ON THE COMPUTATIONAL COMPLEXITY
AND GEOMETRY OF THE FIRST-ORDER
THEORY OF THE REALS
Part III
Quantifier elimination

By

James Renegar

This research was supported by NSF Grant DMS-8800835.
1. INTRODUCTION

This paper is the third in a series of three papers. An introduction to this series is provided in Part I. We assume that the reader has read that introduction and here only provide a synopsis of the main results proven in this paper.

In this paper we develop a quantifier elimination method for formulae of the form

\[ (Q_{1}x^{[1]} \in \mathbb{R}^{n_{1}})...(Q_{\omega}x^{[\omega]} \in \mathbb{R}^{n_{\omega}})P(y,x^{[1]},...,x^{[\omega]}) \]  

where

(i) each \( Q_{k} \) is one of the quantifiers \( \exists \) or \( \forall \);
(ii) \( y = (y_{1},...,y_{\ell}) \) are free variables;
(iii) \( P(y,x^{[1]},...,x^{[\omega]}) \) is a quantifier free Boolean formula with atomic predicates

\[ g_{i}(y,x^{[1]},...,x^{[\omega]})\Delta_{i}0 \quad i = 1,\ldots,m \]

each \( g_{i}: \mathbb{R}^{\ell} \times \times_{k=1}^{\omega} \mathbb{R}^{n_{k}} \rightarrow \mathbb{R} \) being a polynomial of degree at most \( d \geq 2 \), and \( \Delta_{i} \) being any one of the standard relations

\[ \geq, >, =, \neq, \leq, < \]  

\[ (1.2) \]

The data describing the formula is \( \omega, Q_{1},...,Q_{\omega}, n_{1},...,n_{\omega}, \ell, m, \Delta_{1},...,\Delta_{m} \), the coefficients of the polynomials \( g_{1},...,g_{m} \) and a Boolean function \( P: \{0,1\}^{m} \rightarrow \{0,1\} \) used to define \( P \) as follows:

\[ P(y,\bar{x}) := P(B(\bar{y},\bar{x})) \]

where

\[ B_{i}(\bar{y},\bar{x}) := \begin{cases} 1 & \text{if} \ g_{i}(\bar{y},\bar{x})\Delta_{i}0 \\ 0 & \text{otherwise} \end{cases} \]
We let $\text{Time}(P, N)$ denote the worst case time (over all vectors in $\{0, 1\}^m$) required to evaluate $P$ using $N$ parallel processors.

If the coefficients of $\{g_i\}_i$ are integers, we assume that they are of bit length at most $L$.

The main theorem we prove in this paper is the following. We assume that $\ell \geq 1$.

**Theorem 1.1.** There is a real number model quantifier elimination method that requires only

$$2^{O(\omega)} \ell \prod_k n_k \text{ operations and } (\text{md})^{O(\ell + \sum_k n_k)} \text{ calls to } P.$$

The method requires no divisions. The method can be implemented in parallel, requiring time

$$[2^{O(\omega)} \ell \prod_k n_k \log(\text{md})]^{O(1)} + \text{Time}(P, N)$$

if $(\text{md})^{2^{O(\omega)} \ell \prod_k n_k}$ processors are used for the operations and $N(\text{md})^{O(\ell + \sum_k n_k)}$ processors are used for the calls (for any $N \geq 1$).

When restricted to formulae involving only polynomials with integer coefficients, the algorithm becomes a bit model quantifier elimination method requiring only

$$L(\log L)(\log \log L)(\text{md})^{2^{O(\omega)} \ell \prod_k n_k}$$

sequential bit operations and $(\text{md})^{O(\ell + \sum_k n_k)}$ calls to $P$. When implemented in parallel the algorithm requires time

$$(\log L)[2^{O(\omega)} \ell \prod_k n_k \log(\text{md})]^{O(1)} + \text{Time}(P, N)$$

if $L^2(\text{md})^{2^{O(\omega)} \ell \prod_k n_k}$ processors are used for bit operations and $N(\text{md})^{O(\sum_k n_k)}$ processors are used for the calls (for any $N \geq 1$).
The quantifier elimination method constructs quantifier free formula of the following simple form:

\[ \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} (h_{ij}(y)\Delta_{ij};0) \]  

where

\[ I \leq (md) 2^{O(\omega)} \prod_k n_k; \]

\[ J_i \leq (md) 2^{O(\omega)} \prod_k n_k; \]

the degree of \( h_{ij} \) is at most \( 2^{O(\omega)} \prod_k n_k; \)

\( \Delta_{ij} \) is one of the standard relations (1.2).

If the coefficients of \( \{g_i\}_i \) are integers of bit length at most \( L \), the coefficients of the polynomials \( h_{ij} \) will be integers of bit length at most \( (L+\ell)(md) 2^{O(\omega)} \prod_k n_k \).

Sections 2 and 3 are devoted to listing the results from the two preceding papers in the series that will be important for the development.

In section 4, the problem of designing an efficient quantifier elimination method to establish the theorem is reduced to a problem we call "the quantifier elimination subproblem."

In section 5, focus is switched to designing a variant of the Ben-Or, Kozen and Reif algorithm for constructing the 'consistent sign vectors' of sets of univariate polynomials.

In sections 6 and 7, ideas developed in section 5 are shown to be relevant for solving the quantifier elimination subproblem.

In section 8, the design of the univariate algorithm for constructing the consistent sign vectors of sets of univariate polynomials is completed.

In section 9, ideas developed in sections 7 and 8 are combined to solve the quantifier elimination subproblem, thereby establishing the theorem.
2. PRELIMINARIES

In this section we collect six propositions and two lemmas from the first two papers in the series. We state the propositions in the order in which they were proven.

For positive integers \( n \) and \( D \), define

\[
\mathcal{B}(n+1,D) := \{(i^{n-1}, i^{n-2}, \ldots, i, 1, 0); \quad i \in \mathbb{Z}, \quad 0 \leq i \leq nD^2\},
\]

a subset of \( \mathbb{R}^{n+1} \). Let \( e_{n+1} := (0, \ldots, 0, 1) \in \mathbb{R}^{n+1} \). For \( X \in \mathbb{C}^{n+1} \) satisfying \( X_{n+1} \neq 0 \), define

\[
\text{Aff}(X) := \frac{1}{X_{n+1}} (X_1, \ldots, X_n),
\]

the “affine image” of \( X \).

The first proposition is a restatement of the second half of proposition 2.3.1 from Part I.

**Proposition 2.1.** Assume that \( R: \mathbb{R}^{n+1} \to \mathbb{R} \) is a polynomial of degree at most \( D \). Assume that \( R \) is not identically zero and factors linearly (over the complex numbers)

\[
R(U) = \prod_i \xi^{(i)} \cdot U,
\]

where \( \xi^{(i)} \cdot U := \sum_j \xi^{(i)}_j U_j \). Then for each \( i \) for which \( \text{Aff}(\xi^{(i)}) \) is well-defined, there exist \( \beta \in \mathcal{B}(n+1,D) \) and \( 0 \leq j \leq D \) such that the univariate polynomial \( t \mapsto R(\beta + te_{n+1}) \) is not identically zero and for some real zero \( t' \) of \( t \mapsto R(\beta + te_{n+1}) \), the vector

\[
\xi' := \frac{d^j}{dt'} \nabla R(\beta + t'e_{n+1})
\]

satisfies \( \text{Aff}(\xi') = \text{Aff}(\xi^{(i)}) \).

The “sign vector” of a set \( \{g_i\}_{i=1}^m \) of polynomials \( g_i: \mathbb{R}^n \to \mathbb{R} \) at a point \( \bar{x} \in \mathbb{R}^n \) is the vector \( \sigma \in \{-1,0,1\}^m \) defined by:

\( \sigma_i = 1 \) if \( g_i(\bar{x}) > 0 \); \( \sigma_i = 0 \) if \( g_i(\bar{x}) = 0 \); \( \sigma_i = -1 \) if \( g_i(\bar{x}) < 0 \).
For a finite set \( \{g_i\}_1 \) of polynomials \( g_i : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R} \), and for \( \bar{x}^{[1]} \in \mathbb{R}^{n_1} \), define the "connected sign partition" \( \text{CSP}\{x^{[2]} \mapsto g_i(\bar{x}^{[1]}, x^{[2]})\}_i \) of \( \mathbb{R}^{n_2} \) to be the partition of \( \mathbb{R}^{n_2} \) whose elements are the maximal connected subsets of \( \mathbb{R}^{n_2} \) with the following property: if \( \bar{x}^{[2]} \) and \( \bar{x}^{[2]} \) are in the same element, then the sign vector of \( \{x^{[2]} \mapsto g_i(\bar{x}^{[1]}, x^{[2]})\}_i \) at \( \bar{x}^{[2]} \) is the same as at \( \bar{x}^{[2]} \).

The next proposition is a restatement of proposition 3.9.1 from Part I.

**Proposition 2.2.** Assume that \( g_1, \ldots, g_m : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R} \) are polynomials of degree at most \( d \). Let \( \bar{m} := \min\{m, n_2\} \). There exists a set \( \mathcal{B}\{g_i\}_1(x^{[1]}_i) \) of \( (\text{mod} \hspace{0.1cm} O(n_2)) \) polynomials in the variables \( (x^{[1]}, U) \in \mathbb{R}^{n_1} \times \mathbb{R}^{n_2+1} \) of degree at most \( D = (\bar{m}d) \hspace{0.1cm} O(n_2) \) with the following properties:

(i) for each \( \bar{x}^{[1]} \in \mathbb{R}^{n_1} \) and for each element of \( \text{CSP}\{x^{[2]} \mapsto g_i(\bar{x}^{[1]}, x^{[2]})\}_i \) there exists \( R \in \mathcal{B}\{g_i\}_1(x^{[1]}) \) such that \( U \mapsto \text{R}(x^{[1]}, U) \) is not identically zero and factors linearly (over the complex numbers) \( \prod \xi^{(i)} \cdot U \) where for some \( i \), \( \text{Aff}(\xi^{(i)}) \) is in the element;

(ii) for each \( \beta \in \mathbb{R}^{n_2+1} \) the entire set of polynomials

\[
(x^{[1]}, t) \mapsto \text{R}(x^{[1]}_i, \beta + t e_{n_2+1}^i)
\]

\[
(x^{[1]}, t) \mapsto \frac{d^i}{dt^i} \nabla U \text{R}(x^{[1]}_i, \beta + t e_{n_2+1}^i)
\]

obtained from all \( R \in \mathcal{B}\{g_i\}_1(x^{[1]}_i) \), \( 0 \leq j \leq D \), can be constructed from \( \beta \) and the coefficients of \( \{g_i\}_i \) with \( (\text{mod} \hspace{0.1cm} O(n_1 n_2)) \) operations (no divisions) in time \( [n_1 n_2 \log(\text{mod})] \hspace{0.1cm} O(1) \) using \( (\text{mod} \hspace{0.1cm} O(n_1 n_2)) \) parallel processors; if the coefficients of \( \beta \) and \( \{g_i\}_i \) are integers of bit length at most \( L \), then all numbers occurring during the construction will be integers of bit length at most \( (L + n_1)(\text{mod}) \hspace{0.1cm} O(n_2) \).

A vector \( \sigma \in \{-1, 0, 1\}^m \) is said to be a "consistent sign vector" for the set \( \{g_i\}_i \) of polynomials \( g_i : \mathbb{R}^n \to \mathbb{R} \) if there exists \( \bar{x} \in \mathbb{R}^n \) for which the sign vector of \( \{g_i\} \) at \( \bar{x} \) is \( \sigma \).

The next proposition is a restatement of proposition 4.1 from Part I.
Proposition 2.3. Any set of polynomials $g_1,\ldots,g_m : \mathbb{R}^n \to \mathbb{R}$, of degree at most $d$, has at most $(md)^{O(n)}$ consistent sign vectors. The entire set of consistent sign vectors can be constructed from the coefficients of $\{g_i\}_i$ with $(md)^{O(n)}$ operations in time $[n \log(md)]^{O(1)}$ using $(md)^{O(n)}$ parallel processors. If the coefficients of $\{g_i\}_i$ are integers of bit length at most $L$ then the construction can be accomplished with $L(\log L)(\log \log L)(md)^{O(n)}$ sequential bit operations, or in time $(\log L)[n \log(md)]^{O(1)}$ using $L^{2(m)}(md)^{O(n)}$ parallel processors. □

The fourth proposition is a restatement of proposition 4.1.1 from Part II. It is very easy to prove.

