leq k(r^{2(d_1+1)}).$$

This shows that the zeros of Q_1 lie inside a bounded ball with center 0.

To prove that $Z(Q_1)$ is smooth, consider the set of polynomials

$$Q_{1,t} = (1-t)Q + t(X_1^{2(d_1+1)} + \cdots + X_k^{2(d_k+1)} - kr^{2(d_1+1)}).$$

The variety $Z(Q_{1,t})$ is smooth if and only if the system of equations,

$$Q_{1,t} = \frac{\partial Q_{1,t}}{\partial X_1} = \cdots = \frac{\partial Q_{1,t}}{\partial X_k} = 0$$

has no solution. The set T, of those t's for which this system has no solution, is Zariski constructible, open, and contains $t = 1$. Hence, it contains ζ, which is transcendental and thus $Z(Q_1)$ is smooth.

(2) Let I be the ideal generated by $\mathfrak{Q}$.

That the polynomials $\mathfrak{Q}$ form a Gröbner basis of I with respect to the degree lexicographical ordering with $X_1 > \cdots > X_k$ follows immediately from Buchberger's algorithm [Buchberger 1985], and the following lemma which we state after introducing the necessary notation. We are given an admissible total ordering on monomials (a total order compatible with multiplication) such that $X_1 > \cdots X_k$. Given a polynomial P we write $\ell(P)$ for its leading monomial with respect to this order, $c(m, P)$ for the coefficient of the monomial m in the polynomial P. Thus $c(\ell(P), P)$ is the coefficient of the leading monomial in P which we call the leading coefficient of P. Given two polynomials P_1, P_2 with leading coefficient 1, the *S-Polynomial* of P_1, P_2 is defined as

$$S(P_1, P_2) = m \times P_1 - n \times P_2,$$

where $m = \ell(P_2)/gcd(\ell(P_1), \ell(P_2))$, $n = \ell(P_1)/gcd(\ell(P_1), \ell(P_2))$. Given a finite set of polynomials, G, with leading coefficients 1, we say that P *is reduced* to P_1 modulo G if there is a $Q \in G$ and a monomial m occurring in P such that, $\ell(Q)|m$, and $P_1 = P - c(m, P)Qm/\ell(Q)$. Moreover, we say that P is *reducible* to P_1 modulo G if there is a finite sequence of reductions modulo G going from P to P_1. According to Buchberger's algorithm [Buchberger 1985], an ideal basis, G, is a Gröbner

basis if the S-polynomial of any pair of polynomials in G is reducible to 0 modulo G.

LEMMA 2.3.8. *If* $c(\ell(Q_1), Q_1) = c(\ell(Q_2), Q_2) = 1$ *and* $gcd(\ell(Q_1), \ell(Q_2)) = 1$, *then the S-polynomial of* Q_1 *and* Q_2, $S(Q_1, Q_2) = \ell(Q_2) \times Q_1 - \ell(Q_1) \times Q_2$ *is reducible to* 0 *modulo* Q_1 *and* Q_2.

PROOF. Let $R_1 = Q_1 - \ell(Q_1)$, $R_2 = Q_2 - \ell(Q_2)$. Then $S(Q_1, Q_2) = \ell(Q_2)R_1 - \ell(Q_1)R_2$ and there is no monomial of $\ell(Q_2)R_1$ appearing in $\ell(Q_1)R_2$ (and vice versa). This is because all monomials in R_1 and R_2 are smaller (in the given ordering) than $\ell(Q_1)$ and $\ell(Q_2)$ respectively, and $gcd(\ell(Q_1), \ell(Q_2)) = 1$.

We successively reduce every monomial of $S(Q_1, Q_2)$ coming from $\ell(Q_2)R_1$ using Q_2. The result is $-\ell(Q_1)R_2 - R_1R_2$ and the monomials in $-\ell(Q_1)R_2$ are distinct from the monomials in R_1R_2. Then we successively reduce every monomial of $-\ell(Q_1)R_2 - R_1R_2$ coming from $-\ell(Q_1)R_2$ using Q_1 and the result is 0.

Thus, $S(Q_1, Q_2)$ is reducible to 0 modulo Q_1 and Q_2. □

(3) Since the polynomials $\mathbb{Q}$ form a Gröbner basis of I with respect to the degree lexicographical ordering with $X_1 > \cdots > X_k$, the quotient ring $A = R[X_1, \ldots, X_k]/I$ is a vector space that is spanned by the monomials not occurring in the ideal generated by the leading terms of the polynomials. These are the *monomials under the staircase*. Hence, the quotient ring is spanned by the monomials $X_1^{e_1}X_2^{e_2} \cdots X_k^{e_k}$, $e_1 < 2(d_1 + 1)$, $e_i < 2d_i + 1$, $2 \leq i \leq k$. Thus, the quotient ring is a finite dimensional vector space, and hence the number of common zeros of the polynomial Q (over $R[i]\langle\zeta\rangle$) is finite (see Proposition 2.4.1).

(4) Since the image of a bounded semi-algebraically connected semi-algebraic set under eval_ζ is again semi-algebraically connected (by Proposition 2.2.1), it is enough to prove that every point y in $Z(Q)$ belongs to the image of $\text{eval}_\zeta(Z(Q_1))$.

Let $y \in Z(Q)$. Then $Q_1(y)$ is a strictly negative element of $R\langle\zeta\rangle$. Now since Q is everywhere non-negative and 0 on a subset of codimension at least 1; fixing a ball, B, centered at y of radius r_1 (r_1 in R) there exists a point y' in B with $Q(y') \in R^k$, $Q(y') > 0$. Hence, $Q_1(y') > 0$ in $(R\langle\zeta\rangle)^k$ (because ζ is infinitesimal). This implies that the sign of Q_1 changes inside the ball $B_{R\langle\zeta\rangle}$ and so there is a z with coordinates in $R\langle\zeta\rangle$ such that $Q_1(z) = 0$ in every ball $B_{R\langle\zeta\rangle}$. Hence, the point of $Z(Q_1)$ with minimal distance to y is infinitesimally close to y and is sent by eval_ζ to y. □

The set of critical points so obtained after perturbation is finite and we need to solve the system

$$Q_1 = \frac{\partial Q_1}{\partial X_2} = \cdots = \frac{\partial Q_1}{\partial X_k} = 0,$$

in order to compute these critical points.

2.4. SOLVING POLYNOMIAL SYSTEMS AND COUNTING REAL SOLUTIONS. In this section, we closely follow Alonso et al. [1996]. This method for solving polyno-

mial systems is very much inspired by the way Canny [1988] and Renegar [1992] use the u-resultant of a system of k polynomials in k variables [Van Der Waerden 1950], but gives a more direct approach.

Let K be a field of characteristic zero and $\bar{K}$ an algebraically closed field containing it. Let $I = (P_1, \cdots, P_s)$ be an ideal and $A = K[X_1, \cdots, X_k]/I$. We define $\bar{A} = A \otimes_K \bar{K}$. The set of common zeros of $P_1, \cdots, P_s$ over a field L which is an extension of K is denoted by $Z_L(I)$.

The following results are well known (see Atiyah [1969] and Roy [to appear]).

PROPOSITION 2.4.1. *The K-algebra $A = K[X_1, \cdots, X_k]/I$ is a finite dimensional vector space if and only if $Z_{\bar{K}}(I)$ is finite. Moreover, the cardinality of $Z_{\bar{K}}(I)$ is at most the dimension of A as a K-vector space.*

In this case, we say that the ideal I is *zero-dimensional* since its set of zeros is a zero-dimensional set as it consists of isolated points.

PROPOSITION 2.4.2. *Let I be a zero-dimensional ideal. For every $\alpha \in Z_{\bar{K}}(I)$ there exists a local ring $\bar{A}_\alpha$ such that, $\bar{A} \cong \Pi_{\alpha \in Z_{\bar{K}}(I)} \bar{A}_\alpha$. More precisely, for every α there exists an element e_α called the idempotent attached to α, such that the canonical surjection of $\bar{A}$ onto $\bar{A}_\alpha$ coincides with multiplication by e_α. Moreover, the following holds*:

—*For all $\alpha \in Z_{\bar{K}}(I)$, $e_\alpha^2 = e_\alpha$.*

—*For all distinct $\alpha, \beta \in Z_{\bar{K}}(I)$, $e_\alpha e_\beta = 0$.*

— $\sum_{\alpha \in Z_{\bar{K}}(I)} e_\alpha = 1$.

We denote by μ_α the dimension of $\bar{A}_\alpha$ as a $\bar{K}$-vector space. We call μ_α the *multiplicity* of the zero $\alpha \in Z_{\bar{K}}(I)$.

The next result is less well known but extremely useful.

PROPOSITION 2.4.3 (STICKELBERGER). *Let I be a zero-dimensional ideal. If $f \in A$ and L_f is the linear endomorphism which is multiplication by f, then $L_f(\bar{A}_\alpha) \subset \bar{A}_\alpha$. Moreover, the restriction of L_f to $\bar{A}_\alpha$, $L_{f,\alpha}$, has only one eigenvalue, $f(\alpha)$, and its multiplicity is μ_α.*

PROOF. It is clear that $L_f(\bar{A}_\alpha) \subset \bar{A}_\alpha$ since $\bar{A}_\alpha$ is the image of $\bar{A}$ under the multiplication by e_α. Since $e_\alpha(f - f(\alpha))$ vanishes on the common zeros of $P_1, \cdots, P_s$ whence, according to the Hilbert Nullstellensatz, there exists m such that $e_\alpha(f - f(\alpha))^m = 0$. This means that $L_{f,\alpha} - f(\alpha)Id$ is nilpotent. □

COROLLARY 2.4.4

—*The trace of L_f is* $\sum_{\alpha \in Z_{\bar{K}}(I)} \mu_\alpha f(\alpha)$.

—*The determinant of L_f is* $\Pi_{\alpha \in Z_{\bar{K}}(I)} f(\alpha)^{\mu_\alpha}$.

We now describe the method in Alonso et al. [1996] for solving systems of polynomial equations. We take for u a *separating* element of A, that is a u with the property that for any distinct zeros α, β of $Z_{\bar{K}}(I)$,$u(\alpha) \neq u(\beta)$. Let $\chi(u, t)$ be the characteristic polynomial of the linear transformation L_u. According to Proposition 2.4.3,

$$\chi(u, t) = \prod_{\alpha \in Z_{\bar{K}(I)}} (t - u(\alpha))^{\mu_\alpha}.$$

We are going to express the points of the variety $Z_{\bar{K}}(I)$ as rational functions of the roots of $\chi(u, t)$.

Introduce a new variable s and consider the polynomial

$$\chi(u + sv, t) \in K[s, t],$$

for some $v \in A$. Since u is a separating element in A, so is $u + sv$ for almost all values of s.

Let

$$g(u, v, t) = \left.\frac{\partial_x(u + vs, t)}{\partial s}\right|_{s=0}$$

and $g(u, t) = \chi'(u, t)$. Let $\mu = \mu_\alpha$, then substituting $t = u(\alpha)$ in the expression for $g^{(\mu-1)}(u, t)$ we have,

$$g^{(\mu-1)}(u, u(\alpha)) = \mu! \prod_{\beta \in Z(I), \beta \neq \alpha} (u(\alpha) - u(\beta))^{\mu_\beta}.$$

Similarly, computing $g^{(\mu-1)}(u, v, t)$ and substituting $t = u(\alpha)$ we have,

$$g^{(\mu-1)}(u, v, u(\alpha)) = -v(\alpha)\mu! \prod_{\beta \in Z(I), \beta \neq \alpha} (u(\alpha) - u(\beta))^{\mu_\beta}$$

(where $g^{(i)}(u, v, t)$, $g^{(i)}(u, t)$ are the ith derivatives with respect to t of $g(u, v, t)$ and $g(u, t)$ respectively). Hence, we have proven:

PROPOSITION 2.4.5. *Let* $Z_\mu = \{\alpha \in Z_{\bar{K}}(I) | \mu_\alpha = \mu\}$. *The following equality holds for every* α *in* Z_μ:

$$v(\alpha) = -\frac{g^{(\mu-1)}(u, v, u(\alpha))}{g^{(\mu-1)}(u, u(\alpha))}.$$

Thus, taking $v = X_i$, for $i = 1, \ldots, k$, we express the coordinates of the points $\alpha \in Z_\mu$, in terms of rational functions of $u(\alpha)$, which in turn are roots of the polynomial $\chi(u, t)$.

We now explain how we compute the polynomials $\chi(u, t)$ and $\chi(u + vs, t)$. Since they are the characteristic polynomials of the linear transformations L_u and L_{u+vs}, we can compute them from a basis of the finite-dimensional vector space A and the multiplication table of A in this basis. This information is known once we have a Gröbner basis for the ideal I.

