On Computing a Set of Points Meeting Every Cell Defined by a Family of Polynomials on a Variety

Saugata Basu* and Richard Pollack*

Courant Institute of Mathematical Sciences, New York University, New York, New York 10012

and

Marie-Françoise Roy†

IRMAR (URA CNRS 305), Université de Rennes, Campus de Beaulieu 35042 Rennes cedex, France

Received August 1, 1996

We consider a family of $s$ polynomials, $\mathcal{P} = \{P_1, \ldots, P_s\}$, in $k$ variables with coefficients in a real closed field $R$, each of degree at most $d$, and an algebraic variety $V$ of real dimension $k'$ which is defined as the zero set of a polynomial $Q$ of degree at most $d$. The number of semi-algebraically connected components of all non-empty sign conditions on $\mathcal{P}$ over $V$ is bounded by $s^{k'}(O(d))^k$. In this paper we present a new algorithm to compute a set of points meeting every semi-algebraically connected component of each non-empty sign condition of $\mathcal{P}$ over $V$. Its complexity is $s^{k'+1}dO(k)$. This interpolates a sequence of results between the Ben-Or–Kozen–Reif algorithm which is the case $k' = 0$, in one variable, and the Basu–Pollack–Roy algorithm which is the case $k' = k$. It improves the results where the same problem was solved in time $s^{k'+1}dO(k')$. ©1997 Academic Press

1. INTRODUCTION

A sign condition for a set of $s$ polynomials $\mathcal{P} = \{P_1, \ldots, P_s\}$ is specified by a sign vector $\sigma \in \{-1, 0, +1\}^s$ and the sign condition $\sigma$ is non-empty over an algebraic variety $V$ (with respect to $\mathcal{P}$) if there is a point $x \in V$ such that

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

*Supported in part by NSF grants CCR-9402640 and CCR-9424398.
†Supported in part by the project ESPRIT-BRA 6846POSSO and by European Community Contract CHRX-CT94-0506.

0885-064X/97 $25.00$
Copyright © 1997 by Academic Press
All rights of reproduction in any form reserved.
The realization space of $\sigma \in \{-1, 0, +1\}^k$ over $V$ is the set

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

If $R(\sigma)$ is not empty then each of its non-empty semi-algebraically connected components is a cell of $P$ over $V$.

We denote by $Z(Q)$ the zero set of a polynomial $Q$ and by $Z(\mathcal{Q})$ the set of common zeros of a set of polynomials $\mathcal{Q} = \{Q_1, \ldots, Q_m\}$.

The following theorem appears in [4].

**Theorem 1.** Let $Q$ (resp. $\mathcal{P}$) be a polynomial (resp., a set of $s$ polynomials) in $k$ variables of degree at most $d$ with coefficients in a real closed field $R$ such that $V = Z(Q)$ is an algebraic variety of real dimension $k'$. Then,

$$\sum_{|\sigma| \geq 1} |\sigma| = s^{k'}(O(d))^k,$$

where $|\sigma|$ denotes the number of cells of $R(\sigma)$.

The bound in Theorem 1 on the number of cells of $P$ on the variety $V$ is separated into a combinatorial part (the dependence on $s$) which depends only on the real dimension of the variety and an algebraic part (the dependence on $d$) which depends on the dimension $k$ of the ambient space.

In this paper we compute a point in each cell of $P$ over $V$ so as to prove the following theorem.

**Theorem 2.** Let $V = Z(Q)$ be a variety of real dimension $k'$ where $Q$ is a polynomial in $R\{X_1, \ldots, X_k\}$, of degree at most $d$, and let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset R\{X_1, \ldots, X_k\}$ with each $P_s \in \mathcal{P}$ also of degree at most $d$.

We present an algorithm which takes as input $Q$, $k'$, and $\mathcal{P}$ and computes a set of points in each non-empty cell of $P$ over $V$. The algorithm also provides the signs of all the polynomials of $\mathcal{P}$ at each of these points. The algorithm uses at most $(O(\delta))^{sD^{O(k)}} = s^{k'+1}d^{O(k)}$ arithmetic operations in $D$ (where $D$ is the ring generated by the coefficients of $Q$ and the $P_s$’s).