Proposition 2.4. ("Thom’s lemma") Assume that $p \neq 0$ is a real univariate polynomial of degree $e$. If $t', t'' \in \mathbb{R}$ are such that $t' < t''$ and for some $0 \leq i \leq e$, there is a zero of the $i$th derivative $p^{(i)}$ contained in the interval $[t', t'']$, then for some $i \leq \ell \leq e$, the sign of $p^{(\ell)}(t')$ differs from the sign of $p^{(\ell)}(t'')$. □

Now assume that $g_1,\ldots,g_m : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R}$ are polynomials of degree at most $d \geq 2$. For each $x^{[1]} \in \mathbb{R}^{n_1}$, define $S(x^{[1]})$ to be the set of consistent sign vectors for the polynomials $\{x^{[2]} \mapsto g_i(x^{[1]}, x^{[2]})\}_i$. Let $S := \{S(x^{[1]}); x^{[1]} \in \mathbb{R}^{n_1}\}$.

The next proposition is a restatement of a special case of proposition 5.1 from Part II.

Proposition 2.5. The family $S$ of sets consists of $(md)^{O(n_1n_2)}$ sets, each of which consists of $(md)^{O(n_1n_2)}$ elements. It can be constructed with $(md)^{O(n_1n_2)}$ operations (no divisions) in time $[n_1n_2 \log(md)]^{O(1)}$ using $(md)^{O(n_1n_2)}$ parallel processors. If the coefficients of $\{g_i\}_i$ are integers of bit length at most $L$, then it can be constructed with $L(\log L)(\log \log L)(md)^{O(n_1n_2)}$ sequential bit operations, or in time $(\log L)[n_1n_2 \log(md)]^{O(1)}$ using $L^{2(m)}(md)^{O(n_1n_2)}$ parallel processors. □

A proof of the following proposition can be found in Appendix A of Part I. The proposition is due to Csanky, but we have slightly modified his approach to avoid divisions.

Proposition 2.6 (Csanky [4]) There is an algorithm which, given any $n \geq 1$ and any complex $n \times n$ matrix $A$, computes $n! \det(A)$ without divisions in time $O(\log^2(n))$ using $n^{O(1)}$ parallel
processors. If the coefficients of $A$ are integers of bit length at most $L$, all numbers occurring during
the computation will be integers of bit length at most $L^{O(1)}$. □

The following easily proven lemma is established in appendix B of Part I.

**Lemma 2.7.** Assume that $f: \mathbb{C}^n \to \mathbb{C}$ is a polynomial of degree at most $d \geq 2$. Then

$$\prod_{0 \leq j < k \leq d} (k-j)^{n} f \text{ can be computed solely from the values } f(x), \quad x \in \{0,1,\ldots,d\}^n,$$

using $d^{O(n)}$ operations (no divisions). The computations can be implemented in parallel, requiring time

$$[n \log(d)]^{O(1)} \text{ if } d^{O(n)} \text{ processors are used. If the values } f(x), \quad x \in \{0,1,\ldots,d\}^n,$$

are integers of bit length at most $L$, all numbers occurring during the computation will be integers of bit length at most

$$L + nd^{O(1)}. \quad □$$

The following well-known lemma is proven as lemma 3.1 in Part II.

**Lemma 2.8.** Assume that

$$p(t) = \sum_{i=0}^{d} a_i t^i, \quad q(t) = \sum_{i=0}^{e} b_i t^i$$

are real univariate polynomials, where $a_d \neq 0 \neq b_e$. Let $0 \leq k < \min\{d,e\}$ and define $M$ to be the $(d+e-k) \times (d+e-2k)$ matrix $[m_{ij}]$ where

$$m_{ij} := \begin{cases} a_{d+j-i} & \text{if } j \leq e-k \\ b_{k+j-i} & \text{if } j > e-k, \end{cases}$$

i.e., the $j$th column of $M$ is the coefficient vector of $t \mapsto t^{e-k-j} p(t)$ if $j \leq e-k$, and is the coefficient
vector of $t \mapsto t^{d+e-2k-j} q(t)$ if $j > e-k$. (Here we define $a_i = 0$ if $i < 0$ or $i > d$, and similarly
for $b_i$.) Then $p$ and $q$ have at least $k+1$ common complex zeros counting multiplicities if and only if

$$\det M^T M = 0. \quad □$$
3. REDUCTION OF THE QUANTIFIER ELIMINATION PROBLEM

In section 6 of Part II we reduced the problem of designing a quantifier elimination method which establishes the claims of theorem 1.1, and which produces quantifier free formula of the simple form (1.3), to a "target problem" which we restate in this section. We restate the target problem using notation that will be helpful in the next section.

Let \( h_1, \ldots, h_M : \mathbb{R}^\ell \times \mathbb{R}^n \rightarrow \mathbb{R} \) be arbitrary polynomials of degree at most \( d \). For \( \bar{y} \in \mathbb{R}^\ell \) define \( S(\bar{y}; \{ h_i \}_i) \) to be the set of consistent sign vectors of \( \{ x \mapsto h_i(\bar{y},x) \}_i \). Let

\[
S(\{ h_i \}_i) := \{ S(\bar{y}; \{ h_i \}_i) ; \ y \in \mathbb{R}^\ell \}.
\]

The "target problem" is this. Design an algorithm which, given arbitrary \( \ell, n, d, M, \)
\( h_1, \ldots, h_M \), and given arbitrary \( S \in \mathbb{S}(\{ h_i \}_i) \), "efficiently" constructs a quantifier free formula \( P_S(y) \) which is satisfied by \( \bar{y} \in \mathbb{R}^\ell \) if and only if \( S(\bar{y}; \{ h_i \}_i) = S \). By "efficiently constructs", we mean with \( (M \cdot D)^{O(n \ell)} \) operations (no divisions) in time \( [n \ell \log(M \cdot D)]^{O(1)} \) using \( (M \cdot D)^{O(n \ell)} \) parallel processors. The formula \( P_S(y) \) should be of the form

\[
\bigvee_{i=1}^I \bigwedge_{j=1}^{J_i} (h_{ij}(y) \Delta_{ij} 0)
\]

where

\[
I \leq (M \cdot D)^{O(n \ell)};
\]

\[
J_i \leq (M \cdot D)^{O(n)};
\]

the degree of \( h_{ij} \) is at most \( (M \cdot D)^{O(n)} \);

\( \Delta_{ij} \) is any of the standard relations (1.2).

Finally, if the coefficients of \( \{ h_i \}_i \) are integers of bit length at most \( L \), we require that all numbers occurring during the construction be integers of bit length at most \( L(\mathbb{S} \cdot D)^{O(n \ell)} \), and we require the coefficients of the resulting polynomials \( h_{ij} \) to be integers of bit length at most \( (L+\ell)(M \cdot D)^{O(n)} \).
4. THE QUANTIFIER ELIMINATION SUBPROBLEM

4.1 In the previous section we recalled the reduction of the problem of efficiently eliminating quantifiers to the “target problem.” In this section we perform yet another reduction, this time reducing the “target problem” to what we dub “the quantifier elimination subproblem.”

The quantifier elimination subproblem is a problem of designing an algorithm to efficiently construct very particular quantifier free formulae. The input to the algorithm will be

arbitrary polynomials \( f, g_1, \ldots, g_m : \mathbb{R}^\ell \times \mathbb{R} \to \mathbb{R} \) and an upper bound \( d \geq 2 \) on their degrees;

non-negative integers \( d_0 \geq 1, d_1, \ldots, d_m \);

sign vectors \( \sigma^{(1)}, \ldots, \sigma^{(M)} \subseteq \{-1, 0, 1\}^m \);

positive integers \( N_1, \ldots, N_M \) satisfying \( N_1 + \ldots + N_M \leq d_0 \).

(4.1.1) \hspace{1cm} (4.1.2) \hspace{1cm} (4.1.3) \hspace{1cm} (4.1.4)

Given the data, the algorithm should efficiently construct a quantifier free formula \( P(y) \) with the property that \( y \in \mathbb{R}^\ell \) satisfies \( P(y) \) if and only if the following three conditions are satisfied:

the degree of \( t \mapsto f(y,t) \) is \( d_0 \) and the degree of \( t \mapsto g_i(y,t) \) is \( d_i \) for all \( i = 1, \ldots, m \);

the number of distinct real zeros of \( t \mapsto f(y,t) \) is \( N_1 + \ldots + N_M \);

\( N_j \) is the number of distinct real zeros of \( t \mapsto f(y,t) \) at which the sign vector of \( \{t \mapsto g_i(y,t)\}_i \) is \( \sigma^{(j)} \) for all \( j = 1, \ldots, M \).

Moreover, we require \( P(y) \) to be of the form

\[
\bigvee_{i=1}^I \bigwedge_{j=1}^{J_i} (f_{ij}(y) \Delta_{ij} 0)
\]

where

(4.1.5)
\[ I \leq (md)^{O(\ell)}; \quad (4.1.6) \]
\[ J_i \leq (md)^{O(1)} \text{ for all } i; \quad (4.1.7) \]
\[ \text{the degree of } f_{ij} \text{ is at most } (md)^{O(1)}; \quad (4.1.8) \]
\[ \Delta_{ij} \text{ is any of the standard relations (1.2).} \]

By "efficiently" construct, we mean that the algorithm should construct \( P(y) \) from the data (4.1.1), (4.1.2), (4.1.3) and (4.1.4) with \( (md)^{O(\ell)} \) operations (no divisions) in time \( \lceil \ell \log(md) \rceil^{O(1)} \) using \( (md)^{O(\ell)} \) parallel processors. Finally, if the coefficients of \( \{g_i\}_i \) are integers of bit length at most \( L \), we require that all numbers occurring during the construction be integers of bit length at most \( L(md)^{O(\ell)} \), and we require the coefficients of the resulting polynomials \( f_{ij} \) be integers of bit length at most \( (L+\ell)(md)^{O(1)} \).

In the remainder of this section we present the reduction of the target problem stated in section 3 to the quantifier elimination subproblem. Of course once the reduction has been established, to prove theorem 1.1 it will suffice to solve the quantifier elimination subproblem.

4.2 In what follows \( \{g_i\}_i \) should not be confused with the polynomials occurring in the atomic predicates of (1.1). Having reduced the problem of efficiently eliminating quantifiers to the "target problem" of section 3, we are free to reuse notation not occurring in the target problem; we do this to avoid excessive notation.

Also, in what follows, we focus on the operation count and leave verification of the bit lengths of the integers occurring (assuming the coefficients of \( \{g_i\}_i \) are integers) to the reader. The bounds on the bit lengths follow easily from the propositions that are cited.

Let \( \{h_i\}_i \) denote the set of polynomials in the "target problem".

Let \( \mathcal{R}\{h_i\}_i(y) \) denote the set of \( (\mathcal{M}\mathcal{B})^{O(n)} \) polynomials \( R: \mathbb{R}^\ell \times \mathbb{R} \to \mathbb{R} \) as in proposition 2.2. Enlarging \( \mathcal{R}\{h_i\}_i(y) \) if necessary, we assume that if \( R \) is an element then so is \( -R \).
These polynomials are of degree at most $D = (\mathcal{M} \mathfrak{D})^O(n)$ and can be constructed with the operation and time bounds given by proposition 2.2.

Let $\mathfrak{B}(n+1, D)$ be as in (2.1).

For $R \in \mathfrak{R}\{h_1\} \{y\}, \beta \in \mathfrak{B}(n+1, D), \ 0 \leq j \leq D$, define

$$p(y, t; R, \beta, j) := R(y, \beta + te_{n+1})$$

$$q(y, t; R, \beta, j) := \frac{d^j}{dt^j} \nabla_U R(y, \beta + te_{n+1}),$$

$\nabla_U$ denoting the vector of derivatives with respect to the last $n+1$ coordinates. Let $H_1, \ldots, H_{\mathfrak{M}}: \mathbb{R}^\ell \times \mathbb{R}^{n+1} \to \mathbb{R}$ denote the homogenization of $h_1(y, x), \ldots, h_{\mathfrak{M}}(y, x)$ with respect to the $x$ variables, i.e., viewing $y$ as constant.

