A New Algorithm to Find a Point in Every Cell Defined by a Family of Polynomials

Saugata Basu[1],
Richard Pollack[2],
Marie-Françoise Roy[3]

November 3, 1995

Abstract

We consider s polynomials $P_1, \ldots, P_s$ in $k < s$ variables with coefficients in an ordered domain A contained in a real closed field R, each of degree at most d. We present a new algorithm which computes a point in each connected component of each non-empty sign condition over $P_1, \ldots, P_s$. The output is the set of points together with the sign condition at each point. The algorithm uses $s(s/k)^k d^{O(k)}$ arithmetic operations in A. The algorithm is nearly optimal in the sense that the size of the output can be as large as $s(O(sd/k))^k$.

Previous algorithms of Canny and Renegar used $(sd)^{O(k)}$ operations [5, 7, 8, 15]. We use either these algorithms in the case $s = 1$ as a subroutine in our algorithm.

As a bonus, our algorithm yields an independent proof of the bound on the number of connected components in all non-empty sign conditions ([14]) and also yields an independent proof of a theorem of Warren

[1]Courant Institute of Mathematical Sciences, New York University, New York, NY 10012, U.S.A.. Supported in part by NSF grant CCR-9122103

[2]Courant Institute of Mathematical Sciences, New York University, New York, NY 10012, U.S.A.. Supported in part by NSF grant CCR-9122103, and NSA grant MDA904-92-H-3075.

[3]IRMAR (URA CNRS 305), Université de Rennes, Campus de Beaulieu 35042 Rennes cedex FRANCE. Supported in part by the project ESPRIT-BRA 6846POSSO

(see [17]) which is used in [14] as well as in many other problems of a combinatorial nature (see Alon [1] for example).

1 Introduction:

A sign condition for a set $\mathcal{P} = \{P_1, \ldots, P_s\}$, of s polynomials in k variables with coefficients in an ordered ring A, is specified by a sign vector $\sigma \in \{-1, 0, +1\}^s$. The sign condition σ is called *non-empty* (with respect to $\mathcal{P}$) if there is a point $x \in R^k$ (where R is a real closed field containing A and extending its order), such that

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

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

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

We will abuse language and have a sign condition denote the realization of the sign condition as well.

We say that a set $\mathcal{P} = \{P_1, \ldots, P_s\}$ of polynomials in k variables is in *general position* if no $k+1$ have a common zero in R. (This is a weak notion of general position as we assume neither smoothness nor transversality).

We will prove the following theorem

Theorem 1 *Let $\mathcal{P} = \{P_1, \ldots, P_s\}$ be a set of polynomials in $k < s$ variables each of degree at most d and each with coefficients in an ordered domain A contained in a real closed field R.*

There is an algorithm which outputs at least one point in each cell (semi-algebraically connected component) of every non empty sign condition on $P_1, \ldots, P_s$ and provides the sign vector

$$(\mathrm{sign}(P_1(x)), \ldots, \mathrm{sign}(P_s(x)))$$

of $\mathcal{P}$ at each output point x.

The algorithm terminates after at most $\binom{O(s)}{k} s d^{O(k)} = (s/k)^k s d^{O(k)}$ arithmetic operations in A .

The idea behind the algorithm is that, if the polynomials are in general position, it is enough to find a point in every semi-algebraically connected component of the algebraic sets defined by a conjunction of less than $k+1$ equations $P_i + e\epsilon$ (where $e \in \{0, 1, -1\}$ and ϵ is small enough) in order to find a test point in every semi-algebraically connected component of every non empty sign condition over $\mathcal{P}$. Since the polynomials may not be in general position, we perturb the polynomials using three additional infinitesimals $\frac{1}{\Omega}, \delta', \delta$, such that the perturbed polynomials are in general position and their zero set is bounded. We can then use the method described above, and finally we let these infinitesimals go to zero in an appropriate way.