We define the complexity of our algorithms to be the number of arithmetic operations in the ring $D$. Moreover, when $D = Z$, and $\tau$ is the bit size of the input, then the bit-complexity of our algorithm is bounded by $(O(\delta))^{sD^{O(k)}\tau \log(\tau)\log(\log(\tau))}$. 

Note that we do not know how to compute the real dimension of an algebraic variety in time $d^{O(k)}$. The known methods have complexity $d^{O(k^2)}$ (see [9]). For this reason, we consider $k'$ as part of the input.

We now give an outline of our algorithm.

Our algorithm uses a technique of approximating varieties which appears in [9]. Given a real variety $V$ of dimension $k'$, this technique produces a family
of algebraic sets of dimension $k'$ such that for every point in $V$ there exists a point in one of the new varieties which is infinitesimally close to it.

A family $\mathcal{P} = \{P_1, \ldots, P_s\}$ of polynomials in $k$ variables is in \textit{general position} with respect to a variety $V$ of real dimension $k'$, if no $k'+1$ polynomials of $\mathcal{P}$ have a common zero in $V$. Our algorithm proceeds by making $\binom{k}{k'}\varepsilon$-perturbations $\mathcal{V}_I = Z(Q_I)$ of the variety $V$ and an $\varepsilon$-perturbation $\mathcal{P}$ of the polynomials $\mathcal{P}$. The variety $\mathcal{V}_I$ has real dimension $k'$ and $\mathcal{P}$ is in general position with respect to $\mathcal{V}_I$.

We will see that for every cell $C$ of $\mathcal{P}$ over $V$ there exist an $I$ and a cell $C'$ of $\mathcal{P}$ over $\mathcal{V}_I$, so that the limit of $C'$ as $\varepsilon$ tends to 0 is contained in $C$. Thus it will suffice to compute points in every cell of every $\mathcal{P}$ over $\mathcal{V}_I$ and then take the limit of these points as $\varepsilon$ tends to 0.

We describe an algorithm which solves the problem for any $\mathcal{P}$ over $\mathcal{V}_I$. This algorithm, together with the observations of the previous paragraph, gives us the algorithm for the general case.

We start with some mathematical preliminaries, then construct approximating varieties and discuss general position. After some algorithmic preliminaries we finally present our algorithm, thus proving Theorem 2.

\section{2. MATHEMATICAL PRELIMINARIES}

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 [6] but we offer a brief summary below.

The order relation on a real closed field $R$ defines, as usual, the Euclidean topology on $R^k$. A semi-algebraic set is the finite union of sets defined by a finite number of polynomial equalities and inequalities, and a semi-algebraic map is one whose graph is a semi-algebraic set.

In particular, we have the following elementary properties of semi-algebraic sets over a real closed field $R$ (see also [6]).

An element $\alpha \in R$, which is a root of a polynomial $f(t) \in D[t]$, is uniquely specified by the polynomial $f$ and the sign vector

$$\text{sign}(f(\alpha)), \text{sign}(f'(\alpha)), \ldots, \text{sign}(f^{(\deg f)}(\alpha)),$$

known as the Thom encoding [7] of the root $\alpha$.

A semi-algebraic set $S$ is \textit{semi-algebraically connected} if it is not the disjoint union of two non-empty closed semi-algebraic sets in $S$. A \textit{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, each of which is a semi-algebraic set. A
A **semi-algebraic path** between $x$ and $x'$ in $\mathbb{R}^k$ is a semi-algebraic subset $\gamma$, which is the image of a semi-algebraic continuous map $f_\gamma$, which maps the unit interval of $\mathbb{R}$ to $\gamma$, which $f_\gamma(0) = x$ and $f_\gamma(1) = x'$. A semi-algebraic path $\gamma$ is defined over $D$ if the graph of $f_\gamma$ is defined by polynomials with coefficients in $D$. A semi-algebraic set is semi-algebraically connected if and only if it is semi-algebraically path connected. In the case of the real numbers, semi-algebraically connected components of semi-algebraic sets are ordinary connected components.

We shall use the following proposition whose proof appears in [3].