By propositions 2.1 and 2.2, $\sigma \in \{-1, 0, 1\}^{\mathfrak{M}}$ is a consistent sign vector for the set of polynomials $\{x \mapsto h_1(y, x)\}$ only if for some $R, \beta$ and $j, \ (0,1,\sigma)$ is a consistent sign vector for the set

$$t \mapsto p(\bar{y}, t; R, \beta, j) \quad (4.2.1)$$

$$t \mapsto q_{n+1}(\bar{y}, t; R, \beta, j) \quad (4.2.2)$$

$$t \mapsto H_i(q(y, t; R, \beta, j)) \quad i = 1, \ldots, \mathfrak{M} \quad (4.2.3)$$

(Here we are using the fact that if $R$ is an element of $\mathfrak{R}\{h_1\} \{y\}$ then so is $-R$.) Conversely, if $(0,1,\sigma)$ is a consistent sign vector of the latter set then $\sigma$ is easily seen to be a consistent sign vector of the former set. In all, $\sigma \in S(\bar{y}; \{h_1\})$ if and only if there exist $R, \beta$ and $j$ such that $(0,1,\sigma)$ is a consistent sign vector of the system (4.2.1), (4.2.2) and (4.2.3).

Consider the set of $m = (\mathcal{M} \mathfrak{D})^O(n)$ polynomials in $y$ and $t$

$$\{g_i(y, t)\} := \bigcup_{R, \beta, j} \{p(y, t; R, \beta, j), q_{n+1}(y, t; R, \beta, j), H_i(q(y, t; R, \beta, j)); \ i = 1, \ldots, \mathfrak{M}\}.$$
These polynomials are of degree at most \( \tilde{d} = (M, 2)^{O(n)} \).

For \( \bar{y} \in \mathbb{R}^\ell \) let \( S(\bar{y}; \{g_i\}_i) \) denote the set of consistent sign vectors for \( \{t \mapsto g_i(\bar{y}, t)\}_i \). For each \( \rho \in S(\bar{y}; \{g_i\}_i) \) and triple \( R, \beta \) and \( j \), let \( \rho(R, \beta, j) \) denote the part of \( \rho \) corresponding to the polynomials in \( \{g_i\}_i \) defined by \( R, \beta \) and \( j \).

The previous discussion shows that \( \sigma \in S(\bar{y}; \{h_i\}_i) \) if and only if there exist \( \rho \in S(\bar{y}; \{g_i\}_i), R, \beta \) and \( j \) such that \( \rho(R, \beta, j) = (0, 1, \sigma) \). Hence, \( S(\bar{y}; \{h_i\}_i) \) is easily determined if \( S(\bar{y}; \{g_i\}_i) \) is known.

Define \( S(\{g_i\}) := \{S(\bar{y}; \{g_i\}_i); \bar{y} \in \mathbb{R}^\ell \} \). Applying proposition 2.5 shows that \( S(\{g_i\}_i) \) consists of \( (M, 2)^{O(n \ell)} \) sets, each of which consists of \( (M, 2)^{O(n)} \) elements. Moreover, the proposition shows that \( S(\{g_i\}_i) \) can be constructed with \( (M, 2)^{O(n \ell)} \) operations (no divisions) in time \( [n \ell \log(M, 2)]^{O(1)} \) using \( (M, 2)^{O(n \ell)} \) parallel processors. By the observation of the preceding paragraph it follows that \( S(\{h_i\}_i) \) consists of \( (M, 2)^{O(n \ell)} \) sets, each of which consists of \( (M, 2)^{O(n)} \) elements. Moreover, from the observation of the preceding paragraph, from each set \( S' \in S(\{g_i\}_i) \) is efficiently determined \( S \in S(\{h_i\}_i) \) defined by the relation

\[
S(\bar{y}; \{g_i\}_i) = S' \Rightarrow S(\bar{y}; \{h_i\}_i) = S. \tag{4.2.4}
\]

By considering all \( S' \in S(\{g_i\}_i) \) we construct not only \( S(\{h_i\}_i) \), we also determine for each \( S \in S(\{h_i\}_i) \) the collection of sets \( S' \in S(\{g_i\}_i) \) satisfying the relation (4.2.4). We denote this collection of sets by \( S(\{g_i\}_i; S) \).

From the operation and time bounds on the construction of \( S(\{g_i\}_i) \) it easily follows that \( S(\{h_i\}_i) \), and \( S(\{g_i\}_i; S) \) for all \( S \in S(\{h_i\}_i) \), can be constructed with \( (M, 2)^{O(n \ell)} \) operations (no divisions) in time \( [n \ell \log(M, 2)]^{O(1)} \) using \( (M, 2)^{O(n \ell)} \) parallel processors.

To solve the target problem of section 3 we focus on the relation (4.2.4) used to define \( S(\{g_i\}_i; S) \). The relation shows that to solve the target problem it suffices for the algorithm to
construct \( P_S(y) \) so that \( y \in \mathbb{R}^\ell \) satisfies \( P_S(y) \) if and only if \( y \) satisfies

\[
S' \in S(\{g_i\}_{i=1}^S): S(y; \{g_i\}_{i=1}^S) = S'
\]

(4.2.5)

Assuming that the quantifier elimination subproblem can be solved (i.e., there exists an algorithm with the requisite properties), we will solve the problem of designing an algorithm which, given arbitrary non-negative integers \( m \) and \( \tilde{d} \), given an arbitrary set of polynomials \( g_1, \ldots, g_m \): \( \mathbb{R}^\ell \times \mathbb{R} \to \mathbb{R} \) of degree at most \( \tilde{d} \geq 2 \), and given a set \( S' = \{\sigma^{(1)}, \ldots, \sigma^{(M)}\} \subseteq \{-1, 0, 1\}^m \) of \( M = (md)^{O(1)} \) sign vectors, “efficiently” constructs a quantifier free formula \( P_{S'}(y) \) of the form (4.1.5) (replacing \( d \) with \( \tilde{d} \) in (4.1.6), (4.1.7), (4.1.8)) that is satisfied by precisely those \( y \in \mathbb{R}^\ell \) for which \( S(y; \{g_i\}_{i=1}^S) = S' \); by “efficiently construct”, we mean with \( (md)^{O(1)} \) operations in time \([\ell \log(md)]^{O(1)}\) using \((md)^{O(1)}\) parallel processors.

Once we have such an algorithm, in light of (4.2.5), it can clearly be combined with the constructions of the preceding discussion to yield an algorithm which serves as a solution to the target problem of section 3. We dub the problem stated in the preceding paragraph “the intermediate problem”; thus, the intermediate problem is the problem of designing an algorithm to efficiently construct \( P_{S'}(y) \) of the form (4.1.5) (replacing \( d \) with \( \tilde{d} \) in (4.1.6), (4.1.7) and (4.1.8)) assuming that the quantifier elimination problem can be solved. Henceforth we consider \( S' \) to be fixed, and focus on the intermediate problem.

Clearly, it can be efficiently determined from \( S' \) which of the polynomials \( t \mapsto g_i(y,t) \) are non-constant if \( y \) satisfies \( S(y; \{g_i\}_{i=1}^S) = S' \). Let \( I \) denote the set of indices corresponding to non-constant polynomials. Let

\[
\bar{f}(y,t) := \begin{cases} 
\left[ \prod_{i \in I} g_i(y,t) \right] \left[ \prod_{i \in I} \frac{d}{dt} g_i(y,t) \right] \frac{d}{dt} \left[ \prod_{i \in I} g_i(y,t) \right] & \text{if } I \neq \emptyset \\
1 & \text{if } I = \emptyset 
\end{cases}
\]

\[
f(y,t) := \bar{f}(y,t-1)\bar{f}(y,t+1) \prod_{i=0}^{\tilde{d}} (t-i).
\]
Let \( d := 10m \); then the degree of \( f \), and \( g_i \) for all \( i \), does not exceed \( d \).

**Lemma 4.2.1.** A point \( y \in \mathbb{R}^\ell \) satisfies \( S(y; \{ g_i \}) = S' \) if and only if all of the following three conditions hold:

(i) \( t \mapsto f(y, t) \) is non-constant;

(ii) the set of sign vectors of \( \{ t \mapsto g_i(y, t) \}_{i \in I} \) occurring at the real zeros of \( t \mapsto f(y, t) \) is precisely \( S' \);

(iii) the only sign vector of \( \{ t \mapsto \frac{d}{dt} g_i(y, t) \}_{i \notin I} \) occurring at real zeros of \( t \mapsto f(y, t) \) is the zero vector.

**Proof.** First assume that \( S(y; \{ g_i \}) = S' \). Then (i) follows from the definition of \( f \) and \( I \), and (iii) follows from the definition of \( I \). To prove (ii), begin by noting that every real zero of every \( t \mapsto g_i(y, t) \), \( i \in I \), is also a zero of \( t \mapsto \frac{d}{dt} g_i(y, t) \) and hence is a zero of \( t \mapsto f(y, t) \). Also, if \( t_1 \neq t_2 \) are real zeros of \( t \mapsto g_{i_1}(y, t), t \mapsto g_{i_2}(y, t) \), respectively, then there is a real zero of \( t \mapsto \frac{d}{dt} g_i(y, t) \) strictly between \( t_1 \) and \( t_2 \); hence there is a real zero of \( t \mapsto f(y, t) \) strictly between \( t_1 \) and \( t_2 \). It now follows that all of the consistent sign vectors of \( \{ t \mapsto g_i(y, t) \}_{i \in I} \) occur at real zeros of \( t \mapsto f(y, t) \) except, perhaps, the sign vectors occurring at points \( t \) greater than, or less than, all of the real zeros of \( t \mapsto g_i(y, t) \), \( i \in I \). However, these two sign vectors also occur at real zeros of \( t \mapsto f(y, t) \) because of the factors \( \frac{d}{dt} (y, t+1) \) and \( \frac{d}{dt} (y, t-1) \) occurring in the definition of \( f \). Hence (ii) is established.

Now assume that (i), (ii) and (iii) are satisfied. Let \( I' \) denote the set of indices \( i \) for which \( t \mapsto g_i(y, t) \) is non-constant. Because of the factor \( \prod_{i \in I} \frac{d}{dt} g_i(y, t) \) in \( \frac{d}{dt} f \), (i) implies \( I \subseteq I' \). By (iii) and the occurrence of the factor \( \prod_{i = 0}^d (t-i) \) in the definition of \( f \), \( I' \subseteq I \). Hence \( I = I' \). Repeating the argument used to prove (ii) in the preceding paragraph now establishes the fact that (ii) implies \( S(y; \{ g_i \}) = S' \) \( \square \)

Let \( \{ f_{i_1} \}_{i_1} \) denote the set of \( (md)^{(1)} \) polynomials consisting of \( f_1 \), \( g_i \) for all \( i \), and all of their derivatives, up to the \( d^{th} \) derivative, with respect to \( t \). For \( y \in \mathbb{R}^\ell \) let \( S(y; \{ f_{i_1} \}) \) denote the set of consistent sign vectors of \( \{ t \mapsto f_{i_1}(y, t) \}_{i_1} \). Let \( S(\{ f_{i_1} \}) := \{ S(y; \{ f_{i_1} \}); y \in \mathbb{R}^\ell \} \). Proposition 2.5, applied to \( \{ f_{i_1} \} \), shows that \( S(\{ f_{i_1} \}) \) is a collection of \( (md)^{(2)} \) sets, each of which consists of
(md) $O(1)$ elements. Moreover, the proposition shows that $S(\{f_i\})$ can be constructed with
(md) $O(\ell)$ operations (no divisions) in time $[\ell \log(md)]^{O(1)}$ using (md) $O(\ell)$ parallel processors.

Let $S(\{f_i\}; S')$ denote the subset of $S(\{f_i\})$ consisting of elements $S''$ satisfying the relation

$$S(y; \{f_i\}) = S'' \Rightarrow S(y; \{g_i\}) = S'.$$

Using criteria (i), (ii) and (iii) of lemma 4.2.1, $S(\{f_i\}; S')$ can be efficiently constructed from $S(\{f_i\})$.

For each $S'' \in S(\{f_i\}; S')$, it is trivially seen that the non-negative integers $d_0(S''), \ldots, d_m(S'')$ satisfying the following relation can be efficiently determined: if $S(y; \{f_i\}) = S''$ then the degree of $t \mapsto f(y, t)$ is $d_0(S'')$ and the degree of $t \mapsto g_i(y, t)$ is $d_i(S'')$. Moreover, for each $\sigma^{(i)} \in \{\sigma^{(1)}, \ldots, \sigma^{(M)}\} = S'$, proposition 2.4 shows that the number $N_j(S'')$ satisfying the following relation can also be efficiently determined from $S''$: if $S(y; \{f_i\}) = S''$, then $N_j(S'')$ is the number of distinct real zeros of $t \mapsto f(y, t)$ at which the sign vector of $\{t \mapsto g_i(y, t)\}$ is $\sigma^{(i)}$. (For proposition 2.4 provides a simple means of distinguishing the sign vectors of $\{t \mapsto f_i(y, t)\}$ occurring at distinct real zeros of $t \mapsto f(y, t)$.)