Previously, algorithms with complexity $(sd)^{O(k)}$, due to Canny [5, 7, 8] and Renegar (part II, sect. 4 of [15]), which test the emptyness of a sign condition, actually produced a point in every semi-algebraically connected component of that sign condition when it is not empty. In the case $s = 1$, it is easy to see, using Bezout's theorem, that these algorithms produce $O(d)^k$ points. We use any one of these algorithms as a subroutine in our algorithm. In our result, we consider an algebraic model in which we measure complexity in terms of the number of algebraic operations in the underlying ring A. We separate this complexity into a combinatorial part of $s\binom{O(s)}{k}$, involving s and k where precise bounds are obtained and an algebraic part, with complexity $d^{O(k)}$.

This idea of separating the complexity into a combinatorial part and an algebraic part already appears in Canny [6] who has an algorithm which also constructs a point in every semi-algebraically connected component of every non empty sign condition with complexity $s^{k+1}d^{O(k^2)}$ in the algebraic model (and $s^{k+1}d^{O(k)}$ randomized).

We are able to obtain as algebraic part of the complexity $d^{O(k)}$ by using the perturbation of Renegar in [15] which uses only three additional infinitesimals.

We shall need the terminology and properties of infinitesimals, semi-algebraically connected components and paths in non archimedean extensions. A full discussion of these can be found in [4] 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-algebric homeomorphisms are homeomorphism whose graph is semi-algebraic.

In particular we have the following elementary definitions and properties of semi-algebraic sets, over a real closed field R (see also [4])

- 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.
- 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 f_γ with $f_\gamma(0) = x$ and $f_\gamma(1) = x'$. A semi-algebraic path γ is *defined over* A if the graph of f_γ is described by polynomials with coefficients in A.
- A semi-algebraic set is semi-algebraically connected if and only if it is semi-algebraically path connected.
- In the case of real numbers, semi-algebraically connected components of semi-algebraic sets are ordinary connected components.
- Let S be a semi-algebraic set in R^k , and R' a real closed field containing R, we write $S_{R'}$ for the subset of R'^k defined by the same boolean combination of inequalities that define S.
- Let A be a subring of the real closed field R. A semi- algebraic set S is defined over A if it can be described by polynomials with coefficients in A.
- Let S be defined over $A \subset R$ and let R' be a real closed field extension of R. The semi-algebraically connected components of $S_{R'}$ are the extensions to R' of the semi-algebraically connected components of S.

We also need the following definitions and properties of ordered rings and Puiseux series. Again, fuller details can be found in [4]. We suggest, in order to understand the following definitions as well as the proof of Proposition 1, that it is helpful to think of ϵ as positive and small enough.

- For a subring $A \subset R$ and a new variable ϵ, we define the order on $A[\epsilon]$ making ϵ infinitesimal and positive by saying that $P \in A[\epsilon]$ is positive iff the tail coefficient of P is positive. Similarly for $Q \in R(\epsilon)$ the order making ϵ infinitesimal and positive is defined by saying that Q is positive iff the tail coefficients of the numerator and denominator of Q have the same sign. It follows that $P(\epsilon) > 0$ iff for $t \in R$ sufficiently small and positive, $P(t) > 0$.

- Let $R\langle\epsilon\rangle$ be the field of Puiseux series in ϵ with coefficients in R. Its elements are 0 and series of the form

  $$\sum_{i \in \mathbf{Z}} a_i \epsilon^{\frac{i}{q}}$$

  with $q \in \mathbf{N}$, $a_{i_0} \neq 0$ for some $i_0 \in \mathbf{Z}, a_i \in R$, and $a_i = 0$ for $i < i_0$.