All that remains is to explain how we find a separating element u. We first prove:

LEMMA 2.4.6. *If* $Z_{\bar{K}}(I)$ *has* N *points, at least one* $u_i = X_1 + iX_2 + \cdots + i^{k-1}X_k$ *for* $0 \leq i \leq (k-1)\binom{N}{2}$ *is separating.*

PROOF OF THE LEMMA. Consider a pair $\{x, y\} = \{(x_1, \cdots, x_k), (y_1, \cdots, y_k)\}$ of distinct points of $Z_{\bar{K}}(I)$ and let $\ell(x, y)$ be the number of i, $0 \leq i \leq (k-1)\binom{N}{2}$, such that $u_i(x) = u_i(y)$. Since the polynomial

$$(x_1 - y_1) + (x_2 - y_2)t + \cdots + (x_k - y_k)t^{k-1}$$

which is not identically zero has no more than $k - 1$ distinct roots, the number $\ell(x, y)$ is at most $k - 1$. Since the total number of pairs of distinct points of $Z_{\bar{K}}(I)$ is less than $\binom{N}{2}$, this completes the proof. □

In order to find a separating element we compute all the $\chi(u, t)$ for $u = X_1 + iX_2 + \cdots + i^{k-1}X_k$ and $0 \leq i \leq (k-1)\binom{N}{2}$ and chose u such that the number of distinct roots of $\chi(u, t)$ is maximal.

We now give a formula that expresses the number of real zeros of a zero-dimensional ideal in terms of quantities already presented.

Let I be a zero-dimensional ideal contained in $R[X_1, \ldots, X_k]$ and $A = R[X_1, \ldots, X_k]/I$. We write Z for $Z_R(I)$.

Given $h \in A$, we define the *Sturm query* of h with respect to Z, $SQ(Z, h)$, as the difference between the number of elements of Z at which $h > 0$ and the number of elements of Z at which $h < 0$. We associate to h a symmetric bilinear form $B_h: A \otimes A \to R$ defined by $B_h(f, g) = Tr(L_{hfg})$ where L_{hfg} is the linear transformation defined above. Let the associated quadratic form, called the Hermite quadratic form, be denoted Q_h.

PROPOSITION 2.4.7 [PEDERSEN ET AL. 1993].

$$SQ(Z, h) = signature(Q_h).$$

PROOF. Let N be the dimension of A as a vector space and M the number of distinct points of $Z_{R[i]}(I)$. Consider a separating element u and a basis of the vector space A of the form $\mathcal{B} = \{1, u, \ldots, u^{M-1}, \omega_{M+1}, \ldots, \omega_N\}$. It is clear from Proposition 2.4.3 that if an element a of A is written in the basis as

$$a_1 + a_2u + \cdots + a_Mu^{M-1} + a_{M+1}\omega_{M+1} + \cdots + a_N\omega_N$$

then

$$Q_h(a) = \sum_{\alpha \in Z_{\bar{R}}(I)} \mu(\alpha)h(\alpha)(a(\alpha))^2.$$

Since u is separating, the linear forms

$$a_1 + a_2u(\alpha) + \cdots + a_Mu(\alpha)^{M-1} + a_{M+1}\omega_{M+1}(\alpha) + \cdots + a_N\omega_N(\alpha)$$

are linearly independent. To compute the signature, we consider separately zeros $\alpha \in Z$ for which $h(\alpha) > 0$ (respectively, $h(\alpha) < 0$). These contribute 1 (respectively, -1) to the signature. Then, observe that the pairs of conjugate zeroes in $Z_{R[i]}(I) \backslash [Z]$ contribute 0 to the signature. □

2.5. SUBRESULTANT COEFFICIENTS. In the elimination phase of our algorithm for the general decision problem, we make use of the classical theory of subresultant coefficients. We give a brief review of the definition of the subresultant coefficients of two polynomials, and of the properties we utilize.

Given two polynomials $P = a_0X^d + \cdots + a_d$ and $Q = b_0X^e + \cdots + b_e$ of degrees d and e respectively, with $a_i, b_j \in R$, the resultant of P and Q is the

determinant of the *Sylvester matrix* of P and Q, which is the following square matrix of size $d + e$:

$$\begin{pmatrix}
a_0 & a_1 & a_2 & \dots & . & . & . & a_d & 0 & . & \dots & 0 \\
0 & a_0 & a_1 & \dots & . & . & . & a_{d-1} & a_d & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & . & . & \dots & 0 & a_0 & a_1 & a_2 & . & . & \dots & a_d \\
b_0 & b_1 & . & \dots & . & . & b_e & 0 & . & . & \dots & 0 \\
0 & b_0 & . & \dots & . & . & b_{e-1} & b_e & 0 & . & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & . & . & \dots & . & 0 & b_0 & b_1 & . & . & \dots & b_e
\end{pmatrix}$$

It is well known that the resultant of P and Q is zero if and only if P and Q have a common factor.

The properties of the subresultant coefficients generalize those of the resultant.

For $0 \leq j < \min(d, e)$, the *jth-subresultant coefficient* of P and Q, denoted $\mathrm{sres}_j(P, Q))$ is the determinant of the minor of size $d + e - 2j$ of the Sylvester matrix of P and Q, obtained by removing the last j rows of coefficients of P, the last j rows of coefficients of Q, and the last $2j$ columns. The resultant of P and Q is $\mathrm{sres}_0(P, Q)$.

The following propositions are classical (see Lemma 7.7.8 of Mishra [1994] and Proposition 3.33 of Roy [to appear]).

PROPOSITION 2.5.1. *Let ℓ be an integer, $0 \leq \ell < min(d, e)$. The GCD of the polynomials P and Q has degree strictly larger than ℓ if and only if*

$$sres_0(P, Q) = \cdots = sres_\ell(P, Q) = 0.$$

PROPOSITION 2.5.2. *The number of distinct real roots of P depends only on the signs of the subresultant coefficients of P and P'.*

2.6. *Replacing Infinitesimals by Small Enough Numbers*

In some phases of our algorithms, we often construct points whose co-ordinates belong to some non-archimedean extension of R. These extensions will typically be fields of the Puiseux series in one or more infinitesimals. The next proposition makes it possible to replace these infinitesimals (respectively, infinitely large elements) with sufficiently small (respectively, large) elements from the field of fractions of D.

Definition 2.6.1. Given a polynomial

$$Q = c_q X^q + \cdots + c_p X^p,\ q > p,\ c_q,\ c_p \neq 0,$$

with coefficients in an ordered domain D, we define

$$C(Q) = \sum_{p \le i \le q} \left(\frac{c_i}{c_q} \right)^2,$$

$$c(Q) = \left(\sum_{p \le i \le q} \left(\frac{c_i}{c_p} \right)^2 \right)^{-1}.$$

Given a set of polynomials $\mathcal{L}$, we define $C(\mathcal{L}) = \max_{Q \in \mathcal{L}} C(Q)$, and $c(\mathcal{L}) = \min_{Q \in \mathcal{L}} c(Q)$.

LEMMA 2.6.2. *Given a polynomial Q with coefficients in a ring D contained in R, the greatest absolute value of the roots of Q is smaller than $C(Q)$, while the smallest absolute value of the nonzero roots of Q is greater than $c(Q)$.*

PROOF. Let α be a root of $Q = c_q X^q + \cdots + c_p X^p$, $q > p$ in R. Then

$$c_q \alpha = - \sum_{p \le i \le q-1} c_i \alpha^{-(q-1-i)}.$$

If the absolute value of α is greater than 1, this gives

$$c_q^2 \alpha^2 \le \left(\sum_{p \le i \le q-1} (c_i)^2 \right).$$

Otherwise, we can bound the absolute value of α by 1. In both cases, the absolute value of α is bounded by $C(Q)$. The bound on $c(Q)$ is obtained by considering the polynomial, $X^q Q(1/X)$. □

Notation 2.6.3. Let $T_i(g)(t)$ be the polynomial obtained by dropping all the terms with degree greater than i from $g(t)$.

Given a set, $\mathcal{L} = \{f(t), g_1(t), \ldots, g_m(t)\} \subset D[t]$, of polynomials with maximum degree d, define $\mathcal{SL}$ as the collection of all the subresultant coefficients for the all pairs of polynomials:

$$(T_i(f), T_j(f^{(\ell)})), (T_i(f), T_j(g_w)),$$

with

$$0 \le i, j, \ell \le d, \qquad 1 \le w \le m.$$

Note that $\mathcal{SL} \subset D[\Omega]$.

PROPOSITION 2.6.4. *Let $\mathcal{L} = \{f(\Omega, t), g_1(\Omega, t), \ldots, g_m(\Omega, t)\} \subset D[\Omega, t]$, be a set of polynomials with maximum degree d in t and $\sigma = \{\sigma_1, \ldots, \sigma_m\}$ be a sign condition such that f has a root $\bar{t} \in R\langle 1/\Omega \rangle$ for which*

$$sign(g_1(\Omega, \bar{t})) = \sigma_1, \ldots, sign(g_m(\Omega, \bar{t})) = \sigma_m.$$

If $v \in R$ and $v > C(\mathcal{SL})$, then,

$$sign(g_1(v, \bar{t}')) = \sigma_1, \ldots, sign(g_m(v, \bar{t}'))) = \sigma_m,$$

where $\bar{t}'$ is the root of $f(v, t)$, having the same Thom encoding as $\bar{t}$.

PROOF. If $v > C(\mathcal{SL})$, then v is greater than the absolute value of all roots of every Q in $\mathcal{SL}$. Hence, by construction, the number of roots of the polynomial $f(v, t)$ as well as the number of its common roots with the polynomials $g_1(v, t), \ldots, g_m(v, t)$ and the Thom encoding of its roots remain invariant for all v satisfying $v > C(\mathcal{SL})$.

Now it is clear from elementary properties of the field of Puiseux series that

$$(\text{sign}(g_1(v, \bar{t}')), \ldots, \text{sign}(g_m(v, \bar{t}'))) = (\text{sign}(g_1(\Omega, \bar{t})), \ldots, \text{sign}(g_m(\Omega, \bar{t}))). \quad \square$$

The following proposition is analogous to the previous one. The only difference is that we deal with an infinitesimal, rather than an infinitely large variable. The proof is completely analogous and hence omitted.

PROPOSITION 2.6.5. *Let $\mathcal{L} = \{f(\epsilon, t), g_1(\epsilon, t), \ldots, g_m(\epsilon, t)\} \subset D[\epsilon, t]$, be a set of polynomials with maximum degree d and $\sigma = \{\sigma_1, \ldots, \sigma_m\}$ be a sign condition such that f has a root $t \in R\langle\epsilon\rangle$ for which*

$$\textit{sign}(g_1(\epsilon, \bar{t})) = \sigma_1, \ldots, \textit{sign}(g_m(\epsilon, \bar{t})) = \sigma_m.$$

Then for any v in R, $0 < v < c(\mathcal{SL})$,

$$\textit{sign}(g_1(v, \bar{t}')) = \sigma_1, \ldots, \textit{sign}(g_m(v, \bar{t}')) = \sigma_m,$$

where $\bar{t}'$ is the root of $f(v, t)$, having the same Thom encoding as $\bar{t}$.

It is clear from the above propositions, that given a list of polynomials, $\mathcal{L} = \{f(\epsilon, t), g_1(\epsilon, t), \ldots, g_m(\epsilon, t)\}$ (respectively, $\{f(\Omega, t), g_1(\Omega, t), \ldots, g_m(\Omega, t)\}$), whose degrees are bounded by d, we can compute $c(\mathcal{SL})$, (respectively, $C(\mathcal{SL})$) which belong to the fraction field of D, using no more than $md^{O(1)}$ arithmetic operations in D.

Note that, if $D = \mathbf{Z}$ and the bit size of the coefficients of the polynomials f, $g_1, \ldots, g_m$, is bounded by τ, then $C(\mathcal{SL})$ (respectively, $c(\mathcal{SL})$) is bounded from above (respectively, below) by rational numbers with numerators and denominators of bit size $\tau d^{O(1)}$. In this case, we do not need to perform any computations in order to replace the infinitely large (respectively, small) elements with appropriately large (respectively, small) rationals.

2.7. SIGN DETERMINATIONS. We now present the preliminary material needed for our Sign determination subroutine. The content of this section is inspired by Ben-Or et al. [1986], Canny [1993b], Pedersen et al. [1993], and Roy [to appear].

Let Z be a finite subset of R^k. A *pseudo-partition* of Z is a list $C = (C_1, \cdots, C_n)$ of n pairwise disjoint subsets of Z whose union is Z. This differs from a partition since some of the C_i may be empty.

For $\sigma \in \{0, 1, -1\}$ and a polynomial h, let $C_\sigma(h)$ denote the set of elements of Z at which h has sign σ and by $c_\sigma(h)$ its cardinal.

Recall that the *Sturm query* of h with respect to Z is

$$SQ(Z, h) = c_1(h) - c_{-1}(h).$$

Similarly, for a list of polynomials $\mathcal{P} = (P_1, \ldots, P_s)$ and a sign condition $\sigma \in \{0, 1, -1\}^s$, we denote by $C_\sigma(\mathcal{P})$ the sets of points of Z at which the sign condition of P_i is σ_i and by $c_\sigma(\mathcal{P})$ its cardinal. In the sequel to this section, lists of sign conditions composed of elements of $\{0, 1, -1\}^s$, will always be ordered according to the lexicographical order on $\{0, 1, -1\}^s$ (defined by $0 < 1 < -1$). A list of distinct sign conditions, Σ, is *complete for* $\mathcal{P}$ over Z if $Z = \cup_{\sigma \in \Sigma} C_\sigma(\mathcal{P})$. If Σ is a list of sign conditions complete for $\mathcal{P}$ over Z, we denote by $C_\Sigma(\mathcal{P})$ the pseudo-partition of Z consisting of the $C_\sigma(\mathcal{P})$ for $\sigma \in \Sigma$, and the corresponding list of cardinals by $c_\Sigma(\mathcal{P})$.