Of course if $S(y; \{f_i\}) = S''$ then the number of distinct real zeros of $t \mapsto f(y, t)$ is

$$N_1(S'') + \cdots + N_M(S'').$$

Clearly, $y \in \mathbb{R}^\ell$ satisfies $S(y; \{g_i\}) = S'$ if and only if there exists $S'' \in S(\{f_i\}; S')$ such that all of the following three conditions are satisfied:

1. $t \mapsto f(y, t)$ is of degree $d_0(S'')$ and $t \mapsto g_i(y, t)$ has degree $d_i(S'')$ for $i = 1, \ldots, m$;  

2. $t \mapsto f(y, t)$ has exactly $N_1(S'') + \cdots + N_M(S'')$ distinct real zeros;  

3. $N_j(S'')$ is the number of distinct real zeros of $t \mapsto f(y, t)$ at which the sign vector of $\{t \mapsto g_i(y, t)\}$ is $\sigma^{(j)}$, for all $j$. 

$$t \mapsto f(y, t) \text{ is of degree } d_0(S'') \quad \text{and } t \mapsto g_i(y, t) \text{ has degree } \quad \text{(4.2.6)}
$$

$$d_i(S'') \text{ for } i = 1, \ldots, m; \quad \text{(4.2.7)}
$$

$$t \mapsto f(y, t) \text{ has exactly } \sum N_j(S'') \text{ distinct real zeros;} \quad \text{(4.2.8)}
$$

$$N_j(S'') \text{ is the number of distinct real zeros of } t \mapsto f(y, t) \text{ at which the sign vector of } \{t \mapsto g_i(y, t)\} \text{ is } \sigma^{(j)}, \text{ for all } j.$$
Assume for the moment that we can solve the quantifier elimination subproblem. For 
\(S'' \in S(\{f_i\}_1: S')\), let \(P_{S''}(y)\) denote the resulting quantifier free formula (of the form (4.1.5)) obtained from the data

\[d, f, g_1, \ldots, g_m, d_0(S''), \ldots, d_m(S''), \sigma^{(1)}, \ldots, \sigma^{(M)}, N_1(S''), \ldots, N_M(S'').\]

Thus, \(\bar{y} \in \mathbb{R}^\ell\) satisfies \(P_{S''}(y)\) if and only if (4.2.6), (4.2.7) and (4.2.8) are true. Hence, \(\bar{y}\) satisfies \(S(\bar{y}; \{g_i\}_1) = S'\) if and only if \(\bar{y}\) satisfies

\[\forall S'' \in S(\{f_i\}_1: S') \ P_{S''}(y)\]

As this expression is of the form (4.1.5) (satisfying (4.1.6), (4.1.7) and (4.1.8)) it follows from the operation and time bounds of the constructions in the preceding discussion, and those occurring in the quantifier elimination subproblem, that we have solved the intermediate problem and hence we have reduced the target problem to the quantifier elimination subproblem.
5. AN ALGORITHM FOR DETERMINING THE CONSISTENT SIGN VECTORS OF A SET OF UNIVARIATE POLYNOMIALS

In this section we begin developing an algorithm for determining the consistent sign vectors of a set of univariate polynomials. The algorithm and analysis are modeled on Ben-Or, Kozen and Reif [1] but differ in ways that expedite our solution to the quantifier elimination subproblem.

Assume that \( g_1, \ldots, g_m \) are real univariate polynomials of respective degrees \( d_1, \ldots, d_m \). Since the signs of constant polynomials are trivially determined, we may assume that all \( d_i \) are positive.

Define

\[
    f(t) := \left[ \prod_i g_i(t) \right] \frac{d}{dt} \left[ \prod_i g_i(t) \right]
\]

Note that the zeros of the polynomials \( g_i \) are also zeros of the polynomial \( f \), and for any two distinct real zeros of \( \prod_i g_i \) there is a zero of \( f \) strictly between them. Hence, each consistent sign vector of \( \{g_i\}_i \) occurs at some real zero of \( f \) except, perhaps, for the sign vectors of points to the right or left of all real zeros of \( \prod_i g_i \). However, the latter two consistent sign vectors are trivially determined from the leading coefficients of the polynomials \( g_i \). Thus, to determine the consistent sign vectors of \( \{g_i\}_i \) it suffices to determine the sign vectors at the real zeros of \( f \).

Henceforth we consider the problem of determining the sign vectors of \( \{g_i\}_i \) at the real zeros of an arbitrary real univariate polynomial \( f \neq 0 \). Let \( I_1, I_2 \subseteq \{1, \ldots, m\} \). The procedure for accomplishing this is recursive and depends on computing certain of the following quantities:

\[
    N(I_1, I_2) := \# \{ t \in \mathbb{R} ; \ f(t) = 0, \ g_i(t) > 0 \ \forall \ i \in I_1, \ \text{and} \ \prod_{i \in I_2} g_i(t) > 0 \} \quad (5.1)
\]

\[
    - \# \{ t \in \mathbb{R} ; \ f(t) = 0, \ g_i(t) = 0 \ \forall \ i \in I_1, \ \text{and} \ \prod_{i \in I_2} g_i(t) < 0 \}
\]

In section 8 we describe a method for computing these quantities. In the remainder of the present section we present an algorithm requiring the computation of only \( (md)^{O(1)} \) of these quantities to determine the sign vectors of \( \{g_i\}_i \) at the real zeros of \( f \), assuming that the degrees of \( f \) and all \( g_i \)
are bounded by \( d \geq 2 \). In the presentation we assume that the values \( N(I_1, I_2) \) can be computed, but for the moment we ignore the cost and time required to do so.

Assume that \( I', I'' \subseteq \{1, \ldots, m\} \), \( I' \cap I'' = \emptyset \). Let \( I := I' \cup I'' \). Assume that \( u^{(1)}, \ldots, u^{(k')} \) (resp. \( v^{(1)}, \ldots, v^{(k'')} \)) are the sign vectors of \( \{g_i\}_{i \in I'} \) (resp. \( \{g_i\}_{i \in I''} \)) occurring at the real zeros of \( f \). Of course \( k' \leq d \) and \( k'' \leq d \). We now show that from these sign vectors and some additional information (including knowledge of some \( N(I_1, I_2) \)) the sign vectors of \( \{g_i\}_{i \in I} \) at the real zeros of \( f \) can be determined. Generation of the additional information required is also part of the recursive procedure; we assume that we have the appropriate information for \( I' \) and \( I'' \) and we show that with it we can generate the appropriate information for \( I \) so that the recursive procedure can continue.

For simplicity of exposition we assume that \( I' = \{1, \ldots, m'\} \), \( I'' = \{m'+1, \ldots, m'+m''\} \).

For \( I'_1, I'_2 \subseteq I' \) (= \( \{1, \ldots, m'\} \)) and \( u \in \mathbb{R}^{m'} \) define

\[
p'(u; I'_1, I'_2) = [\prod_{j \in I'_1} (1-u_j^2)] [\prod_{j \in I'_2} u_j],
\]

replacing the corresponding factor with \( 1 \) if either \( I'_1 \) or \( I'_2 \) is the empty set. Hence,

\[u \mapsto p'(u; I'_1, I'_2)\]

is a polynomial.

For simplicity of exposition we will assume that coordinates of vectors in \( \mathbb{R}^{m''} \) are numbered \( m'+1, \ldots, m'+m'' \). Then, analogous to the above, for \( I''_1, I''_2 \subseteq I'' \) (= \( \{m'+1, \ldots, m'+m''\} \)) and \( v \in \mathbb{R}^{m''} \) define

\[
p''(v; I''_1, I''_2) = [\prod_{j \in I''_1} (1-v_j^2)] [\prod_{j \in I''_2} v_j].
\]

As remarked, to efficiently carry out the procedure for determining the sign vectors of \( \{g_i\}_{i \in I} \) at the real zeros of \( f \) we need more information than just the sign vectors \( u^{(1)}, \ldots, u^{(k')}, v^{(1)}, \ldots, v^{(k'')} \).

We also assume that we have available a set \( g' \) of \( k' \) pairs \((I'_1, I'_2)\), where \( I'_1, I'_2 \subseteq I' \), for which
\begin{equation}
\{[p'(u^{(1)}: I'_1, I'_2), \ldots, p'((u^{(k')}: I''_1, I''_2)]; (I'_1, I'_2) \in \mathcal{I}'\}
\end{equation}

is a basis for $\mathbb{R}^{k'}$. Similarly, we assume that we have available a set of $k''$ pairs $(I''_1, I''_2)$, where $I''_1, I''_2 \subseteq I''$, for which

\begin{equation}
\{[p''(v^{(1)}: I''_1, I''_2), \ldots, p''((v^{(k'')}: I''_1, I''_2)]; (I''_1, I''_2) \in \mathcal{I}''\}
\end{equation}

is a basis for $\mathbb{R}^{k''}$.

Of course having assumed that this additional information is available, besides showing how to construct the sign vectors $w^{(1)}_1, \ldots, w^{(k)}_1$ of $\{g_i\}_{i \in I}$ at the real zeros of $f$, we must also show how to construct a set of $k$ pairs $(I_1, I_2)$, where $I_1, I_2 \subseteq I (= \{1, \ldots, m'+m''\})$, for which

\begin{equation}
\{[p(w^{(1)}: I_1, I_2), \ldots, p(w^{(k)}: I_1, I_2)]; (I_1, I_2) \in \mathcal{I}\}
\end{equation}

is a basis for $\mathbb{R}^{k}$; here we define

\[ p(w: I_1, I_2) = \prod_{j \in I_1} (1-w^2_j) \prod_{j \in I_2} w_j, \]

for $w \in \mathbb{R}^{m'+m''}$.

At the beginning of the recursive procedure, to determine the signs of a single polynomial, say $g_1$, at the real zeros of $f$, enough information is clearly provided by the quantities $N(\emptyset, \emptyset)$, $N(\{1\}, \emptyset)$, and $N(\emptyset, \{1\})$; the values of these three quantities together allow one to easily determine the number of distinct real zeros of $f$ at which $g_1$ is positive, the number at which $g_1$ is negative, and the number at which $g_1$ is zero. Assuming $\mathcal{I}' = \{1\}$, an appropriate set $\mathcal{I}'$ is then easily determined; let $\mathcal{I}' = \{\emptyset, \emptyset\}$ if only one distinct sign vector occurs, let $\mathcal{I}' = \{\emptyset, \emptyset, (\emptyset, \{1\})\}$ if two occur, and let...
$J' = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\{1\}, \emptyset)\}$ if all three occur. (If $f$ has no real zeros, i.e., $N(\emptyset, \emptyset) = 0$, then of course we are finished.)

Observe that the condition of (5.2) being a spanning set for $\mathbb{R}^{k'}$ is equivalent to the condition that for each of the sign vectors $u^{(i)}$ there exists a polynomial $F_{i}$ in the variables $u_{1}^{\prime \prime}, \ldots, u_{m'}^{\prime \prime}$ such that all of the following three conditions are satisfied by $F_{i}$:

$F_{i}$ is a linear combination of polynomials of the form

$$u \mapsto p'(u; l_{1}', l_{2}') \text{ where } (l_{1}', l_{2}') \in J';$$

$$F_{i}(u^{(i)}) = 1;$$

$$F_{i}(u^{(j)}) = 0 \text{ if } j \neq i.$$

Similarly, for each $v^{(i)}$ there exists a polynomial $G_{i}$ in the variables $v_{m'+1}^{\prime \prime}, \ldots, v_{m'+m''}^{\prime \prime}$ which is a linear combination of polynomials of the form $v \mapsto p''(v; l_{1}'', l_{2}'')$, where $(l_{1}'', l_{2}'') \in J''$, and which satisfies $G_{i}(v^{(i)}) = 1$ and $G_{i}(v^{(j)}) = 0$ if $j \neq i$.

Note that the sign vectors of $\{g_{i}\}_{i \in I}$ at the real zeros of $f$ are contained among the set

$\{\tilde{w}^{(1)}, \ldots, \tilde{w}^{(k' k'')}\}$ of vectors of the form $(u^{(i)}, v^{(j)})$.