  The field $R\langle\epsilon\rangle$ is real closed ([4]). An element x' of $R\langle\epsilon\rangle$ is *infinitesimal* (with respect to R) if and only if its absolute value is strictly smaller than any positive element in R. The element ϵ of $R\langle\epsilon\rangle$ is infinitesimal positive. The elements of $R\langle\epsilon\rangle$ bounded over R form a *valuation ring* denoted $V(\epsilon)$; the elements of $V(\epsilon)$ are 0 or Puiseux series

  $$\sum_{i \in \mathbf{Z}} a_i \epsilon^{\frac{i}{q}}$$

  with $a_i = 0$ for $i < 0$. We denote by eval the ring homomorphism from $V(\epsilon)$ to R which maps $\sum_{i \in \mathbf{Z}} a_i \epsilon^{\frac{i}{q}}$ (with $a_i = 0$ for $i < 0$) to a_0. If the Puiseux series is infinitesimal ($i_0 > 0$), it is mapped by eval to 0. We can think of eval as the evaluation of the Puiseux series at 0.

- A Puiseux series $f(\epsilon) \in R\langle\epsilon\rangle$ is algebraic over $A[\epsilon]$ if it is a root of a polynomial $P_\epsilon(X)$ with coefficients in $A[\epsilon]$. The root $f(\epsilon)$ is distinguished among the other roots of P, by its Thom encoding (see [9], using for example Algorithm RAN in [16]). For t sufficiently small and positive, we may replace ϵ by t in the polynomials which are the coefficients of $P_\epsilon(X)$ to obtain the polynomial $P_t(X)$ and (since inequalities in $A[\epsilon]$ will agree with the corresponding inequalities in $A[t]$ for t positive and small enough) $P_t(X)$ will have the same number of roots in R as $P_\epsilon(X)$ has in $R\langle\epsilon\rangle$, with the corresponding Thom encodings and the algebraic Puiseux series $f(\epsilon)$ thus defines a semi-algebraic function $f(t)$ for t small enough.

- Let $S(\epsilon)$ be a semi-algebraic set in $R\langle\epsilon\rangle^k$ defined over $A[\epsilon]$ and for $t \in R$ let $S(t)$ be the semi-algebraic set in R^k obtained by substituting t for ϵ. Let $P(S(\epsilon))$ be a property of the semi-algebraic set $S(\epsilon)$ in $R\langle\epsilon\rangle^k$ defined over $A[\epsilon]$ which is expressible by a first order formula $\Phi(\epsilon)(x_1, \ldots, x_k)$ with parameters in $A[\epsilon]$. Then for t positive and small enough $P(S(t))$ is satisfied.

  This is an easy consequence of quantifier elimination and of the preceeding lemma on the ways signs are computed in $A[\epsilon]$.

  We will use this property to replace ϵ by t in a path defined over $A[\epsilon]$ to obtain a "neighboring" path defined over $A[t]$.

We can now be a little more precise about the output of our computation. The coordinates of the points that we construct in every semi-algebraically connected component of a non-empty sign condition will not necessarily belong to the realization C of the sign condition in R but to its realization $C_{R\langle\frac{1}{\Omega},\delta\rangle}$ in some non archimedean real closed extension $R\langle\frac{1}{\Omega}, \delta\rangle$ of the ordered domain $A[\Omega, \delta]$, where $\frac{1}{\Omega}, \delta$, are infinitesmals with $\frac{1}{\Omega} \gg \delta$. Nevertheless, whenever we output a point $x = (x_1, \ldots, x_k)$ what we actually output will be:

1. A univariate polynomial f, with coefficients in $A[\Omega, \delta]$,

2. A root, say α of f which is distinguished among the other real roots of f by the sign vector $(\mathrm{sign} f(\alpha), \mathrm{sign} f'(\alpha), \ldots, \mathrm{sign} f^{\{deg f\}})$. This sign vector is called the *Thom encoding* of α after Thom's lemma (see [9]).

3. k rational functions $R_1, \ldots, R_k$ with coeficients in $A[\Omega, \delta]$ and $x_i = R_i(\alpha)$ for $i = 1, \ldots, k$.

All the computations will take place in these polynomial rings, and our complexity analysis counts the number of arithmetic operation in A (algebraic operations and sign determinations).