A list of polynomials $H = (h_1, \cdots, h_m)$ is *adapted* to a pseudo-partition $C = (C_1, \cdots, C_n)$ of Z if the signs of the polynomials of H are fixed on each C_i. If H is adapted to C, the *matrix of signs of* H on C, $A(C, H)$ is the $m \times n$ matrix whose (i, j)th entry is the sign of h_i on C_j.

For example $(1, h, h^2)$ is adapted to

$$(C_0(h), C_1(h), C_{-1}(h))$$

and the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix}$$

is the matrix of signs of $(1, h, h^2)$ on

$$(C_0(h), C_1(h), C_{-1}(h)).$$

If $H = [(h_1, \cdots, h_m)$ and $H' = (h'_1, \cdots, h'_\mu)$ are two lists of polynomials, $H \cdot H'$ is the list of $m\mu$ polynomials

$$(h_1 \cdot h'_1, \ldots, h_m \cdot h'_1, \ldots, h_1 \cdot h'_\mu \cdots h_m \cdot h'_\mu).$$

For $\mathcal{P} = (P_1, \ldots, P_s)$, $H(\mathcal{P})$ is the list of 3^s polynomials defined inductively by

$$H(\{P_1\}) = (1, P_1, P_1^2), H(\mathcal{P}) = H(\mathcal{P} \backslash \{P_s\}) \cdot (1, P_s, P_s^2).$$

If Σ is complete for $\mathcal{P}$ over Z, the list of polynomials $H(\mathcal{P})$ is adapted to $C_\Sigma(\mathcal{P})$. Given a pseudo-partition C of Z, we denote by $c(C)$ the list of cardinals of the list C. Given a list of polynomials H, we denote by $SQ(Z, H)$ the list of Sturm queries of the list H.

PROPOSITION 2.7.1. *Given a pseudo-partition C of Z, and a list of polynomials H adapted to C,*

$$A(C, H) \cdot c(C) = SQ(Z, H).$$

PROOF. It is obvious since the ith row of $A(C, H)$ is the list of signs of h_i on the list C. □

COROLLARY 2.7.2. *Given a finite subset Z of R^k, and $h \in D[X]$,*

$$A \cdot \begin{bmatrix} c_0(h) \\ c_1(h) \\ c_{-1}(h) \end{bmatrix} = \begin{bmatrix} SQ(Z, 1) \\ SQ(Z, h) \\ SQ(Z, h^2) \end{bmatrix}.$$

PROOF. We have seen that A is the matrix of signs of $(1, h, h^2)$ on

$$(C_0(h), C_1(h), C_{-1}(h)). \qquad \square$$

If $C = (C_1, \cdots, C_n)$ and $C' = (C'_1, \cdots, C'_\nu)$ are two pseudo-partitions of the finite subset Z of R^k, $C \cap C'$ denotes

$$(C_1 \cap C'_1, \cdots, C_n \cap C'_1, \cdots, C_1 \cap C'_\nu, \cdots, C_n \cap C'_\nu),$$

which is a pseudo-partition of Z.

If A and A' are $n \times m$ and $\nu \times \mu$ matrices, we define $A \otimes A'$ to be the $n\nu \times m\mu$ matrix obtained by replacing each entry $a'_{i,j}$ of A' by the matrix $a'_{i,j}A$.

PROPOSITION 2.7.3. *Let Z be a finite subset of R^k. Consider two pseudo-partitions C and C' of Z and two lists of polynomials H and H' such that H (respectively, H') is adapted to C (respectively, C'). Then, $H \cdot H'$ is adapted to $C \cap C'$ and*

$$A(C, H) \otimes A(C', H') = A(C \cap C', H \cdot H').$$

PROOF. This follows immediately from the definitions. $\square$

COROLLARY 2.7.4. *Let Z be a finite subset of R^k. Consider two pseudo-partitions C and C' of Z, and two lists of polynomials H and H' such that H (respectively, H') is adapted to C (respectively, C'). Then*

$$(A(C, H) \otimes A(C', H'))c(C \cap C') = SQ(Z, H \cdot H').$$

PROOF. Immediate from the preceding propositions. $\square$

Let $\Sigma(\mathcal{P})$ be the ordered list of nonempty sign conditions of $\mathcal{P}$ over Z, then we denote by $C(\mathcal{P})$ the corresponding partition of Z and by $c(\mathcal{P})$ the corresponding list of cardinals of $C_\sigma(\mathcal{P})$ for σ in $\Sigma(\mathcal{P})$ (i.e., $C(\mathcal{P}) = C_{\Sigma(\mathcal{P})}(\mathcal{P})$ and $c(\mathcal{P}) = c_{\Sigma(\mathcal{P})}(\mathcal{P})$.

We define $L(\mathcal{P})$ as the smallest sublist of $H(\mathcal{P})$ (according to the lexicographical ordering) such that the matrix $A(C(\mathcal{P}), L(\mathcal{P}))$ is invertible.

We need the following definition: given h and k in $H(\mathcal{P})$, *h precedes k* if $h \in H(\mathcal{Q})$ with $\mathcal{Q} \subset \mathcal{P}$ and there exists a polynomial $h' \in H(\mathcal{P} \backslash \mathcal{Q})$ with $k = h \cdot h'$.

PROPOSITION 2.7.5. *Let h and k be in $H(\mathcal{P})$. If $k \in L(\mathcal{P})$ and h precedes k, then $h \in L(\mathcal{P})$.*

PROOF. Since h precedes k, let $k = hh'$ for an appropriate h'. Given $h \in H(\mathcal{P})$, denote by $\text{sign}(h)$ the vector of signs of h on $C(\mathcal{P})$. The vector $\text{sign}(h)$ is a row of the matrix $A(C(\mathcal{P}), H(\mathcal{P}))$. Suppose that $h \notin L(\mathcal{P})$ so that $\text{sign}(h)$ is a linear combination of the rows above it in the matrix $A(C(\mathcal{P}), H(\mathcal{P}))$, then

$$\text{sign}(h) = \sum_{h^* \in H} a_{h^*} \text{ sign}(h^*)$$

with all $h^* \in H$ being before h in $H(\mathcal{P})$. It is clear that

$$\text{sign}(k) = \text{sign}(hh') = \sum_{h^* \in H} a_{h^*} \text{sign}(h^*h')$$

and given the construction of the list $H(\mathcal{P})$, if h^* is before h in $H(\mathcal{P})$, h^*h' is before $hh' = k$ in $H(\mathcal{P})$. Hence, $k \notin L(\mathcal{P})$. □

COROLLARY 2.7.6. *If r is the number of elements of Z, and $\mathcal{P} = (P_1, \ldots, P_s)$, the elements of $L(\mathcal{P})$ are products of at most $\lceil \log_2(r) \rceil$ polynomials of*

$$\{1, P_1, P_1^2, \ldots, P_s, P_s^2\}.$$

PROOF. The number of distinct sign conditions in $\Sigma(\mathcal{P})$ is not greater than r, so the length of $L(\mathcal{P})$ is not greater than r as well. If h is a product of ℓ polynomials of the form $\{1, P_1, P_1^2, \ldots, P_s, P_s^2\}$, there are at least 2^ℓ polynomials in $H(\mathcal{P})$ preceding h. □

Note also that if $\mathcal{P}$ is the list $(P_1, \ldots, P_s)$ and $\mathcal{Q} = (P_1, \ldots, P_\ell)$ with $1 \leq \ell \leq s$, $L(\mathcal{P}) \subset L(\mathcal{Q}) \cdot L(\mathcal{P} \backslash \mathcal{Q})$.

3. *The Existential Theory of Reals*

3.1. ALGORITHMIC PRELIMINARIES. We solve the decision problem for the existential theory of the reals by finding the set of all realizable sign conditions of the set of polynomials $\mathcal{P}$. Once we have this set, we can check whether there exists a sign condition in the set which satisfies the given Boolean formula $F(P_1, \ldots, P_s)$. In order to generate the set of all possible sign conditions for the set of polynomials $\mathcal{P}$, we actually construct points in every *cell* of $\mathcal{P}$. We then generate the set of realizable sign conditions, by computing the sign condition of the set $\mathcal{P}$ at these points.

We use a subroutine that constructs univariate representations of the zeros of a zero dimensional ideal, using the theory and notation given in the previous section. We call it the *Univariate Representation Subroutine.*

3.1.1. *Univariate Representation Subroutine*. This subroutine takes as input a Gröbner basis, with coefficients in D, of a zero-dimensional ideal $I \subset R[X_1, \ldots, X_k]$ and outputs a finite set of $(k + 2)$-tuples, $(f, g_0, \ldots, g_k) \in D[t]^{k+2}$ such that the complex zeros of I are among the points obtained by evaluating the rational functions $(g_1/g_0, \ldots, g_k/g_0)$ at the roots of the univariate polynomial f for all the tuples $(f, g_0, \ldots, g_k)$ in the output. We say that the points so obtained from the tuple $(f, g_0, \ldots, g_k)$ are *associated* to the tuple, and the tuple itself is a *univariate representation* of these points. We use the following notation:

Notation 3.1.1.1. Given a univariate representation $u(t) = (f(t), g_0(t), \ldots, g_k(t))$, and a polynomial $P(X_1, \ldots, X_k)$, we denote by $P_u(t)$ the polynomial obtained by substituting g_i for X_i in $X_0^{d'} P(X_1/X_0, \ldots, X_k/X_0)$ (where d' is the smallest even number greater than the degree of P).

We follow the notations in Section 2.4. Let N be the dimension of the vector space A. The output is obtained by taking for all

$$u \in \{X_1 + iX_2 + i^2X_3 + \cdots + i^{k-1}X_k | 1 \leq i \leq (k-1)\binom{N}{2} + 1\}$$

the $(k+2)$-tuples of polynomials

$$(f(u, t) = \chi(u, t), g_0(u, t) = g^{(\mu-1)}(u, t), g_1(u, t) = -g^{(\mu-1)}(u, X_1, t), \ldots, g_k(u, t) = -g^{(\mu-1)}(u, X_k, t)),$$

for $1 \leq \mu \leq \text{degree}(f)$.

For the $O(kN^2)$ choices of the polynomial u, we produce $\deg(f) = O(N)$ tuples of polynomials. Thus, the set of tuples is of size $O(kN^3)$. Moreover, the degree of each polynomial in the output is bounded by $O(N)$.

3.1.2. Cell Representatives Subroutine. As mentioned earlier, using Proposition 2.3.1, we can reduce the problem of computing the sample points in every cell of a set of polynomials to constructing points on every semi-algebraically connected component of certain algebraic sets.

This subroutine takes as input a polynomial Q and outputs a set of points that meets every semi-algebraically connected component of $Z(Q)$. A similar algorithm is implicit in Canny [1988] and Renegar [1992].

Given a polynomial Q of total degrees $d_1, \ldots, d_k$ in $X_1, \ldots, X_k$ (with $d_1 \geq \cdots \geq d_k$) and with coefficients in an ordered domain D, the subroutine computes a set of univariate representations of size $(d_1 \cdots d_k)^{O(1)}$ associated with these univariate representations which intersects every semi-algebraically connected component of the set $Z(Q)$. Each univariate polynomial in the output univariate representations has degree bounded by $O(d_1) \cdots O(d_k)$. The subroutine uses $(d_1 \cdots d_k)^{O(1)}$ arithmetic operations in D.

In the subroutine, we introduce extra variables Ω and ζ. In order to prove the correctness of our subroutine using Proposition 2.3.7, we will interpret Ω to be infinitely big and ζ to be a positive infinitesimal with the ordering $1/\Omega \gg \zeta$. However, the cell representatives subroutine treats Ω and ζ only as extra variables. Since we do not perform any sign determination in this subroutine, we do not make use of the ordering in the field of coefficients.

We first introduce two new variables X_{k+1} and Ω, and replace Q by

$$Q^2 + (X_1^2 + \cdots + X_k^2 + X_{k+1}^2 - \Omega^2)^2.$$

We then introduce another new variable ζ and define

$$Q_1 = (1-\zeta)Q + \zeta(X_1^{2(d_1+1)} + \cdots + X_k^{2(d_k+1)} + X_{k+1}^6 - (k+1)(\Omega+1)^{2(d+1)}).$$

We next apply the univariate representation subroutine to

$$Q_1, \frac{\partial Q_1}{\partial X_2}, \ldots, \frac{\partial Q_1}{\partial X_{k+1}}$$

to get a set of $(k+2)$-tuples $(f, g_0, \ldots, g_{k+1})$. Notice that, according to Proposition 2.3.7, the above set of polynomials form a Gröbner basis, G, for the ideal they generate with the ordering being the degree lexicographical ordering. Moreover, its quotient ring is spanned by the monomials under the staircase.

This is the set of all monomials $X_1^{e_1} \cdots X_{k+1}^{e_{k+1}}$, with $e_1 < 2(d_1 + 1)$, $e_i < 2d_i + 1$, $2 \leq i \leq k$, $e_{k+1} < 5$.

Thus, the quotient ring is a finite dimensional vector space of dimension $10(d_1 + 1)(2d_2 + 1)\cdots(2d_k + 1)$. The multiplication table for this basis is of size $(d_1 \cdots d_k)^{O(1)}$, and the characteristic polynomial $f(t) = \chi(u, t)$ is a polynomial in t of degree at most $O(d_1)\cdots O(d_k)$.