Let $\tilde{J}$ denote the set of $k' k''$ pairs $(I_{1}, I_{2}) = (I_{1}', I_{2}', I_{1}'', I_{2}'')$ obtained as $(I_{1}', I_{2}')$,

$(I_{1}'', I_{2}'')$, range over $J'$, $J''$, respectively. Because

$$F_{i_{1}}(u^{(j_{1})})G_{i_{2}}(v^{(j_{2})}) = \begin{cases} 1 & \text{if } i_{1} = j_{1} \text{ and } i_{2} = j_{2} \\ 0 & \text{otherwise} \end{cases}$$

it follows that the set of vectors

$\{[p(\tilde{w}^{(1)}; I_{1}, I_{2}), \ldots, p(\tilde{w}^{(k' k'')}; I_{1}, I_{2})]; (I_{1}, I_{2}) \in \tilde{J}\}$

(5.4)

spans $\mathbb{R}^{k' k''}$; since there are $k' k''$ vectors in this set it is in fact a basis for $\mathbb{R}^{k' k''}$. 
Consider the following system of \( k'k'' \) linear equations in the variables \( y_{1},...,y_{k'k''} \):

\[
\sum_{i} p(w^{(i)}: I_{1,1} I_{2})y_{i} = N(I_{1,1} I_{2}) \quad (I_{1,1} I_{2}) \in \mathcal{F}.
\] (5.5)

Let \( y_{1}^{*} \) denote the number of distinct real zeros of \( f \) at which the sign vector of \( \{g_{i}\}_{i \in I} \) is \( w^{(i)} \). It is easily checked that \( y_{1}^{*} \) is a solution of the above equations. Since (5.4) is a basis for \( \mathbb{R}^{k'k''} \), \( y_{1}^{*} \) is the unique solution. Consequently, to determine which \( w^{(i)} \) are indeed sign vectors of \( \{g_{i}\}_{i \in I} \) at real zeros of \( f \), i.e., which \( y_{1}^{*} \) are non-zero, we need only compute \( N(I_{1,1} I_{2}) \) for \( (I_{1,1} I_{2}) \in \mathcal{F} \) and determine which numerator determinants arising from Cramer's rule for the above system of linear equations are non-zero. This can be accomplished efficiently using the determinant evaluation algorithm of proposition 2.6.

Let \( w^{(1)},...,w^{(k)} \in \{w^{(i)}\}_{i} \) denote the sign vectors of \( \{g_{i}\}_{i \in I} \) at the real zeros of \( f \) as determined in the above manner. Of course \( k \leq d \). To complete our description of the recursive procedure we show how to determine a subset \( \mathcal{F} \) of \( \mathcal{F} \) such that (5.3) is a basis for \( \mathbb{R}^{k} \).

Since (5.4) is a basis for \( \mathbb{R}^{k'k''} \),

\[
\{p(w^{(1)}: I_{1,1} I_{2}),...,p(w^{(k)}: I_{1,1} I_{2}); \ (I_{1,1} I_{2}) \in \mathcal{F}\}
\] (5.6)

spans \( \mathbb{R}^{k} \). Hence, an appropriate set \( \mathcal{F} \) is obtained simply by determining \( k \) pairs \( (I_{1,1} I_{2}) \in \mathcal{F} \) for which the corresponding vectors in (5.6) are linearly independent. This can be accomplished simply as follows.

Order the vectors in (5.6) from 1 to \( k'k'' \) and let \( M_{\ell} \) denote the matrix whose rows are the first \( \ell \) vectors in (5.6). Determine the rank of the matrices \( M_{\ell} \); this rank equals \( \ell \) minus the multiplicity of 0 as a zero of \( \lambda \leftarrow \det(M_{\ell}M_{\ell}^{T} - \lambda I) \), the latter univariate polynomial being constructed quickly in parallel using the algorithms of proposition 2.6 and lemma 2.7. If the rank of \( M_{\ell-1} \) differs from the rank of \( M_{\ell} \), then include in \( \mathcal{F} \) the pair \( (I_{1,1} I_{2}) \) corresponding to the \( \ell^{th} \)
vector in (5.6); also include the pair corresponding to the first vector. The resulting set \( \mathcal{J} \) is easily seen to have the desired properties.

To make certain statements in the next section unambiguous, we need to tie down the only loose end in the preceding recursive procedure, the determination of which sets \( I' \) and \( I'' \) to consider in conjunction at any given time during the parallel implementation. For definiteness we assume the usual pattern:

- first step \{1\} and \{2\}; \{3\} and \{4\}; ...
- second step \{1,2\} and \{3,4\}; \{5,6\} and \{7,8\}; ...
- etc.

To conclude the description of the algorithm for determining the sign vectors of \( \{g_i\}_1 \) at the zeros of \( f \) we need only discuss how to compute the quantities \( N(I_1, I_2) \). This is done in section 8.
6. A FEW OBSERVATIONS

In this section we make a few observations regarding the recursive procedure discussed in section 5. These observations will be crucial in our solution of the quantifier elimination subproblem. The observations regard arbitrary real univariate polynomials $f \neq 0, g_1, \ldots, g_m$.

Assume that

$$\sigma^{(1)}, \ldots, \sigma^{(M)}$$

are the distinct sign vectors of $g_1, \ldots, g_m$ at the real zeros of $f$; \hfill (6.1)

$$N_j$$ is the number of distinct real zeros of $f$ at which the sign vector is $\sigma^{(j)}$. \hfill (6.2)

Note that the quantities $N(I_1, I_2)$, and their values, which must be computed as the recursive procedure unfolds are entirely a function of $\sigma^{(1)}, \ldots, \sigma^{(M)}, N_1, \ldots, N_M$, not being dependent on the particular $f, g_1, \ldots, g_m$ satisfying (6.1) and (6.2). In particular, the final set $\mathcal{J}$ of $M$ pairs $(I_1, I_2)$, where $I_1, I_2 \subseteq \{1, \ldots, m\}$, is solely a function of $\sigma^{(1)}, \ldots, \sigma^{(M)}, N_1, \ldots, N_M$, as are the corresponding quantities $N(I_1, I_2)$. We indicate this dependence by writing

$$\mathcal{J} = \mathcal{J}^*(\sigma^{(1)}, \ldots, \sigma^{(M)}, N_1, \ldots, N_M)$$

$$N(I_1, I_2) = N^*(I_1, I_2) \text{ for } (I_1, I_2) \in \mathcal{J}^*.$$

The recursive procedure is trivially adapted to provide a method for quickly computing $\mathcal{J}^*$ and the corresponding quantities $N^*(I_1, I_2)$ in parallel, solely from $\sigma^{(1)}, \ldots, \sigma^{(M)}, N_1, \ldots, N_M$. Moreover, given arbitrary $\sigma^{(1)}, \ldots, \sigma^{(M)} \in \{-1, 0, 1\}^m$ and positive integers $N_1, \ldots, N_M$, the analysis of section 5 shows that for the resulting set $\mathcal{J}^*(\sigma^{(1)}, \ldots, \sigma^{(M)}, N_1, \ldots, N_M)$, the set of vectors

$$\{[p(\sigma^{(1)}: I_1, I_2), \ldots, p(\sigma^{(M)}: I_1, I_2)]; (I_1, I_2) \in \mathcal{J}^*\}$$

(6.3)
is a basis for $\mathbb{R}^M$, and for the resulting values $N^*(I_1, I_2)$ the unique solution of the system

$$\sum_{j=1}^{M} p(\sigma^{(j)}: I_1, I_2)y_j = N^*(I_1, I_2) \quad (I_1, I_2) \in \mathcal{S}^*$$

is $y_j = N_j$. However, given arbitrary real univariate polynomials $f \neq 0$, $g_1, \ldots, g_m$ with corresponding values $N(I_1, I_2)$ defined by (5.1), a solution of

$$\sum_{j=1}^{M} p(\sigma^{(j)}: I_1, I_2)y_j = N(I_1, I_2) \quad (I_1, I_2) \in \mathcal{S}^*$$

is easily seen to be

$$y_j = \text{the number of distinct real zeros of } f \text{ at which the sign vector of } g_1, \ldots, g_m \text{ is } \sigma^{(j)}.$$ 

It follows that given arbitrary real univariate polynomials $f, g_1, \ldots, g_m$, these polynomials satisfy both (6.1) and (6.2) if and only if

$$N(\emptyset, \emptyset) = N_1 + \ldots + N_M$$

$$N(I_1, I_2) = N^*(I_1, I_2) \text{ for all } (I_1, I_2) \in \mathcal{S}^*(\sigma^{(1)}, \ldots, \sigma^{(k)}, N_1, \ldots, N_K).$$
7. A LEMMA REGARDING THE QUANTIFIER ELIMINATION SUBPROBLEM

Let \( f, g_1, \ldots, g_m : \mathbb{R}^\ell \times \mathbb{R} \to \mathbb{R} \) denote the polynomials occurring in the statement of the quantifier elimination subproblem.

For all \( \bar{y} \in \mathbb{R}^\ell \) such that \( t \mapsto f(\bar{y}, t) \neq 0 \), and for \( I_1, I_2 \subseteq \{1, \ldots, m\} \), define

\[
N(\bar{y} : I_1, I_2) := \# \{ t \in \mathbb{R} ; f(\bar{x}, t) = 0, \ g_1(\bar{x}, t) = 0 \ \forall \ i \in I_1, \ \text{and} \ \prod_{i \in I_2} g_i(\bar{x}, t) > 0 \} \\
- \# \{ t \in \mathbb{R} ; f(\bar{x}, t) = 0, \ g_1(\bar{x}, t) = 0 \ \forall \ i \in I_1, \ \text{and} \ \prod_{i \in I_2} g_i(\bar{x}, t) < 0 \} \tag{7.1}
\]

Let \( \sigma^{(1)} , \ldots , \sigma^{(M)} \in \{-1, 0, 1\}^m \) denote the vectors occurring in the quantifier elimination subproblem and let \( N_1, \ldots, N_M \) denote the corresponding positive integers. The observations of section 6 provide us with the following lemma.

**Lemma 7.1.** With \((\text{md})^O(1)\) operations (no divisions) performed in time \([\log(\text{md})]^O(1)\) using \((\text{md})^O(1)\) parallel processors, a set \( \mathcal{S}^* \) of at most \( d \) pairs \((I_1, I_2), \ I_1, I_2 \subseteq \{1, \ldots, m\}, \) and corresponding integer values \( N^*(I_1, I_2) \), can be constructed (solely from \( \sigma^{(1)} , \ldots , \sigma^{(M)} , N_1, \ldots, N_M \)) for which the following is true. If \( \bar{y} \in \mathbb{R}^\ell \) satisfies \( t \mapsto f(\bar{y}, t) \neq 0 \), then both

(i) the number of distinct real zeros of \( t \mapsto f(\bar{y}, t) \) is \( N_1 + \ldots + N_M \)

and

(ii) \( N_j \) is the number of distinct real zeros of \( t \mapsto f(\bar{y}, t) \) at which the sign vector of \( \{ t \mapsto g_i(\bar{y}, t) \} \) is \( \sigma^{(j)} \) for all \( j \)

if and only if

\[
N(\bar{y} : I_1, I_2) = N^*(I_1, I_2) \text{ for all } (I_1, I_2) \in \mathcal{S}^*. \quad \square
\]
8. COMPLETION OF THE ALGORITHM FOR CONSTRUCTING THE CONSISTENT SIGN

VECTORS OF A SET OF UNIVARIATE POLYNOMIALS

Now we return to the problem of computing the quantities $N(I_1, I_2)$ defined by (5.1) for arbitrary real univariate polynomials $f \neq 0, g_1,...,g_m$. Having accomplished this, the algorithm for determining the consistent sign vectors of an arbitrary set $g_1,...,g_m$ of real univariate polynomials will be complete.

Note that the following equality holds:

$$N(I_1, I_2) = \# \{ t \in \mathbb{R}; [f(t)]^2 + \sum_{j \in I_1} [g_j(t)]^2 = 0 \text{ and } \prod_{j \in I_2} g_j(t) > 0 \}$$

$$- \# \{ t \in \mathbb{R}; [f(t)]^2 + \sum_{j \in I_1} [g_j(t)]^2 = 0 \text{ and } \prod_{j \in I_2} g_j(t) < 0 \}. \tag{8.1}$$

Henceforth, we can focus on the following problem: given arbitrary real univariate polynomials $f \neq 0$ and $g$, compute

$$N(f, g) := \# \{ t \in \mathbb{R}; f(t) = 0 \text{ and } g(t) > 0 \}$$

$$- \# \{ t \in \mathbb{R}; f(t) = 0 \text{ and } g(t) < 0 \}. \tag{8.1}$$

We let $d, e$ denote the degree of $f, g$, respectively.

The following proposition provides the main tool for computing $N(f, g)$; an additional trick beyond the proposition is needed because we may not assume that $f$ and $g$ are relatively prime in our applications. Essentially the same ideas were used by Tarski [5] and Ben-Or, Kozen and Reif [1], but with the assumption that $f$ is simple.