The fact that the sample points constructed may belong to a non archimedean real closed extension $R\langle\frac{1}{\Omega}, \delta\rangle$ of R is quite unusual but is not a problem at all because of the relationship between semi-algebraically connected components in $R\langle \frac{1}{\Omega}, \delta\rangle$ and in R for semi-algebraic sets defined over A (see the ninth bullet above).

We can answer any sign question concerning these sample points by algebraic computations and sign evaluations in A and the complexity is evaluated in A.

If we are only interested in the existental theory of reals, our algorithm outputs the set of non-empty sign conditions over R, even if the sample points belong to $R\langle \frac{1}{\Omega}, \delta\rangle$.

The following proposition will easily assure the correctness of our algorithms (see also [10] , Lemma 1 (b)).

Proposition 1 *Let C be a semi-algebraically connected component of a non-empty sign condition of the form $P_1 = \ldots = P_\ell = 0, P_{\ell+1} > 0, \ldots, P_s > 0$. Then we can find an algebraic set V in $R\langle\epsilon\rangle^k$ defined by equations $P_1 = \ldots = P_\ell = P_{i_1} - \epsilon = \ldots P_{i_m} - \epsilon = 0$, such that a semi-algebraically connected component of V is contained in $C_{R\langle\epsilon\rangle}$, where $R\langle\epsilon\rangle$ is the real closed field of Puiseux series over R in the variable ϵ.*

Proof:

If C is closed, it is a semi-algebraically connected component of the algebraic set defined by $P_1 = \ldots = P_\ell = 0$. If not, we consider Γ, the set of all semi-algebraic paths γ in R going from some point $x(\gamma)$ in C to a $y(\gamma)$ in $\bar{C} \setminus C$ such that $\gamma \setminus \{y(\gamma)\}$ is entirely contained in C. For any $\gamma \in \Gamma$, there exists an $i > \ell$ such that P_i vanishes at $y(\gamma)$. Then on $\gamma_{R\langle\epsilon\rangle}$ there exists a point $z(\gamma,\epsilon)$ such that one of the $P_i - \epsilon$ vanishes at $z(\gamma,\epsilon)$ and that on the portion of the path between x and $z(\gamma,\epsilon)$ no such $P_i - \epsilon$ vanishes. We write I_γ for the set of indices between $\ell + 1$ and s such that $i \in I_\gamma$ if and only if $P_i(z(\gamma,\epsilon)) - \epsilon = 0$.

Now choose a path $\gamma \in \Gamma$ so that the set $I_\gamma = \{i_1, \ldots, i_m\}$ is maximal under set inclusion and let V be defined by $P_1 = \ldots = P_\ell = P_{i_1} - \epsilon = \ldots = P_{i_m} - \epsilon = 0$.

It is clear that at $z(\gamma,\epsilon)$, defined above, we have $P_{\ell+1} > 0, \ldots, P_s > 0$ and $P_j - \epsilon > 0$ for every $j \notin I_\gamma$. Let C' be the semi-algebraically connected component of V containing $z(\gamma,\epsilon)$. We shall prove that no polynomial $P_{\ell+1}, \ldots, P_s$ vanishes on this semi-algebraically connected component, and thus that C' is contained in $C_{R\langle\epsilon\rangle}$.

Let us suppose on the contrary that some new P_i $(i > l, i \notin I_\gamma)$ vanishes on C', say at y_ϵ. We can suppose without loss of generality that y_ϵ is defined over $A[\epsilon]$. Take a semi-algebraic path γ_ϵ defined over $A[\epsilon]$ connecting $z(\gamma,\epsilon)$ to y_ϵ with $\gamma_\epsilon \subset C'$. Denote by $z(\gamma_\epsilon,\epsilon)$ the first point of γ_ϵ with $P_1 = \ldots = P_\ell = P_{i_1} - \epsilon = \ldots = P_{i_m} - \epsilon = P_j - \epsilon = 0$ for some new j not in I_γ.