**Proposition 1.** Let $C$ be a non-empty semi-algebraically connected component of a basic closed semi-algebraic set defined by

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

There exists an algebraic set $W$ defined by equations

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

(with $\{i_1, \ldots, i_m\} \subset \{\ell+1, \ldots, s\}$) such that a semi-algebraically connected component $C'$ of $C$ is contained in $W$.

Let $S$ be a semi-algebraic set in $\mathbb{R}^k$, and $R'$ be a real closed field containing $\mathbb{R}$. Then we write $S_{R'}$ for the extension of $S$ to $R'$, i.e., the subset of $\mathbb{R}^k$ defined by the same Boolean combination of inequalities that define $S$. 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 [6]. We suggest that in order to understand the following definitions it is helpful to think of $\varepsilon$ as positive and very small and $\varepsilon_0$ as the limit as $\varepsilon$ tends to 0.

Let $\mathbb{R}(\varepsilon)$ (resp. $\overline{\mathbb{R}}(\varepsilon)$) be the field of Puiseux series in $\varepsilon$ with coefficients in $\mathbb{R}$ (resp. in $\overline{\mathbb{R}} = \mathbb{R}[i]$). Its elements are 0 and the series of the form

$$\sum_{i_0 \geq 0, \ i \in \mathbb{Z}} a_i \varepsilon^{i/q}$$

with $i_0 \in \mathbb{Z}$, $a_i \in \mathbb{R}$ (resp. $\overline{\mathbb{R}}$), $a_{i_0} \neq 0$, and $q \in \mathbb{N}$. The field $\mathbb{R}(\varepsilon)$ is real closed [6] and the field $\overline{\mathbb{R}}(\varepsilon)$ is algebraically closed [10]. An element of $\mathbb{R}(\varepsilon)$ is infinitesimal (with respect to $\mathbb{R}$) if and only if its absolute value is strictly smaller than any positive element in $\mathbb{R}$. The element $\varepsilon$ of $\mathbb{R}(\varepsilon)$ is infinitesimal positive. The elements of $\mathbb{R}(\varepsilon)$ bounded over $\mathbb{R}$ form a valuation ring denoted $V(\varepsilon)$; the elements of $V(\varepsilon)$ are 0 or Puiseux series

$$\sum_{i \in \mathbb{N}} a_i \varepsilon^{i/q}.$$
We denote by $\ev_{\mathcal{L}}$ the ring homomorphism from $V(\mathcal{L})$ to $R$ which maps $\sum_{i \in \mathbb{N}} a_i e^{i/q}$ to $a_0$. A Puiseux series is infinitesimal if and only if it is mapped by $\ev_{\mathcal{L}}$ to 0. We can also think of $\ev_{\mathcal{L}}$ as the evaluation of the Puiseux series at 0. Whenever we write $\ev_{\mathcal{L}}(S)$ we understand it to be the map $\ev_{\mathcal{L}}$ restricted to $S \cap V(\mathcal{L})$.

If $\alpha$ belongs to the valuation ring of $R[\mathcal{L}]$ and $f(\alpha) = 0$, where $f \in D[\mathcal{L}, 1/\mathcal{L}][t]$ and $f(t) = \sum_{\nu(f) \leq i} f_i(t) e^i$ for some integer $\nu(f)$, then $\ev_{\mathcal{L}}(\alpha) \in R$, and is a root of the polynomial $f_{\nu(f)}(t)$.

We shall also use the following proposition (see [3]).

**Proposition 2.** If $S' \subseteq R[\mathcal{L}]^k$ is a semi-algebraic set defined over $D[\mathcal{L}]$ and $S = \ev_{\mathcal{L}}(S')$, then $S$ is a semi-algebraic set. Moreover, if $S'$ is connected and bounded then $S$ is connected.

### 3. Constructing the Approximating Varieties

We recall the construction and results in [9].

Let $V = Z(Q)$ be a real algebraic variety. We assume that $Q$ has degree at most $d$ and is non-negative. This assumption causes no loss of generality as we can replace $Q$ with $\bar{Q}^2$ at the cost of doubling the degree of $Q$.