Notice that the construction of the multiplication table for the algebra A, involves reductions by polynomials in the Gröbner basis G. Moreover, the leading terms of the polynomials in G are, $\zeta X_1^{2(d_1+1)}$, $\zeta X_i^{2d_i+1}$, for $2 \leq i \leq k$, and ζX_{k+1}^5. Thus, the product of two basis monomials in the multiplication table will be a polynomial in $D[\Omega, \zeta, 1/\zeta, X_1, \ldots, X_{k+1}]$. Hence, the polynomials in the tuples produced by the univariate representation subroutine, $f, g_0, \ldots, g_{k+1}$, are in $D[\Omega, \zeta, 1/\zeta][t]$.

In the next step, we let ζ go to 0 and retain only those points that do not go to infinity in the process. We do this purely algebraically. However, if we interpret ζ to be an infinitesimal, then this has the same effect as applying the eval_ζ map to the points (which are bounded) associated to the tuples, $(f, g_0, \ldots, g_{k+1})$, produced in the previous step.

Let us describe this more precisely. Given a nonzero polynomial $h \in D[\Omega, \zeta, 1/\zeta, t]$ we write it as

$$h\left(\Omega, \zeta, \frac{1}{\zeta}, t\right) = \sum_{i \geq \nu(h)} h^{[i]}(\Omega, t)\zeta^i, h^{[\nu(h)]} \neq 0.$$

We call $\nu(h)$ the order of h with respect to ζ. For every tuple $(f, g_0, \ldots, g_{k+1})$ produced in the previous step, we only consider those for which $\nu(f) = \nu(g_0)$ and $\nu(g_i) \geq \nu(g_0)$, and ignore the rest.

For each tuple $(f, g_0, \ldots, g_k)$ retained in the previous step, we replace it by the tuple

$$(f^{[\nu(f)]}, g_0^{[\nu(f)]}, \ldots, g_{k+1}^{[\nu(f)]}).$$

It follows from Lemma 2.1.1 that the set of points associated to the tuples obtained above includes the image of those points bounded over $R\langle 1/\Omega \rangle$ which are associated to the original set of tuples under the eval_ζ map.

We now project the points constructed above onto their first k coordinates. For each tuple,

$$u = (f(\Omega, t), g_0(\Omega, t), \ldots, g_k(\Omega, t)),$$

so obtained, compute the polynomial $Q_u(\Omega, t)$. Let $\mathcal{L}$ be the set of polynomials $f(\Omega, t)$, $Q_u(\Omega, t)$, and compute $C(\mathcal{SL})$ using Proposition 2.6.4. Substituting, $C(\mathcal{SL})$ for Ω in the polynomials,

$$(f(\Omega, t), g_0(\Omega, t), \ldots, g_k(\Omega, t)),$$

and clearing denominators we obtain polynomials with coefficients in D.

The proof of correctness of the above subroutine follows from Lemma 2.3.6 and Proposition 2.3.7. The bound of $d^{O(k)}$ on the complexity of this algorithm and on the degree and number of the polynomials in the output univariate

representations follows from the complexity analysis of the univariate representation subroutine.

3.1.3. *Sample Points Subroutine*. We are now in a position to outline the Sample Points Subroutine (see Basu et al. [to appear] and also Basu et al. [1995]) to generate sample points in every cell of $\mathcal{P}$.

The input is a set of s polynomials, $\mathcal{P} = \{P_1, \ldots, P_s\} \subset D[X_1, \ldots, X_k]$, each of degree at most d and the output is a set of $s^k(O(d))^k$ univariate representations of the form $(f, g_0, \ldots, g_k) \in D[t]^{k+2}$ such that the associated points meet every cell of $\mathcal{P}$.

The algorithm is the following: Replace the set $\mathcal{P}$ by the set $\mathcal{P}^*$ of $4s$ polynomials where:

$$\mathcal{P}^* = \bigcup_{i=1,\ldots,s} \{(1-\delta')P_i - \delta H_{4i-3},\ (1-\delta')P_i + \delta H_{4i-2},$$
$$(1-\delta')P_i - \delta'\delta H_{4i-1},\ (1-\delta')P_i + \delta'\delta H_{4i}\}$$

with $H_i = (1 + \sum_{1\le j\le k} i^j x_j^{d'})$ and d' an even number greater than the degree of any P_i.

For every $\ell \le k$-tuple of polynomials $Q_{i_1}, \ldots, Q_{i_\ell}$ in $\mathcal{P}^*$ consider

$$Q = Q_{i_1}^2 + \cdots + Q_{i_\ell}^2 + (X_1^2 + \cdots + X_k^2 + X_{k+1}^2 - \Omega^2)^2$$

and use the cell representatives subroutine with Q as input. Omit the first step to obtain a set of univariate representations

$$(f(t), g_0(t), \ldots, g_k(t)) \in (D[\Omega, \delta, \delta'][t])^{k+2}.$$

Note that in the proof of correctness of the algorithm, we make use of the ordering $1/\Omega \gg \delta \gg \delta'$. It is useful to keep this ordering in mind while understanding the subroutine even though the subroutine itself makes no use of this ordering.

Apply the $\mathrm{eval}_{\delta'}$ map, by letting $\delta' \to 0$, and obtain polynomials and rational functions defined over $D[\Omega, \delta]$. Next, we replace Ω and δ by appropriately large and small elements from the field of quotients of D using Propositions 2.6.4 and 2.6.5. Then, clear denominators to obtain univariate representations belonging to in $D[t]^{k+2}$.

The proof of correctness of the above subroutine follows from Lemma 2.3.3, Propositions 2.3.1 and 2.3.5 and the correctness of the cell representatives subroutine.

For the complexity analysis, note that since we have introduced only four additional variables and all algebraic computations are done in the ordered ring $D[\Omega, \delta, \delta', \zeta]$ using only linear algebra subroutines, the asymptotic complexity is not affected by the introduction of these variables.

The total number of $\ell \le k$-tuples examined is $\sum_{\ell\le k} \binom{4s}{\ell} = O(s/k)^k$. Hence, the number of calls to the cell representatives subroutine is also bounded by $\sum_{\ell\le k} \binom{4s}{\ell} = O(s/k)^k$. Each such call costs $d^{O(k)}$ arithmetic operations in D and produces $d^{O(k)}$ univariate representations whose polynomials have degree bounded by $O(d)^k$. Thus, the total number of univariate representations pro-

duced, as well as the number of arithmetic operations performed, is bounded by $s^k d^{O(k)}$.

When using Propositions 2.6.4 and 2.6.5, this requires a further overhead of $sd^{O(k)}$ arithmetic operations, for every univariate representation output. Thus the number of arithmetic operations is bounded by $s^{k+1}d^{O(k)}$. However, the number of points actually constructed is only $s^k O(d)^k$.

In the special case when the ring of coefficients is Z and the bit size of the coefficients of the input polynomials is τ, we can substitute a rational number, with numerator and denominator of bit size $\tau d^{O(k)}$, in place of the variables Ω and δ and thus get points defined over Z. In this case, we do not pay any extra overhead to remove the infinitesimal.

3.1.4. *Sign Determination Subroutine*. The input is a Gröbner basis for a zero-dimensional ideal I and a list of s polynomials $\mathcal{P} = (P_1, \ldots, P_s)$. Denote by A the quotient $R[X_1, \ldots, R_k]/I$ and by N, its dimension. We write Z for the set of zeros of I in R^k and r for its cardinality. Note that r is no greater than the dimension of A.

We use the notations of Section 2.7. The output is the list of nonempty sign-conditions $\Sigma(\mathcal{P})$ and its list of cardinalities, $c(\mathcal{P})$.

The subroutine is best described in two parts, a combinatorial part and an algebraic part. The algebraic part is a subroutine computing Sturm queries for various polynomials $h \in H(\mathcal{P})$ whereas, the combinatorial part combines the answers to these queries.

We first give an outline of the combinatorial part, treating the algebraic subroutine as a black box.

There are $\lceil \log_2 s \rceil$ stages. In Stage 0, we consider each polynomial P_i separately and compute the Sturm queries for the polynomials 1, P_i and P_i^2 with $P_i \in \mathcal{P}$ and for $\sigma \in \{0, 1, -1\}$, the corresponding $c_\sigma(P_i)$.

The output of Stage i, consists of a partition of $\mathcal{P}$ into $m = \lceil s/2^i \rceil$ subsets $\mathcal{P}_{i,1}, \ldots, \mathcal{P}_{i,m}$ each of size 2^i (except possibly the last one), and for every (i, j), the following:

(1) the list $\Sigma(\mathcal{P}_{i,j})$,
(2) the vector $c(\mathcal{P}_{i,j})$,
(3) the list of polynomials $L(\mathcal{P}_{i,j})$ consisting of products of at most $\log r$ polynomials, or squares of polynomials of $\mathcal{P}_{i,j}$ (see Corollary 2.7.6),
(4) the vector of Sturm queries $SQ(Z, L(\mathcal{P}_{i,j}))$,
(5) the matrix $A_{i,j} = A(C(\mathcal{P}_{i,j}), L(\mathcal{P}_{i,j}))$.

In Stage $i + 1$, we define $\mathcal{P}_{i+1,j+1}$ as the list $\mathcal{P}_{i,2j+1}$ followed by the list $\mathcal{P}_{i,2j+2}$, we then compute $L(\mathcal{P}_{i,2j+1}) \cdot L(\mathcal{P}_{i,2j+2})$ and all Sturm queries for polynomials in $L(\mathcal{P}_{i,2j+1}) \cdot L(\mathcal{P}_{i,2j+2})$. We use Corollary 2.7.4 to get a vector c whose coordinates are the cardinals of $C(\mathcal{P}_{i,2j+1}) \cap C(\mathcal{P}_{i,2j+2})$. This gives us the list $\Sigma(\mathcal{P}_{i+1,j+1})$ as well as the list $c(\mathcal{P}_{i+1,j+1})$. If the ℓth component of c is zero, we prune off the ℓth column of the matrix $A_{i,2j+1} \otimes A_{i,2j+2}$ and then look for the first rows of $A_{i,2j+1} \otimes A_{i,2j+2}$ giving an invertible matrix $A_{i+1,j+1}$, which gives as well the list $L(\mathcal{P}_{i+1,j+1})$. Thus, the dimension of the matrices $A_{i+1,j+1}$ never exceeds r. The subroutine uses $O(sr^2)$ Sturm queries for products of less

than $\log r$ polynomials or squares of polynomials in $\mathcal{P}$, according to Proposition 2.7.5.

We now describe the algebraic subroutine that answers the Sturm queries. We have already seen in Proposition 2.4.7 that in order to compute the answer to a Sturm query for h it suffices to compute the signature of the quadratic form Q_h.

Since we are given a Gröbner basis, we easily construct (taking monomials under the staircase) a basis for the vector space A and a multiplication table for the R-algebra A with respect to this basis. Using this multiplication table, the signature of the quadratic form Q_h associated to h, is computed by first computing the characteristic polynomial of the associated $N \times N$ symmetric matrix and then using Descartes' rule of signs to find the number of positive and negative roots (counted with multiplicities) of this characteristic polynomial whose roots are all real.

Since the computation of each signature involves computing the characteristic polynomial of a matrix of size $N \times N$, each signature can be computed using $N^{O(1)}$ operations in D. Thus, the sign determination subroutine has a total complexity of $sN^{O(1)}$.

We shall use this general multivariate sign determination subroutine in various contexts. In the special case when all the polynomials are univariate, we shall use three subroutines called the reality checking subroutine, the real root characterization subroutine, and the univariate sign determination subroutine.

3.1.4.1. Reality Checking Subroutine. Given a univariate representation $u(t) = (f(t), g_0(t), \ldots, g_k(t))$ of degree $d^{O(k)}$ and a polynomial $P(X_1, \ldots, X_k)$ of degree d it outputs yes, if $f(t)$ has real roots satisfying $P_u(t) = 0$, and no if no such root exists.

We compute $P_u(t)$ and use the sign determination subroutine to check whether there is a real root of $f(t)$ satisfying $P_u(t) = 0$.

The time complexity of the above subroutine is $d^{O(k)}$.

3.1.4.2. Real Root Characterization Subroutine. In this case, we are given a univariate polynomial $f(t)$ of degree bounded by d, and output a list of the Thom encodings of the real roots of $f(t)$.

We just apply the sign determination subroutine to the set

$$\{f'(t), \ldots, f^{\{\deg f\}-1}(t)\},$$

and output the list of sign conditions.

The time complexity is $d^{O(1)}$.

3.1.4.3. Univariate Sign Determination Subroutine. Here we are given a univariate representation $u(t) = (f(t), g_0(t), \ldots, g_k(t))$ of degree $d^{O(k)}$ and a list of polynomials $P_1, \ldots, P_s$ in k variables, $X_1, \ldots, X_k$, of degree bounded by d and we compute the Thom encoding of the real roots of $f(t)$ and the list of signs of $P_{i_u}(t)$ (see Notation 3.1.1.1) at these roots of $f(t)$.

We apply the sign determination subroutine to the set

$$\{f'(t), \ldots, f^{\{\deg f\}-1}(t)\} \bigcup_{1 \le i \le s} \{P_{i_u}(t)\}.$$

The complexity of this subroutine is bounded by $sd^{O(1)}$.