For t in R small enough, the set γ_t (obtained by replacing ϵ by t in γ_ϵ) defines a semi-algebraic path from $z(\gamma,t)$ to $z(\gamma_\epsilon,t)$ contained in C. Replacing ϵ by t in the Puiseux series which give the coordinates of $z(\gamma_\epsilon,\epsilon)$ defines a path γ' containing $z(\gamma_\epsilon,\epsilon)$ from $z(\gamma_\epsilon,t)$ to $y = \mathrm{eval}(z(\gamma_\epsilon,\epsilon))$ (which is a point of $\bar{C} \setminus C$). Let us consider the new path γ^* consisting of the beginning of γ (up to the point z_t for which $P_{i_1} = \ldots, P_{i_m} = t$), followed by γ_t and then followed by γ'. Now the first point in γ^* such that there exists a new j with $P_j - \epsilon = 0$ is $z(\gamma_\epsilon,\epsilon)$ and thus $\gamma^* \in \Gamma$ with I_{γ^*} strictly larger than I_γ. This is impossible by the maximality of I_γ. $\square$

2 Proof of the theorem:

2.1 The Algorithm

First we introduce some notation. Let $\Omega, \delta, \delta', \epsilon$ be new variables.

We order $A[\Omega]$, requiring that Ω be positive and bigger than any positive element of A. Similarly, we order $A[\Omega,\delta]$, (resp. $A[\Omega,\delta,\delta']$, $A[\Omega,\delta,\delta',\epsilon]$), such that δ is positive and smaller than any positive element of $A[\Omega]$, (resp. δ' positive and smaller than any positive element of $A[\Omega,\delta]$, ϵ positive and smaller than any positive element of $A[\Omega,\delta,\delta']$. In short, the ordering is $\frac{1}{\Omega} \gg \delta \gg \delta' \gg \epsilon$, where $a \gg b$ stands for , " b is positive and infinitesmal with respect to a".

Let $R\langle\frac{1}{\Omega}\rangle$ be the field of Puiseux series in $\frac{1}{\Omega}$ with coefficients in R,

$R\langle\frac{1}{\Omega},\delta\rangle$ the field of Puiseux series in δ with coefficients in $R\langle\frac{1}{\Omega}\rangle$, $R\langle\frac{1}{\Omega},\delta,\delta'\rangle$ the field of real Puiseux series in δ' with coefficients in $R\langle\frac{1}{\Omega},\delta\rangle$, $R\langle\frac{1}{\Omega},\delta,\delta',\epsilon\rangle$ the field of real Puiseux series in ϵ with coefficients in $R\langle\frac{1}{\Omega},\delta,\delta'\rangle$.

Let $V(\frac{1}{\Omega},\delta,\delta',\epsilon)$ the valuation ring of elements of $R\langle\frac{1}{\Omega},\delta,\delta',\epsilon\rangle$ bounded by elements of $R\langle\frac{1}{\Omega},\delta\rangle$, and eval the corresponding map from $V(\frac{1}{\Omega},\delta,\delta',\epsilon)$ to $R\langle\frac{1}{\Omega},\delta\rangle$ sending δ' and ϵ to 0.

We are now in a position to describe the algorithm for finding a point in every semi-algebraically connected component of every non-empty sign condition.

The algorithm is as follows:

Step 1: Replace the set $\mathcal{P}$ by the set $\mathcal{Q}$ of $4s+1$ polynomials $\{P_0 = x_1^2 + \ldots + x_k^2 - \Omega^2\} \cup_{i=1,\ldots,s} \{(1-\delta)P_i - \delta H_i, (1-\delta)P_i + \delta H_i, (1-\delta)P_i - \delta'\delta H_i, (1-\delta)P_i + \delta'\delta H_i\}$ where $H_i = (1 + \sum_{1\le j\le k} i^j x_j^{d'})$ and d' is an even number bigger than the degree of the P_i.