We denote by $B(\mathcal{L}_r)$ the ball of center $\mathcal{L}$ and radius $r$. For any index set $I = \{i_{k'+1}, \ldots, i_k\} \subseteq [1, k]$ let

$$B = B_0(\delta_0^{-1}),$$
$$a = (k - k')\delta_0^{2(d+1)},$$
$$Q_I = (1 - \delta_1)Q - \delta_1(x_{i_{k'+1}}^{2(d+1)} + \cdots + x_{i_k}^{2(d+1)} - a),$$
$$Q_I = \left\{ Q_I, \frac{\partial Q_I}{\partial x_{i_{k'+2}}}, \ldots, \frac{\partial Q_I}{\partial x_{i_k}} \right\},$$
$$V_I = Z(Q_I)$$
$$V' = Z(Q) \cap B,$$
$$W = \bigcup_{I \subseteq [1, k], |I| = k - k'} V_I.$$

With these notations, the following key proposition appears in [9].

**Proposition 3 [9].** Let $V_{k'}$ be the points of $V'$ which have local dimension $k'$. Then for every $x \in V_{k'}$ there exists $y \in W$ such that $\ev_{\mathcal{L}_1}(y) = x$.

The following corollary is an immediate consequence of the proposition.
**Corollary 1.** Let $V$ be an algebraic set of real dimension $k'$. Then for every $x \in V$ there exists $y \in \mathcal{W}$ such that $\text{eval}_{\delta_1}(y) = x$.

In order to take advantage of this proposition, we need the following proposition.

**Proposition 4.** Suppose that $V = Z(Q)$ is a variety of real dimension $k'$ and $\mathcal{P}$ is a set of $s$ polynomials, $P_1, \ldots, P_s$. Let $C$ be a connected component of the sign condition,

$$
Q = 0, \\
P_1 = P_2 = \cdots = P_{\ell} = 0, \\
P_{\ell+1} > 0, \ldots, P_s > 0,
$$

containing a point $x \in V$. Let $\delta_0 \gg 1/\Omega \gg \varepsilon_0 \gg \varepsilon_1 \gg \delta_1$ be infinitesimals.

Then there exists a multi-index $I = (i_{k'+1}, \ldots, i_k)$ and a connected component $C'$ of the semi-algebraic set

$$
\mathcal{V}_I \cap \{x \mid -\varepsilon_1 < P_i(x) < \varepsilon_1, \ P_j(x) > \varepsilon_0, \ 1 \leq i \leq \ell, \ \ell < j \leq s\} \cap B_0(\Omega)
$$

such that

$$
\text{eval}_{\varepsilon_1}(C') \subset C.
$$

**Proof.** By Corollary 1 there exists a multi-index $I$ and a point $y \in \mathcal{V}_I$ such that $\text{eval}_{\delta_1}(y) = x$. Thus, $y$ satisfies the inequalities

$$
-\varepsilon_1 < P_i < \varepsilon_1, \\
P_j > \varepsilon_0, \\
x_1^2 + \cdots + x_k^2 - \Omega^2 \leq 0,
$$

for $1 \leq i \leq \ell, \ \ell < j \leq s$.

Let $C'$ be the connected component of

$$
\mathcal{V}_I \cap \{u \mid -\varepsilon_1 < P_i(u) < \varepsilon_1, \ P_j(u) > \varepsilon_0, \ 1 \leq i \leq \ell, \ \ell < j \leq s\} \cap B_0(\Omega)
$$

which contains $y$. Then, $\text{eval}_{\varepsilon_1}(C')$ is connected and is contained in the set defined by

$$
Q = 0, \quad P_1 = P_2 = \cdots = P_{\ell} = 0, \quad P_{\ell+1} > 0, \ldots, P_s > 0.
$$
Moreover, \( x \in \text{ev}_{c_1}(C') \). Hence \( \text{ev}_{c_1}(C') \subset C \). ■

4. GENERAL POSITION

We use the notations of the preceding section for \( Q_I \) and \( \mathcal{V}_I \). The set \( \mathcal{P} = \{ P_1, \ldots, P_s \} \) is a subset of \( R[X_1, \ldots, X_k] \).