Proposition 8.1. (aka Generalized Sturm’s Theorem) Assume that $f \neq 0, g$ are relatively prime real univariate polynomials. Let $f_1 = f, f_2 = f'g, f_3, ..., f_K$ be the Euclidean remainder sequence of $f$ and $f'g$, as defined by

$$f_i = q_i f_{i+1} - f_{i+2}$$
where degree($f_{i+2}$) < degree($f_{i+1}$). Let $e_i := \text{degree}(f_i)$ and let $a_i$ be the leading coefficient of $f_i$. Let $S^+(f,g)$ denote the number of sign changes in the sequence $a_1, \ldots, a_K$ and let $S(f,g)$ denote the number of sign changes in the sequence $(-1)^{e_1}a_1, \ldots, (-1)^{e_K}a_K$. Then

$$N(f,g) = S(f,g) - S^+(f,g).$$

**Proof.** For each $t \in \mathbb{R}$ that is not a zero of any $f_i$ define $S(t)$ to be the number of sign changes in the sequence $f_0(t), \ldots, f_K(t)$. Note that $S(t)$ is constant on intervals where it is defined. Also note that $S^+$ equals $S(t)$ for sufficiently large $t$ and $S^-$ equals $S(t)$ for sufficiently small (i.e., negative) $t$. We now examine how $S(t)$ changes as $t$ skips across a zero $\bar{t}$ of some $f_i$. There are several cases to consider.

First assume that $f_0(\bar{t}) \neq 0$. We will show that as $t$ skips across $\bar{t}$, $S(t)$ is unchanged. Assume that $f_{i}(\bar{t}) = 0$. Because $f_K$ divides $f_0, f_K(\bar{t}) \neq 0$ and hence $0 < i < k$. Moreover, since $f_K$ is the greatest common divisor (gcd) of any adjacent pair in the sequence $f_0, \ldots, f_K$, we have that $f_i(\bar{t}) = 0$ implies $f_{i-1}(\bar{t}) \neq 0 \neq f_{i+1}(\bar{t})$. To prove that $S(t)$ is unchanged as $t$ skips across $\bar{t}$ it now suffices to prove that the number of sign changes in the sequence $f_{i-1}(t), f_i(t), f_{i+1}(t)$ is unchanged as $t$ skips across $\bar{t}$. However this is a trivial consequence of the fact that $f_{i-1}$ and $f_{i+1}$ are of opposite sign in a neighborhood of $\bar{t}$, as follows from the definition of $f_{i+1}$.

Next assume that $\bar{t}$ is a zero of $f = f_0$ of multiplicity exactly equal to one. Because $f$ and $g$ are relatively prime it follows that $f_K(\bar{t}) \neq 0$. Since $f_K$ is the gcd of $f_i$ and $f_{i+1}$ for all $i < K$, we have that if $f_i(\bar{t}) = 0$ and $i > 0$, then $f_{i-1}(\bar{t}) \neq 0$ and $f_{i+1}(\bar{t}) \neq 0$. Hence, as before, if $f_i(\bar{t}) = 0$ and $i > 0$, the number of sign changes in the three number sequence $f_{i-1}(t), f_i(t), f_{i+1}(t)$ is unchanged as $t$ skips across $\bar{t}$. Thus, to assess the change in $S(t)$ as $t$ skips across $\bar{t}$ we need only assess the change in the signs of $f_0(t), f_i(t)$. 
When \( t \) skips across a simple zero of \( f = f_0 \), either \( f(t) \) is going from positive to negative in which case \( f'(t) < 0 \), or from negative to positive in which case \( f'(t) > 0 \). Since \( f_1 = f'g \), it easily follows that \( S(t) \) increases by one if \( g(t) < 0 \) and decreases by one if \( g(t) > 0 \).

Finally, assume that \( t \) is a zero of \( f = f_0 \) of multiplicity \( m > 1 \). Then \( t \) is a zero of \( f_K \) of multiplicity \( m-1 \), and \( t \) is a zero of multiplicity at least \( m-1 \) for every \( f_i \). Let \( I \) denote the set of those indices \( i \) such that \( t \) is a zero of \( f_i \) of multiplicity exactly \( m-1 \). Clearly, \( 1 \in I, \ K \in I \) and if \( i \not\in I \) then \( i+1 \in I \).

Assume that \( i \in I \). Then either \( i+1 \in I \), or both \( i+1 \not\in I \) and \( i+2 \in I \). If \( i+1 \in I \), the number of sign changes in the two number sequence \( f_i(t), f_{i+1}(t) \) as \( t \) skips across \( t \) is trivially unchanged. If \( i+1 \not\in I \), then the multiplicity of \( t \) as a zero of \( f_{i+1} \) is at least \( m \) and hence the sign of \( f_{i+2}(t) = -f_i(t) + q_i(t)f_{i+1}(t) \) just to the left, and just to the right, of \( t \) is the same as that of \( -f_i(t) \). Consequently, if \( i \in I \) but \( i+1 \not\in I \), the number of sign changes in the three number sequence \( f_i(t), f_{i+1}(t), f_{i+2}(t) \) is unchanged as \( t \) skips across \( t \).

Once again, to assess the change in \( S(t) \) as \( t \) skips across \( t \) we need only assess the change in the signs of \( f_0(t), f_1(t) \). This simple task is left to the reader. □

As has been discussed, in our application we may not assume that the relevant polynomials \( f \) and \( g \) share no real zeros, and hence the proposition does not seem to provide a useful identity for \( N(f,g) \). However, note the following. For \( \epsilon \in \mathbb{R} \), let \( g+\epsilon \) denote the polynomial \( t \mapsto g(t) + \epsilon \). For any \( f \neq 0 \), \( g \), and all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of \( 0 \), \( f \) is relatively prime to \( g+\epsilon \). Moreover, for \( \epsilon_1 > 0 \), \( \epsilon_2 < 0 \) sufficiently close to \( 0 \),

\[
N(f,g) = \frac{1}{2} [N(f,g+\epsilon_1) + N(f,g-\epsilon_2)].
\]

Hence, if we can determine \( S^+(f,g+\epsilon) \) and \( S^-(f,g+\epsilon) \) for \( \epsilon \neq 0 \) in a sufficiently small neighborhood of \( 0 \), then the proposition provides a method for computing \( N(f,g) \).
Now we discuss a fast parallel method for computing $S^+(f,g)$ and $S^-(f,g)$ for arbitrary real univariate polynomials $f \neq 0 \neq g$. After developing this, we will discuss a slight extension of the method so that we can compute $S^+(f,g+\epsilon)$ and $S^-(f,g+\epsilon)$ for all $\epsilon \neq 0$ in a sufficiently small neighborhood of 0.

Letting $f_0 = f, f_1 = f'g, \ldots, f_K$ be the remainder sequence as in the previous proposition, to compute $S^+(f,g)$ and $S^-(f,g)$ it of course suffices to determine the degrees and the signs of the leading coefficients of the polynomials $f_i$. As will be shown, these are easily determined if we know the polynomials $f_i$ up to similarity, i.e., we know a non-zero constant multiple of each $f_i$. The following proposition provides the basis for a fast parallel method to compute each $f_i$ up to similarity. The ideas behind the proposition are well known (e.g. Collins [3], Brown and Traub [2]).

The proposition applies to general Euclidean remainder sequences $f_0, f_1, \ldots, f_K$. We let $e_i$ denote the degree of $f_i$. The computations implicit in the proposition only involve $f_0$ and $f_1$.

In developing the proposition we assume that $e_0 \geq e_1$. There is no loss of generality in assuming this since otherwise the remainder sequence is $f_0, f_1, f_2 = -f_0, \ldots, f_K$ and we then need only be concerned with determining the polynomials in the remainder sequence $f_1, -f_0, f_3, \ldots, f_K$ up to similarity, both $f_1$ and $-f_0$ being known.

For $i \geq 0$, let $P_i$ denote the vector space consisting of real univariate polynomials of degree at most $i$, letting the polynomial $\sum_{j=0}^{i} b_j x^j$ correspond to the vector $(b_0, \ldots, b_i)$.

For $0 \leq e < e_1$ define $T_e : P_{e_1 - e - 1} \times P_{e_0 - e - 1} \rightarrow P_{e_0 + e_1 - e - 1}$ to be the linear transformation $T_e(p,q) = pf_0 + qf_1$. Let $\tilde{T}_e$ denote the composition of $T_e$ with projection onto the coordinates corresponding to coefficients of terms of degree at least $e$; hence $\tilde{T}_e$ is a linear transformation from a real vector space of dimension $e_0 + e_1 - 2e$ into a real vector space of the same dimension.

**Proposition 8.2.** (Assume that $e_0 \geq e_1$.) The transformation $\tilde{T}_e$ is invertible if and only if $e \in \{e_2, \ldots, e_K\}$. Moreover, if we define $(p_1, q_1) := \tilde{T}_e^{-1}([0, \ldots, 0, 1])$ then $p_1 f_0 + q_1 f_1$ is similar to $f_1$.

**Proof.** First, we show that $\tilde{T}_e$ is invertible only if $e \in \{e_2, \ldots, e_K\}$. 


By the recursive definition of the remainder sequence it is easily show that for each $i = 2, \ldots, K$ there exists $(p_i, q_i) \in P_{e_{i-1}} \times P_{e_0, e_{i-1}}$ such that $p_i f_0 + q_i f_1 = f_i$. In particular, if $e_{i-1} > e > e_i$ then $(p_i, q_i) \in P_{e_1, e_{i-1}} \times P_{e_0, e_{i-1}}$ and $T_e(p_i, q_i) = 0$. Similarly, for $e < e_K$. Hence, $T_e$ is invertible only if $e \in \{e_2, \ldots, e_K\}$.

Now we show that $T_e$ is indeed invertible if $e \in \{e_2, \ldots, e_K\}$. Our proof is by induction on the length $K + 1$ of the remainder sequence $f_0, \ldots, f_K$. Of course we may assume that $K \geq 2$.

We consider the case $e = e_2$ separately. Assume that $(p, q) \in P_{e_1, e_2, 1} \times P_{e_0, e_2, 1}$ and $T_{e_2}(p, q) = 0$. We want to show that $(p, q) = 0$. Let $q^*$ denote the polynomial satisfying $f_0 = q^* f_1 - f_2$. Note that $pf_0 + qf_1 = (q + pq^*)f_1 - pf_2$ is a polynomial of degree less than $e_2$ since $T_{e_2}(p, q) = 0$. Since $pf_2 \in P_{e_1, 1}$ and $f_1$ is of degree $e_1$, it follows that $q + pq^* = p = 0$ and hence, $p = q = 0$. So $T_{e_2}$ is invertible.

Now assume that $i > 2$, $(p, q) \in P_{e_1, e_i, 1} \times P_{e_0, e_i, 1}$ and $T_{e_i}(p, q) = 0$. Note that $pf_0 + qf_1 = (q + pq^*)f_1 - pf_2$ is a polynomial of degree less than $e_i$ since $T_{e_i}(p, q) = 0$. Since $p \in P_{e_1, e_i, 1}$ it follows that $q + pq^* \in P_{e_2, e_i, 1}$. By the inductive assumption applied to the remainder sequence $f_1, f_2, \ldots, f_K$ we must thus have that $q + pq^* = p = 0$ since $(q + pq^*)f_1 - pf_2$ is of degree less than $e_i$. Consequently, $p = q = 0$ and hence $T_{e_i}$ is invertible.

The final claim of the proposition is now easily established. □

Now we show how the proposition provides the basis for a fast parallel method to compute each $f_i$ up to similarity. We rely on the algorithm of proposition 2.6 to compute determinants quickly in parallel.

First compute a non-zero multiple of $\det(T_e)$ for $0 \leq e < e_1$ where $\det(T_e)$ refers to the determinant of the matrix representing $T_e$ with respect to the usual coordinate system for polynomials. Let $e_2 > \ldots > e_K$ denote the indices $e$ for which $\det(T_e) \neq 0$. Using Cramer's rule and again using the algorithm of proposition 2.6, solve $T_{e_i}(p, q) = (0, \ldots, 0, 1)$ up to a non-zero constant by only evaluating the numerator determinants in Cramer's rule, thereby avoiding division.
Let \((p_{e_i}, q_{e_i})\) denote the resulting solution and let \(\bar{f}_{i+1} := p_{e_i}f + q_{e_i}g\). The previous proposition implies that \(\bar{f}_{i+1}\) is similar to \(f_i\).