Step 2: Enlarge the set of $4s+1$ polynomials to the following set of $3(4s+1)$ polynomials.

$$\{Q_{i,e}\}_{1\le i\le s, e\in\{0,1,-1\}}$$

where ϵ is an infinitesimal positive element and $Q_{i,e} = Q_i + e\epsilon$,

Step 3: For every $\ell \le k$-tuple of polynomials $Q_{i_1,e_1}, \ldots, Q_{i_\ell,e_\ell}$ consider $Q = Q_{i_1,e_1}^2 + \ldots Q_{i_\ell,e_\ell}^2$, test if $Q = 0$ defines the empty set, and if it does not construct at least one point in every semi-algebraically connected component of the zero set of Q (using, say, the construction in section 4, part II of [15]).

(The i^{th} coordinate of one of these points is a univariate rational function $R_i(\alpha)$ where α is defined over $A[\Omega, \delta, \delta', \epsilon]$. Recall items 1, 2, 3 of the introduction). Apply the eval map, by letting $\epsilon, \delta' \to 0$, on the points satisfying $P_0 < 0$, and obtain points defined over $A[\Omega, \delta]$.

Step 4: Apply the eval map, by letting $\epsilon, \delta' \to 0$, on the points satisfying $P_0 < 0$, and obtain points defined over $A[\Omega, \delta]$.

Step 5: Characterize the coordinates of these points using Thom's lemma and determine at these points the sign of the other polynomials $P_i \in \mathcal{P}$ (using the algorithms RAN and RANSI in [16]). Note that now all polynomials are univariate with coefficients in $A[\Omega, \delta,]$ (again, recall items 1, 2, 3 of the introduction).

In practical applications, it might be useful to check as a first step, whether the given polynomials are in general position. That is for each $k+1$ tuple of polynomials $P_{i_1}, \ldots, P_{i_{k+1}}$, determine whether the polynomial $Q = P_{i_1}^2 + \ldots + P_{i_{k+1}}^2 = 0$ defines the empty set or not. If every such $k+1$ tuple defines the empty set, then the polynomials are in general position. Thus we could do without the additional infinitesmals $\frac{1}{\Omega}$, δ and δ'. In this case, we omit Step 1 and Step 4 of the algorithm. As a result, we generate points in $R\langle\epsilon\rangle^k$, defined over $A[\epsilon]$, where $R\langle\epsilon\rangle$ is the field of Puiseux series in ϵ

with coefficients in R. This would lead to a significant practical (though not asymptotic) improvement in the run-time of the algorithm.

2.2 Proof of the correctness of the algorithm :

We first prove that the polynomials in $\mathcal{Q}$ are in general position. This is an easy consequence of the fact that the polynomials $(1-\delta)P_i + \delta H_i$ are in general position ([15] lemma 3.11.1).

We recall this proof. If H is a polynomial we denote by H^h its homogenization with respect to the variable x_0.

Lemma 1 *The $H_i^h = (x_0^{d'} + \sum_{1\leq j\leq k} i^j x_j^{d'})$ are in general position inside the complex projective space.*

Proof: Take $H = ({x_0}^{d'} + \sum_{1\leq j\leq k} t^j x_j^{d'})$. If $k+1$ of the H_i^h (say $H_{j_1}^h, \ldots, H_{j_{k+1}}^h$ had a common zero $\bar{x}$, in the complex projective space, substituing this root in H would give a non zero univariate polynomial of degree at most k with $k+1$ distinct roots $(j_1, \ldots, j_{k+1})$, 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 1 *The polynomials H_i are in general position.*

Lemma 2 *Polynomials $(1-\delta)P_i + \delta H_i$ are in general position.*

Proof: Let $Q_{i,t} = (1-t)P_i + tH_i$. Let $Q_{i,t}^h$ denote the homogenization of $Q_{i,t}$ with respect to x_0. Let us consider the set T of t such that the $Q_{i,t}$ are in general position in the complex projective space, which means that no $k+1$ subset of the $Q_{i,t}^h$ has a common zero in the projective complex space. The set T contains 1, according to the preceeding lemma , it contains an open interval containing 1, since being in general position in the complex projective space is a stable condition. It is also Zariski constructible, since it can be defined by a first order formula of the language of algebraically closed fields. So the transcendental element δ belongs to the extension of T, which proves the lemma. □