In order to modify the polynomials of \( \mathcal{P} \) so that they are in general position over \( \mathcal{V}_I \), we use certain special polynomials \( H_i(c, k) = c + \sum_{1 \leq j \leq k} \bar{i} X_j^{d^i} \), for \( 1 \leq i \leq s \), where \( d^i \) is the least even integer greater than \( d \), the maximum degree of the polynomials in \( \mathcal{P} \), and \( c \) is a positive element of \( R \).

The following lemma is an easy modification of a result in Renegar [8] (see also [3]).

**Lemma 1.** The polynomials \((1 - \delta)P_i + \delta H_i(c, k)\) are in general position.

We now prove

**Proposition 5.** Let \( \delta \) be an infinitesimal with \( \delta_0 \gg \delta \gg \delta_1 \). The polynomials \((1 - \delta)P_i + \delta H_i(c, k)\) are in general position over \( \mathcal{V}_I \).

**Proof.** Let \( H = (X_{ik}^{2(d+1)} + \cdots + X_{ik}^{2(d+1)} - a) \). The system

\[
\begin{align*}
H &= \frac{\partial H}{\partial X_{ik}^{j+2}} = \cdots = \frac{\partial H}{\partial X_{ik}^{j}} = 0
\end{align*}
\]

has only two solutions in \( R^{k-k'} \), namely \((a^{-2(d+1)}, 0, \ldots, 0)\) and \((-a^{-2(d+1)}, 0, \ldots, 0)\). Substituting these two solutions in the polynomials \( H_i(c, k) \) gives a unique polynomial of the form \( H_i(c', k') \) where \( c' \) is a positive element of \( R \). We can thus apply the preceding lemma in \( R^{k-k'} \) space.

Since, as we just saw, the property is true for \( \delta_1 = 1 \) and is stable, the proposition is proved. ■

The following proposition holds.

**Proposition 6.** Let \( \mathcal{P} \) be any set of \( s \) polynomials, \( P_1, \ldots, P_s \), and let \( C \) be a connected component of the sign condition,

\[
Q_I = \frac{\partial Q_I}{\partial X_{ik+2}} = \cdots = \frac{\partial Q_I}{\partial X_{ik}} = 0, \quad P_1 = P_2 = \cdots = P_\ell = 0, \quad P_{\ell+1} > 0, \cdots, P_s > 0.
\]

Then there is a connected component \( C' \) in \( R(1/\Omega, \delta, \delta^k) \), of the semi-algebraic set defined by the equalities and inequalities.
Computing a set of points

\[ Q_I = \frac{\partial Q_I}{\partial X_{i_{k+1}}} = \cdots = \frac{\partial Q_I}{\partial X_{i_k}} = 0 \]

\[-\delta^l \delta H_i \leq P_i \leq \delta^l \delta H_i, \quad 1 \leq i \leq l, \]

\[ P_i \geq \delta H_i, \quad l + 1 \leq i \leq s, \quad X_1^2 + \cdots + X_k^2 - \Omega^2 \leq 0 \]

such that \( \operatorname{eval}_{i'}(C') \) is contained in the extension of \( C \) to \( R(1/\Omega, \delta) \).

**Proof.** The proof is an easy consequence of Proposition 1.

---

5. ALGORITHMIC PRELIMINARIES

In this section we outline a few basic subroutines used in our algorithm. We refer the reader to [3] for a detailed description of these subroutines.

5.1. Cell Representatives Subroutine

This subroutine takes as input a polynomial \( Q \) and outputs points in every semi-algebraically connected component of \( Z(Q) \).

If the polynomial \( Q \) has total degrees \( d_1, \ldots, d_k \) in \( X_1, \ldots, X_k \) (with \( d_1 \geq \cdots \geq d_k \)) with coefficients in an ordered domain \( D \), the subroutine computes a set of size \( (d_1 \cdots d_k)^{O(1)} \). The elements of this set, called univariate representations, are \( (k+2) \)-tuples composed of a univariate polynomial \( f \) and \( k+1 \) polynomials \( (g_0, \ldots, g_k) \). The set of output points associated to these univariate representations are obtained by evaluating the rational functions \( g_i/g_0 \) at the real roots of the corresponding polynomial \( f \), known through their Thom encoding. This set 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 \( D \).

5.2. Sign Determination Subroutine

The input is a univariate representation and the output is the sign of a family of polynomials at the points associated to this univariate representation.