3.2. Finding Realizable Sign Conditions and Deciding the Existential Theory of Reals. We are now in a position to solve the decision problem for the existential theory, by computing the list of all realizable sign conditions of the input set of polynomials $\mathcal{P}$. Polynomials of $\mathcal{P}$ have coefficients in a real closed field R, and D is the subring of R generated by the coefficients of the polynomials in $\mathcal{P}$.

For the first step, we use the sample points subroutine to compute the set of univariate representations. Each univariate representation is of the form,

$$(f(t), g_0(t), \ldots, g_k(t)),$$

where $f(t), g_i(t) \in D$ and have degrees bounded by $d^{O(k)}$.

For each univariate representation $(f(t), g_0(t), \ldots, g_k(t))$ so generated we call the univariate sign determination subroutine with the following input: the univariate representation $(f(t), g_0(t), \ldots, g_k(t))$, and the set of polynomials $\mathcal{P}$. The set SIGN($\mathcal{P}$) consists of all the realizable sign conditions for the set $\mathcal{P}$ so obtained. We decide the truth or falsity of the given formula from the set SIGN($\mathcal{P}$).

The call to the sample points subroutine in the first step, requires $s^k d^{O(k)}$ arithmetic operations. For each of the $s^k d^{O(k)}$ univariate representations generated in the first step, the call to the univariate sign determination subroutine takes $sd^{O(k)}$ arithmetic operations. Note that in this step the computations for the univariate sign determination subroutine are performed in the ordered ring $D[\Omega, \delta]$, rather than in D. However, since the degrees of Ω and δ do not exceed $d^{O(k)}$ in any of the polynomials and because all the computations are based on linear algebra subroutines the asymptotic complexity is not affected.

The complexity of computing SIGN($\mathcal{P}$) is thus $s^{k+1}d^{O(k)}$ and the total complexity of our algorithm for deciding the existential theory is $s^{k+1}d^{O(k)}$.

4. *A Few Applications*

4.1. A Bound on the Size of a Ball Containing Points in Every Cell. As a consequence of the preceding algorithm, we can prove the following theorem, which is an improvement of results appearing in Grigor'ev and Vorobjov [1992] and Koiran [1993].

Theorem 4.1.1. *Given a set $\mathcal{P}$ of s polynomials of degree d in k variables with coefficients in $\mathbf{Z}$ of bit length at most τ, there exists a ball of radius $2^{O(\tau d^{O(k)})}$ intersecting every cell of $\mathcal{P}$.*

Proof. This follows from the computation made in the Sample Points Subroutine. The degrees of the univariate representations obtained are bounded by $O(d)^k$ while the size of the integer coefficients of these univariate representations are bounded by $\tau d^{O(k)}$ using Proposition 2.6.5. The theorem follows from the standard bounds on the absolute values of the roots of polynomials with integer coefficients. □

We can also prove the following result.

Theorem 4.1.2. *Given a set $\mathcal{P}$ of s polynomials of degree d in k variables with coefficients in $\mathbf{Z}$ of bit length at most τ such that*

$$S = \{x \in R^k | P(x) > 0,\ P \in \mathcal{P}\}$$

is a non-empty set, then in each semi-algebraically connected component of S, there exists a point whose coordinates are rational numbers a_i/b_i with a_i and b_i of bit length $\tau d^{O(k)}$.

PROOF. This too follows from the computation made in the Sample Points Subroutine. The degrees of the univariate representations obtained are bounded by $O(d)^k$ while the size of the integer coefficients of these univariate representations are bounded by $\tau O(d)^k$ using Proposition 2.6.5. We consider a point α belonging to C associated to a univariate representation $u = (f(t), g_0(t), \ldots, g_k(t))$ output by the algorithm, so that

$$\alpha_i = \frac{g_i(t_\alpha)}{g_0(t_\alpha)}$$

with t_α a root of f in R known by its Thom encoding. Using Notation 2, each $P_u(t)$ is of degree $O(d)^k$ and the size of its integer coefficients is bounded by $\tau d^{O(k)}$. Moreover for every $P \in \mathcal{P}$, $P_u(t_\alpha) > 0$. Since the minimal distance between two roots of a univariate polynomial of degree $O(d)^k$ with coefficients in $\mathbf{Z}$ of size $\tau d^{O(k)}$ is at least $2^{O(\tau d^{O(k)})}$ (see Theorem 4.6 of Mignotte [1992]), we get, considering polynomials $f(t)P_u(t)$, for $P \in \mathcal{P}$, that there exists a rational number c/d with c and d of bit length $\tau d^{O(k)}$ such that $P_u(c/d)$ is positive. Thus, defining the k-tuple a/b by $a_i/b_i = g_i/g_0(c/d)$, we get $P(a/b) > 0$ for all $P \in \mathcal{P}$ with bit size as announced. □

4.2. REAL AND COMPLEX DECISION PROBLEMS. We apply our techniques to the algorithmic problem of checking whether a variety defined by a polynomial has real dimension zero. We prove the following theorem, which improves the results in Pedersen et al. [1993].

Note that the only assumption we require in the second part of the theorem, is that the real dimension of the variety is 0 (the dimension of the complex part could be greater).

THEOREM 4.2.1. *Let $Q \in R[X_1, \ldots, X_k]$ have degree at most d, and D be the subring of R generated by its coefficients. There is an algorithm that checks if the real dimension of the variety $Z(Q)$ is 0 using $d^{O(k)}$ arithmetic operations in D.*

If the real dimension of the variety is 0, the algorithm also outputs a univariate representation of its real points using $d^{O(k)}$ arithmetic operations in D. Moreover, if $D = \mathbf{Z}$ and the bit size of the coefficients is bounded by τ, these points are contained in a ball of radius a/b with a and b in $\mathbf{Z}$ of bit size $\tau d^{O(k)}$. Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset R[X_1, \ldots, X_k]$ have degrees at most d and D be the subring of R generated by their coefficients, then the signs of all the polynomials in $\mathcal{P}$ at the points of $Z(Q)$ can be computed in $sd^{O(k)}$ arithmetic operations in D.

PROOF. In order to check whether the real variety $Z(Q)$ is zero-dimensional, we apply the cell representatives subroutine to Q. We then use the real root characterization and the sign determination subroutines, applied to the homogenization of Q, and retain from amongst the finite set of points obtained by the cell representatives subroutine, only those satisfying $Q = 0$. Call this finite set of points that intersects every semi-algebraically connected component of the real

variety $Z(Q)$, K. Now, $Z(Q)$ is zero-dimensional, if and only if every point in K has a sufficiently small sphere centered around it, which does not intersect $Z(Q)$. For every tuple, $(f(t), g_0(t), \ldots, g_k(t))$, and for every root of f that is retained above, we introduce a new polynomial,

$$P(X_1, \ldots, X_k, t) = Q(X_1, \ldots, X_k) + f^2(t) + ((g_0(t)X_1 - g_1(t))^2 + \cdots + (g_0(t)X_k - g_k(t))^2 - g_0^2(t)\epsilon)^2,$$

where ϵ is a new positive infinitesimal. We apply the cell representatives subroutine to this $(k + 1)$-variate polynomial, and again using the sign determination subroutine, retain only those points that satisfy $P(X_1, \ldots, X_k, t) = 0$. Notice that the last coordinate of the points so obtained, are also roots of $f(t)$. Moreover, if any of these roots correspond to a point on $Z(Q)$, then $Z(Q)$ is not zero-dimensional. Use the univariate sign determination subroutine to construct the Thom encodings of these roots, and check whether any of these roots correspond to a real point on the variety $Z(Q)$.

If $D = \mathbf{Z}$, the bounds claimed follow from the fact that the polynomials in the univariate representations computed have integer coefficients of bit size $\tau O(d)^k$.

For the third part, we just apply the sign determination subroutine. The first part uses only the cell representatives subroutine, and the $d^{O(k)}$ calls to sign determination subroutine. Hence, the complexity is still $d^{O(k)}$. The second part of the algorithm has complexity $sd^{O(k)}$. □

The following corollary follows immediately from the proof of Theorem 4.2.1:

COROLLARY 4.2.2. *Let $\mathcal{Q}$ be a finite set of m polynomials in $R[X_1, \ldots, X_k]$ of degree at most d, D the subring of R generated by their coefficients. Then the coordinates of the isolated points of $\mathbf{Z}(\mathcal{Q})$ are zeros of polynomials of degrees $O(d)^k$.*

Our techniques can be applied to decision problems in complex geometry, which slightly improves the results of Giusti and Heintz [1991] and Krick and Pardo [1996]. The improvement is that our algorithms have the same complexity, but are deterministic rather than probabilistic.

PROPOSITION 4.2.3. *Given a set $\mathcal{P}$ of m polynomials of degree d in k variables with coefficients in $R[i]$, we can decide in $md^{O(k)}$ arithmetical operations over D (where D is the subring of R generated by the real and imaginary parts of the coefficients of polynomials in $\mathcal{P}$) whether the set of zeros of $\mathcal{P}$ is empty in $R[i]^k$.*

PROOF. Define Q as the sums of squares of the real and imaginary parts of the polynomials in $\mathcal{P}$ and apply the cell representatives subroutine. □

PROPOSITION 4.2.4. *Given a set $\mathcal{P}$ of m polynomials of degree d in k variables with coefficients in $R[i]$, we can decide in $md^{O(k)}$ arithmetical operations over D (where D is the subring of R generated by the real and imaginary parts of the coefficients of polynomials in $\mathcal{P}$) whether the set of zeros of $\mathcal{P}$ is zero-dimensional in $R[i]^k$.*

PROOF. Define Q as the sums of squares of the real and imaginary parts of the polynomials in $\mathcal{P}$ and apply Theorem 4.2.1. □

PROPOSITION 4.2.5. *Given an algebraic variety V defined as the zero set of m polynomials of degree d in k variables with coefficients in $R[i]$, then the real and imaginary parts of the coordinates of the isolated points of V are zeros of polynomials with coefficients in D (where D is the subring of R generated by the real and imaginary parts of the coefficients of polynomials in $\mathcal{P}$) of degrees bounded by $O(d)^k$. Moreover, if $D = Z$, and the bit size of the coefficients of the polynomials is bounded by τ, then these points are contained in a ball of radius a/b with a and b in Z of bit size $(\tau + log(m))d^{O(k)}$ in $R^{2k} = R[i]^k$.*

PROOF. As in Theorem 4.1.2. □

5. *The General Decision Problem*

5.1. ALGORITHMIC PRELIMINARIES. For the general decision problem, we need parametrized versions of the cell representatives subroutine and the sample points subroutine described earlier. In both these subroutines, the coefficients of the input polynomials will come from a polynomial ring $D[Y] = D[Y_1, \ldots, Y_\ell]$, where the variables $Y = (Y_1, \ldots, Y_\ell)$ are referred to as parameters. Since, the parametrized versions of both subroutines are very similar to the original ones described previously, we will avoid duplication by referring the reader to them whenever possible.

First, we outline a parametrized version of the algorithm that was implicit in Proposition 2.6.4. This allows us to remove extra variables in the parametrized cell representatives subroutine.

5.1.1. *Parametrized Removal of Infinitely Large Variables*. The input to the subroutine is a set $\mathcal{L}$ of polynomials

$$f(Y, \Omega, t), g_1(Y, \Omega, t), \ldots, g_m(Y, \Omega, t) \in D[Y, \Omega, t],$$

with maximum degree d. The output is a set of $md^{O(1)}$ pairs of polynomials

$$(a_i(Y), b_i(Y)), \qquad 1 \leq i \leq md^{O(1)}$$

such that, for any fixed $y \in R^\ell$, and all $v \in R$ satisfying

$$v \geq \max_{1 \leq i \leq md^{O(1)},\, b_i(y) \neq 0} \frac{a_i(y)}{b_i(y)},$$

the following remains invariant:

(1) the number of roots of $f(y, v, t)$, and their Thom encoding,
(2) the signs of the polynomials $g_1, \ldots, g_m$ at these roots.

The algorithm is as follows: Follow the same technique and notation that was used in the proof of Proposition 2.6.4, treating the polynomials of $\mathcal{L}$ as polynomials with coefficients in $D[\Omega, Y]$. For each polynomial $Q_i \in \mathcal{PL}$, we output

$$C(Q_i) = \frac{a_i(Y)}{b_i(Y)}.$$

The correctness of this subroutine follows from Proposition 2.6.4 since the maximum of the

$$\frac{a_i(y)}{b_i(y)}$$

is greater than the absolute value of any root of a polynomial in $\mathcal{PL}$ with Y specialized to y.

This subroutine uses $md^{O(1)}$ arithmetic operations in D.

Using the same technique, we can also remove infinitesimally small elements.

5.1.2. Parametrized Cell Representatives Subroutine. The input is a polynomial $Q \in D[Y_1, \ldots, Y_\ell][X_1, \ldots, X_k]$, where D is an ordered domain, contained in a real closed field R. The degree of Q is bounded by d.

The output is a set of tuples of polynomials

$$(f(Y, t), g_0(Y, t), \ldots, g_k(Y, t)).$$

We call each such tuple a *parametrized univariate representation*. The set of tuples has the property that for every $y \in R^\ell$, the union of the sets of points associated to the tuples $(f(y, t), g_0(y, t), \ldots, g_k(y, t))$ (provided that $g_0(y, t) \not\equiv 0$), intersects every semi-algebraically connected component of the algebraic set defined by $Q(y, X) = 0$.