Let C be a semi-algebraically connected component of $P_1 = \ldots = P_\ell = 0, P_{\ell+1} > 0, \ldots, P_s > 0$. We shall prove that the extension of C to $R\langle \frac{1}{\Omega}, \delta\rangle$,

$C_{R\langle\frac{1}{\Omega},\delta\rangle}$, contains eval$(D_{R\langle\frac{1}{\Omega},\delta,\delta',\epsilon\rangle})$ for some bounded, semi-algebraically connected component, D of the set S defined in $R\langle\frac{1}{\Omega},\delta,\delta'\rangle^k$ by the sign conditions $P_0 < 0, -\delta'\delta H_1 < (1-\delta)P_1 < \delta'\delta H_1, \ldots, -\delta'\delta H_\ell < (1-\delta)P_\ell < \delta'\delta H_\ell, (1-\delta)P_{\ell+1} > \delta H_{\ell+1}, \ldots, (1-\delta)P_s > \delta H_s$.

Let x be a point of C, then x belongs to S . Now let D be the bounded semi-algebraically connected component of S containing x. We know that $D_{R\langle\frac{1}{\Omega},\delta,\delta',\epsilon\rangle}$ is again semi-algebraic and bounded. Since the image under eval of a bounded semi- algebraically connected set (defined over $A[\Omega,\delta,\delta',\epsilon]$) is again semi-algebraically connected, (see [12]) it is clear that eval$(D_{R\langle\frac{1}{\Omega},\delta,\delta',\epsilon\rangle})$ is contained in $C_{R\langle\frac{1}{\Omega},\delta\rangle}$. □

The correctness of the algorithm is now an easy consequence of Proposition 1, since by Lemma 2, it suffices to consider sets of polynomials of size $< k+1$. □

2.3 Complexity analysis of the algorithm

First note that, since we have introduced only four infinitesmals, and all the algebraic computations are done in the ordered ring $A[\Omega,\delta,\delta',\epsilon]$ using only linear algebra subroutines, the asymptotic complexity is not affected because of the introduction of these infinitesmals.

The total number of $\ell \leq k$-tuples to be examined is $\sum_{\ell\leq k}\binom{12s+3}{\ell} = (O(s/k))^k$.

For each of these ℓ-tuples, we test whether the zero set of the corresponding polynomial is empty or not, and if not compute a point in each of its semi-algebraically connected components.

For each subset of size ℓ for which the zero set of the corresponding polynomial is non-empty we produce at most $(O(d))^k$ points. So the total number of points constructed will be $(O(sd/k)^k$. The Thom characterization and sign evaluation of the other polynomials at these points is done with complexity $sd^{O(k)}$ (using the variant of Ben-Or Kozen Reif algorithm that is algorithm RAN and RANSI in[16]).

2.4 Generalizations

In a forthcoming paper [2] we show that

Theorem 2 *Let $\mathcal{V}$ be a k' dimensional variety which is the zero set of the polynomial $Q \in A[X_1, \ldots X_k]$ and Q has degree at most d. Let $\mathcal{P} = \{P_1, \ldots, P_s\}$ be a set of polynomials in $k < s$ variables each of degree at most d and each with coefficients in an ordered domain A contained in a real closed field R.*

There is an algorithm $\mathcal{A}$, which determines whether the family $\mathcal{P}$ is in general position with respect to $\mathcal{V}$ (which means that no $k'+1$ polynomials in $\mathcal{P}$ have a common zero on $\mathcal{V}$) and if it is in general position, outputs at least one point in each cell (semi-algebraically connected component) in $\mathcal{V}$ of every sign condition of $\mathcal{P}$ which is non-empty in $\mathcal{V}$ and provides the signs of all the polynomials at each of these points.