Recall that our present goal is to construct a method for computing \(S^+(f, g)\) and \(S^-(f, g)\) as defined by proposition 8.1. Hence we need to know the degrees of the polynomials \(f_0, f_1, \ldots, f_K\) and the signs of their leading coefficients. We now show how this can be accomplished by knowing \(f_0, f_1, f_2, \ldots, f_K\). Of course the degrees are trivially determined.

Define \(\bar{f}_0 := f_0, \bar{f}_1 = f_1\).

For \(i = 2, \ldots, K\), by definition of the remainder sequence, either \(\bar{f}_{i-2} + \bar{f}_i\) has \(\bar{f}_{i-1}\) as a factor or \(\bar{f}_{i-2} - \bar{f}_i\) has \(\bar{f}_{i-1}\) as a factor, but not both; otherwise \(f_{i-1}\) divides \(f_{i-2}\) contradicting \(f_i \neq 0\). Relying on lemma 2.8, determining which of these two possibilities does in fact hold simply amounts to determining whether or not the \((e_{i-2} + 1) \times (e_{i-2} - e_{i-1} + 2)\) matrix whose columns are the coefficient vectors of \(\bar{f}_{i-2} + \bar{f}_i\) and \(\bar{f}_{i-1}\) for \(j = 0, \ldots, e_{i-2} - e_{i-1}\), is rank deficient. As the lemma shows, this can be accomplished quickly simply by computing the determinant of the matrix formed as the product of the matrix and its transpose. If the determinant is zero, let \(\delta_i = 1\); if the determinant is not zero, let \(\delta_i = -1\). Relying on the definition of the remainder sequence it is trivially proven that if \(i\) is even then \(\delta_2 \delta_4 \ldots \delta_i f_{i-1}\) is a positive multiple of \(f_i\), and if \(i\) is odd then \(\delta_3 \delta_5 \ldots \delta_{i-1} f_{i-1}\) is a positive multiple of \(f_i\).

In all, we have presented a method for computing \(S^+(f, g)\) and \(S^-(f, g)\).

Now we reintroduce the variable \(\epsilon\) recalling that we will have completed a method for determining the consistent sign vectors of an arbitrary set of real univariate polynomials \(g_1, \ldots, g_m\) if we can show how to determine \(S^+(f, g + \epsilon)\) and \(S^-(f, g + \epsilon)\) for all \(\epsilon \neq 0\) in a sufficiently small neighborhood of \(0\), for any pair \(f \neq 0, g\) of real univariate polynomials.

Let \(f_0(t, \epsilon) := f(t), f_1(t, \epsilon) = f'(t)[g(t) + \epsilon]\). Let \(e_0 = d\) and \(e_1 = d-1+\epsilon\), where \(d\) is the degree of \(f\) and \(\epsilon\) is the degree of \(g\). We assume that \(e_0 \geq e_1\); otherwise reverse the definitions of \(f_0\) and \(f_1\), and of \(e_0\) and \(e_1\).
The following arguments are just a rehashing of the preceding arguments. The notation is more cumbersome than is needed here, but it will make the arguments of the next section more understandable; there we solve the quantifier elimination subproblem. The main change of notation from the preceding argument will be that $f_i$ is replaced with "$t \mapsto h_{e_i}(t, \epsilon)".

Let $(p,q) \mapsto \bar{T}_e(p,q; \epsilon)$ denote the linear transformation obtained by replacing $f_0$ and $f_1$ in the definition of $\bar{T}_e$ with $t \mapsto f_0(t, \epsilon)$ and $t \mapsto f_1(t, \epsilon)$, respectively. Using the algorithms of proposition 2.6 and lemma 2.7, compute a non-zero constant multiple of $\det((p,q) \mapsto \bar{T}_e(p,q; \epsilon))$ for $0 \leq \epsilon < e_1$. The resulting expressions will be polynomials in $\epsilon$. Let $e_2 > \ldots > e_K$ denote the indices for which the resulting polynomial is not identically zero. For all $\epsilon \neq 0$ in a sufficiently small neighborhood of 0 there will be $K$ polynomials in the remainder sequence of $t \mapsto f_0(t, \epsilon)$ and $t \mapsto f_1(t, \epsilon)$, and their respective degrees will be $e_0, e_1, \ldots, e_K$.

Using Cramer's rule, interpolation and the algorithm of proposition 2.6, solve

$$(p,q) \mapsto \bar{T}_{e_1}(p,q; \epsilon) = (0, \ldots, 0, 1)$$

up to a non-zero constant multiple for $i = 2, \ldots, K$, by only evaluating the numerator determinants in Cramer's rule.

Let $t \mapsto (p_{e_i}(t, \epsilon), q_{e_i}(t, \epsilon))$ denote the solution and let

$$h_{e_i}(t, \epsilon) := p_{e_i}(t, \epsilon)f_0(t, \epsilon) + q_{e_i}(t, \epsilon)f_1(t, \epsilon)$$

a polynomial in the variables $t$ and $\epsilon$. Then for all $\epsilon \neq 0$ in a sufficiently small neighborhood of 0, $t \mapsto h_{e_i}(t, \epsilon)$ is similar to the $i^{th}$ polynomial in the remainder sequence of $t \mapsto f_0(t, \epsilon)$ and $t \mapsto f_1(t, \epsilon)$. Also, the degree of $t \mapsto h_{e_i}(t, \epsilon)$ is then $e_i$.

Define $h_0(t, \epsilon) := f_0(t, \epsilon)$, $h_1(t, \epsilon) := f_1(t, \epsilon)$. 
For \( i = 2, \ldots, K \) let \( M_{e_i}(\epsilon) \) denote the \((e_{i-2}+1) \times (e_{i-2} - e_{i-1} + 2)\) matrix whose columns are the coefficient vectors of the polynomials \( t \mapsto h_{e_{i-2}}(t, \epsilon) + h_{e_{i-1}}(t, \epsilon) \) and \( t \mapsto \epsilon^j h_{e_{i-1}}(t, \epsilon) \) for \( j = 0, \ldots, e_{i-2} - e_{i-1} \), and let
\[
\beta_{e_i}(\epsilon) := \det((M_{e_i}(\epsilon))^T M_{e_i}(\epsilon)),
\]
a polynomial in \( \epsilon \). A non-zero constant multiple of \( \beta_{e_i}(\epsilon) \) can be computed quickly in parallel using the algorithms of proposition 2.6 and lemma 2.7.

If \( \beta_{e_i}(\epsilon) \equiv 0 \) let \( \delta_i = 1 \) and if \( \beta_{e_i}(\epsilon) \neq 0 \) let \( \delta_i = -1 \). Then for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0, if \( i \) is even then
\[
t \mapsto \delta_2 \delta_4 \cdots \delta_1 h_{e_1}(t, \epsilon)
\]
is similar to the \( i^{th} \) polynomial in the remainder sequence of \( t \mapsto f_0(t, \epsilon) \) and \( t \mapsto f_1(t, \epsilon) \), and if \( i \) is odd then
\[
t \mapsto \delta_3 \delta_5 \cdots \delta_1 h_{e_1}(t, \epsilon)
\]
is similar to the \( i^{th} \) polynomial.

Expand
\[
h_{e_i}(t, \epsilon) := \sum_{j=0}^{e_i} \sum_k a_{ijk} \epsilon^k
\]
and define \( k_i \) to be the integer satisfying
\[
a_{i e_i k_i} \neq 0
\]
\[
a_{i e_i k} = 0 \text{ if } k < k_i.
\]

Define \( a_i := a_{i e_i k_i} \). Then for all sufficiently small \( \epsilon > 0 \), \( S^+(f, g + \epsilon) \) equals the number of sign
changes in the sequence

\[ a_0, a_1, \delta_2a_2, \delta_3a_3, \delta_2\delta_4a_4, \delta_3\delta_5a_5, \ldots \]

and \( S(f,g+\epsilon) \) equals the number of sign changes in the sequence

\[ (-1)^{e_0}a_0, (-1)^{e_1}a_1, (-1)^{e_2}\delta_2a_2, (-1)^{e_3}\delta_3a_3, (-1)^{e_4}\delta_2\delta_4a_4, \ldots \]

For all sufficiently small \( \epsilon < 0 \), \( S^+(f,g+\epsilon) \) equals the number of sign changes in the sequence

\[ (-1)^{k_0}a_0, (-1)^{k_1}a_1, (-1)^{k_2}\delta_2a_2, \ldots \]

and \( S^-(f,g+\epsilon) \) equals the number of sign changes in the sequence

\[ (-1)^{e_0+k_0}a_0, (-1)^{e_1+k_1}a_1, (-1)^{e_2+k_2}\delta_2a_2, \ldots \]

Combining the above constructions with those of section 5 and performing the tedious check that if all coefficients of \( \{g_i\}_i \) are integers of bit length at most \( L \) then all numbers occurring during the above procedure are integers of bit length at most \( L(\text{md})^{O(1)} \), we finally obtain the following proposition.

**Proposition 8.3** (Ben-Or, Kozen and Reif [1]). There exists an algorithm for determining the consistent sign vectors of arbitrary finite sets \( \{g_i\}_i \) of real univariate polynomials. If there are \( m \) polynomials in the set, all of degree at most \( d \geq 2 \), then \( (\text{md})^{O(1)} \) operations (no divisions) suffice and the computations can be performed in time \( [\log(\text{md})]^{O(1)} \) using \( (\text{md})^{O(1)} \) parallel processors. If the coefficients of \( \{g_i\}_i \) are integers of bit length at most \( L \), then the computations can be performed with \( L(\log L)(\log \log L)(\text{md})^{O(1)} \) sequential bit operations, or in time \( (\log L)[\log(\text{md})]^{O(1)} \) using \( L^{2}(\text{md})^{O(1)} \) parallel processors. \( \Box \)
9. SOLUTION OF THE QUANTIFIER ELIMINATION SUBPROBLEM

Now we can solve the quantifier elimination subproblem, thereby establishing Theorem 1.1. We rely on the notation in the statement of the problem (at the beginning of section 4).

Let \( J^* \) be as in lemma 7.1. By that lemma, to design an algorithm which serves as a solution to the quantifier elimination subproblem, it suffices to design an algorithm that efficiently constructs a quantifier free formula \( P(y) \), of the form (4.1.5), which is satisfied by \( \bar{y} \in \mathbb{R}^\ell \) if and only if \( \bar{y} \) satisfies the following two conditions:

\[
\text{the degree of } t \mapsto f(\bar{y},t) \text{ is } d_0 \text{ and the degree of } t \mapsto g_i(\bar{y},t) \text{ is } d_i, \\
\text{for } i = 1, \ldots, m; \tag{9.1}
\]

\[
N(\bar{y}; I_1, I_2) = N^*(I_1, I_2) \text{ for all } (I_1, I_2) \in J^*. \tag{9.2}
\]

By "efficiently" construct, we mean with \((md)^{O(\ell)}\) operations in time \([\ell \log(md)]^{O(1)}\) using \((md)^{O(\ell)}\) parallel processors. Moreover, if the coefficients of \( \{g_i\}_i \) are integers of bit length at most \( L \), we require that all numbers occurring during the construction be integers of bit length at most \( L(md)^{O(\ell)} \), and we require the coefficients of the final formula to be integers of bit length at most \( (L+\ell)(md)^{O(1)} \).

Again we focus on the operation count, leaving the tedious, but routine, check of the bit bounds (assuming the coefficients of \( \{g_i\}_i \) are integers) to the reader.

For each pair \((I_1, I_2) \in J^*\), define

\[
f(y,t; I_1) := f^2(y,t) + \sum_{i \in I_1} g_i^2(y,t) \\
g(y,t,\epsilon; I_2) := \epsilon + \prod_{i \in I_2} g_i(y,t).
\]
Of course if \( t \mapsto f(\bar{y}, t; I_1) \neq 0 \), then

\[
N(\bar{y}: I_1, I_2) = N(t \mapsto f(\bar{y}, t; I_1), t \mapsto g(\bar{y}, t, 0; I_2)) \tag{9.3}
\]

where for real univariate polynomials \( \bar{f} \neq 0 \) and \( \bar{g} \), we define

\[
N(\bar{f}, \bar{g}) := \# \{ t \in \mathbb{R}; \bar{f}(t) = 0 \text{ and } \bar{g}(t) > 0 \} - \# \{ t \in \mathbb{R}; \bar{f}(t) = 0 \text{ and } \bar{g}(t) < 0 \}.
\]

Proposition 8.1 and the discussion just thereafter show that if \( t \mapsto f(\bar{y}, t; I_1) \neq 0 \), then the right hand side of (9.3) can be efficiently computed if we know the values

\[
S^\pm(t \mapsto f(\bar{y}, t; I_1), t \mapsto g(\bar{y}, t, \epsilon; I_2)) \tag{9.4}
\]

for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0.