We follow the same steps as in the cell representatives subroutine, and compute parametrized univariate representations that consists of tuples of polynomials in $D[Y, \Omega, \zeta, 1/\zeta][t]$, by calling the univariate representation subroutine. Note, that the univariate representation subroutine is completely uniform, and hence works equally well in the parametrized case.

For each parametrized univariate representation,

$$(f(Y, \Omega, t), g_0(Y, \Omega, t), \ldots, g_k(Y, \Omega, t)),$$

so obtained express each polynomial in powers of ζ. Thus,

$$f(Y, \Omega, t) = \sum_j f^{[j]}(Y, \Omega, t)\zeta^j,$$

and

$$g_i(Y, \Omega, t) = \sum_j g_i^{[j]}(Y, \Omega, t)\zeta^j, \qquad 0 \le i \le k,$$

Consider the set of all nonzero tuples of the form

$$(f^{[j]}(Y, \Omega, t), g_0^{[j]}(Y, \Omega, t), \ldots, g_k^{[j]}(Y, \Omega, t))$$

for all j occurring as powers of ζ in the expressions for f and the g_i's. The polynomials in the tuples generated above belong to $D[\Omega, Y]$. Remove the infinitely large element Ω from each of the univariate representations obtained above. This is done by replacing the univariate representation by a set of representations which we get by substituting certain rational fractions, $a(Y)/b(Y)$ for Ω. The polynomial fractions are computed using the parametrized version of

the subroutine for removing infinitely large elements, which was described in Section 5.1.1.

PROOF OF CORRECTNESS. We prove that for any fixed $y \in R^{\ell}$, the set of points associated to the set of tuples produced by the above subroutine intersects every semi-algebraically connected component of the algebraic set $Q(y, X) = 0$.

However, since all steps other than the last step of the unparameterized version of the subroutine are uniform, we need only check the last step. The rest of the proof is identical to the proof of correctness of the unparameterized version. For the last step, notice that for a given parametrized representation,

$$(f(Y, \Omega, t), g_0(Y, \Omega, t), \ldots, g_k(Y, \Omega, t)),$$

and any specialization $Y = y$, the valuation of f with respect to the infinitesimal ζ depends on y. However, by retaining all possible coefficients of the powers of ζ, we guarantee that we will always obtain a correct tuple, regardless of the valuation of f. □

The number of parametrized univariate representations generated is still $d^{O(k)}$ and the degrees are still bounded by $O(d)^k$. However, since we are doing arithmetic in a polynomial ring with $\ell + 2$ variables, the total number of arithmetic operations in the ring D is $d^{O(k\ell+k)}$.

Removal of the variable Ω causes replacement of each univariate representation by a set of $d^{O(k)}$ univariate representations. However, this does not affect the asymptotic complexity.

We now use this subroutine to give a parametrized version of the sample points subroutine.

5.1.3. *Parametrized Sample Points Subroutine*. The input is a set of s polynomials

$$\mathcal{P} = \{P_1, \ldots, P_s\} \subset R[Y_1, \ldots, Y_{\ell}][X_1, \ldots, X_k],$$

each of degree at most d, and D is the subring of the real closed field R generated by the coefficients of $\mathcal{P}$.

The output is a set of $s^k d^{O(k)}$ parametrized univariate representations of the form,

$$(f(Y, \Omega, \delta, t), g_0(Y, \Omega, \delta, t), \ldots, g_k(Y, \Omega, \delta, t)),$$

where $f(Y, \Omega, \delta, t), g_i(Y, \Omega, \delta, t) \in D[\Omega, \delta, Y]$. The set of tuples has the property that for any point $y \in R^{\ell}$, the union of the sets of points associated to the univariate representations $(f(y, t), g_0(y, t), \ldots, g_k(y, t))$ (provided that $g_0(y, t) \not\equiv 0$), intersects every cell of the set $\mathcal{P}(y)$ in $R\langle 1/\Omega, \delta\rangle^k$.

The subroutine for doing this is a modification of the sample points subroutine. We take advantage of the fact that apart from the last step, all other steps of the sample points subroutine are uniform. The reader should refer to the description of the sample points subroutine while reading the description below.

The first three steps are identical, except that we call the parametrized cell representatives subroutine rather than the cell representatives subroutine. The output of the parametrized cell representatives subroutine is a set of parametrized univariate representations, with coefficients $D[Y, \Omega, \delta, \delta']$.

Next, we replace each parametrized univariate representation, $(f, g_0, \ldots, g_k)$ obtained above, by a set of parametrized univariate representations, in such a way that for any fixed specialization of the parameters Y the set of points associated with the latter includes the set of points obtained by applying the $\mathrm{eval}_{\delta'}$ map to the set of points associated with $(f, g_0, \ldots, g_k)$.

However, since the univariate representations now depend on Y we need to be careful. For each univariate representation, $(f(Y, t), g_0(Y, t), \ldots, g_k(Y, t))$, we write $f(Y, t)$ and the $g_i(Y, t)$ in ascending powers of δ'. Thus,

$$f(Y, t) = \sum_{\alpha} f^{(\alpha)}(Y, \Omega, \delta, t)\delta'^{\alpha}.$$

and

$$g_i(Y, t) = \sum_{\alpha} g_i^{(\alpha)}(Y, \Omega, \delta, t)\delta'^{\alpha}.$$

We replace the tuple,

$$(f(Y, t), g_0(Y, t), \ldots, g_k(Y, t)),$$

by the set of all possible tuples of the form,

$$(f^{(\alpha)}(Y, \Omega, \delta, t), g_0^{(\alpha)}(Y, \Omega, \delta, t), \ldots, g_k^{(\alpha)}(Y, \Omega, \delta, t)).$$

Note that the cardinality of this set is $d^{O(k)}$, its elements belong to $D[\Omega, \delta][t]$ and their degrees in all variables are also bounded by $d^{O(k)}$. Note too, that in contrast to the sample point subroutine, we do not remove δ and Ω.

The correctness of the subroutine follows from the correctness of the parametrized cell representatives subroutine.

As each of the $O(s)^k$ calls to the parametrized cell representatives subroutine costs $d^{O(\ell k+k)}$ arithmetic operations in D, the total complexity is $s^k d^{O(\ell k+k)}$.

5.2. Block Elimination Subroutine. In the *Elimination Phase* of our algorithm for the general decision problem, we successively eliminate one block of variables at a time, using the following subroutine, which we call the *Block Elimination Subroutine.*

The input to this subroutine is a set of s polynomials

$$\mathcal{P} = \{P_1, \ldots, P_s\} \subset R[Y_1, \ldots, Y_\ell][X_1, \ldots, X_k],$$

each of degree at most d, for some real closed field R. Denote by D the subring of R generated by the coefficients of the polynomials in $\mathcal{P}$. Let $Y = (Y_1, \ldots, Y_\ell)$ and $X = (X_1, \ldots, X_k)$. The algorithm eliminates the block X.

The output consists of two sets, $\mathcal{U}$ and $\mathcal{Q}$. The set $\mathcal{U} \subset D[Y, \Omega, \delta, t]^{k+2}$ consists of parametrized univariate representations

$$u(Y, \Omega, \delta, t) = (f(Y, \Omega, \delta, t), g_0(Y, \Omega, \delta, t), \ldots, g_k(Y, \Omega, \delta, t)).$$

The set $\mathcal{Q} \subset D[Y]$, has the property that for any cell C, of $\mathcal{Q}$,

$$\mathrm{SIGN}(\mathcal{P}(y, X_1, \ldots, X_k))$$

is fixed as y varies over C, and the union of the sets of points associated with all tuples $(f(y, \Omega, \delta, t), g_0(y, \Omega, \delta, t), \ldots, g_k(y, \Omega, \delta, t))$ in $\mathcal{U}$ for which $g_0(y, \Omega, \delta, t) \not\equiv 0$, intersects every cell of the set $\mathcal{P}(y)$, in $(R\langle\Omega, \delta\rangle)^k$.

We apply the parametrized sample points subroutine to the set of polynomials, $\{P_1, \ldots, P_s\}$, to obtain the set $\mathcal{U}$ of parametrized univariate representations.

For every $u(Y, \Omega, \delta, t) = (f(Y, \Omega, \delta, t), g_0(Y, \Omega, \delta, t), \ldots, g_k(Y, \Omega, \delta, t))$ in $\mathcal{U}$ and for $0 \leq j \leq \deg(f)$, compute the subresultant coefficients of the pairs of polynomials (as polynomials in t) $(T_j(f)(Y, \Omega, \delta, t), T_{j-1}(f')(Y, \Omega, \delta, t))$ treating $T_j(f)$ as a polynomial in t. Also, for each polynomial P in $\mathcal{P}$ and for $0 \leq j \leq \deg(f)$, compute the subresultant coefficients of the polynomial pairs $(T_j(f)(Y, \Omega, \delta, t), P_u(Y, \Omega, \delta, t))$ treating $T_j(f)(Y, \Omega, \delta, t)$ and $P_u(Y, \Omega, \delta, t)$ as polynomials in t. Note that these subresultant coefficients belong to $D[Y, \Omega, \delta]$. Collect together all the subresultant coefficients computed above, as well as the polynomials $f_i(Y, \Omega, \delta)$. Express these polynomials in powers of Ω and δ and denote by $\mathcal{Q}$ the set of coefficients of these polynomials in Ω and δ. Note that $\mathcal{Q} \subset D[Y]$.

We claim that the cells of $\mathcal{Q}(Y)$ have the stated properties. Consider a cell C of $\mathcal{Q}$. Then, for all $P_i \in \mathcal{P}$, $y \in C$,

$$u(Y, \Omega, \delta, t) = (f(Y, \Omega, \delta, t), g_0(Y, \Omega, \delta, t), \cdots, g_k(Y, \Omega, \delta, t)) \in \mathcal{U},$$

the number of common roots in $R\langle 1/\Omega, \delta\rangle$ (in fact, in $R[i]\langle 1/\Omega, \delta\rangle$) of $f(y, \Omega, \delta, t)$ and $P_{i_u}(y, \Omega, \delta, t)$ as well as the number of real roots of $f(y, \Omega, \delta, t)$ remains invariant as y varies over C. These are consequences of the properties of subresultant coefficients (see Section 2.4), and the fact that the signs of the corresponding subresultant coefficients (which are polynomials in $D[\Omega, \delta]$) remain invariant over C.

The complexity of computing the univariate representations is $s^k d^{O(k\ell+k)}$. The degrees of the polynomials generated in this process are bounded by $d^{O(k)}$ (independent of ℓ), in each of the variables as well as in the variables Ω and δ.

The size of the set $\mathcal{Q}$ is $s^{k+1}d^{O(k)}$ which follows from the fact that the number of subresultant coefficients of a pair of polynomials is bounded by their degrees.

5.3. Algorithm for the General Decision Problem. We are now in a position to give the algorithm for the general decision problem. As noted before, the algorithm has two phases. The first phase, is an elimination phase, in which we eliminate blocks of variables at a time, using inductively the block elimination subroutine. The second phase is the sign determination phase in which we construct the set $\mathrm{SIGN}_\Pi(\mathcal{P})$, using the sign determination subroutine.

5.3.1. Computation of $\mathrm{SIGN}_\Pi(\mathcal{P})$. The input is a set of s polynomials, $\mathcal{P} = \{P_1, \ldots, P_s\} \subset D[X_1, \ldots, X_k]$, and a partition, Π, of the variables into ω blocks, $X^{[1]}, \ldots, X^{[\omega]}$. The output is $\mathrm{SIGN}_\Pi(\mathcal{P})$.

We denote by $\bar{X}^{[i]}$ the variables $(X^{[\omega]}, \ldots, X^{[i]})$. The algorithm consists of three phases: the Elimination Phase, the Substitution Phase and the Sign Determination Phase.

There are ω stages in the Elimination Phase, one for each block of variables. In each stage of the Elimination Phase we output two sets $\mathcal{U}_i$, and $\mathcal{Q}_i$. The set $\mathcal{U}_i \subset (D[\bar{X}^{[i]}, \Omega, \delta_i, t_i])^{k+2}$ consists of parametrized univariate representations generated by calls to the block elimination subroutine. The set $\mathcal{Q}_i$ consists of polynomials in the variables $\bar{X}^{[i+1]}$, with the property that the set

$\mathrm{SIGN}_{\Pi,i}(x^{[\omega]}, \ldots, x^{[i+1]})$ stays invariant, as $(x^{[\omega]}, \ldots, x^{[i+1]})$ varies over a cell of $\mathcal{Q}_i$. In the Substitution Phase for each $\bar{u} = (u_1, \ldots, u_\omega) \in \bar{\mathcal{U}} = \Pi_{1 \le i \le \omega} \mathcal{U}_i$ we define the *associated triangular system* and the *associated list of polynomials*, $\mathcal{T}_{\bar{u}}$ and $\mathcal{P}_{\bar{u}}$, as follows:

Let

$$u_i = (f^{[i]}(\bar{X}^{[i+1]}, \Omega_i, \delta_i, t_i), g_0^{[i]}(\bar{X}^{[i+1]}, \Omega_i, \delta_i, t_i), \ldots, g_{k_{i+1}}^{[i]}(\bar{X}^{[i+1]}, \Omega_i, \delta_i, t_i)).$$

For a polynomial $P(X^{[\omega]}, \ldots, X^{[1]})$, let $P_{\bar{u}}(t_1, \ldots, t_\omega)$ denote the polynomial obtained by successively replacing the blocks of variables $X^{[i]}$, with the rational fractions associated with the tuple u_i.