In case the family is not in general position with respect to $\mathcal{V}$, there is an algorithm, $\mathcal{B}$, which gives the same output as algorithm $\mathcal{A}$.

Algorithm $\mathcal{A}$ terminates after at most $\binom{O(s)}{k'} sd^{O(k)} = s^{k'} sd^{O(k)}$ arithmetic operations in A while algorithm $\mathcal{B}$ terminates after at most $\binom{O(s)}{k'} sd^{O(k^2)} = s^{k'} sd^{O(k^2)}$ arithmetic operations in A.

Corollary 2 *The number of semi-algebraically connected components of all non- empty sign conditions defined by a family of s polynomials in $k < s$ variables, on a variety $\mathcal{V}$ of dimension k' with each polynomial of degree at most d is $s^{k'} O(d/k)^k$.*

In the case $k' = 0$ we get, being slightly more specific, an algorithm evaluating the signs of a family of s polynomials at a finite set of points defined by ℓ polynomials in time $sd^{O(k)}$

This is a multivariate version of the Ben-Or Kozen Reif algorithm improving the complexity of [13].

We plan to use the methods in this paper in order to describe a new quantifier elimination algorithm of single exponential complexity when the number of alternation of quantifiers is fixed. In this new algorithm the degrees of the polynomials in the quantifier free equivalent formula will be independent of the number of equations, which is new for single exponential methods, and the time complexity in terms of the number of input polynomials will be more precise than in [11] and [15].

References

[1] N. Alon, *Tools from higher algebra* to appear in Handbook of Combinatorics, R.L. Graham, M. Grotschel and L. Lovász, eds, North Holland.

[2] S. Basu R. Pollack, M.-F. Roy, *An algorithm to find a point in every cell on a variety defined by a family of polynomials*, in preparation.

[3] M. Ben-Or, D. Kozen , J. Reif, *The complexity of elementary algebra and geometry.* J. of Computation and Systems Sciences, 32:251–264, (1986).

[4] J. Bochnak, M. Coste, M.-F. Roy, "Géométrie algébrique réelle". Springer-Verlag (1987).

[5] J. Canny, *Some algebraic and geometric computations in PSPACE*, In Proc. Twentieth ACM Symp. on Theory of Computing, 460- 467, (1988).

[6] J. Canny, *Some practical tools for algebraic geometry*, Technical report in Spring school on robot motion planning, PROMOTION ESPRIT, (1993).

[7] J. Canny, *Computing road maps in general semi-algebraic sets*, The Computer Journal, vol 36, 5 504-514 (1993).

[8] J. Canny, *Improved algorithms for sign determination and existential quantifier elimination*, The Computer Journal, vol 36, 5 409-418(1993).

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

[10] D. Grigor'ev, N. Vorobjov *Counting connected components of a semialgebraic set in subexponential time.* Comput. Complexity, 2 :133-186 (1992).

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

[12] J. Heintz, M.-F. Roy, P. Solernò, Single exponential path finding in semi-algebraic sets II : The general case. Algebraic geometry and its applications. Bajaj editor, Springer Verlag (1993) 467-481.

[13] P. Pedersen, M.-F. Roy, A. Szpirglas

Counting real zeroes in the multivariate case, Computational algebraic geometry, Eyssette et Galligo ed. Progress in Mathematics 109 , 203-224, Birkhauser (1993).

[14] R. Pollack, M..-F. Roy, *On the number of cells defined by a set of polynomials*, C. R. Acad. Sci. Paris, 316:573–577, (1993).

[15] J. Renegar, *On the computational complexity and geometry of the first-order theory of the reals, parts I, II and III.* Journal of Symbolic Computation, 13(3):255–352, 1992.

[16] M.-F. Roy, A. Szpirglas *Complexity of computations with real algebraic numbers*, J. of Symbolic Comput., 10:39–51, (1990).

[17] , H. E. Warren *Lower bounds for approximation of nonlinear manifolds.* Trans. Amer. Math. Soc., 133:167–178, (1968).