---

6. THE ALGORITHM

In our algorithm we first replace the input variety by an approximating variety such that the input family of polynomials is in general position with respect
to this approximating variety. We first describe a subroutine that we use to compute points in every cell of the perturbed variety, which we then use in the main algorithm.

### 6.1. A Subroutine

We define $Q_I$ and $\mathcal{V}_I$ as before (cf. Section 3).

The input to the subroutine is $Q_I$ and a set of polynomials $\mathcal{P}$. The output is a set of points intersecting every cell of $\mathcal{P}$ over $\mathcal{V}_I$ and the sign condition they satisfy.

We define $H_i$ as $H_i(1, k)$ using the notation of Section 4.

**Step 1.** Introduce three new infinitesimals $1/\Omega, \delta,$ and $\delta'$ and replace the set $\mathcal{P}$ by the set $\overline{\mathcal{P}}$ of $4s + 1$ polynomials

$$\bigcup_{i=1, \ldots, s} \{(1 - \delta)P_i - \delta H_i, (1 - \delta)P_i + \delta H_i, (1 - \delta)P_i - \delta' \delta H_i, (1 - \delta)P_i + \delta' \delta H_i\} \cup \{X_1^2 + \cdots + X_k^2 - \Omega^2\}.$$

**Step 2.** For every $k'$ tuple of polynomials from $\overline{\mathcal{P}}$, use the Cell Representatives Subroutine to compute a set of points intersecting every connected component of the algebraic set defined by these polynomials and those of $Q_I$. Then compute the images of these points under the $\text{eval}_{k'}$ map.

**Step 3.** Use the sign determination subroutine [3] to compute the signs of the family of polynomials $\mathcal{P}$ at every point constructed above.

### 6.2. The Algorithm

Now we describe the algorithm.

We assume that the given variety $V$ of dimension $k'$ is described as the zero set of $Q$. The input of the algorithm is $Q, k'$, and a set of $s$ polynomials, $\mathcal{P}$. The output is a set of points intersecting every cell of $\mathcal{P}$ over $\overline{Z(Q)}$ and the sign conditions they satisfy at these points.

**Step 1.** Introduce the infinitesimals $\delta_0 \gg 1/\Omega \gg \varepsilon_0 \gg \varepsilon_1 \gg \delta_1$.

For every multi-index $I = (i_{k'+1}, \ldots, i_k), 1 \leq i_{k'+1} < \cdots < i_k \leq k, 0 < p \leq k'$, consider the variety $\mathcal{V}_I$ following the notation in Section 3.

**Step 2.** Replace the family of polynomials $\mathcal{P}$ by a new family, $\overline{\mathcal{P}}$, of $4s + 1$ polynomials $\bigcup_{1 \leq i \leq s} \{P_i \pm \varepsilon_0, P_i \pm \varepsilon_1\} \cup \{X_1^2 + \cdots + X_k^2 - \Omega^2\}$.

**Step 3.** For every index $I$ in Step 1 use the preceding algorithm for approximating varieties with input variety $\mathcal{V}_I$ and the family of polynomials $\overline{\mathcal{P}}$.

**Step 4.** Compute the images of the points computed in Step 3 under the $\text{eval}_{\varepsilon_1}$ map. Also compute the signs of the polynomials in $\mathcal{P}$ at these points.
6.3. Proof of Correctness and Complexity

The correctness of the subroutine follows immediately from Proposition 6 and the correctness of the subroutines used. It is clear that in Step 3 \( \binom{O(s)}{k'} \) tuples are considered. The cost for each such tuple is \( d^{O(k)} \) (see [3] for details). The cost of Step 4 is \( sd^{O(k)} \) per point constructed in Step 3. Hence, the total complexity is bounded by \( \binom{O(s)}{k'}sd^{O(k)} \).

The correctness of the algorithm now follows from Proposition 4 and the correctness of the subroutine. The total number of multi-indices considered in Step 1 is bounded by \( \binom{k'}{k'} \). It follows that the complexity of the algorithm is again bounded by \( \binom{O(s)}{k'}sd^{O(k)} \).

This complexity analysis proves Theorem 2.

REFERENCES