Define $T_{\bar{u}}^{[i]}(t_\omega, \ldots, t_i) = f_{\bar{u}}^{[i]}$,

$$\mathcal{T}_{\bar{u}} = (T_{\bar{u}}^{[\omega]}(t_\omega), T_{\bar{u}}^{[\omega-1]}(t_\omega, t_{\omega-1}), \ \ldots \ , T_{\bar{u}}^{[1]}(t_\omega, t_{\omega-1}, \ldots, t_1)),$$

and $\mathcal{P}_{\bar{u}}$ as $\{P_{\bar{u}} | P \in \mathcal{P}\}$.

Let $\mathcal{Z}_{\bar{u}}$ be the set

$$\{\alpha \in R\langle 1/\Omega_1, \delta_1, \ldots, 1/\Omega_\omega, \delta_\omega\rangle^\omega | \alpha \text{ a zero of } \mathcal{T}_{\bar{u}}\}.$$

We define $\mathcal{Z}$ and $\bar{\mathcal{P}}$ by $\mathcal{Z} = \cup_{\bar{u} \in \bar{\mathcal{U}}} \mathcal{Z}_{\bar{u}}$ and $\bar{\mathcal{P}} = \cup_{\bar{u} \in \bar{\mathcal{U}}} \mathcal{P}_{\bar{u}}$. For any $x = (x_\omega, \ldots, x_1) \in R^\omega$ let $\bar{x}_i$ denote $(x_\omega, \ldots, x_i)$. For $\alpha \in \mathcal{Z}_{\bar{u}}$, we denote the sign conditions of $\mathcal{P}_{\bar{u}}$, at α, by $\mathrm{SIGN}_0(\bar{\mathcal{P}}, \alpha)$ and,

$$\mathrm{SIGN}_{i+1}(\bar{\mathcal{P}}, \bar{\alpha}_{i+1}) = \{\mathrm{SIGN}_i(\bar{\mathcal{P}}, (\bar{\alpha}_{i+1}, a)) | \quad \beta \in \mathcal{Z}, \bar{\beta}_i = (\bar{\alpha}_{i+1}, a)\}.$$

Then for $0 \le i \le \omega$, $\mathcal{Z}$ has the following property

$$\{SIGN_i(\bar{\mathcal{P}}, \bar{\alpha}_i) | \alpha \in \mathcal{Z}\} = \{SIGN_{\Pi,i}(\mathcal{P})(x) | x \in R^{k_\omega + \cdots + k_{i+1}}\}. \tag{1}$$

Thus, in order to inductively construct the set $\mathrm{SIGN}_\Pi(\mathcal{P})$ it suffices to compute the signs of $\mathcal{P}_{\bar{u}}$ at the zeros of $\mathcal{T}_{\bar{u}}$ and this is what we do in the Sign Determination Phase.

The algorithm is as follows:

—*Elimination Phase.* We first apply the block elimination subroutine to $\mathcal{P}$ and the first block of variables $X^{[1]}$. Let $\mathcal{U}_1$, and $\mathcal{Q}_1$ be the output of the block elimination subroutine.

Repeat the following for $i = 2$ to ω. In substep $1.i$ apply the block elimination subroutine to $\mathcal{Q}_{i-1}$ and the ith block of variables $X^{[i]}$ to obtain $\mathcal{U}_i$, and $\mathcal{Q}_i$ as output.

—*Substitution Phase.* Compute the set of pairs $\{(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}}) | \bar{u} \in \bar{\mathcal{U}}\}$. Note, that the polynomials in $\mathcal{T}_{\bar{u}}$ and $\mathcal{P}_{\bar{u}}$ have coefficients in $D[\Omega_1, \delta_1, \ldots, \Omega_\omega, \delta_\omega]$.

—*Sign Determination Phase.* Using the sign determination subroutine we evaluate the sign condition of the set of polynomials $\mathcal{P}_{\bar{u}}$ at $\mathcal{Z}_{\bar{u}}$. Next, using the property (1) of the set $\mathcal{Z}$ we inductively construct the set $SIGN_\Pi(\mathcal{P})$.

5.3.2. *Proof of Correctness*. We first prove the correctness of the Elimination Phase. Thus, we need to prove that the set $\mathcal{Z}$ has the property (1). This follows from the following two lemmas.

LEMMA 5.3.2.1. *For $1 \leq i \leq \omega$, the set $SIGN_{\Pi,i}(\mathcal{P})(x)$ stays invariant as x varies over a cell of $\mathcal{Q}_i$.*

PROOF. The proof is by induction on i. The base case is $i = 1$. In this case, $\mathcal{Q}_1$ is the set of polynomials obtained by applying the block elimination subroutine to the polynomials $\mathcal{P}$ with the variables $\bar{X}_1$ as parameters. From the correctness of the block elimination subroutine, it follows that the set $SIGN_{\Pi,1}(x)$ stays invariant as x varies over a cell of $\mathcal{Q}_1$.

Now, assume that the property is true for $\mathcal{Q}_{i-1}$. The set $\mathcal{Q}_i$ is obtained by applying the block elimination subroutine to the set $\mathcal{Q}_{i-1}$, with $\bar{X}_{i-1}$ as parameters. Hence, as x varies over a cell of $\mathcal{Q}_i$, the set of cells of $\mathcal{Q}_{i-1}$ intersected by the k_i dimensional fibre over x stays invariant. However, by the induction hypothesis we know that the set $SIGN_{\Pi,i-1}(y)$ stays invariant, as y varies over a cell of $\mathcal{Q}_{i-1}$.

This shows that the set

$$SIGN_{\Pi,i}(\mathcal{P})(x) = \{SIGN_{\Pi,i-1}(\mathcal{P})(x, w) | w \in R^{k_i}\},$$

stays invariant as x varies over a cell of $\mathcal{Q}_i$, which completes the induction. □

For a triangular system $\mathcal{T}_{\bar{u}}$ with $\bar{u} \in \mathcal{U}$, and one of its real zeros α, let $x_{\bar{u},\alpha}$ be the point obtained by substituting α in the rational functions associated to $\bar{u}$. Let $\mathcal{Y}$ be the set of such points obtained by considering all such triangular systems $\mathcal{T}_{\bar{u}}$ and all their real zeros.

LEMMA 5.3.2.2. *With $\bar{x}_i = (x^{[\omega]}, \ldots, x^{[i]})$, the set $\mathcal{Y}_i = \{\bar{x}_i | x = (x^{[\omega]}, \ldots, x^{[1]}) \in \mathcal{Y}\}$ intersects every cell of $\mathcal{Q}_i$, where $\bar{x}_i = (x^{[i+1]}, \ldots, x^{[\omega]})$.*

PROOF. The proof is again by induction on i. The base case is $i = \omega$. The set of points $\mathcal{Y}_\omega$ is obtained by applying the sample points subroutine to the set of polynomials $\mathcal{Q}_\omega$, and it follows from the correctness of this subroutine that $\mathcal{Y}_\omega$ intersects every cell of $\mathcal{Q}_\omega$.

Now assume that the set $\mathcal{Y}_{i+1}$ satisfies the hypothesis. Fix $x \in \mathcal{Y}_{i+1}$. The set of points $\{(x, y) | (x, y) \in \mathcal{Y}_i\}$ intersects every cell of $\mathcal{Q}_i$ intersected by the fibre over x. This follows from the correctness of the parametrized sample points subroutine, as the set of points $\{(x, y) | (x, y) \in \mathcal{Y}_i\}$ is obtained by applying the parametrized sample points subroutine to the set $\mathcal{Q}_i$, and then specializing the parameters to x. This, together with the induction hypothesis, and the fact that as a point varies over a cell of $\mathcal{Q}_{i+1}$, the set of cells of $\mathcal{Q}_i$ intersected by the k_{i+1} dimensional fibre over the point stays invariant (see the proof of the previous lemma), implies that the set $\mathcal{Y}_i$ intersects every cell of $\mathcal{Q}_i$. □

It follows from the previous two lemmas that the set $\mathcal{Z}$ has the stated property (1).

The correctness of the algorithm now follows from the correctness of the sign determination subroutine.

5.3.3. *Complexity Analysis*. The number and degrees of univariate representations produced in Step (1.1) is bounded by $s^{k_1} d^{O(k_1)}$. The number of arithmetic operations in this step is bounded by $s^{k_1} d^{O(k-k_1)k_1}$, using the bound on the complexity of the parametrized sample points subroutine.

The number of polynomials produced by the subresultant coefficient sequence computation for two polynomial is bounded by their degrees. Thus, the size of the set $\mathcal{Q}_1$, is $s^{k_1+1}d^{O(k_1)}$. An easy inductive argument shows that the number of univariate representations produced in Step (1.i) is bounded by $s^{(k_1+1)\cdots(k_{i-1}+1)k_i}d^{O(k_1)\cdots O(k_i)}$. By a similar argument, one can show that the degrees of the univariate representations in $\mathcal{U}_i$ are bounded by $d^{O(k_1)\cdots O(k_i)}$. The number of arithmetic operations is bounded by

$$s^{(k_1+1)\cdots(k_{i-1}+1)k_i}d^{O(k_1)\cdots O(k_{i-1})O(k_i)(k_i+\cdots+k_\omega+2i+2)},$$

since the arithmetic is done in a polynomial ring with $k_{i+1} + \cdots + k_\omega + 2i + 2$ variables.

A similar inductive argument shows that the size of the set $\mathcal{Q}_i$ is bounded by $s^{(k_1+1)\cdots(k_i+1)}d^{O(k_1)\cdots O(k_i)}$, and their degrees are bounded by $d^{O(k_1)\cdots O(k_i)}$.

The above analysis shows that the size of the set of pairs $(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}})$, constructed at the end of the Substitution Phase is $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$, and the degrees are bounded by $d^{\Pi O(k_i)}$. It should also be clear that the number of arithmetic operations in D for the Substitution Phase is also bounded by $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$.

Since the number of triangular systems $\mathcal{T}$ is $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$, and each call to the multi-variate sign determination subroutine takes time $d^{\Pi O(k_i)}$, the time taken for the Sign Determination Phase, is $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$.

Since each of the sign conditions generated in Step (1) of the sign determination phase is included in at most ω nested sets, the time required to construct $\mathrm{SIGN}_\Pi(\mathcal{P})$ is again bounded by $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$.

Thus the total time bound for the elimination and sign determination phase is $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$ as claimed.

Using the set $\mathrm{SIGN}_\Pi(\mathcal{P})$, it is now easy to solve the general decision problem without using any additional arithmetic operations.

5.3.4. *The General Decision Algorithm*. The input is a formula

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

where, $Q_i \in \{\ \ ,\ \ \}$, $Q_i \neq Q_{i+1}$, $X^{[i]}$ is a block of k_i variables, $\sum_{1\le i\le\omega} k_i = k$, and $F(P_1, \ldots P_s)$ is a quantifier-free Boolean formula with atoms of the form $P_i(X^{[\omega]}, \ldots, X^{[1]})\sigma\ 0$, where $\sigma \in \{0, 1, -1\}$ and the output is 0 or 1 depending on whether the input sentence is true or false.

The algorithm simply computes $\mathrm{SIGN}_\Pi(\mathcal{P})$ and then checks whether or not the formula is satisfied. Thus, the total time bound for the general decision algorithm is $s^{\Pi(k_i+1)}d^{\Pi O(k_i)}$ as claimed.

Note that the algorithm given above, proves Theorems 1.3.2 and 1.3.4.

6. *Quantifier Elimination*

6.1. Inverse Sign Determination Subroutine. In the quantifier elimination algorithm, we use the sign determination subroutine in an inverse way, to solve the following problem.

Given a triangular system of polynomials,

$$T = \{T^{[\omega]}(Y, t_\omega), T^{[\omega-1]}(Y, t_\omega, t_{\omega-1}), \ \ldots, T^{[1]}(Y, t_\omega, t_{\omega-1}, \ldots, t_1)),$$

a set of polynomials $\mathcal{P} \subset R[Y, t_1, \ldots, t_\omega]$ and a point $y \in R^\ell$, we denote by $\Sigma(T, \mathcal{P}, y)$ the list of sign conditions satisfied by $\mathcal{P}(y)$ at the zeros of $T(y)$. Note that (T), the ideal generated by T, is zero-dimensional and, by Lemma 2.3.8, the polynomials T are a Gröbner basis for this ideal. We want to compute a quantifier free formula $A(Y)$ such that for any $z \in R^\ell$, $A(z)$ is true if and only if $\Sigma(T, \mathcal{P}, y) = \Sigma(T, \mathcal{P}, z)$.

We use the sign determination subroutine to compute $\Sigma(T, \mathcal{P}, y)$. The combinatorial part of the subroutine generates a list of polynomials $\mathcal{L}$ whose elements are subject to Sturm queries which are answered by computing the signature of the associated quadratic form. Recall that this is done by computing the characteristic polynomial of the associated symmetric matrix and then evaluating the signs of its coefficients in order to use Descartes law of signs. It is only this last step at which we use the particular specialization of Y to y.

We keep the set of coefficients of these characteristic polynomials which consists of polynomials in Y. We then compute the set of all consistent sign conditions of this set of polynomials using the sample points subroutine followed by calls to the sign determination subroutine. We now output those sign conditions that give rise to the same signature value as that of $Q_h(y)$, as a Boolean formula.