Momentarily we will show how to construct a set \( \{H_{1}\}_i \) of \((md)^{O(1)}\) polynomials \( H_i: \mathbb{R}^\ell \rightarrow \mathbb{R} \) of degree at most \((md)^{O(1)}\) with the property that the sign vector of \( \{H_{1}\}_i \) at \( \bar{y} \in \mathbb{R}^\ell \) can be used (i) to efficiently determine if \( \bar{y} \) satisfies (9.1) and (ii) if \( \bar{y} \) satisfies (9.1), to efficiently determine the values (9.4) for all \( (I_1, I_2) \in \mathcal{S}^* \) and all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0. In other words, the sign vector of \( \{H_{1}\}_i \) at \( \bar{y} \) can be used to efficiently determine if \( \bar{y} \) satisfies both (9.1) and (9.2).

Before describing the construction of \( \{H_{1}\}_i \) and substantiating the claims of the previous paragraph, we show how such a set of polynomials can be used to solve the quantifier elimination subproblem.

Let \( \tau(\bar{y}) \) denote the sign vector of \( \{H_{1}\}_i \) at \( \bar{y} \).
Define \( S := \{ \tau(y); \bar{y} \in \mathbb{R}^\ell \} \). By proposition 2.3, \( S \) consists of \( (\log(md))^O(\ell) \) vectors all of which can be constructed from the coefficients of \( \{ H_i \}_{i} \) with \( (\log(md))^O(\ell) \) operations in time \( \ell \log(md))^O(1) \) using \( (\log(md))^O(\ell) \) parallel processors.

Let \( S^* \) denote the set consisting precisely of those vectors \( \tau \in S \) satisfying the property that if \( \tau(y) = \tau \), then \( \bar{y} \) satisfies (9.1) and (9.2) (recalling that our as of yet unsubstantiated claim regarding \( \{ H_i \}_{i} \) implies that \( S^* \) can be efficiently constructed from \( S \)). Trivially, \( \bar{y} \in \mathbb{R}^\ell \) satisfies (9.1) and (9.2) if and only if \( \bar{y} \) satisfies

\[
\bigvee_{\tau \in S^*} \bigwedge_i (H_i(y) \Delta_{\tau_i} 0)
\]

where \( \Delta_{\tau_i} \) is the standard relation corresponding to \( \tau_i \); e.g., if \( \tau_i = 1 \) then \( \Delta_{\tau_i} \) is "\( \land \)".

A moments reflection should convince the reader that we will have solved the quantifier elimination subproblem if we can show how to efficiently construct a set \( \{ H_i \}_{i} \) with the stated properties.

We now turn to constructing the set \( \{ H_i \}_{i} \). Our development closely parallels that of section 8, and is written assuming that the reader has carefully read that section.

We begin with a rather lengthy set of definitions leading up to the definition of \( \{ H_i \}_{i} \). After defining \( \{ H_i \}_{i} \), we show that this set has the desired properties.

For each \( (I_1, I_2) \in \mathcal{I}^* \), define \( e_0(I_1, I_2) \) to be the larger of the two quantities (or, say, the first if they are equal)

\[
\max\{2d_0, 2d_i; i \in I_1\} + \left( \sum_{i \in I_2} d_i \right) + \max\{2d_0, 2d_i; i \in I_1\} - 1
\]}
and define \( e_1(I_1, I_2) \) to be the other quantity. If \( e_0(I_1, I_2) \) equals the first quantity, then define

\[
\bar{r}_0(y, t, \epsilon; I_1, I_2) := f(y, t; I_1)
\]

\[
\bar{r}_1(y, t, \epsilon; I_1, I_2) := g(y, t, \epsilon; I_2) \frac{d}{dt} f(y, t; I_1).
\]

If \( e_0(I_1, I_2) \) equals the second quantity, then define

\[
\bar{r}_0(y, t, \epsilon; I_1, I_2) := g(y, t, \epsilon; I_2) \frac{d}{dt} f(y, t; I_1).
\]

\[
\bar{r}_1(y, t, \epsilon; I_1, I_2) := -f(y, t; I_1).
\]

Let \( f_0(y, t, \epsilon; I_1, I_2) \) (resp. \( f_1(y, t, \epsilon; I_1, I_2) \)) be the polynomial obtained from \( \bar{r}_0 \) (resp. \( \bar{r}_1 \)) by deleting all terms involving \( t \) to a power greater than \( e_0(I_1, I_2) \) (resp. \( e_1(I_1, I_2) \)).

For \( 0 \leq \epsilon < e_1(I_1, I_2) \) define \((p, q) \mapsto T_{e}(p, q; y, \epsilon, I_1, I_2)\) to be the linear transformation from \( P_{e_1-e-1} \times P_{e_0-e-1} \) to \( P_{e_0+e_1-e-1} \) that takes \((p(t), q(t))\) to the polynomial

\[
t \mapsto p(t) f_0(y, t, \epsilon; I_1, I_2) + q(t) f_1(y, t, \epsilon; I_1, I_2).
\]

(Here, \( e_0 := e_0(I_1, I_2), e_1 := e_1(I_1, I_2).\))

Let \((p, q) \mapsto \bar{T}_{e}(p, q; y, \epsilon, I_1, I_2)\) denote composition of \( T_{e} \) with projection onto those coordinates corresponding to coefficients of terms of degree at least \( \epsilon \) in \( t \).

Let

\[
det[(p, q) \mapsto \bar{T}_{e}(p, q; y, \epsilon, I_1, I_2)]
\]

denote the determinant of the matrix representing the linear transformation. This determinant is a polynomial in \( y \) and \( \epsilon \).
Define the pair

\[(t \mapsto p_e(y,t,\epsilon; I_1, I_2), \ t \mapsto q_e(y,t,\epsilon; I_1, I_2))\]

to be the polynomials whose combined coefficient vector (as polynomials in \(t\)) has \(k^\text{th}\) coordinate \((1 \leq k \leq e_0(I_1, I_2) + e_1(I_1, I_2) - 2e)\) equal to the determinant of the matrix obtained by replacing the \(k^\text{th}\) column in the matrix representing

\[(p,q) \mapsto \bar{T}_e(p,q; y,\epsilon; I_1, I_2)\]

with \((0,...,0,1)\).

Define \(h_e(y,t,\epsilon; I_1, I_2)\) to be the polynomial \(p_{e_0}f^0 + q_{e_1}f^1\) and define \(h_{e_0} := f^0, \ h_{e_1} := f^1\).

For all \(j_1,j_2,j_3 \in \{0,1,...,e_1(I_1, I_2), \ e_0(I_1, I_2)\}\) satisfying \(j_1 > j_2 > j_3\), define

\[M_{j_1,j_2,j_3}(y,\epsilon; I_1, I_2)\]

to be the \((j_1+1) \times (j_1-j_2+2)\) matrix whose first column is the coefficient vector of

\[t \mapsto h_{j_1}(y,t,\epsilon; I_1, I_2) + h_{j_3}(y,t,\epsilon; I_1, I_2)\]  \( (9.5) \)

and whose latter columns are the coefficient vectors of

\[t \mapsto t^j h_{j_2}(y,t,\epsilon; I_1, I_2)\]

for \(j = 0,...,j_1-j_2\).

Define

\[\beta_{j_1,j_2,j_3}(y,\epsilon; I_1, I_2) := \text{det}([M_{j_1,j_2,j_3}(y,\epsilon; I_1, I_2)]^\text{T} M_{j_1,j_2,j_3}(y,\epsilon; I_1, I_2)).\]
Letting \((I_1,I_2)\) range over \(S^*\), and letting \(e,j_1,j_2\) and \(j_3\) range over all indices for which the expressions were defined, expand all of the following polynomials in powers of \(t\) and \(e\):

\[
f(y,t)\]
\[
g_i(y,t) \quad i = 1,...,m\]
\[
det\{[p,q) \mapsto T_e[p,q; y,e; I_1,I_2]\}\]
\[
h_0(y,t,e; I_1,I_2)\]
\[
\beta_{j_1j_2j_3}(y,e; I_1,I_2)\]

Let \(\{H_1\}_1\) denote the set of all of the coefficient polynomials; these coefficient polynomials are polynomials in \(y\) alone. Since \(S^*\) contains \(d^{O(1)}\) elements, \(\{H_1\}_1\) contains \((md)^{O(1)}\) polynomials, all of degree at most \((md)^{O(1)}\). Using the algorithms of proposition 2.6 and lemma 2.7, positive multiples of the entire set \(\{H_1\}_1\) can be constructed with \((md)^{O(e)}\) operations in time \([\ell \log(md)]^{O(1)}\) using \((md)^{O(e)}\) parallel processors. Since we will only be relying on sign information of \(\{H_1\}_1\), we only need the polynomials \(H_1\) up to positive multiples. For simplicity of exposition, we assume that we have constructed the set \(\{H_1\}_1\) exactly.

We claim that the sign vector of \(\{H_1\}_1\) at \(y\) can be used to quickly determine if \(y\) satisfies (9.1), and we claim that if \(y\) does satisfy (9.1), then the sign vector can be used to quickly determine the values (9.4) for all \((I_1,I_2) \in S^*\) and for all \(\epsilon \neq 0\) in a sufficiently small neighborhood of \(0\). Once we have established these claims, we will have solved the quantifier elimination subproblem.

The first claim is trivial. To establish the second claim assume that \(y\) does satisfy (9.1). We want to show that for each \((I_1,I_2) \in S^*\), the sign vector of \(\{H_1\}_1\) at \(y\) provides enough information to quickly determine the degrees, and the signs of the leading coefficients, of the polynomials in the remainder sequence of

\[
t \mapsto f(y,t; I_1), \quad t \mapsto g(y,t,e; I_2) \frac{d}{dt} f(y,t; I_1)\]  \hspace{1cm} (9.6)
for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0.

It is easily seen that the sign vector provides enough information to efficiently compute the signs of the leading coefficients of the two polynomials (9.6) for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0. Consequently, it suffices to show that it provides enough information to compute the degrees, and the signs of the leading coefficients, of the polynomials in the remainder sequence of

\[
t \mapsto f_0(\bar{y}, t, \epsilon; I_1, I_2), \quad t \mapsto f_1(\bar{y}, t, \epsilon; I_1, I_2)
\]

(9.7)

for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0. (By our assumption that \( \bar{y} \) satisfies (9.1), the first of these polynomials has degree \( e_0(I_1, I_2) \) in \( t \), and the second has degree \( e_1(I_1, I_2) \)).

Let \( e_2 > \ldots > e_K \) denote the indices \( e \) for which

\[
\det[(p, q) \mapsto \bar{T}_e(p, q; \bar{y}, \epsilon, I_1, I_2)]
\]

is not identically zero in \( \epsilon \). These indices can certainly be efficiently determined from the sign vector of \( \{H_i\}_{i=1} \) at \( \bar{y} \).

The analysis of section 8 shows that, up to similarity, the remainder sequence of (9.7) is

\[
t \mapsto h_e(\bar{y}, t, \epsilon; I_1, I_2) \quad e = e_0e_1\ldots e_K
\]

for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0.

For each \( e = 2, \ldots, K \), the sign vector of \( \{H_i\}_{i=1} \) at \( \bar{y} \) allows one to quickly determine if \( \beta_e(\bar{y}, \epsilon) \) is identically zero in \( \epsilon \). If \( \beta_e(\bar{y}, \epsilon) \equiv 0 \), then define \( \delta_e = 1 \); otherwise, define \( \delta_e = -1 \).

The analysis of section 8 shows that the \( i \)-th polynomial in the remainder sequence of (9.7) is a positive multiple of
\[ t \mapsto \delta_2 \delta_4 \ldots \delta_i h_{\epsilon_1}(\bar{y}, t, \epsilon; I_1, I_2) \text{ if } i \text{ is even} \]
\[ t \mapsto \delta_3 \delta_5 \ldots \delta_i h_{\epsilon_1}(\bar{y}, t, \epsilon; I_1, I_2) \text{ if } i \text{ is odd} \]

for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0. It now follows easily that the degrees, and the signs of the leading coefficients, of the polynomials in the remainder sequence of (9.7) are easily determined from the sign vector of \( \{H_i\}_1 \) at \( \bar{y} \), for all \( \epsilon \neq 0 \) in a sufficiently small neighborhood of 0. Thus we have solved the quantifier elimination subproblem, thereby concluding the series of papers.
REFERENCES