Assuming that the degrees of all the input polynomials were bounded by d, and using the bound on the multivariate sign determination subroutine, it is easy to see that the number of arithmetic operations is bounded by $sd^{O(\ell\omega)}$. The same bound applies to the size of the formula $A(Y)$ produced by the subroutine.

6.2. Algorithm for Quantifier Elimination. We now describe our algorithm for the quantifier elimination problem. We make crucial use of our algorithm for the general decision procedure described above, as well as the inverse sign determination subroutine. The main ideas behind the algorithm are the same as those of Renegar [1992]. However, we achieve a better time complexity, by using the new and better algorithm for finding sample points in every cell of a set of polynomials.

We proceed in the same manner as the algorithm for the general decision problem, starting with the set $\mathcal{P}$ of polynomials appearing in Φ and eliminating blocks of quantified variables, to obtain a set of polynomials, $\mathcal{Q}_\omega$ in the variables Y. We continue with the general decision algorithm considering Y as the $(\omega + 1)$-st block of variables to obtain the set $\mathrm{SIGN}_\Pi(\mathcal{P})$. For a fixed $y \in R^\ell$, the formula $\Phi(y)$ can be decided from the set $\mathrm{SIGN}_{\Pi,\omega}(\mathcal{P})(y)$.

We next apply the Sample Points Subroutine to the set of polynomials $\mathcal{Q}_\omega$, to obtain points in every cell of $\mathcal{Q}_\omega$. For each sample point y so obtained, we determine whether or not y satisfies the given formula using the set $SIGN_{\Pi,\omega}(\mathcal{P})(y)$. If it does, then we use the inverse sign determination subroutine with the various $(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}})$, y, $\Sigma(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}}, y)$ as inputs to construct a formula $\Psi_y(Y)$. The only problem left is that this formula contains the infinitesimals introduced by the general decision procedure. However, we can replace each equality, or inequality in $\Psi_y(Y)$, by an equivalent larger formula without the infinitesimals by using the ordering amongst the infinitesimals. We output the disjunction of the formulae $\Psi_y(Y)$ constructed above.

We now give a formal description of the algorithm, and prove the bounds on the time complexity, and the size of the output formula.

The input is a first order formula

$$\Phi(Y) = Q_\omega(X^{[\omega]})Q_{\omega-1}(X^{[\omega-1]})\cdots Q_1(X^{[1]})F(P_1, \ldots, P_s),$$

which we read and output the list of polynomials $\mathcal{P}$. The output is a quantifier free formula $\Psi(Y)$ equivalent to $\Phi(Y)$. The algorithm follows:

—*Elimination Phase.* Perform the elimination phase of the general decision algorithm on the set of polynomials $\mathcal{P}$, treating Y as an extra block of variables, to obtain the set consisting of triangular systems $\mathcal{T}_{\bar{u}}$ and sets of polynomials $\mathcal{P}_{\bar{u}}$.

—Formula building phase: For every $\bar{u} \in \bar{\mathcal{U}}$ (following the notation in the General Decision Algorithm) and every point y associated to $u_{\omega+1}$, construct $\Sigma(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}}, y)$, using the sign determination subroutine. Then, as in the algorithm for the General Decision Problem, we construct the set $SIGN_\Pi(\mathcal{P})(y)$ from the set, $\{\Sigma(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}}, y) | \bar{u} \in \bar{\mathcal{U}}\}$, and hence decide whether the formula $\Phi(y)$ is true. If it is true, we apply the inverse sign determination subroutine, with $(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}})$, y, $\Sigma(\mathcal{T}_{\bar{u}}, \mathcal{P}_{\bar{u}}, y)$ as inputs to get the formulae $\Psi_{\bar{u},y}(Y)$. Let $\Psi(Y) = \Psi_y(Y) = \wedge_{\bar{u}}\Psi_{\bar{u},y}(Y)$, and let $\Psi(Y) = \vee_y\Psi_y(Y)$, where the disjunction is over all the y for which $\Phi(y)$ is true in the previous step.

Each atom of the formula $\Psi(Y)$ is of the form,

$$\text{sign}(g(Y)) = \sigma,\ \sigma \in \{0, 1, -1\},$$

where $g \in D[\Omega_1, \delta_1, \ldots, \Omega_{\omega+1}, \delta_{\omega+1}][Y]$, and

$$1/\Omega_1 \gg \delta_1 \gg \cdots \gg 1/\Omega_{\omega+1} \gg \delta_{\omega+1},$$

are infinitesimals introduced by the general decision algorithm. Express $g(Y)$ as a polynomial in $D[Y]$, and arrange the monomials in descending order. Then each inequality or equality of the form, $\text{sign}(g(Y)) = \sigma$, can be replaced by a new formula, involving only Y and of size no more than N^2 where N is the number of terms in the expansion of g in terms of the monomials. We do this for every atom occurring in the formula $\Psi(Y)$.

We output this enlarged formula.

The correctness of the algorithm follows from the correctness of the algorithm for the general decision problem, and the inverse sign determination subroutine.

The elimination phase takes at most $s^{(\ell+1)\Pi(k_i+1)}d^{(\ell+1)\Pi O(k_i)}$ arithmetic operations, and the number of sign conditions produced is also bounded by

$$s^{(\ell+1)\Pi(k_i+1)}d^{(\ell+1)\Pi O(k_i)}.$$

The degrees in the variables $t_1, \ldots, t_\omega, t_{\omega+1}, \Omega_1, \delta_1, \ldots, \Omega_{\omega+1}, \delta_{\omega+1}$ in the polynomials produced, are all bounded by $d^{(\ell+1)\Pi O(k_i)}$.

Invoking the bound on the inverse sign determination subroutine, and the bound on the number of tuples produced in the elimination phase, we see that the formula building phase takes no more than $s^{(\ell+1)\Pi(k_i+1)}d^{(\ell+1)\Pi O(k_i)}$ operations. Since the degrees of the variables $\Omega_{\omega+1}, \delta_{\omega+1}, \ldots, \Omega_1, \delta_1$, are all bounded by $d^{(\ell+1)\Pi O(k_i)}$, each atom is expanded to a formula of size at most $d^{(\ell+1)\Pi O(k_i)}$.

The bound on the size of the formula is an easy consequence of the bound on the number of tuples produced in the elimination phase, and the bound on the formula size produced by the inverse sign determination subroutine.

This proves Theorem 1.3.1.

ACKNOWLEDGMENTS. We would like to thank the referees for their useful suggestions, and in particular to one who pointed out an error in the proof of Proposition 2.2.1, observing the need for the additional hypothesis that S is bounded.

REFERENCES

ALONSO, M. E., BECKER, E., ROY, M.-F., AND WORMANN, T. 1996. Zero's, multiplicities, and idempotents for zero dimensional systems. In *Algorithms in Algebraic Geometry and Applications*. L. Gonzalez-Vega and T. Recio, eds. Birkhauser, pp. 6–16.

ATIYAH, M. F., AND MACONALD, I. G. 1969. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, Pa.

BASU, S., POLLACK, R., AND ROY, M.-F. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*. B. Caviness and J. Johnson, eds. Springer-Verlag, New York, to appear.

BASU, S., POLLACK, R., AND ROY, M.-F. 1995. Computing a set of points meeting every cell defined by a family of polynomials on a variety. In *Algorithmic Foundations of Robotics*. K. Y. Goldberg, D. Halperin, J.-C. Latombe, R. H. Wilson, eds. A. K. Peters, Boston, Mass., pp. 537–555.

BASU, S., POLLACK, R., AND ROY, M. F. 1996. On the number of cells defined by a family of polynomials on a variety. *Mathematika 43*, 120–126.

BASU, S., POLLACK, R., AND ROY, M. F. 1994. On the combinatorial and algebraic complexity of quantifier elimination. In *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*. IEEE, New York, pp. 632–641.

BEN-OR, M., KOZEN, D., AND REIF, J. 1986. The complexity of elementary algebra and geometry. *J. Comput. Syst. Sci. 18*, 251–264.

BERKOWITZ, S. J. 1984. On computing the determinant in small parallel time using a small number of processors. *Inform. Process. Lett. 32*, 147–150.

BOCHNAK, J., COSTE, M., AND ROY, M. F. 1987. *Géométrie algébrique réelle*. Springer-Verlag, New York.

BUCHBERGER, B. 1985. Gröbner bases: An algorithmic method in polynomial ideal theory. In *Recent Trends in Multidimensional Systems Theory*. Reider, ed. Bose.

CANNY, J. 1988. Some algebraic and geometric computations in PSPACE. In *Proceedings of the 20th ACM Symposium on Theory of Computing*. (Chicago, Ill., May 2–4). ACM, New York, pp. 460–467.

CANNY, J. 1993a. Some practical tools for algebraic geometry. Tech. rep. Spring school on robot motion planning at Rodez, France. PROMOTION ESPRIT, pp. 39–52.

CANNY, J. 1991. An improved sign determination algorithm. AAECC, New Orleans.

CANNY, J. 1993b. Improved algorithms for sign determination and existential quantifier elimination. *Comput. J. 36*, 409–418.

COLLINS, G. E. 1975. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Springer Lecture Notes in Computer Science 33*, 515–532.

COSTE, M., AND ROY, M. F. 1988. Thom's lemma, the coding of real algebraic numbers and the topology of semi-algebraic sets. *J. Symb. Comput. 5*, 121–129.

GIUSTI, M., AND HEINTZ, J. 1991. La détermination des points isolés d'une variété algébrique peut se faire en temps polynomial. In *Proceedings of the International Meeting on Commutative Algebra*. Cortona.

GRIGOR'EV, D. 1988. The Complexity of deciding Tarski algebra. *J. Symb. Comput. 5*, 65–108.

GRIGOR'EV, D., AND VOROBJOV, N. 1988. Solving systems of polynomial inequalities in subexponential time. *J. Symb. Comput. 5*, 37–64.

GRIGOR'EV, D., AND VOROBJOV, N. 1992. Counting connected components of a semi-algebraic set in subexponential time. *Comput. Complexity 2*, 133–186.

HEINTZ, J., ROY, M.-F., AND SOLERNÒ, P. 1990. Sur la complexité du principe de Tarski-Seidenberg. *Bull. Soc. Math. France 118*, 101–126.

HEINTZ, J., ROY, M.-F., AND SOLERNÓ, P. 1989. On the Complexity of Semi-Algebraic Sets. In *Proceedings of IFIP '89* (San Francisco, Calif.). North-Holland, Amsterdam, The Netherlands, pp. 293–298.

KOIRAN, P. 1993. A weak version of the Blum, Shub & Smale model. In *Proceedings of the 34th IEEE Symposium on Foundations of Computer Science*. IEEE, New York, pp. 486–495.

KRICK, T., AND PARDO, L. M. 1996. A computational method for diophantine approximation. In *Algorithms in Algebraic Geometry and Applications*, L. Gonzalez-Vega and T. Recio, eds. Birkhauser, pp. 193–253.

MIGNOTTE, M., 1992. Some useful bounds. In *Mathematics for Computer Algebra*. Springer-Verlag, New York.

MISHRA, B. 1994. *Algorithmic Algebra*. Springer-Verlag, New York.

POLLACK, R., AND ROY, M.-F. 1993. On the number of cells defined by a set of polynomials. *C. R. Acad. Sci. Paris 316*, 573–577.

PEDERSEN, P., ROY, M.-F., AND SZPIRGLAS, A. 1993. Counting real zeros in the multivariate case. In Computational algebraic geometry, Eyssette et Galligo, eds. *Progress in Mathematics*, vol. 109. Birkhauser, pp. 203–224.

RENEGAR, J. 1991. Recent progress on the complexity of the decision problem for the reals. In Discrete and Computational Geometry: Papers from the DIMACS Special Year. *DIMACS series in Discrete Mathematics and Theoretical Computer Science*, vol. 6. AMS-ACM, New York, pp. 287–308.

RENEGAR, J. 1992. On the computational complexity and geometry of the first order theory of the reals. *J. Symb. Comput. 13*, 3, 255–352.

ROY, M.-F. Basic algorithms in real algebraic geometry: From Sturm theorem to the existential theory of reals. Lectures on real geometry in memoriam of Mario Raimondo. In *de Gruyter Expositions in Mathematics*, to appear.

ROY, M.-F., AND SZPIRGLAS, A. 1990. Complexity of computations with real algebraic numbers. *J. Symb. Comput. 10*, 39–51.

ROY, M.-F., AND VOROBJOV, N. 1994. Finding irreducible components of some real transcendental varieties. *Comput. Complexity 4*, 107–132.

SEIDENBERG, A. 1954. A new decision method for elementary algebra. *Ann. Math. 60*, 365–374.

TARSKI, A. 1951. A decision method for elementary algebra and geometry. University of California Press.

VAN DER WAERDEN, B. L. 1950. Modern Algebra, Volume II. F. Ungar Publishing Co.

VOROBJOV, N. 1984. Bounds of real roots of a system of algebraic equations. In *Notes of Science Seminars of Leningrad Department of Math*, Vol. 137. (St. Petersburg, Fla.). Steklov Institute, 7–19.

WALKER, R. J. 1950. *Algebraic curves*. Princeton University Press, Princeton, NJ.

RECEIVED DECEMBER 1994; REVISED AUGUST 1996; ACCEPTED SEPTEMBER 1995